**ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ**

## CARRERA INFORMÁTICA

**TESIS PREVIA LA OBTENCIÓN DEL TÍTULO DE INGENIERAS EN INFORMÁTICA**

**TEMA:**

# PLAN DE GESTIÓN DE INCIDENTES QUE AFECTAN A LOS EQUIPOS INFORMÁTICOS DE LA ESPAM MFL

**AUTORAS:**

**MARÍA GABRIELA CUZME ROMERO**
**ROXANNA ELIZABETH PINARGOTE ANCHUNDIA**

**TUTOR:**

**ING. SERGIO ANTONIO INTRIAGO BRIONES, MGS**

**CALCETA, JULIO 2015**

# DERECHOS DE AUTORÍA

María Gabriela Cuzme Romero y Roxanna Elizabeth Pinargote Anchundia, declaran bajo juramento que el trabajo aquí descrito es de nuestra autoría, que no ha sido previamente presentado para ningún grado o calificación profesional, y que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos los derechos de propiedad intelectual a la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, según lo establecido por la Ley de Propiedad Intelectual y su reglamento.

…….... ……...……...……

**MARÍA G. CUZME ROMERO** **ROXANNA E. PINARGOTE ANCHUNDIA**

# CERTIFICACIÓN DE TUTOR

Sergio Antonio Intriago Briones certifica haber tutelado la tesis **PLAN DE GESTIÓN DE INCIDENTES INFORMÁTICOS DE LA ESPAM MFL**, que ha sido desarrollada por María Gabriela Cuzme Romero y Roxanna Elizabeth Pinargote Anchundia, previa la obtención del título de Ingenieras en Informática, de acuerdo al **REGLAMENTO PARA LA ELABORACIÓN DE TESIS DE GRADO DE TERCER NIVEL** de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López.

……..……..……

**ING. SERGIO A. INTRIAGO BRIONES, MGS**

# APROBACIÓN DEL TRIBUNAL

Los suscritos integrantes del tribunal correspondiente, declaran que han **APROBADO** la tesis **PLAN DE GESTIÓN DE INCIDENTES INFORMÁTICOS DE LA ESPAM MFL**, que ha sido propuesta, desarrollada y sustentada por María Gabriela Cuzme Romero y Roxanna Elizabeth Pinargote Anchundia, previa la obtención del título de Ingenieras en Informática, de acuerdo al **REGLAMENTO PARA LA ELABORACIÓN DE TESIS DE GRADO DE TERCER NIVEL** de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López.

| | |
|---|---|
| **.....** | **….....** |
| **ING. ORLANDO AYALA PULLAS** | **ING. MARLON R. NAVIA MENDOZA** |
| **MIEMBRO** | **MIEMBRO** |

**.....**
**ING. DANIEL A. MERA MARTÍNEZ**
**PRESIDENTE**

# AGRADECIMIENTO

A la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López que nos brindó una excelente formación profesional y en ella hemos formado nuestros conocimientos.

A nuestro creador, pilar fundamental sobre el que se edifican todas las cosas.

A nuestros padres, hermanos y familia quienes con su apoyo incondicional nos guían para alcanzar nuestras metas.

A nuestros amigos que siempre estuvieron presentes con consejos y motivación para seguir adelante a pesar de las dificultades.

A nuestro tutor quien con sus conocimientos, experiencia y dedicación nos orientó en el camino para alcanzar nuestra meta.

A los docentes de la carrera de Informática de la ESPAM MFL que aportaron con un granito de arena para nuestra formación.

**Las autoras**

# DEDICATORIA

El camino ha sido largo, pero sentir ahora que estoy cumpliendo uno de mis objetivos me llena de satisfacción, por eso deseo dedicarle esta tesis con mucho cariño y amor a las siguientes personas:

A mi Padre Salomón Cuzme, sé que no estás conmigo pero desde el cielo me proteges y te sientes orgulloso de la hija que me he convertido a pesar de tu partida, que desde pequeña me enseñaste a ser quien soy, con valores y principios que me han permitido desarrollarme como persona.

A mi madre Ramona Romero López, quien ha sido uno de mis pilares fundamentales que siempre ha estado conmigo motivándome a seguir adelante, que con sus consejos, perseverancia, amor incondicional y apoyo me supo ayudar en cada momento, para que no me rindiera por alcanzar mis sueños.

A mis Hermanas: Sergia, Mariana, Carmen y Anita, porque no mencionarlas, si ellas me han acompañado en todo este largo camino, que siempre me han brindado ayuda en los buenos y malos momentos; y con su alegría, entusiasmo y consejos siempre han estado presentes para poder realizarme como persona.

A toda mi familia, que de una u otra manera han estado presente en el trayecto de mi vida.

**MARÍA G. CUZME ROMERO**

# DEDICATORIA

Con todo mi amor y cariño dedico este trabajo investigativo:

A mi madre Jesús Anchundia, ser increíble, mujer luchadora que jamás flaquea ante las adversidades, a quien admiro mucho, quien con amor, esfuerzo, perseverancia y dedicación me impulsó a cumplir cada una de mis metas.

A mi padre Gary Pinargote, por ser el ejemplo de respeto y firmeza, por su apoyo incondicional, y estar alli cuando más lo necesitaba y sé que está orgulloso de la persona en la cual me he convertido.

A mi esposo Gerardo Loor a quien amo infinitamente, por ser mi mejor amigo, compañero, guía en cada uno de mis pasos, por estar dispuesto siempre a escucharme y compartir conmigo buenos y malos momentos.

A mi pequeño hijo Cristopher Gerard, lo más bello que Dios puso en mi camino, mi fuerza para combatir las dificultades de la vida, por él y para el serán todos mis triunfos.

A mis hermanos Gary, Gregorio, Fernanda y Gema por sus locuras, risas y peleas, que siempre han estado junto a mí brindándome apoyo y compartiendo conmigo alegrías y fracasos.

A mi abuelo Miguel Anchundia, a quien quiero como a un padre, a pesar de nuestra distancia física siento que siempre está conmigo, apoyándome, guiándome y bendiciéndome siempre.

A mi abuela, tías y tíos partes fundamentales de mi vida, quienes desde pequeña me inculcaron los mejores valores y velaron por mí en este arduo camino para convertirme en una verdadera profesional.

**ROXANNA E. PINARGOTE ANCHUNDIA**

# CONTENIDO

DERECHOS DE AUTORÍA ..... ii
CERTIFICACIÓN DE TUTOR ..... iii
APROBACIÓN DEL TRIBUNAL ..... iv
AGRADECIMIENTO ..... v
DEDICATORIA ..... vi
DEDICATORIA ..... vii
CONTENIDO ..... viii
CONTENIDO DE CUADROS Y FIGURAS ..... xi
RESUMEN ..... xv
PALABRAS CLAVE ..... xv
ABSTRACT ..... xvi
KEY WORDS ..... xvi
CAPÍTULO I. ANTECEDENTES ..... 1
1.1. PLANTEAMIENTO Y FORMULACIÓN DEL PROBLEMA ..... 1
1.2. JUSTIFICACIÓN ..... 3
1.3. OBJETIVOS ..... 5
1.3.1. OBJETIVO GENERAL ..... 5
1.3.2. OBJETIVOS ESPECÍFICOS ..... 5
1.4. IDEA A DEFENDER ..... 5
CAPÍTULO II. MARCO TEÓRICO ..... 6
2.1. PROCESO DE NEGOCIO ..... 6
2.2. TECNOLOGÍA DE LA INFORMACIÓN ..... 7
2.3. INCIDENTE ..... 8
2.3.1. IMPACTO DEL INCIDENTE ..... 9
2.3.2. URGENCIA DEL INCIDENTE ..... 9

2.3.3. PRIORIDAD DEL INCIDENTE ..... 9

2.3.4. INCIDENTES INFORMÁTICOS ..... 10

2.4. GESTIÓN..... 14

2.4.1. PLAN DE GESTIÓN ..... 14

2.5. NORMAS ISO ..... 16

2.5.1. NORMA ISO 27001 ..... 17

2.6. GESTIÓN DE SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN 17

2.6.1. METODOLOGÍA ITIL..... 18

2.7. ANÁLISIS Y EVALUACIÓN DEL RIESGO DE LA INFORMACIÓN..... 31

2.7.1. METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN (MAGERIT) ..... 32

2.8. TÉCNICAS PARA EL ANÁLISIS DE DATOS ..... 35

2.8.1. CUESTIONARIOS..... 36

2.8.2. ENTREVISTAS..... 36

2.8.3. CHECKLIST ..... 37

2.8.4. MATRIZ DE RIESGO ..... 37

2.9. GLPI..... 37

CAPÍTULO III. DESARROLLO METODOLÓGICO ..... 39

3.1. METODOLOGÍA ITIL – GESTIÓN DE INCIDENTES ..... 39

3.1.1. REGISTRO..... 39

3.1.1.1. METODOLOGÍA MAGERIT..... 40

3.1.2. CLASIFICACIÓN DE LOS INCIDENTES INFORMÁTICOS..... 44

3.1.3. DIAGNÓSTICO Y RESOLUCIÓN..... 48

3.1.3.1. METODOLOGÍA ITIL – GESTIÓN DE SERVICIOS ..... 48

CAPÍTULO IV. RESULTADOS Y DISCUSIÓN..... 50

4.1. RESULTADOS..... 50

4.1.1. REGISTRO..... 50

4.1.1.1. METODOLOGÍA MAGERIT ..... 60
4.1.2. CLASIFICACIÓN DE LOS INCIDENTES INFORMÁTICOS ..... 167
4.1.3. DIAGNÓSTICO Y RESOLUCIÓN ..... 168
4.1.3.1. METODOLOGÍA ITIL – GESTIÓN DE SERVICIOS ..... 168
4.2. DISCUSIÓN ..... 196
CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES ..... 198
5.1. CONCLUSIONES ..... 198
5.2. RECOMENDACIONES ..... 199
BIBLIOGRAFÍA ..... 200
ANEXOS ..... 206
ANEXO 1 ..... 207
OFICIO DE AUTORIZACIÓN DEL RECTOR DE LA ESPAM-MFL ..... 207
ANEXO 2 ..... 209
CERTIFICACIÓN EMITIDA POR EL JEFE DE ALMACÉN ..... 209
ANEXO 3 ..... 211
FICHA DE REGISTRO DE EQUIPOS INFORMÁTICOS ..... 211
ANEXO 4 ..... 213
CUESTIONARIO DE INCIDENCIAS INFORMÁTICAS ..... 213
ANEXO 5 ..... 222
FICHA DE REGISTRO DE INCIDENTES INFORMÁTICOS ..... 222
ANEXO 6 ..... 224
PLAN DE GESTIÓN DE INCIDENTES QUE AFECTAN A LOS EQUIPOS INFORMÁTICOS DE LA ESPAM-MFL ..... 224
ANEXO 7 ..... 256
CERTIFICADO DEL TUTOR ..... 256
ANEXO 8 ..... 258
CERTIFICACIÓN DEL CENTRO DE IDIOMAS ..... 258

# CONTENIDO DE CUADROS Y FIGURAS

**Cuadro 3.1.** Escalas de probabilidad de ocurrencia ..... 43
**Cuadro 3.2.** Escalas de impacto ..... 43
**Cuadro 3.3**. Escalas de frecuencia ..... 43
**Gráfico 3.1** Organigrama de funciones del Departamento de Tecnología ..... 45
**Cuadro 3.4** Definición de prioridades de la Gestion de Incidentes ..... 46
**Cuadro 3.5** Velocidad para responder a un incidente ..... 46
**Cuadro 3.6** Descripción del impacto ..... 47
**Gráfico 4.1.** Porcentaje de equipos informáticos en la carrera de medio ambiente de la ESPAM - MFL ..... 52
**Gráfico 4.2.** Porcentaje de equipos informáticos en la carrera de agroindustrias de la ESPAM - MFL ..... 52
**Gráfico 4.3**. Porcentaje de equipos informáticos en la carrera de pecuaria de la ESPAM – MFL ..... 53
**Gráfico 4.4**. Porcentaje de equipos informáticos en la carrera de agrícola de la ESPAM – MFL ..... 54
**Gráfico 4.5.** Porcentaje de equipos informáticos en la carrera de turismo de la ESPAM – MFL ..... 54
**Gráfico 4.6.** Porcentaje de equipos informáticos en la carrera de informática de la ESPAM – MFL ..... 55
**Gráfico 4.7.** Porcentaje de equipos informáticos en la carrera de administración de la ESPAM – MFL ..... 56
**Gráfico 4.8.** Porcentaje de equipos informáticos en el Data Center de la ESPAM –MFL ..... 56
**Gráfico 4.9.** Porcentaje de equipos informáticos en el área de cultura de la ESPAM – MFL ..... 57
**Gráfico 4.10.** Porcentaje de equipos informáticos en el área de bienestar politécnico de la ESPAM – MFL ..... 57
**Gráfico 4.11.** Porcentaje de equipos informáticos del departamento de acreditación de la ESPAM – MFL ..... 58
**Gráfico 4.12.** Porcentaje de equipos informáticos de las oficinas del centro de la Ciudad ..... 58
**Gráfico 4.13.** Porcentaje de equipos informáticos del departamento de tecnologia de la ESPAM – MFL ..... 59
**Gráfico 4.14**. Total de equipos informáticos de la ESPAM – MFL ..... 59

**Cuadro 4.1** Servicio: secretaria ..... 61
**Cuadro 4.2.** Servicio: centro de datos ..... 67
**Cuadro 4.3.** Servicio: Unidad de Producción de Software (UPS) ..... 76
**Cuadro 4.4.** Servicio: departamento de tecnología..... 81
**Cuadro 4.5. Servicio:** sala de docentes..... 86
**Cuadro 4.6.** Servicio: laboratorios ..... 93
**Cuadro 4.7**. Servicio: aulas de clases ..... 100
**Cuadro 4.8**. Servicio: coordinacion investigacion cientifica, emprendimiento, dirección de planificación, diseño e ingeniería ..... 103
**Cuadro 4.9**. Servicio: biblioteca..... 108
**Cuadro 4.10**. Servicio: postgrado y talento humano..... 113
**Cuadro 4.11**. Servicio: acreditación..... 117
**Cuadro 4.12.** Servicio: jefatura de almacén, vicerrectorado de extensión y bienestar politécnico, vinculación y coordinación de cultura ..... 122
**Cuadro 4.13**. Servicio:FEPAM..... 127
**Cuadro 4.14.** Servicio: dirección administrativa y financiera ..... 131
**Cuadro 4.15**. Servicio:Rectorado y Jurídico ..... 135
**Cuadro 4.16.** Servicio:audiovisuales ..... 139
**Cuadro 4.17.** Servicio: control de acceso ..... 143
**Cuadro 4.18.** Total de incidentes informáticos que se presentan en la ESPAM-MFL ..... 144
**Gráfico 4.15.** Frecuencia de incidentes con fuego ..... 145
**Gráfico 4.16.** Tiempo promedio de solución a incidentes con fuego ..... 145
**Gráfico 4.17.** Frecuencia de incidentes con agua ..... 146
**Gráfico 4.18.** Tiempo promedio de solución a incidentes con agua ..... 146
**Gráfico 4.19.** Frecuencia de desastres industriales..... 147
**Gráfico 4.20.** Tiempo promedio de solución a desastres industriales ..... 147
**Gráfico 4.21.** Frecuencia de robos de equipos informáticos ..... 148
**Gráfico 4.22.** Tiempo promedio de solución a robo de equipos informáticos 148
**Gráfico 4.23.** Frecuencia de cortes de suministro eléctrico..... 149
**Gráfico 4.24.** Tiempo promedio de solución a cortes de suministro eléctrico 149
**Gráfico 4.25.** Frecuencia de denegación del servicio..... 150
**Gráfico 4.26.** Tiempo promedio de solución a denegación del servicio..... 150

**Gráfico 4.27.** Frecuencia de problemas con la conexión de internet..... 151

**Gráfico 4.28.** Tiempo promedio de solución a problemas con la conexión de internet ..... 151

**Gráfico 4.29**. Frecuencia de inconvenientes con el correo electrónico institucional..... 152

**Gráfico 4.30.** Tiempo promedio de solución a inconvenientes con el correo electrónico institucional ..... 152

**Gráfico 4.31.** Frecuencia de problemas por suministro de componentes a computadoras de escritorio ..... 153

**Gráfico 4.32.** Tiempo promedio de solución a problemas por suminstro de componentes a computadoras de escritorio..... 153

**Gráfico 4.33.** Frecuencia de incidentes con deperfectos de hardware..... 154

**Gráfico 4.34.** Tiempo promedio de solución a incidentes de deperfectos de hardware ..... 154

**Gráfico 4.35.** Frecuencia de problemas de video ..... 155

**Gráfico 4.36.** Tiempo promedio de solución a problemas de video..... 155

**Gráfico 4.37.** Frecuencia de problemas por virus en las computadoras..... 156

**Gráfico 4.38.** Tiempo promedio de solución a problemas por virus en las computadoras..... 156

**Gráfico 4.39.** Frecuencia de incidentes por reinicio de computadoras ..... 157

**Gráfico 4.40.** Tiempo promedio de solución de incidentes por reinicio de computadoras..... 157

**Gráfico 4.41.** Frecuencia de problemas al actualizar programas ..... 158

**Gráfico 4.42.** Tiempo promedio de solución de problemas al actualizar programas ..... 158

**Gráfico 4.43.** Frecuencia de problemas al ejecutar los programas ..... 159

**Gráfico 4.44.** Tiempo promedio de solución a problemas al ejecutar los programas ..... 159

**Gráfico 4.45.** Frecuencia de alertas por licenciamiento de programas..... 160

**Gráfico 4.46.** Tiempo promedio de solución de alertas por licenciamiento de programas ..... 160

**Gráfico 4.47.** Frecuencia de incidentes referentes a la falta de mantenimiento preventivo..... 161

**Gráfico 4.48.** Tiempo promedio de solución a la falta de mantenimiento preventivo..... 161

**Gráfico 4.49.** Frecuencia de la falta de mantenimiento correctivo..... 162

**Gráfico 4.50.** Tiempo promedio de solución a la falta de mantenimiento correctivo ..... 162

**Gráfico 4.51.** Frecuencia de daños en las impresoras multifunción ..... 163

**Gráfico 4.52.** Tiempo promedio de solución a daños en las impresoras multifunción ..... 163

**Gráfico 4.53.** Frecuencia de incidentes por cambio de suministros a los equipos de impresión ..... 164

**Gráfico 4.54.** Tiempo promedio de solución a incidentes por cambio de suministros a los equipos de impresión ..... 164

**Gráfico 4.55.** Frecuencia de daños en el hardware de scanner ..... 165

**Gráfico 4.56.** Tiempo promedio de solución a daños en el hardware de scanner ..... 165

**Gráfico 4.57.** Efectos que se derivan de los incidentes ..... 166

**Cuadro 4.19.** Tipología de incidentes informáticos ..... 167

**Cuadro 4.20.** Catálogo de Servicios tecnológicos de la ESPAM-MFL ..... 170

# RESUMEN

La presente investigación tiene como finalidad elaborar un plan de gestión de incidentes que afectan a los equipos informáticos de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, estableciendo cursos de acción para reducir el impacto y mejorar la productividad de los usuarios. Para tal efecto, se empleó el apartado gestión de incidentes de la metodología ITIL, la cual se divide en cuatro fases: registro, incluyó la determinación de los equipos informáticos, con lo cual, se identificaron y clasificaron los riesgos a los que estaban expuestos mediante la metodología MAGERIT (versión 3.0), concluyendo con el registro de las incidencias informáticas; la fase de clasificación permitió establecer niveles de prioridad para cada incidente de acuerdo a criterios de urgencia e impacto; mediante las fases de diagnóstico y resolución, se elaboraron el catálogo de servicios tecnológicos disponibles y los acuerdos de servicios entre el personal encargado de los equipos informáticos y responsables de cada departamento y carrera de la ESPAM-MFL. En base a los resultados obtenidos mediante el plan de gestión de incidentes, se limitó el impacto de tales eventos, con la asignación de un equipo responsable para gestionarlos, situación que se comprueba con los acuerdos de servicios elaborados, por lo que al ejecutar los procedimientos de respuesta a incidentes se pueden contener y mitigar los mismos, por lo tanto, resulta conveniente adoptar medidas de seguridad eficientes para proteger los activos de información de la institución.

# PALABRAS CLAVE

Gestión, Plan de Gestión, Incidentes Informáticos, ITIL.

# ABSTRACT

This research aims to develop a management plan for incidents affecting the computers of the Polytechnic School of Manabi Agricultural Manuel Felix Lopez, establishing courses of action to reduce the impact of incidents and improve user productivity. To this end, the Incident Management ITIL methodology, which is divided into four phases paragraph was employed: Registration, included the determination of the computers, which were identified and ranked the risks to which they were exposed by the MAGERIT (version 3.0) methodology, concluding with the registration of computer incidents; allowed qualifying set priority levels for each incident according to criteria of urgency and impact; through the stages of diagnosis and resolution service agreements between the personnel and equipment of the IT department managers and career-MFL ESPAM they were developed. Based on the results obtained through the Incident Management Plan, the impact of such events was limited, with the assignment of a team responsible for managing them, a situation that checks with service agreements made, so when performing the procedures incident response you can contain and mitigate them, it is therefore appropriate to adopt effective measures to protect information assets from security institution.

# KEY WORDS

Management, Plan Management, IT incidents, ITIL.

# CAPÍTULO I. ANTECEDENTES

## 1.1. PLANTEAMIENTO Y FORMULACIÓN DEL PROBLEMA

La protección a la información es de vital importancia, ya que constituye uno de los activos más significativos de las organizaciones, por ello, se deben considerar los riesgos que involucran los procesos gestionados por el área de sistemas, lo cual conlleva que los equipos informáticos no se estén aprovechando de la mejor manera y exponen a peligros, información relevante para las instituciones.

Gran parte de las incidencias que se dan a conocer en las empresas, se deben a interrupciones en el correcto funcionamiento de los equipos informáticos correspondientes a cada uno de los departamentos. En ocasiones, el impacto que presentan este tipo de incidencias, genera la paralización de las actividades, afecta la seguridad de la información y por ende, reduce la calidad de los servicios que ofrecen estos equipos.

Así pues, considerando que la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, cuenta con equipos informáticos, los cuales apoyan las labores que el personal brinda a la institución, ayudando además, a los docentes y estudiantes a cumplir con sus trabajos académicos. Se encuentra, que a menudo surgen incidencias que se producen en los equipos y generan interrupción en los servicios, por lo que resulta conveniente establecer mecanismos para gestionarlos, permitiendo reestablecer el servicio lo más rápido posible.

Según lo expuesto, el plan de gestión presenta alternativas para reducir el impacto de los incidentes informáticos de la ESPAM-MFL, con el fin de estandarizar el tiempo que se debe emplear para que las actividades se lleven a cabo con normalidad.

Por lo antes manifestado, las autoras se plantean la siguiente interrogante:

¿Cómo gestionar los incidentes que afectan a los equipos informáticos de la ESPAM MFL para reducir el impacto de los mismos y mejorar la productividad de los usuarios?

## 1.2. JUSTIFICACIÓN

Las organizaciones son cada vez más dependientes de la tecnología de información, ya que soportan y mejoran los procesos de negocio requeridos para cumplir las necesidades de los clientes y de la propia organización, debido a la gran cantidad de información que se maneja. Por ello, se debe garantizar la seguridad de los datos correspondientes a cada área, para evitar pérdidas y reducir riesgos.

La Constitución de la República establece en su artículo 227, que la administración pública constituye un servicio a la colectividad que se rige en principios de eficacia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia y evaluación, por tanto, es de vital importancia adoptar políticas y procedimientos necesarios para mantener la seguridad de la información que se genera y custodia en diferentes medios y formatos de las entidades de la administración pública.

Al mismo tiempo, en el segundo suplemento del registro oficial número 88 del 05 de septiembre de 2013, la secretaría nacional de la administración pública considera que las Tecnologías de la Información y Comunicación son herramientas imprescindibles para el cumplimiento de la gestión institucional e inter-institucional de la administración pública en tal virtud, deben cumplir con estándares de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la información.

Conjuntamente, en su primer artículo declara: “Disponer a las entidades de la administración pública central, institucional y que dependen de la función ejecutiva el uso obligatorio de la Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la información”.

El plan de gestión está enfocado a tratar los incidentes que provoquen interrupción en los servicios que brindan los equipos informáticos, permitiendo la calidad y continuidad de las actividades regulares de la institución y se acatará a la Ley Orgánica de Educación Superior (LOES, 2010) que establece en su Art. 8 literal h lo siguiente: “Contribuir con el desarrollo local y nacional de manera

permanente, a través del trabajo comunitario o extensión universitaria”, de tal forma, se contribuirá en temas afines a la gestión de incidentes de seguridad informática.

Es importante para las instituciones establecer procedimientos estructurados y contar con personal especializado que permita resolver los incidentes informáticos. Para ello, el plan ayuda a disminuir los tiempos de resolución de este tipo de situaciones, gestionándolas de forma correcta y asignando un procedimiento de acuerdo a la urgencia y el impacto del incidente.

La elaboración de un plan de gestión de incidentes identificará cualquier evento que cause una interrupción en el servicio, de la forma más rápida posible, asignándole al equipo encargado la tarea de restaurar normalmente las actividades, permitiendo de esta manera disminuir el tiempo requerido para atender cada uno de los inconvenientes que se presentan en los departamentos de la ESPAM MFL;  por lo cual, las autoras justifican el tema mediante la metodología ITIL, la misma que involucra la definición de procedimientos estándares, que permite desarrollar eficaz y eficientemente cada uno de los procesos que cubren las actividades más importantes de las organizaciones.

## 1.3. OBJETIVOS

### 1.3.1. OBJETIVO GENERAL

Elaborar un plan de gestión de incidentes que afectan a los equipos informáticos de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, estableciendo cursos de acción para reducir el impacto y mejorarando la productividad de los usuarios.

### 1.3.2. OBJETIVOS ESPECÍFICOS

- ✓ Determinar los equipos informáticos pertenecientes a la ESPAM-MFL, para la identificación de los incidentes que afectan la calidad y continuidad de los servicios.
- ✓ Evaluar los incidentes encontrados estableciendo niveles de prioridad de acuerdo a criterios de urgencia e impacto.
- ✓ Elaborar un catálogo que defina los servicios disponibles.
- ✓ Desarrollar un plan de gestión de incidentes que afectan a los equipos informáticos de la ESPAM MFL.

## 1.4. IDEA A DEFENDER

La elaboración de un plan de gestión de incidentes que afectan a los equipos informáticos de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, permitirá establecer cursos de acción que reduzcan el impacto y mejoren la productividad de los usuarios.

# CAPÍTULO II. MARCO TEÓRICO

## 2.1. PROCESO DE NEGOCIO

Un proceso de negocio es un conjunto de tareas o actividades, lógicamente estructuradas, que ayudan a transformar varios insumos (input), en un producto final (output) por medio de la aplicación de varios factores, con el que se persigue obtener un valor para la organización (Nacipucha, 2013).

Para Hitpass (2012) un proceso de negocio es un conjunto de actividades que impulsadas por eventos y ejecutándolas en una cierta secuencia crean valor para un cliente (interno o externo).

Ocaña (2012), considera a un proceso de negocio como una combinación de distintos modos de hacer una actividad con el objetivo de generar valor por los modos diferentes de hacer una actividad siendo eficientes y generar valor por los modos eficientes de hacer una actividad con algún grado de diferencia.

Después del análisis, se elige para la presente investigación, la definición de Nacipucha (2013), quien determina que un proceso de negocio es un conjunto de tareas o actividades lógicamente estructuradas, que ayudan a transformar varios insumos (input), en un producto final (output).

En la actualidad, las empresas han admitido que disponer de productos con una adecuada calidad no es suficiente ventaja competitiva. Persiguiendo el objetivo de ofrecer el máximo valor añadido a sus clientes, las empresas requieren una gestión flexible con el fin de reaccionar de manera eficaz y eficiente a los continuos cambios del entorno. En el paradigma preponderante en las pasadas décadas, la organización era vista como un conjunto jerárquico de áreas funcionales que respondían a los requerimientos del entorno con unas tareas, funciones y objetivos, bien definidos y acotados, pero actualmente se exige una nueva estructura, con el objetivo de superar las expectativas de los clientes así como ser ágiles para poder reconfigurar rápidamente los procesos de negocio con el fin de satisfacer las nuevas necesidades (Sanchis *et al.*, 2009).

## 2.2. TECNOLOGÍA DE LA INFORMACIÓN

Se conoce como tecnología de información (TI) a la utilización de tecnología, específicamente computadoras y ordenadores electrónicos, para el manejo y procesamiento de información, concretamente la captura, transformación, almacenamiento, protección, y recuperación de datos e información (Arancibia *et al.*, 2010).

Graniel (2011) manifiesta que la TI no se restringe a equipamientos (hardware), programas (software) y comunicación de datos. Existen tecnologías relativas a la planificación de informática, al desarrollo de sistemas, al soporte del software, a los procesos de producción y operación y al soporte de hardware.

Las autoras asumen para la presente investigación, que la tecnología de la información es la utilización de tecnología específicamente computadoras y ordenadores electrónicos, para el manejo y procesamiento de información; con la cual, si se utiliza eficientemente, se pueden obtener ventajas competitivas mediante procedimientos acertados que mantienen tales ventajas como una constante.

Los orígenes de la TI son recientes. Aunque el nombre de tecnología de información se remonta a los años 70, su utilización en los negocios se remonta a mediados del siglo XX, durante la segunda guerra mundial. Sin embargo, ha sido en los últimos 20 años donde ha alcanzado niveles de uso y aplicaciones tan variadas y ubicuas, que se ha convertido en un área de gran amplitud e impacto en todos los aspectos de la vida cotidiana – incluyendo la gerencia de cualquier empresa, en la cual hoy en día es casi indispensable (Arancibia *et al.*, 2010).

Las tecnologías de la información y las comunicaciones (TIC's) se han constituido en uno de los recursos más importantes de la sociedad, trayendo como consecuencia una explosión exponencial en la transmisión e intercambio de datos, información y conocimientos, a los cuales se puede acceder sin tener

en cuenta barreras geográficas o limitaciones del tiempo, transformando elementos fundamentales que condicionan la comunicación tales como el espacio y el tiempo, a lo que se adiciona la capacidad de interacción en el proceso de comunicación (Prieto *et al.,* 2011).

En la actualidad, las TIC (Tecnología de Información y las Comunicaciones) juegan un papel protagónico en el día tras día del desarrollo de la sociedad, hasta el punto de convertirse en el área contemporánea de mayor dinamismo económico, técnico y jurídico; debido a esto la dependencia a las redes de comunicaciones es cada vez más fuerte, creando la necesidad de acceder a la información desde cualquier lugar, desde cualquier dispositivo, a cualquier momento y de manera segura (León *et al*., 2014).

## 2.3. INCIDENTE

Según las apreciaciones de Kolthof *et al.* (2012), un incidente es un suceso que no forma parte de la operación estándar de un servicio y que puede provocar, la interrupción o reducción en la calidad del mismo. Un incidente incluye no solo errores de hardware y software, sino también Peticiones de Servicio- porque ambas se gestionan de una manera similar.

VenCERT (2008) define a un incidente como un evento, anomalía o interrupción de un servicio de seguridad de la información imprevisto, que puede comprometer de manera significativa el correcto funcionamiento de un sistema y amenazar la seguridad de la información.

La mayoría de las investigaciones señalan, que un incidente es un suceso que no pertenece a los procedimientos regulares de un servicio, y que puede provocar la interrupción del mismo; además, tiene la probabilidad significativa de comprometer las operaciones de un sistema y de amenazar la seguridad de la información.

### 2.3.1. IMPACTO DEL INCIDENTE

Es el grado de desviación sobre la operativa normal, en términos de número de usuarios o de procesos del negocio afectados. Incidentes graves son los que el grado de impacto en la comunidad de usuarios es extremo. Los incidentes en los cuales la escala de tiempo de interrupción – incluso a un relativamente pequeño porcentaje de usuarios – es excesiva deberían también ser considerados como grave (Kolthof *et al.,* 2012).

Las apreciaciones de Puello (2012) señalan que el impacto es una medición del efecto de un incidente, un problema o un cambio en los procesos de negocio.

De acuerdo con Puello (2012) se corrobora que el impacto del incidente es la medición del efecto del mismo.

### 2.3.2. URGENCIA DEL INCIDENTE

Es la demora aceptable para el usuario o el proceso de negocio, para resolver un incidente (Kolthof *et al.,* 2012).

Las investigaciones de Puello (2012) manifiestan que la urgencia es la medición de cuánto tiempo tarda un incidente, un problema o un cambio en tener impacto significativo en el negocio.

Considerando las indagaciones de Kolthof *et al.* (2012) puede concluirse que la urgencia del incidente es la demora aceptable para el usuario o el proceso de negocio, para resolver un incidente.

### 2.3.3. PRIORIDAD DEL INCIDENTE

Puello (2012) hace alusión de que una prioridad está basada en un impacto y urgencia, y es utilizada para identificar el tiempo que se necesita para que las acciones se llevan a cabo.

La prioridad se determina primeramente sobre la base de la urgencia y el impacto. Para cada prioridad se define un número de personas y cierta cantidad de recursos. Para incidentes con la misma prioridad, el esfuerzo requerido para resolverlo puede determinar el orden. Por ejemplo, un incidente con poco impacto que requiere poco esfuerzo se puede resolver antes que otro con un más alto impacto para el que se necesite más esfuerzo (Kolthof *et al.,* 2012).

La mayoría de los autores consideran que la prioridad del incidente está basada en el impacto y urgencia del mismo.

### 2.3.4. INCIDENTES INFORMÁTICOS

Un incidente de seguridad informática se define como cualquier evento que atente contra la confidencialidad, integridad y disponibilidad de la información y los recursos tecnológicos (CAES S.A., s.f.).

Velasco y Arean (2008) específica a los incidentes informáticos como aquellas situaciones que atentan, vulneran o destruyen información valiosa de la organización, además del impacto psicológico y económico que puede generar en el mercado accionario o en los accionistas cuando se informa sobre intrusiones y pérdidas de información en un ente empresarial.

Las autoras, toman para la presente investigación la definición de CAES S.A. (s.f.) quien define a un incidente de seguridad informática como cualquier evento que atente contra la confidencialidad, integridad y disponibilidad de la información y los recursos tecnológicos.

Los incidentes de Seguridad Informática se pueden clasificar en 5 categorías:

- **Acceso no Autorizado.-** esta categoría comprende todo tipo de ingreso y operación no autorizada a los sistemas, sea o no exitoso. Son parte de esta categoría:
  - ✓ Accesos no autorizados exitosos, sin perjuicios visibles a componentes tecnológicos.

- ✓ Robo de información.
- ✓ Borrado de información.
- ✓ Alteración de la información.
- ✓ Intentos recurrentes y no recurrentes de acceso no autorizado.
- ✓ Abuso y/o mal uso de los servicios informáticos internos o externos que requieren autenticación.

- **Código Malicioso.-** se refiere a la introducción de códigos maliciosos en la infraestructura tecnológica de la Entidad. Ejemplos:
  - ✓ Virus informáticos
  - ✓ Troyanos
  - ✓ Gusanos informáticos
- **Denegación del servicio.-** incluye los eventos que ocasionan pérdida de un servicio en particular. Los síntomas para detectar un incidente de este tipo son:
  - ✓ Tiempos de respuesta muy bajos sin razones aparentes.
  - ✓ Servicio(s) interno(s) inaccesibles sin razones aparentes.
  - ✓ Servicio(s) Externo(s) inaccesibles sin razones aparentes.
- **Escaneos, pruebas o intentos de obtener información, redes o servidores sin autorización.-** agrupa los eventos que buscan obtener información de la infraestructura tecnológica de la Entidad y comprenden:
  - ✓ Sniffers (software utilizado para capturar información que viaja por la red).
  - ✓ Detección de Vulnerabilidades.
- **Mal uso de los recursos tecnológicos.-** incluye los eventos que atentan contra los recursos tecnológicos por el mal uso y comprenden:
  - ✓ Mal uso y/o abuso de servicios informáticos internos o externos.
  - ✓ Violación de las normas de acceso a Internet.
  - ✓ Mal uso y/o abuso del correo electrónico de la Entidad.
  - ✓ Violación de políticas, normas y procedimientos de seguridad Informática (CAES S.A., s.f.).

#### 2.3.4.1. SEGURIDAD INFORMÁTICA

La seguridad informática se puede entender como las reglas técnicas destinadas a prevenir, proteger y resguardar lo que es susceptible a robo, pérdida o daño, la misma, abarca multiples áreas relacionadas con los sistemas de información. Áreas que van desde la protección física del ordenador como componentes del hardware, de su entorno, hasta la protección de la información que contiene o de las redes que lo comunican con el exterior (Teopanta, 2006)

Las apreciaciones de Morlanes (2012), señalan, que para conseguir tal objetivo, es necesario evaluar y cuantificar los bienes a proteger, y en base al análisis, establecer medidas preventivas y correctivas que eliminen o reduzcan los riegos asociados hasta niveles manejables.

Una de las vías para conseguir que el proceso de la gestión de la seguridad informática sea un proceso menos complejo y más efectivo, en un entorno de constantes amenazas de seguridad, y teniendo en cuenta la gran cantidad de medidas a implementar; es la automatización de controles de seguridad informática (Montesino *et al*., 2013).

Velasco *et al.,* (2008) manifiesta, que la seguridad informática ha hecho tránsito de un esquema caracterizado por la implantación de herramientas de software, que neutralicen el acceso ilegal y los ataques a los sistemas de información, hacia un modelo de gestión de la seguridad de la información en el que prima lo dinámico sobre lo estacional.

En relación con Teopanta (2006) se puede concluir que la seguridad informática se refiere a la protección del ordenador y sus componentes, y de la información que contiene o de las redes que la comunican con el exterior.

- **Amenazas.-** es la causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o a la organización (Carrasco, 2013).

  Los usuarios finales están siendo víctimas de distintos delitos cibernéticos que afectan su economía o su privacidad, como el fraude en línea o el robo de información personal como contraseñas de correo electrónico. La seguridad informática es hoy en día, un tema crítico de las comunicaciones efectuadas mediante internet, a causa del gran número de amenazas que exponen a los datos al viajar mediante este medio. Este tipo de amenazas, se dan a conecer de diferentes formas, tieneniendo como objetivo principal provocar el mayor daño posible a la información que se almacena en los sistemas (Jiménez, 2008).

  Marrero (2003) considera que las amenazas sobre los sistemas informáticos presentan orígenes diversos. Así, el hardware puede ser físicamente dañado por la acción del agua, el fuego, los sabotajes, etcétera. Ellos también pueden dañar los medios magnéticos de almacenamiento externo. Pero, además, la información almacenada en estos últimos, también puede afectarse como resultado de la influencia de campos magnéticos intensos y, frecuentemente, por errores de operación. Las líneas de comunicación pueden interferirse o "pincharse". Otra clase de amenaza es la que representan usuarios o empleados infieles, que pueden usurpar la personalidad de usuarios autorizados para acceder y manipular indebidamente los datos de una o más organizaciones.

  Además, agrega, que las menazas más sutiles provienen de los controles inadecuados de la programación, como es el problema de los residuos, es decir, de la permanencia de información en memoria principal cuando un usuario la libera o, en el caso de dispositivos externos, cuando se borra incorrectamente.

## 2.4. GESTIÓN

Es un concepto global o globalizador, que se utiliza para denominar un conjunto de actividades más los medios necesarios para lograr un objetivo determinado. Se refiere al conjunto de actividades que permite que una empresa manufacture sus productos o brinde sus servicios, organizados de forma tal que el uso de recursos necesarios sea eficaz y rentable, lo cual le permite vender sus productos y servicios en un mercado competitivo (Gerbrandy y Hoogendam, 1998).

Las consideraciones de Gerbrandy y Hoogendam (1998) infieren que la gestión es concepto global o globalizador, que se utiliza para denominar un conjunto de actividades más los medios necesarios para lograr un objetivo determinado.

La gestión podría verse orientada a la acción en redes de participantes donde éstos requieren, en medio de condiciones heterodoxas, ser estimulados para la creatividad conjunta, tal vez con medidas que podrían agredir los cánones propios de la administración superando ciertos paradigmas de la acción (Ortiz y Pedroza, 2006).

### 2.4.1. PLAN DE GESTIÓN

Las indagaciones de Rabinowitz (c2014), comprueban, que un plan de gestión es un esquema que permite manejar de la mejor forma la organización en el transcurso de sus actividades diarias y a largo plazo. Contiene, métodos acertados que permitirán administrar el dinero, realizar las tareas de la organización y tratar la forma en que las personas de la organización llevan a cabo su trabajo.

Para APN (2010) el plan de gestión (o plan de manejo) es el máximo instrumento de planificación estratégica que contiene las directrices necesarias para orientar la gestión (manejo y administración) de las organizaciones, para su seguimiento y evaluación. Es un documento realista elaborado en base a los recursos disponibles (financiero, material, humano, institucional, tecnológico) que no deja

por ello de plantear lo imprescindible; es una herramienta clave para la toma de decisiones y para la formulación del plan operativo anual.

Las autoras de la presente investigación, toman la noción de APN (2010) quien manifiesta que el plan de gestión es el máximo instrumento de planificación estratégica que contiene las directrices necesarias para orientar la gestión de las organizaciones, para su seguimiento y evaluación.

El plan de gestión para una organización en particular depende de varios factores:

- ¿Qué está tratando de lograr la organización?
- ¿Qué se debe hacer, diariamente, para que la organización funcione?
- ¿Quién es el responsable, cuánto personal será necesario y qué mecanismos permitirán lograrlo?
- ¿Qué nivel de libertad requiere el personal para realizar bien su trabajo?
- ¿Qué recursos existen disponibles para implementar un plan de gestión?
- ¿Cómo se ajusta el plan de gestión con la misión y filosofía de la organización? (Rabinowitz, c2014).

Un buen plan de gestión permitirá lograr las metas de diferentes maneras:

- Define responsabilidades y roles del personal de la organización. Además, el personal esta al tanto de cuáles son los límites de su puesto.
- Asigna de manera equilibrada y responsable el trabajo de la organización, para que además de estar definido el trabajo de cada uno, también sea factible.
- Incrementa la obligación del personal en rendir cuentas de algo, tanto interna, como externamente.
- Afirma que las tareas sean concedidas al personal apropiado, y establece un plazo para que se culminen.
- Facilita a que la organización se defina a sí misma. Mediante un plan consistente con su misión y filosofía, la organización conocerá notoriamente

en lo que cree y se le comunicará esa convicción a todo su personal y a toda la comunidad (Rabinowitz, c2014).

## 2.5. NORMAS ISO

La normalización es un proceso dinámico y continuo imprescindible para el funcionamiento óptimo de toda organización y la obtención de buenos resultados económicos (Valdés, 1996).

La necesidad de realizar el análisis y procesamiento de los documentos, tanto a nivel nacional como internacional, de forma tal que éstos sean comprensibles y compatibles entre sí, resulta cada vez más urgente. Con este fin, se han desarrollado diferentes normas internacionales en el campo de la documentación y de la información científica (Valdés, 1996).

La organización Internacional para la Estandarización, ISO por sus siglas en inglés (International Organization for Standardization), es una federación mundial que agrupa a representantes de cada uno de los organismos nacionales de estandarización (como lo es el IRAM en la Argentina), y que tiene como objeto desarrollar estándares internacionales que faciliten el comercio internacional (Monterroso, s.f.).

Las investigaciones de Del Castillo (2012), señalan que el término ISO proviene de un vocablo griego que significa ‘igual’, y es aplicable tanto a las normas como a la institución, el mismo tiene como objetivo coordinar el sistema de estándares internacionales.

La International Standard Organization (ISO) tiene como propósito fundamental promover (a nivel mundial) el desarrollo de la normalización y de actividades afines, con el objetivo de permitir el intercambio internacional de productos y servicios en los sectores industrial, comercial, científico, tecnológico, económico y otros (Valdés, 1996).

### 2.5.1. NORMA ISO 27001

La norma consagra un conjunto significativo de dominios que pretenden establecer un ciclo de seguridad lo más completo posible, advirtiendo que no todos ellos tienen impacto jurídico. Desde ya es importante mencionar que el enfoque que se propone se alimenta tanto de normatividad nacional como internacional, así como de otras fuentes del Derecho, en razón de la escasa legislación que existe.

La norma ISO 27 001, contempla diez dominios:

1. Política de Seguridad de la Información
2. Organización de la Seguridad de la Información
3. Gestión de Activos
4. Seguridad de Recursos Humanos
5. Seguridad Física y del Entorno
6. Gestión de Comunicaciones y Operaciones
7. Control de Acceso
8. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información
9. Gestión de Incidentes de la Seguridad de la Información
10. Cumplimiento

Estos dominios están compuestos por un conjunto de subdominios y sus correspondientes controles, los cuales han de ser abordados adoptando un modelo PHVA (Planificar, Actuar, Verificar y Actuar) (Velasco y Arean, 2008).

## 2.6. GESTIÓN DE SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN

Actualmente las organizaciones proveedoras de servicios de Tecnologías de la Información (TI) necesitan disponer de una gestión de servicios efectiva para cumplir las demandas de sus clientes. Para estas organizaciones ya no es suficiente apostar por la mejor tecnología, una orientación a procesos en el desarrollo de sus productos y en su propia organización interna, sino que

también deben considerar la calidad de los servicios que proporcionan a sus clientes. En este sentido, surge una nueva disciplina, la gestión de servicios de Tecnologías de la Información (ITSM, del inglés Information Technology Service Management), que se centra en la perspectiva del cliente como principal aporte al negocio. La gestión de servicios de Tecnologías de la Información es un conjunto de capacidades organizacionales especializadas en proporcionar valor a los clientes en forma de servicios. Para proveer y gestionar de forma eficaz los servicios ofrecidos a lo largo de todo su ciclo de vida, resulta imprescindible definir y adoptar un conjunto de buenas prácticas. Si estas prácticas se agrupan y estructuran en procesos, este conjunto de procesos del área de provisión y gestión de servicios, puede utilizarse para ampliar el concepto de ciclo de vida de procesos de software hacia un ciclo de vida de producto completo que abarque también todos los aspectos relacionados con la provisión y gestión de los servicios (Mesquida *et al*., 2009).

### 2.6.1. METODOLOGÍA ITIL

Los negocios tienden a tener una mayor dependencia de las Tecnologías de Información. Los departamentos de Sistemas de Información, y las actividades desarrolladas, han sido tradicionalmente vistos como un área de soporte al negocio, descuidando muchas veces el uso de criterios racionales para medir su rentabilidad, eficacia y la calidad del servicio ofrecidos a toda la organización (Ocampo *et al.*, 2009).

La metodología ITIL fue desarrollada a finales de 1980, y corresponde a la expresión Biblioteca de Infraestructura de Tecnologías de la Información (ITIL) y se ha transformado en un estándar mundial para la Gestión de Servicios Informáticos. Iniciada como una guía para el gobierno de Inglaterra, la estructura base ha demostrado ser útil para las organizaciones en todos los sectores a través de su adopción por innumerables compañías como base de consulta, educación y soporte de herramientas de software.

ITIL se desarrolló al mostrarse, que las organizaciones dependen cada vez más de la Tecnología de la Información para lograr sus objetivos. Lo cual, da como

consecuencia la necesidad creciente de servicios de calidad que brinda la tecnología de la información, los cuales, deben corresponderse con los objetivos del negocio y satisfacer las necesidades de los clientes (Toro, 2013).

ITIL consolida diferentes aspectos estratégicos y operacionales de la organización, los cuales incluyen una estructura (framework) de dominio público que permite el acceso al modelo libremente, facilitando su uso en una amplia gama de industrias. Igualmente, incluye un marco referenciado en las mejores prácticas que proporciona un esquema fácilmente incorporable a métodos y actividades ya existentes orientadas al Manejo del Servicio, y que implica no necesariamente una nueva forma de actuar y pensar, sino la adaptación de éstas en un contexto estructurado, haciendo énfasis en las relaciones entre los procesos. La estandarización es otro aspecto estratégico y operacional determinante cuya ventaja radica en el uso de un lenguaje común, que permita a los individuos y grupos de trabajo comprender las políticas y reglas establecidas, fortaleciendo una visión compartida orientada al servicio (Ortiz y Hoyos, 2005).

El grado de preocupación actual ha provocado que ITIL haya resurgido como la aproximación más ampliamente aceptada a nivel internacional, y haya sido adoptado por grandes empresas, como IBM, Microsoft, SUN y HP entre otras, como base para sus soluciones de la Gestión de Servicios. Aunque estas empresas han desarrollado sus propias metodologías de servicios basadas en ITIL, los criterios de implantación seguidos por cada una de ellas, al no estar establecidos explícitamente en ITIL, han sido guiados en cada caso por intereses o experiencias empresariales. A pesar del gran reto planteado, se ha dedicado poco esfuerzo de investigación en la línea de sistematizar los criterios de implantación de los procesos de Gestión de Servicios de TI (Arcilla *et al*., 2007).

#### 2.6.1.1. ESTRUCTURA DE ITIL

Las Librerías de Infraestructura de Tecnologías de Información, se soportan en cinco elementos principales totalmente interrelacionados (Ortiz y Hoyos, 2005).

**La perspectiva del negocio**: las nuevas tendencias administrativas y de gestión basadas en las mejores prácticas requieren un enfoque gerencial totalmente neoclásico, donde se dispongan los medios para el establecimiento de estrategias globales que fortalezcan la cultura organizacional, la administración del cambio, la planeación estratégica y el pensamiento sistémico, entre otros, encaminados a consolidar la visión del negocio. En un ambiente de constante cambio, la transformación de mentalidad en todas las esferas es decisiva. Como pilar fundamental, ITIL requiere que la alta gerencia se comprometa y dirija cambios radicales en el interior de sus organizaciones, no sólo en inversiones físicas y tangibles, sino en escenarios más complejos, procesos, estructura organizacional, cultura, relaciones, conocimiento, experiencia, habilidades y destrezas, con la exigencia de involucrar e integrar todos los agentes que componen la empresa, proveedores, talento humano interno, clientes y otros; todo esto en concordancia con los estándares que se indican en los sistema de calidad y del servicio.

**Entrega del servicio:** en un ambiente de constante competitividad, son determinantes para la continuidad del negocio, las condiciones en la que se entrega el producto requerido por el cliente; la garantía de calidad, la oportunidad, el costo, la utilidad, el beneficio y la aplicabilidad son algunas de las condiciones mínimas que se exigen a diario. ITIL permite gestionar la entrega y monitorización del producto dentro de los acuerdos establecidos con el cliente, permitiendo al negocio administrar la capacidad, la disponibilidad, los aspectos financieros, el nivel y la continuidad del servicio.

**Soporte del servicio:** garantiza la continuidad de las relaciones con el cliente en la medida que las nuevas demandas, requerimientos, cambios o fallas sean soportadas integralmente. Con ITIL se permite la administración de las incidencias, problemas, cambios, configuraciones y remisiones solicitadas por el cliente, acorde a las tendencias de cada sector.

**Manejo de la infraestructura:** con ITIL se proporciona el esquema integral que apoya la instalación y adecuación de redes, comunicaciones, hardware

complementario, procesadores, servidores, sistema operativo y software que necesita la organización para garantizar el servicio al cliente con altos niveles y estándares de calidad.

**Manejo de aplicaciones**: elemento que proporciona a la empresa las condiciones necesarias para implementar sus procesos internos y adaptarlos a los cambios que se vayan presentado, reflejados en los sistemas de información que soportan la estructura tecnológica. La mayor concentración del modelo se observa en el desarrollo de los elementos entrega del servicio y soporte del servicio.

#### 2.6.1.2. PROCESOS DE LA METODOLOGÍA ITIL

**Centro de servicios:** el objetivo primordial, aunque no único, del Centro de Servicios es ser de punto de contacto entre los usuarios y la Gestión de Servicios TI.

Un Centro de Servicios, en su concepción más moderna, debe funcionar como centro neurálgico de todos los procesos de soporte al servicio: registrando y dando seguimiento a incidentes, empleando medidas de solución temporales a errores conocidos con la colaboración de la Gestión de Problemas, ayudando a la Gestión de Configuraciones para cerciorar la actualización de las bases de datos correspondientes, tramitando modificaciones requeridas por los clientes mediante peticiones de servicio con la asistencia de la Gestión de Cambios y Versiones.

Pero también, deberá dar soporte al negocio, identificando nuevas oportunidades en sus contactos con usuarios y clientes (OSIATIS S.A., s.f.).

**Gestión de problemas:** las funciones principales de la Gestión de Problemas son:

- Investigar las causas de toda alteración, real o potencial, del servicio TI.

- Establecer posibles soluciones a las mismas.
- Plantear las peticiones de cambio (RFC) requeridas para restaurar la calidad del servicio.
- Efectuar Revisiones Post Implementación (PIR) que permitan certificar que los cambios arrojan los efectos buscados, sin generar inconvenientes de carácter secundario.

La Gestión de Problemas puede ser:

- ✓ **Reactiva:** analiza los incidentes ocurridos para revelar su causa y plantea soluciones a los mismos.
- ✓ **Proactiva:** controla la calidad de la infraestructura TI y estudia su configuración, con el propósito de prevenir incidentes, incluso antes de que estos ocurran (OSIATIS S.A., s.f.).

**Gestión de cambios:** los principales motivos para realizar cambios en la infraestructura TI son:

- Solucionar errores conocidos.
- Desarrollor nuevos servicios.
- Mejorar los servicios existentes.
- Imperativo legal.

El propósito fundamental de la Gestión de Cambios, es la evaluación y planificación del proceso de cambio, para cerciorar que se lleve a cabo de la forma más eficiente, siguiendo los procedimientos determinados y asegurando en todo momento la calidad y continuidad del servicio TI (OSIATIS S.A., s.f.).

**Gestión de la disponibilidad:** la Gestión de la Disponibilidad es responsable de optimizar y monitorizar los servicios TI para que funcionen ininterrumpidamente y de manera fiable, cumpliendo los SLAs (acuerdos de servicios) y a un coste razonable (OSIATIS S.A., s.f.).

**Gestión de la capacidad:** la Gestión de la Capacidad se encarga de que todos los servicios TI se vean respaldados por una capacidad de proceso y almacenamiento suficiente y adecuademente dimensionada.

Sin una correcta Gestión de la Capacidad los recursos no se aprovechan apropiadamente y se efectúan inversiones innecesarias que generan gastos adicionales de mantenimiento y administración.

Entre las responsabilidades de la Gestión de la Capacidad se encuentran:

- Asegurar que se cubren las necesidades de capacidad TI tanto presentes como futuras.
- Controlar el rendimiento de la infraestructura TI.
- Desarrollar planes de capacidad asociados a los niveles de servicio acordados.
- Gestionar y racionalizar la demanda de servicios TI (OSIATIS S.A., s.f.).

**Gestión de incidentes:** la Gestión de Incidentes es una tarea reactiva. Por esta razón los incidentes se registran, se clasifican y se asignan a los especialistas adecuados, luego se controlan y por último se resuelven y se cierran (Kolthof *et al.,* 2012).

Pacheco y Jara (2012) consideran la gestión de incidentes como el proceso que contempla desde la identificación o reporte del incidente, hasta su resolución y el análisis de las lecciones aprendidas, de forma tal de evitar que el mismo incidente vuelva a ocurrir.

La Gestión de Incidentes tiene como propósito solucionar cualquier incidente que interrumpa el servicio de la manera más rápida y eficaz posible (Aquino *et al.*, 2011).

La Gestión de incidentes a diferencia de la gestión de problemas, no se preocupa de encontrar y analizar las causas de un determinado incidente, sino unicamente a restaurar el servicio. Sin embargo, existe una fuerte interrelación entre ambas (OSIATIS S.A., s.f.).

OVERTI (c2011) hace énfasis en que el proceso de gestión de incidencias abarca todo tipo de incidencias, ya sean fallos, consultas realizadas por usuarios (generalmente mediante llamada al Centro de Servicio al Usuario) o por el personal técnico, inclusive aquéllas reveladas de forma automática por herramientas de monitorización de eventos.

Después del análisis, se determina que la gestión de incidentes es una tarea reactiva, mediante la cual se contempla desde la identificación o reporte del incidente, hasta su resolución y el análisis de las lecciones aprendidas, con la finalidad de impedir que se interrumpa el servicio y evitar que el mismo incidente vuelva a ocurrir.

Dado que toda esta actividad precisa de un estrecho contacto con los usuarios, el eje del proceso de Gestión del Incidente es a través de la función del Centro de Servicio al Usuario que sirve como la oficina de entrada a los departamentos de especialistas y proveedores subyacentes. La Gestión de Incidentes es esencial para los otros procesos ITIL ya que proporciona información valiosa sobre los errores de la infraestructura (Kolthof *et al.,* 2012).

- **Objetivo.-** El objetivo de la Gestión del Incidente es restituir el servicio, lo más pronto que sea posible, con el menor impacto posible sobre la actividad del negocio de la organización y el usuario. La Gestión del Incidente también debe mantener registros eficaces de los incidentes por lo que puede medir y evaluar el proceso, proporcionar información a los otros procesos de la gestión de servicio e informes de progreso (Kolthof *et al.,* 2012).

- **Benefícios.-** Para el negocio en conjunto:

  a. Mayor resolución dentro del tiempo estipulado de los incidentes reduciendo el impacto en el negocio.
  b. Mayor productividad para el usuario.
  c. Monitorización de incidentes como proceso independiente, centrado en el cliente.
  d. Disponibilidad de información de producción centrada en la gestión del negocio.

Si no se implementa la Gestión del Incidente se puede enfrentar con los siguientes efectos adversos:

  a. Al no tener un responsable de monitorizar y escalar los incidentes, éstos se pueden volver innecesariamente severos y reducir el nivel de servicio. Los usuarios pueden ser derivados a otras autoridades sin que se les resuelva el problema.
  b. Se interrumpe continuamente a los especialistas con llamadas de usuarios que impiden que ellos realicen su trabajo. En consecuencia, mucha gente puede estar trabajando sobre el mismo incidente, puede que perdiendo tiempo innecesariamente, y puede que dando soluciones conflictivas.
  c. Hay falta de información administrativa sobre el dominio del usuario y los servicios.
  d. Dados todos los problemas mencionados, el cliente y la organización gastan más de lo necesario (Kolthof *et al.,* 2012).

- **Actividades de la gestión de incidentes**

  1. Identificación
  2. Registro
  3. Clasificación
  4. Priorización
  5. Diagnóstico (inicial)

6. Escalado
7. Investigación y diagnóstico
8. Resolución y Recuperación
9. Cierre OVERTI (c2011).

- **Proceso de la gestión de incidentes**

a. Registro
b. Clasificación
c. Diagnóstico
d. Resolución (OSIATIS S.A., s.f.).

**Registro.-** la admisión y registro del incidente es el primer y necesario paso para una correcta gestión del mismo (OSIATIS SA., s.f.).

Las incidencias pueden derivarse de diversas fuentes tales como: usuarios, gestión de aplicaciones, el mismo Centro de Servicios o el soporte técnico, entre otros (OSIATIS SA., s.f.).

El proceso de registro deberá realizarse de manera inmediata, ya que es mucho más costoso hacerlo posteriormente y se corre el riesgo de que la aparición de nuevas incidencias atrace indefinidamente el proceso (OSIATIS SA., s.f.).

- **La admisión a trámite del incidente:** el Centro de Servicios debe de ser capaz de evaluar en primera instancia si el servicio requerido se incluye en el SLA del cliente y en caso contrario reenviarlo a una autoridad competente.
- **Comprobación de que ese incidente aún no ha sido registrado:** es moneda corriente que más de un usuario notifique la misma incidencia y por lo tanto ha de evitarse duplicaciones innecesarias.
- **Asignación de referencia:** al incidente se le asignará una referencia que le identificará unívocamente tanto en los procesos internos como en las comunicaciones con el cliente.

- **Registro inicial:** se han de introducir en la base de datos asociada la información básica necesaria para el procesamiento del incidente (hora, descripción del incidente, sistemas afectados…).
- **Información de apoyo:** se incluirá cualquier información relevante para la resolución del incidente que puede ser solicitada al cliente a través de un formulario específico, o que pueda ser obtenida de la propia CMDB (hardware interrelacionado), etc.
- **Notificación del incidente:** en los casos en que el incidente pueda afectar a otros usuarios estos deben ser notificados para que conozcan como esta incidencia puede afectar su flujo habitual de trabajo (OSIATIS S.A., s.f.).

**Clasificación.-** es muy frecuente que cuncurran múltiples incidencias, por lo que es necesario fijar un nivel de prioridad para dar solución de las mismas.

El nivel de prioridad se basa en dos parámetros:

- **Impacto:** establece la importancia del incidente, dependiendo de cómo afecta a los procesos de negocio y del número de usuarios afectados.
- **Urgencia:** obedece al tiempo máximo que acepte el cliente para la resolución del incidente y/o el nivel de servicio acordado en el SLA (OSIATIS S.A., s.f.).

Además, se deben tomar en cuenta, factores auxiliares tales como el tiempo de resolución esperado y los recursos necesarios: los incidentes “sencillos” se tramitarán cuanto antes. Según la prioridad se asignarán los recursos necesarios para la resolución del incidente (OSIATIS S.A., s.f.).

La prioridad del incidente puede variar durante su ciclo de vida. Por ejemplo, se pueden encontrar soluciones temporales que restauren los niveles de servicio y que permitan retrasar el cierre del incidente sin graves repercusiones. Es conveniente establecer un protocolo para determinar, en primera instancia, la prioridad del incidente (OSIATIS S.A., s.f.).

La clasificación de un incidente tiene como objetivo principal recopilar toda la información que pueda ser utilizada para la resolución del mismo (OSIATIS S.A., s.f.).

El proceso de clasificación debe implementar, al menos, los siguientes pasos:

- **Categorización:** se fija una categoría (que puede estar a su vez subdividida en más niveles) tomando en cuenta el tipo de incidente o del grupo de trabajo responsable de su resolución. Se identifican los servicios afectados por el incidente.
- **Establecimiento del nivel de prioridad:** según el impacto y la urgencia se establece un nivel de prioridad tomando en cuenta criterios preestablecidos.
- **Asignación de recursos:** si el Centro de Servicios no da solución al incidente en primera instancia, delega al personal de soporte técnico responsable de su resolución (segundo nivel).
- **Monitorización del estado y tiempo de respuesta esperado:** se relaciona un estado al incidente (por ejemplo: registrado, activo, suspendido, resuelto, cerrado) y se estipula el tiempo de resolución del incidente en base al SLA correspondiente y a la prioridad (OSIATIS S.A., s.f.).

**Escalado y soporte.-** resulta habitual que el Centro de Servicios no resuelva en primera instancia un incidente y para ello, se deba acudir a un especialista o a algún superior que pueda decidir en aspectos que se escapan de su responsabilidad. A este proceso se le denomina escalado (OSIATIS S.A., s.f.).

En el caso de que no pueda resolverse un incidente en la primera línea de soporte dentro del tiempo acordado, se tendrá que acudir a un grupo de mayor experiencia o a una autoridad en la materia. Esto se conoce como escalado y puede tener lugar en cualquier momento y en cualquier nivel de soporte (grado) en el proceso de resolución (Kolthof *et al.,* 2012).

Básicamente hay dos tipos diferentes de escalado:

- **Escalado funcional:** significa involucrar más personal especializado o con privilegios de acceso (autoridad técnica) para solucionar el incidente. Con este tipo de escalado se pueden exceder los límites del departamento y eventualmente incluye a proveedores externos (Kolthof *et al.,* 2012).

  En el escalado funcional se demanda el apoyo de un experto de más alto nivel para resolver el problema (OSIATIS S.A., s.f.).

  OVERTI (c2011) es del criterio que en el escalado funcional se debe transferir un incidente, problema o cambio a un equipo técnico con mayor experiencia para ayudar en un escalado.

  Teniendo en cuenta las apreciaciones de Kolthof *et al.* (2012), se determina que el escalado funcional significa involucrar personal especializado o con privilegios de acceso (autoridad técnica) para solucionar el incidente.

- **Escalado jerárquico:** significa comprometer a niveles más altos de autoridad en la organización, cuando parece que el nivel actual de autoridad es insuficiente para asegurar que el incidente será resuelto en tiempo y satisfactoriamente (Kolthof *et al.,* 2012).

  Se deberá solicitar la ayuda de un responsable de mayor autoridad para tomar decisiones que se escapen de las responsabilidades asignadas a ese nivel, como, por ejemplo, asignar más recursos para la resolución de un incidente específico (OSIATIS S.A., s.f.).

  Las valoraciones de OVERTI (c2011) señalan que el escalado jerárquico es la información o involucración de niveles de gestión más elevados para ayudar en un escalado.

> Atendiendo las apreciaciones de Kolthof *et al.* (2012) se puede concluir que el escalado jerárquico significa comprometer a niveles más altos de autoridad en la organización, cuando el nivel actual de autoridad no asegura la resolución del incidente satisfactoriamente.

El Gestor de Incidentes, que es responsable del proceso de Gestión de Incidente, procurará hacer reserva de capacidad para atender el escalado funcional de un incidente para que no sea necesario el escalado jerárquico para resolver el incidente (Kolthof *et al.,* 2012).

**Análisis, resolución y cierre del incidente.-** en primera instancia, se evalúa el incidente con ayuda de la Base de Conocimientos, para establecer si se logra identificar con alguna incidencia ya resuelta y aplicar el procedimiento asignado (OSIATIS S.A., s.f.).

En caso, que la resolución del incidente se escape de las posibilidades del Centro de Servicios, éste redirecciona el mismo a un nivel superior para su indagación por los expertos asignados. Si estos expertos no resuelven el incidente, se seguirán los protocolos de escalado predeterminados (OSIATIS S.A., s.f.).

Cuando se haya dado solución al incidente se:

- Corrobora con los usuarios la solución satisfactoria del mismo.
- Agrega el proceso de resolución a la base de conocimientos.
- Reclasifica el incidente si fuera necesario.
- Actualiza la información en la CMDB (Base de datos de la gestión de configuraciones) sobre los elementos de configuración implicados en el incidente.
- Cierra el incidente (OSIATIS S.A., s.f.).

## 2.7. ANÁLISIS Y EVALUACIÓN DEL RIESGO DE LA INFORMACIÓN

El avance tecnológico ha traído consigo un reto mayor para quienes se dedican al combate de programas con características maliciosas, la difusión de nuevas técnicas y metodologías de ataques y amenazas informáticas cada vez más sofisticadas y eficaces. No es un secreto la cantidad de recursos que invierten las organizaciones para evitar intrusiones y manipulaciones que pongan en riesgo, desde la integridad de la data hasta las operaciones propias de la entidad (De Freitas, 2009).

Hoy en día, las organizaciones son más dependientes de sus redes informáticas y un problema que las afecte, por pequeño que sea, puede llegar a comprometer la continuidad de las operaciones, situación que inevitablemente se traduce en pérdida económica, retraso en las operaciones y crisis de confianza por parte de los usuarios. Si la empresa no conoce sobre el riesgo que corren sus activos de información, difícilmente llegará a estar preparada para evitar su posible ocurrencia, de allí la importancia de conocerlo y crear controles para disminuir o eliminar su posible ocurrencia (De Freitas, 2009).

Para Ramos (2002) la protección de los sistemas y de la información no elimina completamente el riesgo de que estos bienes sufran daños. Por lo tanto, los gestores deben instaurar medidas de seguridad que lleven los riesgos hasta niveles aceptables, contando para ello, con el coste de las medidas a establecer, con el valor de los bienes a proteger y con la cuantificación de las pérdidas que podrían generarse con la aparición de determinados incidentes de seguridad.

Dussan (2006) sostienen que el análisis y evaluación de riesgos permite a las compañías tener una visión más clara sobre sus vulnerabilidades y de los esfuerzos que deben hacer para mejorar.

### 2.7.1. METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN (MAGERIT)

El modelo MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas), es una guía para investigar los riesgos que soportan los sistemas de información y para establecer las medidas indicadas que deberían acogerse para controlar los riesgos. Permite un seguimiento exhaustivo de la seguridad del sistema ajustándose a criterios como los de ITSEC (Information Technology Security Evaluation Criteria) o Criterios Comunes de Evaluación de la Seguridad de los Productos y Sistemas de Información, que permitan la posterior homologación y certificación del sistema de información desde el punto de vista de la seguridad (Hernández *et al.,* 2013).

La razón de ser de Magerit está ligada con la generalización del uso de los medios electrónicos, informáticos y telemáticos, que presume beneficios evidentes para los usuarios; pero también, da lugar a riesgos que deben minimizarse con medidas de seguridad que generen confianza en el uso de tales medios (EAR/PILAR, s.f.).

**Valoración del modelo.-** este modelo posee guías técnicas, las cuales proporcionan las claves para comprender y seleccionar las técnicas más adecuadas para los procedimientos de análisis y gestión de riesgos, de seguridad de los sistemas de información. Este modelo garantiza un control eficiente de la información del proyecto ya que basa sus fortalezas en los riesgos referentes a la seguridad (Hernández *et al.,* 2013).

#### 2.7.1.1. MAGERIT VERSIÓN 3.0

Estimar el riesgo al que están expuestos los elementos de trabajo es, simplemente, imprescindible para gestionarlos y por ello, han aparecido multitud de guías informales, aproximaciones metódicas y herramientas de soporte, todas ellas, buscan objetivar el análisis para conocer cuán seguros (o inseguros) están. El gran reto de todas estas aproximaciones es la complejidad del problema al

que se exponen; complejidad en el sentido de que hay muchos elementos que considerar y que, si no se es riguroso, las conclusiones serán de poco fiar. Es por ello, que se busca una aproximación metódica que no de lugar a la improvisación, ni este en manos de la arbitrariedad del analista (EAR/PILAR, s.f.).

Pese a que se ha puesto en manos de los sistemas de información graves responsabilidades para cumplir los objetivos de las organizaciones, no deja de ser un tema recurrente la inquietud por su seguridad. Los afectados, que frecuentemente no son técnicos, se preguntan si estos sistemas merecen su confianza, confianza que se ve mermada por cada fallo y, sobre todo, cuando la inversión en defensa de los medios de trabajo no se traduce en la ausencia de fallos. Lo ideal es que los sistemas no fallen. Pero lo cierto es que se acepta convivir con sistemas que fallan. El asunto no es tanto la ausencia de incidentes como la confianza en que están bajo control: se sabe qué puede pasar y se sabe qué hacer cuando pasa. El temor a lo desconocido es el principal origen de la desconfianza y, en consecuencia, aquí se busca conocer para confiar: conocer los riesgos para poder afrontarlos y controlarlos (EAR/PILAR, s.f.).

Amutio (s.f.) hace referencia que la versión 3 de MAGERIT, mantiene en gran medida la estructura de la versión 2 y se ha actualizado para brindar una mejor alineación con la normativa ISO. Se busca integrar las tareas de análisis de riesgos en un marco organizacional de gestión de riesgos dirigido desde los órganos de gobierno.

MAGERIT versión 3 se ha estructurado en tres guías (Amutio, s.f.).

- **Método.-** se estructura de la siguiente forma:

  El capítulo 2 muestra conceptos informalmente. En específico, se enmarcan actividades de análisis y tratamiento en un proceso integral de gestión de riesgos.

El capítulo 3 delimita los pasos y precisa las actividades de análisis de los riesgos.

El capítulo 4 detalla opciones y criterios de tratamiento de los riesgos y establece las actividades de gestión de riesgos.

El capítulo 5 se enfoca en los proyectos de análisis de riesgos, proyectos en los que se ven sumergidos para efectuar el primer análisis de riesgos de un sistema y casualmente cuando existen cambios sustanciales y hay que restablecer el modelo ampliamente.

El capítulo 6 determina las acciones de los planes de seguridad, tambien denominados planes directores o planes estratégicos.

El capítulo 7 enfatiza el desarrollo de sistemas de información y la forma en que el análisis de riesgos sirve para gestionar la seguridad del producto final, desde su concepción inicial hasta su puesta en producción, así como a la defensa del propio proceso de desarrollo.

El capítulo 8 se anticipa a problemas que surgen recurrentemente cuando se efectúan análisis de riesgos.

- **Catálogo de elementos.-** establece pautas en cuanto a:

  - Tipos de activos
  - Dimensiones de valoración de los activos.
  - Criterios de valoración de los activos.
  - Amenazas típicas sobre los sistemas de información.
  - Salvaguardas a tomar en cuenta para proteger sistemas de información.

  Se persiguen dos objetivos:

  - Facilitar la tarea de las personas que acometen el proyecto, en el sentido de proporcionarles elementos estándar a los que logren

adscribirse rápidamente, centrándose en lo específico del sistema objeto del análisis.

- Homogeneizar los resultados de los análisis, iniciando una terminología y criterios uniformes, que permitan comparar e incluso integrar análisis realizados por diferentes equipos.

Cada sección incluye una notación XML que se usará para publicar regularmente los elementos en un formato estándar, capaz de ser procesado automáticamente por herramientas de análisis y gestión.

- **Guía de técnicas.-** orienta sobre algunas técnicas que se utilizan habitualmente para llevar a cabo proyectos de análisis y gestión de riesgos:

  Técnicas específicas para el análisis de riesgos:

  - ✓ Análisis mediante tablas
  - ✓ Análisis algorítmico
  - ✓ Árboles de ataque

  Técnicas generales

  - ✓ Técnicas gráficas
  - ✓ Sesiones de trabajo: entrevistas, reuniones y presentaciones
  - ✓ Valoración Delphi

## 2.8. TÉCNICAS PARA EL ANÁLISIS DE DATOS

Según Piattini *et al.,* (2008) para obtener evidencias se pueden emplear diferentes tipos de técnicas, procedimientos y herramientas, de los cuales destacan, el análisis de datos, ya que para las organizaciones el conjunto de datos o información son de vital importancia, por lo que resulta necesario verificarlos y comprobarlos; utilizando diversas técnicas para el análisis de datos.

### 2.8.1. CUESTIONARIOS

Cayssials (2006), aprecia que el cuestionario como técnica de recolección de datos, se presenta asociado a una metodología cuantitativa y propone una evaluación en un tiempo breve sin renunciar a dicha intensidad.

Además, establece que tanto la profundidad como la validez de los datos recogidos en un cuestionario, dependerán de los criterios adoptados para su elaboración, los cuales deben estipularse a partir de: a) un profundo conocimiento del tema a indagar y b) un no menos profundo conocimiento de las características de los sujetos, a los cuales esta destinado.

Se remiten cuestionarios preimpresos a personas concretas, sin que sea obligatorio que dichas personas sean responsables de las áreas a auditar. Estos cuestionarios, no pueden ni deben ser repetidos para instalaciones distintas, sino diferentes y muy específicos para cada situación, y muy cuidados en su fondo y su forma (Piattini *et al.,* 2008).

### 2.8.2. ENTREVISTAS

El auditor incia a relacionarse personalmente con el auditado. Lo hace de tres formas:

- Con la petición de documentación concreta sobre alguna materia de su responsabilidad.
- Mediante entrevistas, en las cuales no se sigue un plan establecido, ni un método estricto de sometimiento a un cuestionario.
- Por medio de entrevistas, en las que el auditor sigue un método preestablecido de antemano y busca finalidades concretas.

La entrevista es una de las actividades personales más importantes del auditor; en ellas, éste reúne mayor cantidad de información, y mejor matizada, que la proporcionada por medios propios puramente técnicos o por respuestas escritas a cuestionarios (Piattini *et al.,* 2008).

### 2.8.3. CHECKLIST

Los Check Lists corresponden al tipo de cuestionarios, que pueden llegar a explicar cómo ocurren los hechos pero no por qué ocurren. El cuestionario debe estar subordinado a la regla, a la norma y al método (Piattini *et al.,* 2008).

Según Cuello *et al.,* (2002) se hacen todas las preguntas que sean necesarias o imaginables, con el fin de reconocer el máximo de información sobre el objeto o problema planteado. De esa manera, se llega a quebrantar su propia naturaleza, combinándolo de todas las formas posibles, aumentándolo, disminuyéndolo, transformándolo, adaptándolo, entre otros.

El profesionalismo para utilizar las checklist, pasa por un procesamiento interno de información, con el fin de obtener respuestas coherentes que permitan una correcta descripción de puntos débiles y fuertes. El profesionalismo pasa por poseer preguntas muy estudiadas que han de formularse flexiblemente. Salvo excepciones, las Checklists deben ser contestadas oralmente, ya que superan en riqueza y generalización a cualquier otra forma (Piattini *et al.,* 2008).

### 2.8.4. MATRIZ DE RIESGO

Una matriz de riesgo es considerada com una herramienta de control y de gestión, regularmente empleada para identificar las actividades (procesos y productos) más importantes de una institución, el tipo y nivel de riesgos inherentes a estas actividades y los factores exógenos y endógenos que engendran estos riesgos (factores de riesgo). De la misma forma, una matriz de riesgo permite evaluar la efectividad de una correcta gestión y administración de los riesgos financieros, operativos y estratégicos que impactan la misión de la organización (Piattini *et al.,* 2008).

## 2.9. GLPI

GLPI de origen francés (Gestionnaire Libre de Parc Informatique, que en español significa: Administrador Libre de Equipos de Cómputo) es una solución de

software abierto, que proporciona no solamente la gestión del inventario informático, sino que además, se encarga del soporte técnico (Help Desk). Es una aplicación web que administra las solicitudes vía software y permite el seguimiento de las peticiones del usuario con un número de ticket (Ochoa, s.f.).

Sus principales funcionalidades son:

- Gestión de recursos informáticos
- Gestión de licencias de software
- Gestión de consumibles
- Base de conocimientos
- Gestión de reservas
- Soporte Técnico
- Automatización de inventario

La aplicación está escrita en PHP y requiere de un servidor Apache con soporte para PHP4 como mínomo, aunque es recomendable PHP5, así como una base de datos de MySQL 4.1.2 (Ochoa, s.f.).

Esta herramienta puede ser instalada tanto en servidores Windows como Linux, siendo de fácil instalación y manejo , lo cual la hace un instrumento eficaz y útil para toda organización (Ochoa, s.f.).

Mediante el uso de GLPI se gestionará y controlará los riesgos que atentan contra la seguridad de la información, ya que se podrá tener un mayor y mejor control del recurso informático de la institución, atendiendo ademas, a los distintos requerimientos de los usuarios, solucionando los inconvenientes de manera eficaz y eficiente.

# CAPÍTULO III. DESARROLLO METODOLÓGICO

El presente trabajo de investigación realizado en cada uno de los departamentos y carreras de la ESPAM – MFL, en la ciudad de Calceta del cantón Bolívar, tuvo la duración de doce meses. Para el inicio del plan de gestión de incidentes que afectan a los equipos informáticos, fue necesario solicitar la autorización de inicio (**Anexo 1**) al rector de la universidad, el Ingeniero Leonardo Félix López. El oficio de autorización, destacaba el objetivo del plan de gestión de incidentes, el personal implicado, las áreas que se iban a abarcar y el tiempo estimado, consiguiendo así el permiso requerido.

## 3.1. METODOLOGÍA ITIL – GESTIÓN DE INCIDENTES

Para el desarrollo del trabajo, se utilizó la metodología ITIL, tomando como referencia el apartado gestión de incidentes, la cual establecía conceptos básicos, procesos y actividades sobre la gestión de incidentes, con el objetivo de restaurar el servicio tan pronto como sea posible y minimizar los impactos adversos de las interrupciones generadas. Esta metodología comprendía los siguientes procesos: registro, clasificación, diagnóstico y resolución, mediante los cuales, las autoras ejecutaron el trabajo de investigación.

El uso de ésta metodología permitió incorporar las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la presente investigación y el esquema gubernamental de la seguridad de la información (EGSI) Versión 1.0, el cual establece en su apartado 9, el procedimiento mediante el cual se gestionan los incidentes de seguridad de la información.

### 3.1.1. REGISTRO

Con el fin de determinar los equipos informáticos con los que contaba la ESPAM-MFL, se consideró elaborar una definición de tales equipos, en base a la información proporcionada por el jefe de almacén (**Anexo 2**), quien corroboró

con el sistema de contabilidad, la clase de registro contable utilizada para administrar este tipo de bienes, lo cual ayudó a elaborar la descripción.

Por consiguiente, una parte fundamental para la recopilación de la información, estuvo basada en diseñar una ficha de registro, con el propósito de reconocer y detallar los equipos informáticos con los que contaban los departamentos y carreras de la ESPAM – MFL (**Anexo 3),** la cual fue dirigida a los custodios de los equipos informáticos de cada carrera y departamento de la universidad, la misma inició el 12 de septiembre y culminó el 30 de octubre de 2014, permitiendo determinar el número de equipos informáticos disponibles en la institución.

Posteriormente, mediante las visitas realizadas a las instalaciones de la universidad para la recopilación de los datos, se obtuvo información general de las actividades y procesos que manejan cada uno de los departamentos y carreras de la institución, lo cual permitió evaluar el medio en el que se desarrollan cada una de las actividades, logrando identificar los riesgos a los que están expuestos cada uno de los equipos, para proceder a evaluarlos con el fin de que reciban una especial atención.

#### 3.1.1.1. METODOLOGÍA MAGERIT

La Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT-versión 3.0) permitió identificar los riesgos, su origen y posible impacto. Para lo cual, se procedió a elaborar un listado de posibles amenazas sobre cada equipo informático según lo establece MAGERIT en su catálogo de elementos correspondiente al tercer libro.

**Amenazas a las que estan expuestos los equipos informáticos:**

- **Desastres naturales (N)**

**N.1** Fuego (Incendios).
**N.2** Daños por Agua (Inundaciones).
**N*** Desastres Naturales (Otros incidentes que se producen sin intervención humana).

- **De origen industrial (I)**

**I.1** Fuego (Incendios).
**I.2** Daños por Agua (Escape, fugas, inundaciones).
**I*** Desastres Industriales (Otros desastres debido a la actividad humana).
**I.3** Contaminación Mecánica (Vibraciones, polvo, suciedad).
**I.4** Contaminación Electromagnética (interferencias de radios, campos magnéticos, luz ultravioleta,…).
**I.5** Avería De Origen Físico O Lógico (Fallos en los equipos o fallos en los programas).
**I.6** Corte De Suministro Eléctrico (Cese de la alimentación de potencia).
**I.7** Condiciones Inadecuadas De Temperatura O Humedad (Climatización).
**I.8** Fallo De Servícios De Comunicaciones (Destrucción o detención física).
**I.11** Emanaciones Electromagnéticas (Fuga de información).

- **Errores y fallos no intencionados (E)**

**E.2** Errores del Administrador.
**E.9** Errores de [re-] Encaminamiento (Ruta incorrecta de envío).
**E.23** Errores de mantenimiento/ Actualización de equipos hardware.
**E.24** Caída del Sistema por Agotamiento de Recursos.
**E.25** Pérdida de Equipos.

- **Ataques intencionados (A)**

**A.5** Suplantación de la identidad del usuario.
**A.6** Abuso de privilegios de acceso.
**A.7** Uso no previsto.
**A.11** Acceso no autorizado.
**A.12** Análisis de tráfico (Monitorización de tráfico).
**A.23** Manipulación de los equipos (Alteración intencionada del funcionamiento de los programas).
**A.24** Denegación de servicio (Saturación del sistema informático).
**A.25** Robo.
**A.26** Ataque destructivo.

Tomando como referencia la clasificación de las amenazas, se procedió a realizar una matriz de riesgo por cada uno de los servicios que se ofrecen en la institución, determinando los desastres a los cuales están expuestos los equipos informáticos. A continuación se detallan los servicios institucionales tomados en cuenta para el análisis de riesgos:

- Secretaria de carreras
- Secretaría general
- Sala de gocentes
- Laboratorios
- Centro de datos
- Departamento de tecnología
- Unidad de Producción de Software (UPS)
- Aulas de clase
- Coordinación de Investigación Científica
- Biblioteca
- Coordinación de emprendimiento
- Dirección de planificación, diseño e ingeniería
- Postgrado
- Talento humano
- Acreditación
- Jefatura de almacén
- Vicerrectorado de extensión y bienestar politécnico
- Vinculación
- FEPAM
- Coordinación de cultura
- Dirección administrativa y financiera
- Tesorería
- Rectorado
- Jurídico
- Audiovisuales
- Control de acceso

Seguidamente, se realizó el análisis mediante tablas, estableciendo así, la probabilidad y el impacto que se generaría si un evento llegara a suceder, tomando en cuenta el precio de los activos y la importancia que tienen dentro de la institución, además, según lo establece la metodología aplicada para el análisis de riesgos, se determinó la frecuencia con la que pueden suceder tales eventos. La siguiente tabla muestra las escalas que permitieron evaluar la probabilidad de ocurrencia el impacto y la frecuencia:

| PROBABILIDAD | | |
|---|---|---|
| **ABREVIATURA** | **DESCRIPCIÓN** | **PORCENTAJE** |
| **MA:** | Practicamente Seguro | 81% - 100% |
| **A:** | Probable | 61% - 80% |
| **M:** | Posible | 41% - 60% |
| **B:** | Poco Probable | 21% - 40% |
| **MB:** | Muy Bajo | 0% - 20% |

**Cuadro 3.1.** Escalas de probabilidad de ocurrencia

| IMPACTO | | |
|---|---|---|
| **ABREVIATURA** | **DESCRIPCIÓN** | **PORCENTAJE** |
| **MA:** | Muy Alto | 81% - 100% |
| **A:** | Alto | 61% - 80% |
| **M:** | Medio | 41% - 60% |
| **B:** | Bajo | 21% - 40% |
| **MB:** | Muy Bajo | 0% - 20% |

**Cuadro 3.2.** Escalas de impacto

| FRECUENCIA | | | |
|---|---|---|---|
| **ABREVIATURA** | **PUNTUACIÓN** | **DESCRIPCIÓN** | **FRECUENCIA** |
| **MA:** | 100 | Muy Frecuente | Diario |
| **A:** | 10 | Frecuente | Mensual |
| **M:** | 1 | Normal | Semestral |
| **B:** | 1/10 | Poco Frecuente | Anual |
| **MB:** | 1/100 | Muy Poco Frecuente | Mas de un año |

**Cuadro 3.3**. Escalas de frecuencia

A continuación, se procedió a realizar el cálculo del riesgo, para lo cual, se multiplicó la probabilidad de cada amenaza por la magnitud del daño (Impacto) al que están expuestos los equipos, tomando valores y condiciones

respectivamente, consiguiendo así, modelar probabilidad, impacto y frecuencia en cada una de las matrices de riesgo.

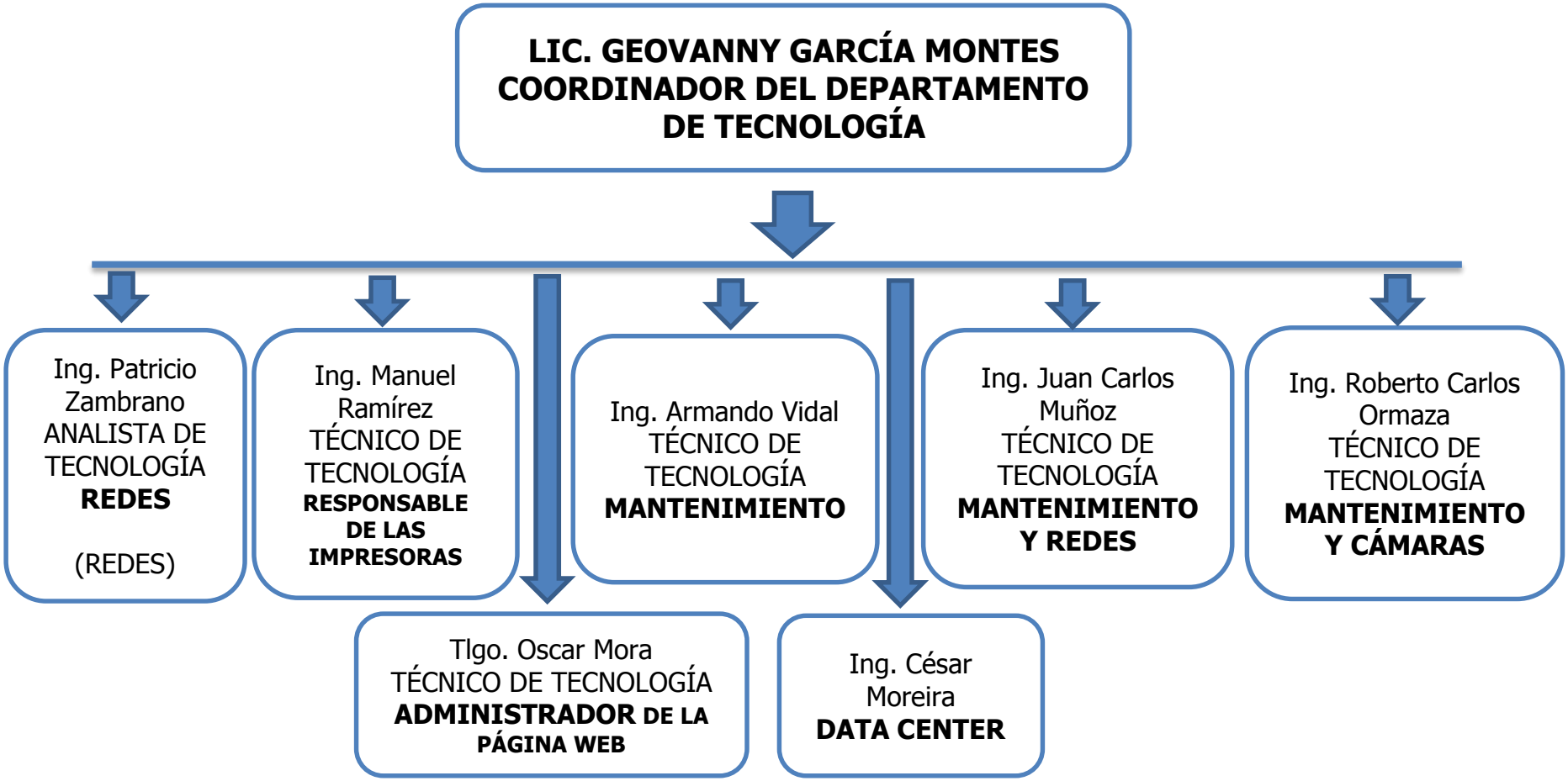
Una vez calculado el riesgo, se elaboró un cuestionario (**Anexo 4**), detallando cada una de las posibles incidencias que se podrían presentar. Consecuentemente, se le aplicaron las preguntas a 26 departamentos de la universidad, la misma que se llevó a efecto del 12 al 15 de mayo de 2015. El cuestionario contenía el objetivo, el área o departamento a evaluar, las incidencias encontradas y el tiempo promedio de solución. Además, se incluyó, el registro de la persona que notifica el incidente, a quién se le comunica y los efectos que se derivan en caso de que ocurra.

Después de obtener la información referente a los principales incidentes informáticos que suceden en la institución, se realizó un análisis estadístico, el mismo que detalla los resultados alcanzados. En este aspecto, se pudo observar cuales eran los inconvenientes mas relevantes, cuales afectaban considerablemente a la organización e impedían efectuar normalmente las actividades diarias.

### 3.1.2. CLASIFICACIÓN DE LOS INCIDENTES INFORMÁTICOS

Analizados los hallazgos de los cuestionarios aplicados al personal de la institución, las autoras de la presente investigación visitaron el departamento de tecnología de la ESPAM-MFL, con el fin de efectuar una entrevista no estructurada con el coordinador el Licenciado Geovanny García Montes, solicitándole información referente al departamento que dirige. En respuesta a lo requerido, se obtuvo el manual de funciones y responsabilidades del departamento de tecnología, el cual guio a las autoras en la elaboración de la estructura general del deparamento.

**Gráfico 3.1** Organigrama de funciones del Departamento de Tecnología



Consecutivamente se establecieron niveles de prioridad por cada una de las incidencias informáticas, formando criterios para determinar el impacto y urgencia. Para tal fin, se adoptaron las observaciones de Nacipucha (2013) quien define patrones para estipular la importancia de los incidentes informáticos, tal como se muestra a continuación:

| **URGENCIA** | **IMPACTO** | | | |
|---|---|---|---|---|
| | **Crítico** | **Alto** | **Medio** | **Bajo** |
| **Crítica** | **Crítica** | Crítica | Alta | Media |
| **Alta** | Crítica | **Alta** | Media | Media |
| **Media** | Alta | Media | **Media** | Baja |
| **Baja** | Media | Media | Baja | **Baja** |

**Cuadro 3.4** Definición de prioridades de la Gestion de Incidentes

| **PRIORIDAD** | **DEFINICIÓN** |
|---|---|
| **CRÍTICA** | Problemas que afectan críticamente a la institución y que traen consecuencias muy severas como son: los desastres naturales, de origen industrial y humano, deperfectos de hardware y los inconvenientes con la red; teniendo un impacto directo e inmediato con el usuario. |
| **ALTA** | Inconvenientes que afectan directamente las aplicaciones que se manejan en la organización y también las que tienen relación con hardware y software, que afectan indirectamente al usuario. |
| **MEDIA** | Incidentes que no son sensibles al tiempo y que esta involucrados con la actualización de aplicaciones, licenciamiento de las mismas, inconvenientes con suministros de computadoras e impresoras y el mantenimiento respectivo a los equipos informáticos. |
| **BAJA** | Un problema que afecta procesos o procedimientos que no tienen mayor impacto en la capacidad de los usuarios para realizar sus operaciones normales y existe una alternativa disponible. |

**Cuadro 3.5** Velocidad para responder a un incidente

Es así, que para fijar el impacto que se tendría si llegara a suceder alguna de las incidencias informáticas encontradas en la investigación, se establecieron los respectivos niveles, basándose en las apreciaciones de Nacipucha (2013), los mismos que se muestran de la siguiente manera:

| IMPACTO | DESCRIPCIÓN |
|---|---|
| **CRÍTICO** (Departamento/ Unidad afectada/s) | Indisponiblidad de servicio/s que afectan significativamente a unos o más departamentos o unidades de trabajo. |
| **ALTO** (Grupos o áreas afectadas) | Indisponiblidad de servicio/s que afectan a determinadas funciones o a un grupo de usuarios. |
| **MEDIO** (Indisponibilidad parcial de un servicio) | Un usuario afectado Indisponibilidad parcial de un servicio/s para un grupo de personas. |
| **BAJO** | Actividades planificadas Requerimientos de servicios negociados con el usuario. |

**Cuadro 3.6** Descripción del impacto

Parte fundamental del proceso de resolución es escalar el incidente, para lo cual se desarrolló el respectivo escalado jerárquico que permitirá la asignación de funcionario (s) que atiendan el mismo. El incidente se escala en primera línea al funcionario en turno, seguidamente al jefe inmediato quien comunica al coordinador del departamento de tecnología para que lo registre y asigne al personal necesario para atender la incidencia, en caso que el analista o técnico no pueda resolver el incidente, se debe solicitar soporte al proveedor del equipo o sistema afectado.

Para constatar la notificación y la atención respectiva al incidente, el departamento que presenta el inconveniente, deberá elaborar un oficio en el que se comunique y describa lo que realizó el técnico encargado. En este aspecto y para llevar un mejor control de los incidentes informáticos que se presentan a diario, las autoras elaboraron una ficha de registro de incidentes (**Anexo 5**), en la cual se detalla el numero de incidencias que se notifican, el nombre del departamento, la fecha y hora de registro, la fecha y hora de solución, el técnico

encargado, el tipo de incidencia, la descripción y la firma del coordinador del departamento de tecnología.

### 3.1.3. DIAGNÓSTICO Y RESOLUCIÓN

#### 3.1.3.1. METODOLOGÍA ITIL – GESTIÓN DE SERVICIOS

Mediante la información obtenida y luego de estar al tanto de los procesos que se llevan a cabo, las autoras procedieron a elaborar un catálago basándose en la metodologia ITIL y su apartado gestión de servicios, enfocandose en alinear los servicios de tecnologías de la información y que correspondan con las necesidades de la institución, de esta manera se clasificó y expuso los requerimientos que presentan los mismos.

El catálogo de servicios, permitió elaborar los acuerdos para establecer compromisos con las autoridades de la ESPAM – MFL, el coordinador y los empleados del departamento de tecnología, de manera tal, que los incidentes se resuelvan en el menor tiempo posible, con el recurso necesario y se evite interrupción en las actividades normales de la universidad .

De esta forma, se desarrolló el respectivo SLA (Acuerdos de Nivel de Servicios), el mismo que incorpora datos generales del departamento, su misión, visión y objetivos. Asi también, se establecieron horarios de atención, los servicios disponibles, los responsables de resolver cada una de las incidencias, el tiempo de respuesta y solución, y su respectivo escalado.

Además, el SLA presenta la estructura del departamento de tecnología, la misma que se encuentra dividida en: área de soporte técnico y capacitación; programa de mantenimiento preventivo y correctivo y áreas de hardware, sistemas y redes. Del mismo modo, el acuerdo incorpora el proceso que lleva resolver los incidentes informáticos, la seguridad de los servicios tanto en el aspecto lógico como físico y la recuperación de desastres; culminando con la finalización del acuerdo y la aprobación de la máxima autoridad de la universidad la Econ. Miriam Félix López y el coordinador del departamento de tecnología.

Finalmente se elaboró el plan de respuesta a incidentes informáticos (**Anexo 6**), basado en las buenas prácticas de ITIL para gestionar los incidentes de seguridad informática, el mismo que establece actividades que se deben tomar en cuenta al momento de brindar un servicio y de esta forma controlar y agilizar el proceso de resolución de los incidentes que se presentan de manera cotidiana en la institución.

# CAPÍTULO IV. RESULTADOS Y DISCUSIÓN

## 4.1. RESULTADOS

En este apartado, se describen los resultados obtenidos en cada una de las fases del plan de gestión de incidentes que afectan a los equipos informáticos.

### 4.1.1. REGISTRO

Para determinar los equipos informáticos que existían en la institución, fue necesario establecer, en primera instancia la definición de dichos equipos, mediante la cual, se procedería a registrar cada uno de ellos. Para tal efecto, se adoptó el Anexo 1 del Acuerdo No. 166 de la Secretaría Nacional de la Administración Pública del Ecuador denominado Esquema Gubernamental de la Seguridad de la Información (EGSI) Versión 1.0, el cual, en su tercer apartado referente a la gestión de activos, indica como inventariar los activos de soporte de hardware, obteniendo como resultado la siguiente definición:

**Equipos Informáticos .-** Representan bienes materiales y físicos que se utilizan en las operaciones regulares de la organización, soportando directa o indirectamente los servicios que se prestan.

Los equipos informáticos sujetos a revisión en la presente investigación son:

**Periféricos de entrada:**

- Teclado
- Mouse
- Scanners

**Periféricos de salida:**

- Proyector
- Monitor
- Pantalla LCD
- Impresoras

**Periféricos de almacenamiento:**

- CPU
- DVR
- Storage

**Equipos de comunicación de la red de datos:**

- Routers Inalámbricos
- Switch
- Access Point

**Equipos Fijos:**

- Portátiles
- Servidores
- Computadoras Todo en uno

**Tableros de Transferencia**

- UPS

**Sistemas de Acceso**

- Biométricos

Mediante la definición obtenida se elaboró una ficha de registro, la cual permitió desarrollar un inventario para detallar cada uno de los equipos. Los siguientes diagramas, muestran los resultados alcanzados mediante la aplicación de las encuestas, las mismas que fueron dirigidas a los responsables de los equipos informáticos de cada departamento y carreras de la institución.

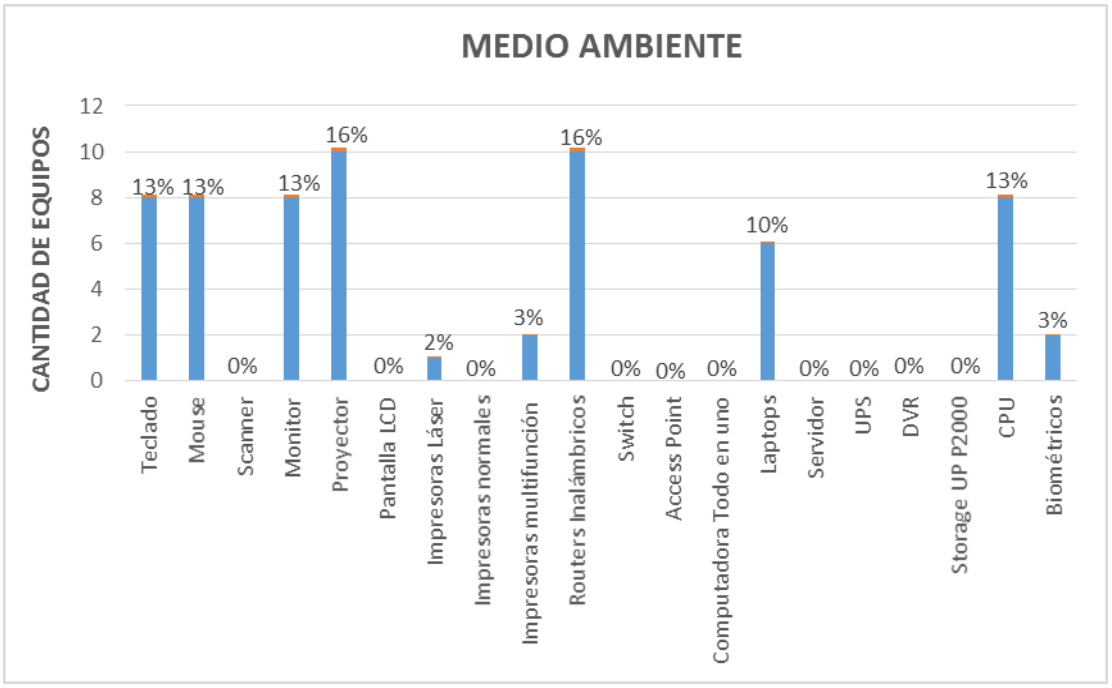



**Gráfico 4.1.** Porcentaje de equipos informáticos en la carrera de medio ambiente de la ESPAM - MFL

La carrera de agroindustrias y las áreas que la conforman como son: los laboratorios del CAI, talleres de procesos cárnicos, talleres de frutas y vegetales, taller de procesos lácteos y las oficinas.

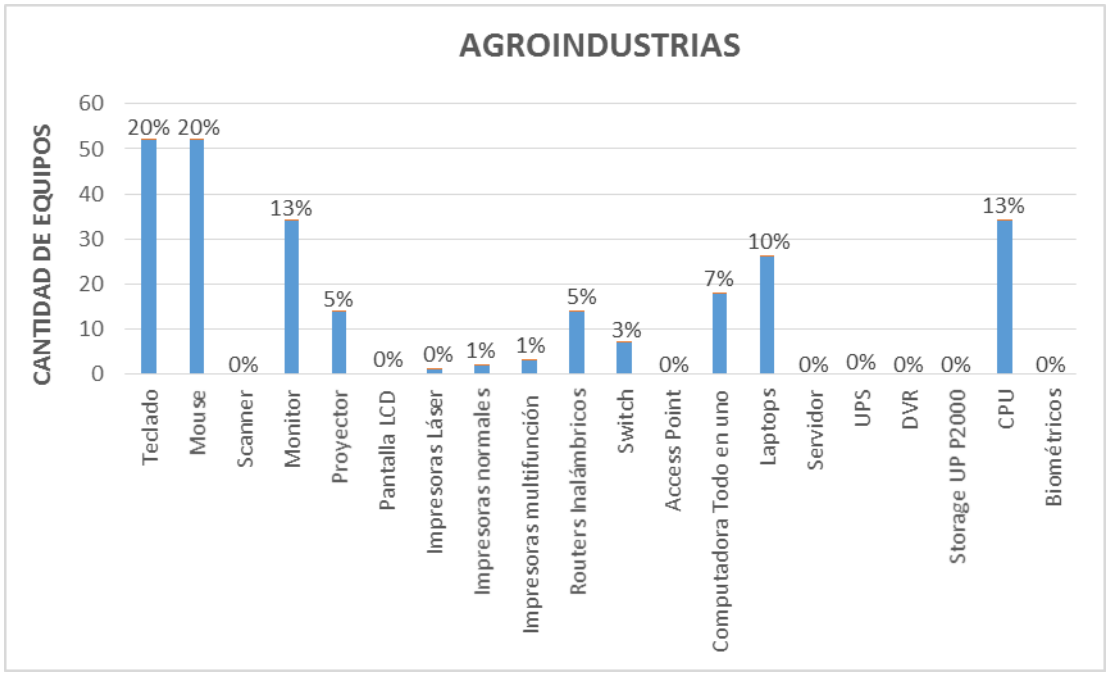



**Gráfico 4.2.** Porcentaje de equipos informáticos en la carrera de agroindustrias de la ESPAM - MFL

La carrera de pecuaria y cada uno de sus departamentos, los cuales incluyen la clínica veterinaria, la unidad de hato bobino, y los laboratorios de química, microbiología, biología Molecular, computación y la incubadora.

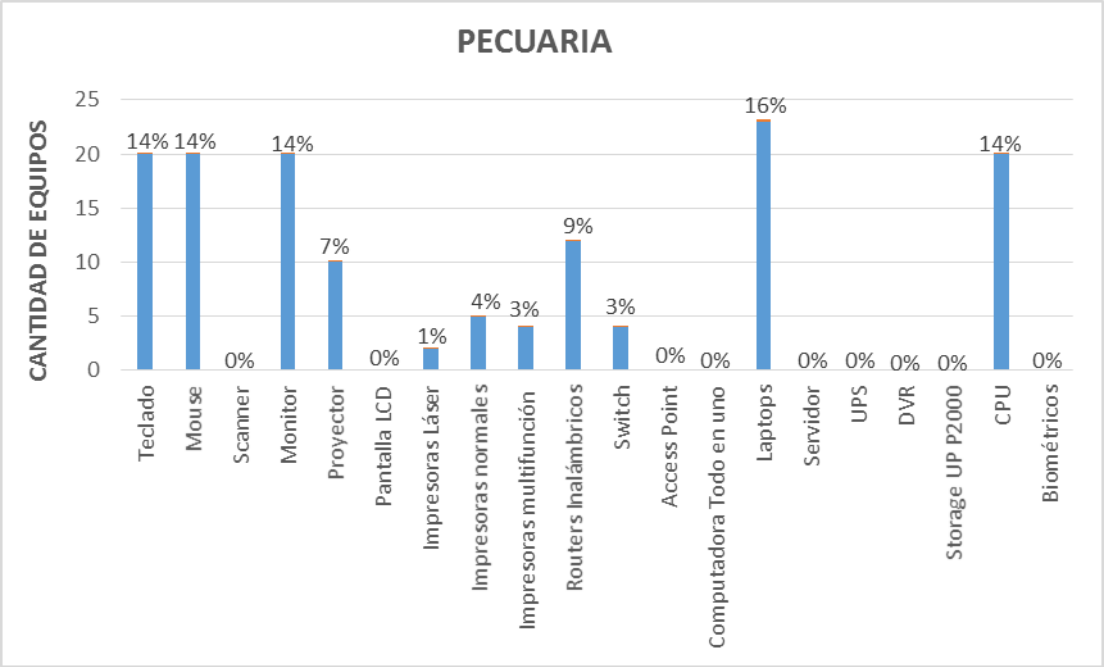



**Gráfico 4.3**. Porcentaje de equipos informáticos en la carrera de pecuaria de la ESPAM – MFL

La Carrera de agrícola y cada uno de sus departamentos, los cuales incluyen los laboratorios de suelo y biotecnología vegetal, así como también, los cubículos, sala de profesores y dirección de carrera.

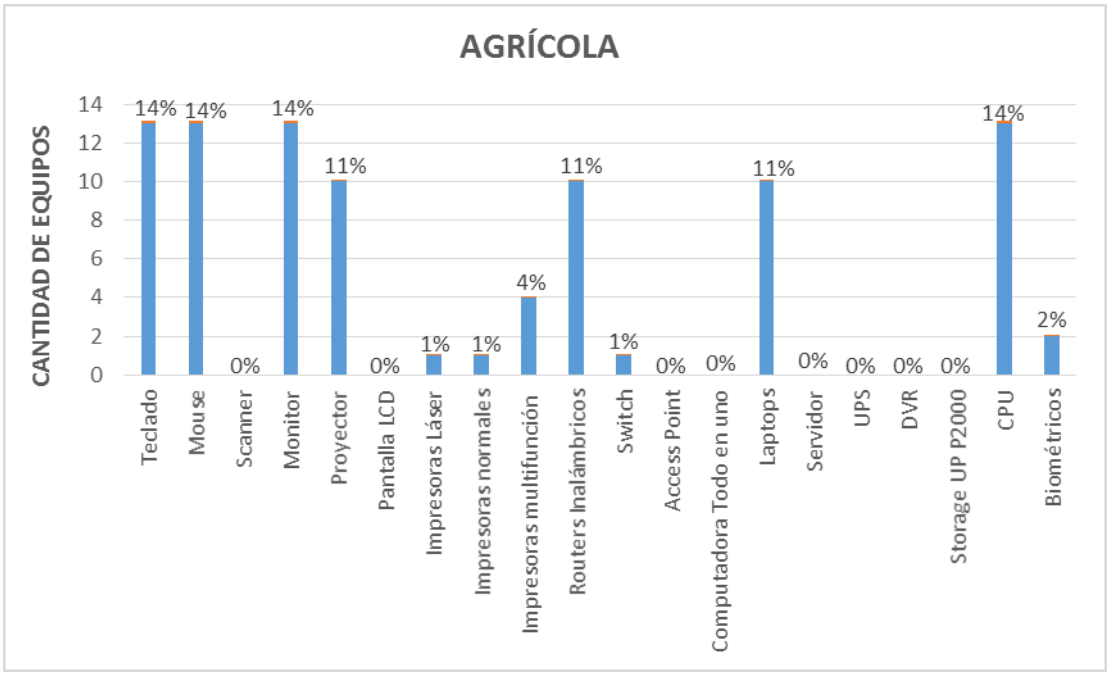



**Gráfico 4.4**. Porcentaje de equipos informáticos en la carrera de agrícola de la ESPAM – MFL

La Carrera de Turismo con cada uno de sus departamentos como son: El hotel Higuerón, cubículos de profesores y dirección de carrera.

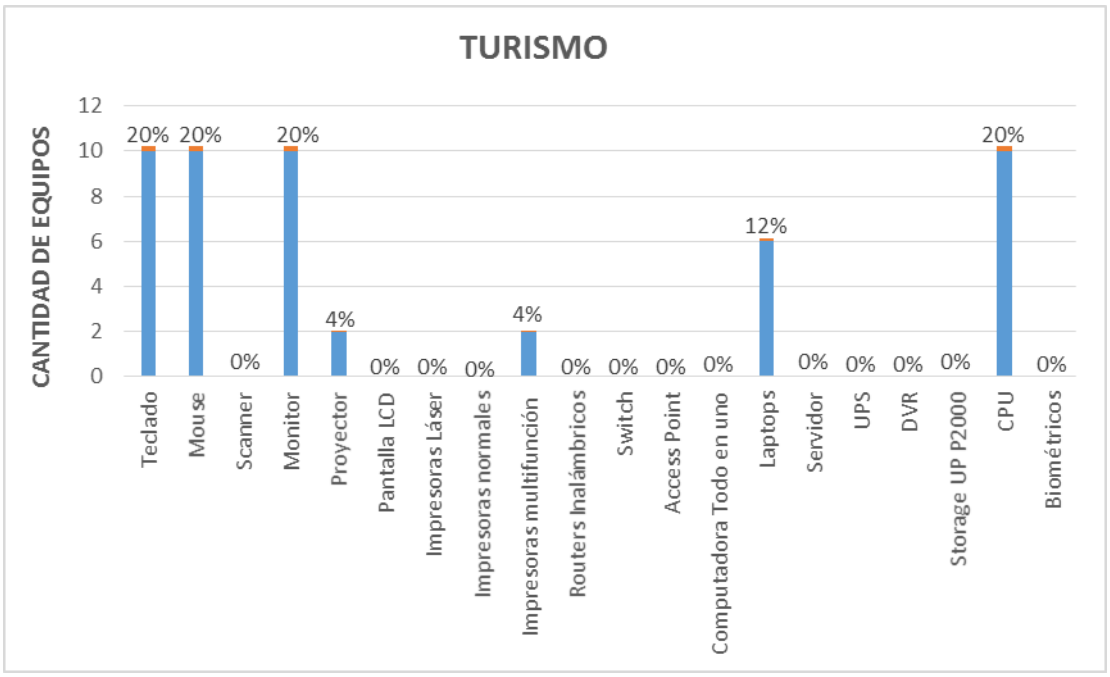



**Gráfico 4.5.** Porcentaje de equipos informáticos en la carrera de turismo de la ESPAM – MFL

La carrera de informatica con cada uno de sus departamentos y oficinas como son: secretaria, cubículos y sala de profesores, la Unidad de Produccion de

Software (UPS); se incluyen además los laboratorios de electronica, redes, diseño gráfico, lenguaje y programación y sistemas multimedia. Adicionalmente el Centros de Aplicaciones Informaticas (CAI) que labora en las instalaciones de la misma.

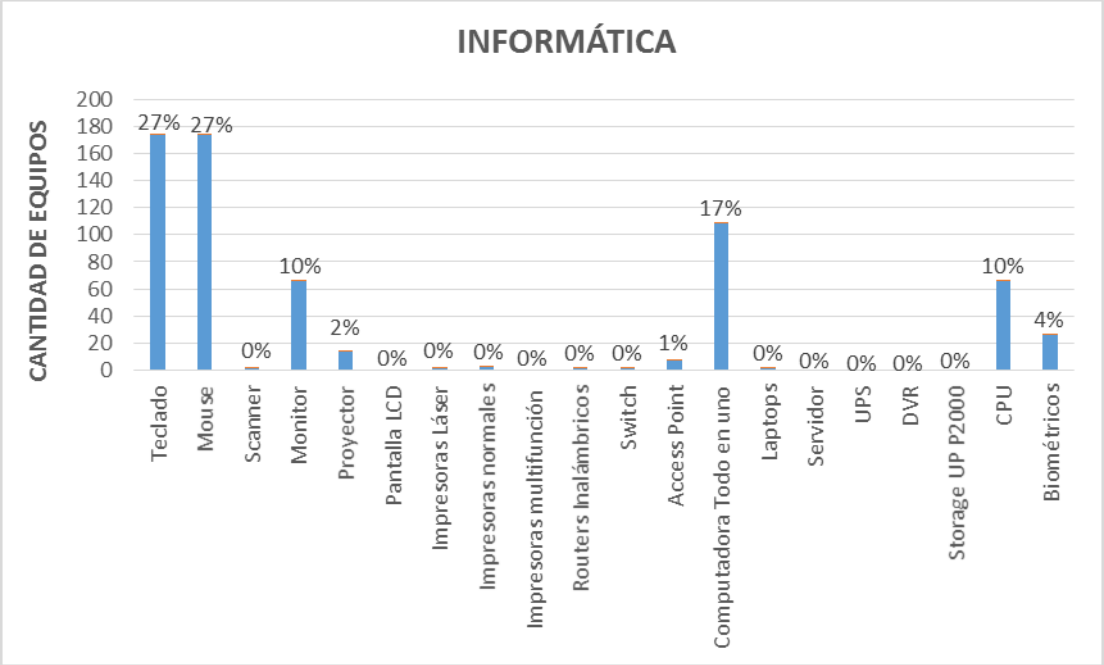



**Gráfico 4.6.** Porcentaje de equipos informáticos en la carrera de informática de la ESPAM – MFL

La carrera de administración con cada uno de sus departamentos que incluyen los cubículos, sala de profesores, aulas de clases y oficinas de dirección de carrera.

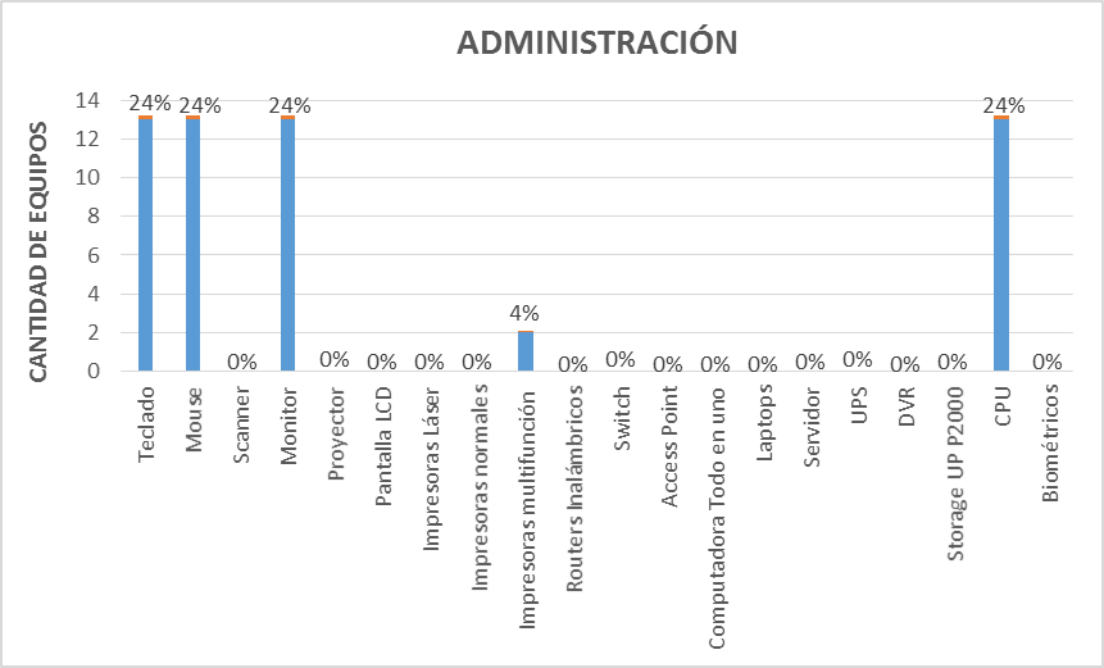



**Gráfico 4.7.** Porcentaje de equipos informáticos en la carrera de administración de la ESPAM – MFL

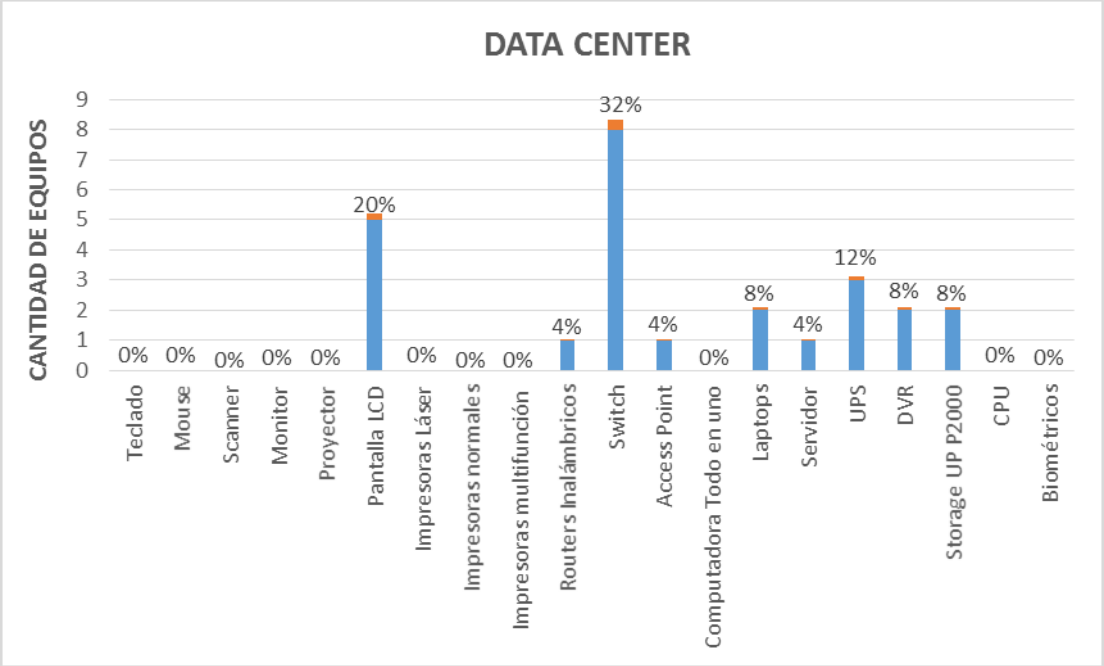



**Gráfico 4.8.** Porcentaje de equipos informáticos en el Data Center de la ESPAM – MFL

El área de cultura, a la cual le corresponden los siguientes departamentos: instituto de idiomas, secretaria general, coordinación de investigación científica, biblioteca, coordinación de emprendimiento, dirección de planificación, diseño e ingeniería, postgrado y talento humano.

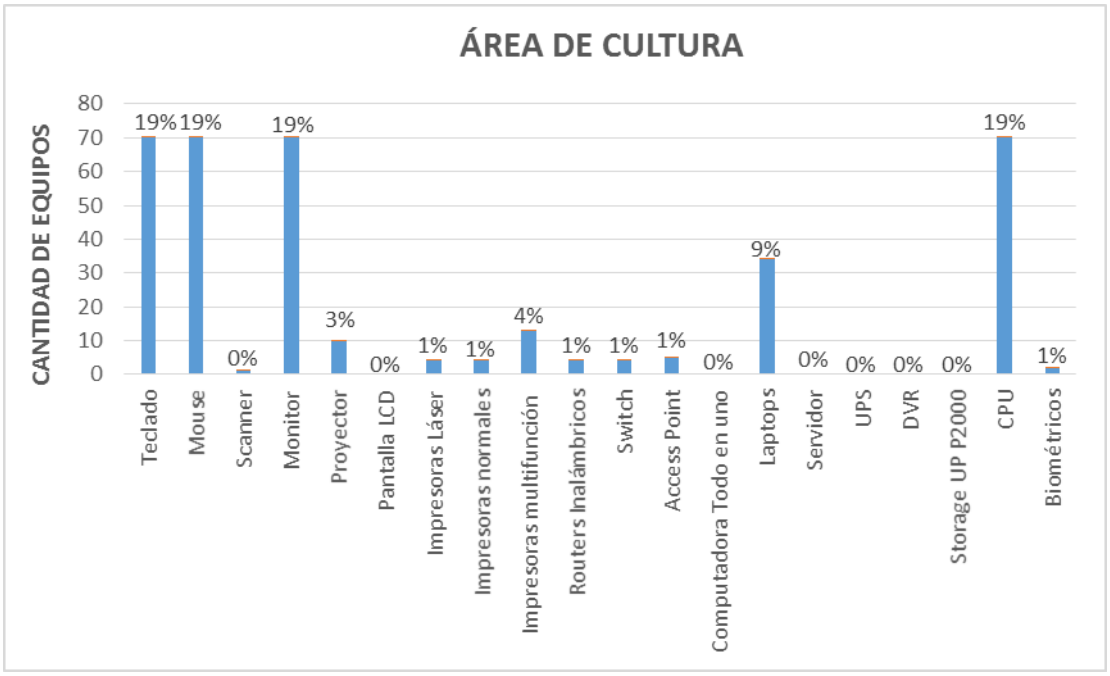



**Gráfico 4.9.** Porcentaje de equipos informáticos en el área de cultura de la ESPAM – MFL

El área de bienestar politécnico con sus departamentos tales como: mantenimiento, cuarto de equipos, coordinación académica, nivelación y admisión, departamento de cómputo, jefatura de almacén, secretaria, vicerrectorado de extensión y bienestar politécnico, vinculación, FEPAM, coordinación de mantenimiento y coordinación de cultura.

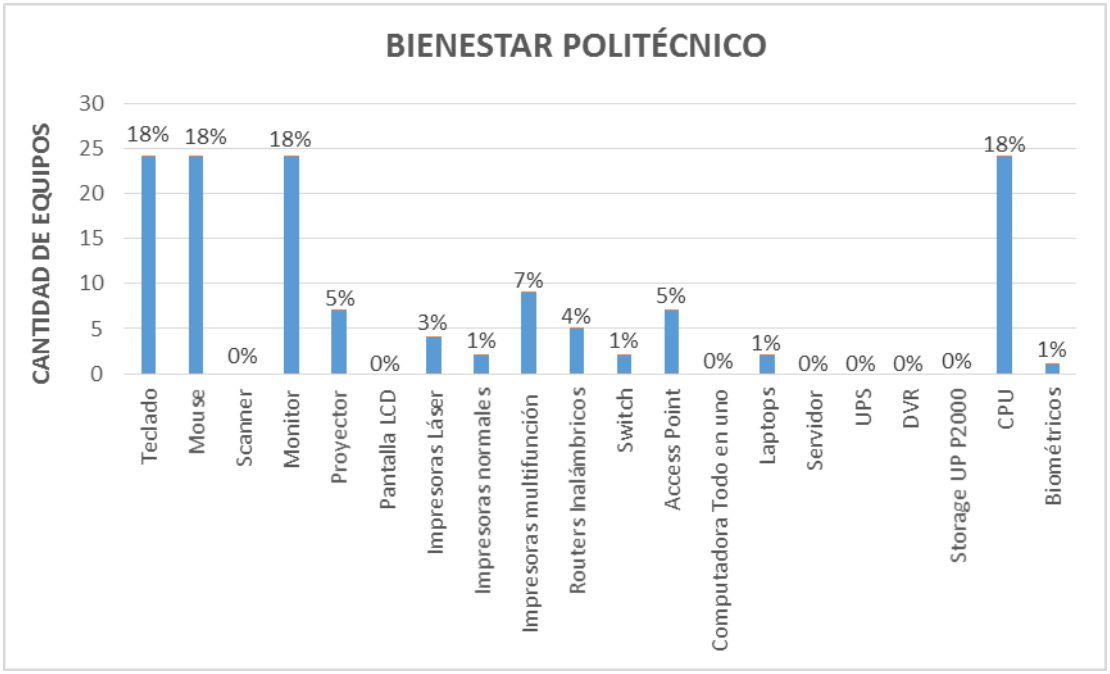



**Gráfico 4.10.** Porcentaje de equipos informáticos en el área de bienestar politécnico de la ESPAM – MFL

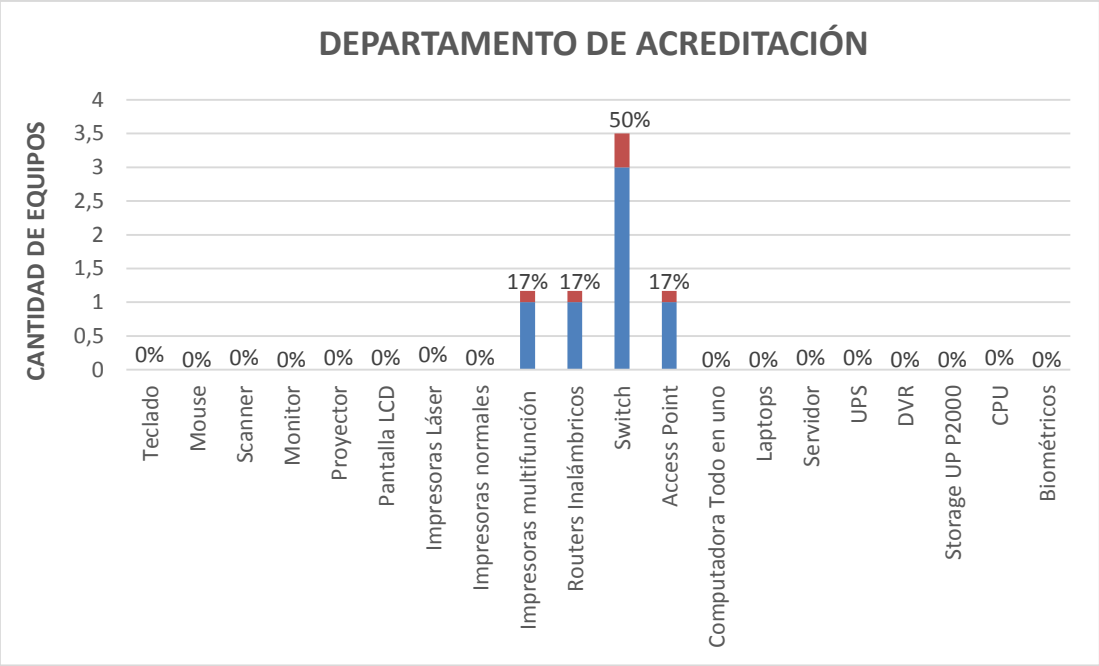



**Gráfico 4.11.** Porcentaje de equipos informáticos del departamento de acreditación de la ESPAM – MFL

El edificio de la institución ubicado en el centro de la ciudad de Calceta, al cual le corresponden las oficinas: recepción, secretaria general, dirección administrativa y financiera, presupuesto, tesorería, contabilidad, rectorado, jurídico, sala de sesiones y el departamento de cómputo.

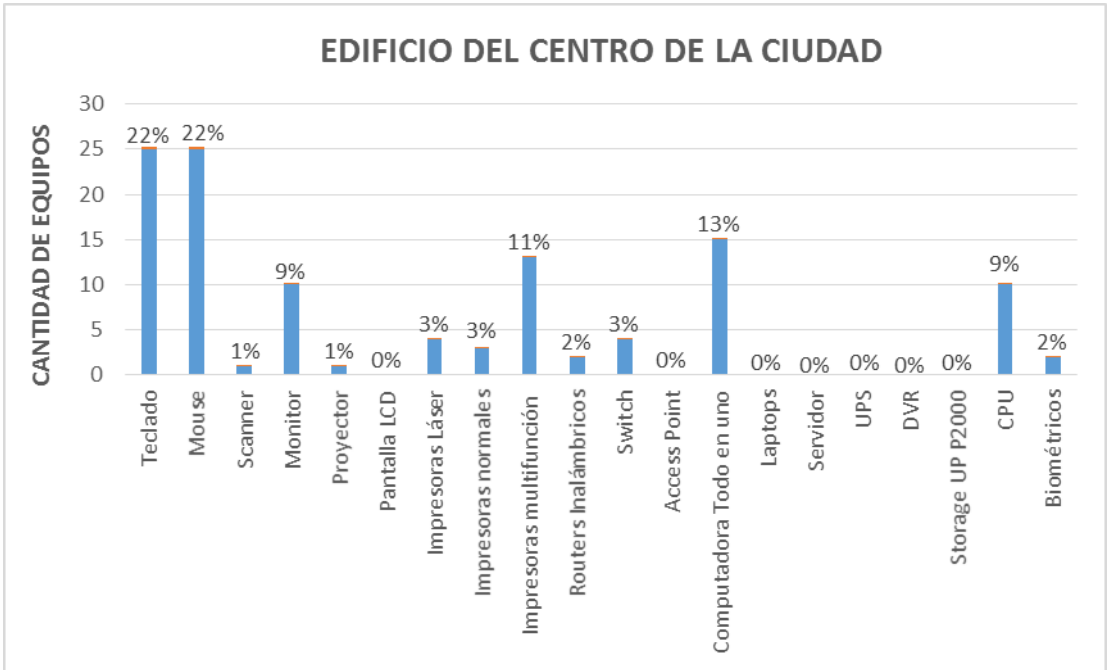



**Gráfico 4.12.** Porcentaje de equipos informáticos de las oficinas del centro de la Ciudad

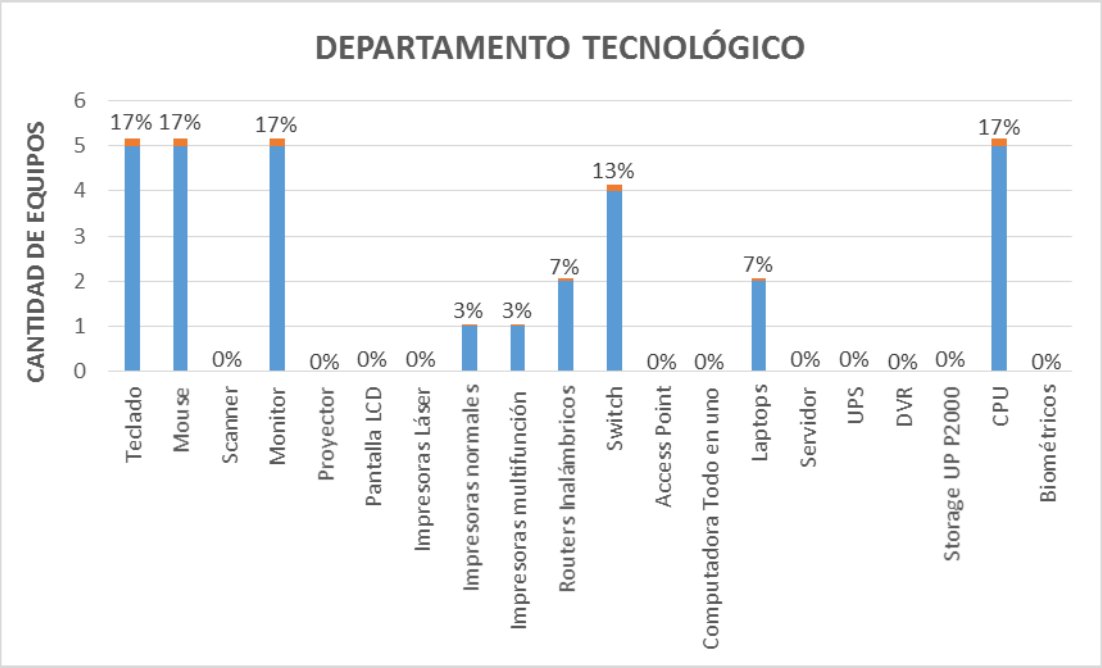



**Gráfico 4.13.** Porcentaje de equipos informáticos del departamento de tecnologia de la ESPAM – MFL

La ESPAM – MFL cuenta con aproximadamente 1969 equipos informáticos, según la encuesta realizada a los custodios de las carreras y departamentos, desde el 12 de septiembre hasta el 30 de octubre de 2014.

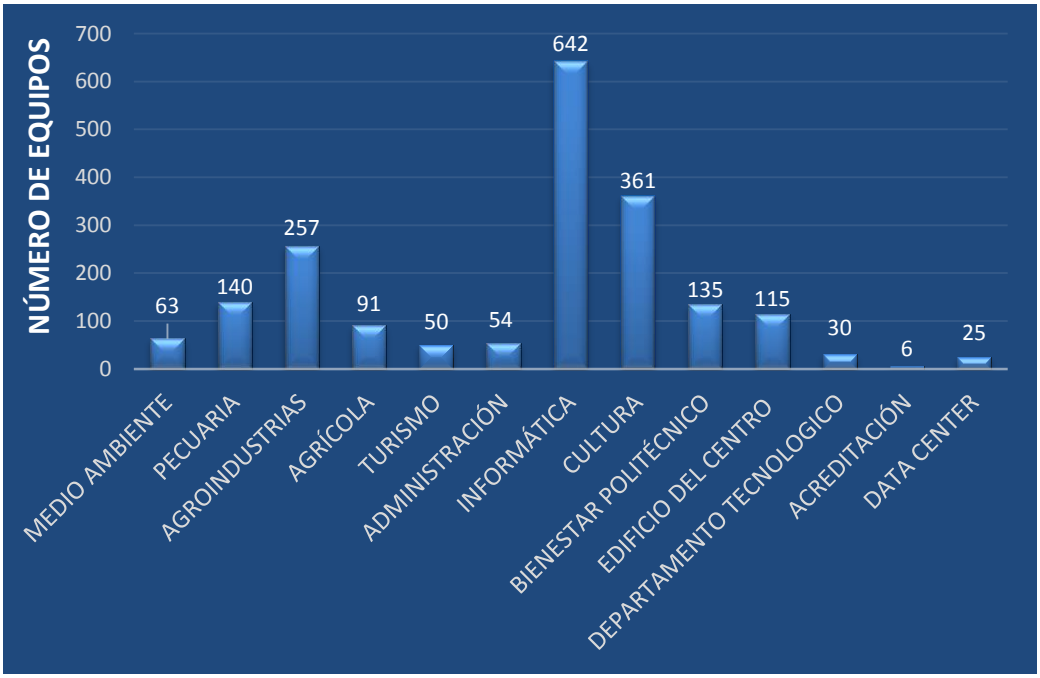



**Gráfico 4.14**. Total de equipos informáticos de la ESPAM – MFL

#### 4.1.1.1. METODOLOGÍA MAGERIT

Obtenida la tabulación de las encuestas, se procedió a realizar la clasificación de las amenazas, tal como lo establece la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT-versión 3.0) en su catálogo de elementos.

Identificadas las causas que provocan incidentes en los equipos informáticos, se continuó determinando de forma cuantitativa la probabilidad, el impacto y la frecuencia de ocurrencia de cada amenaza, para lo cual fue necesario realizar una matriz de riesgo por cada servicio que se brinda en la institución, lo que permitió estimar el riesgo de que ocurra tal evento.

**Cuadro 4.1** Servicio: secretaria

| AMENAZAS | CPU | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | DAÑO EN EL DISCO DURO | | | | | DAÑO EN LA FUENTE DE PODER | | | | |
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,90 | 1/100 | Muy Poco frecuente | **0,09** | 0,10 | 0,83 | 1/100 | Muy Poco frecuente | **0,08** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,75 | 1/10 | Poco frecuente | **0,12** | 0,16 | 0,75 | 1/10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,60 | 1/10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 1/10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,90 | 1/100 | Muy Poco frecuente | **0,09** | 0,10 | 0,90 | 1/100 | Muy Poco frecuente | **0,09** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,18 | 0,75 | 1/10 | Poco frecuente | **0,14** | 0,18 | 0,75 | 1/10 | Poco frecuente | **0,14** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,20 | 0,70 | 1/10 | Poco frecuente | **0,14** | 0,20 | 0,70 | 1/10 | Poco frecuente | **0,14** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,25 | 0,55 | 1 | Normal | **0,14** | 0,35 | 0,80 | 1 | Normal | **0,28** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,30 | 0,60 | 1 | Normal | **0,18** | 0,45 | 0,75 | 1 | Normal | **0,34** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,45 | 0,90 | 1 | Normal | **0,41** | 0,45 | 0,90 | 1 | Normal | **0,41** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,50 | 0,80 | 10 | Frecuente | **0,40** | 0,50 | 0,90 | 10 | Frecuente | **0,45** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,10 | 0,45 | 1/10 | Poco frecuente | **0,05** | 0,10 | 0,45 | 1/10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,60 | 1 | Normal | **0,07** | 0,12 | 0,60 | 1 | Normal | **0,07** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | 0,50 | 0,95 | 1 | Normal | **0,48** | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | 0,05 | 0,60 | 1 | Normal | **0,03** | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | 0,05 | 0,60 | 1 | Normal | **0,03** | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,25 | 0,80 | 1 | Normal | **0,20** | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | 0,60 | 0,65 | 10 | Frecuente | **0,39** | | | | | |
| **E.25** Pérdida de equipos | 0,45 | 0,80 | 1/10 | Poco frecuente | **0,36** | 0,45 | 0,80 | 1/10 | Poco frecuente | **0,36** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | 0,05 | 0,80 | 1/10 | Poco frecuente | **0,04** | | | | | |
| **A.6** Abuso de Privilegios de Acceso | 0,05 | 0,50 | 1/10 | Poco frecuente | **0,03** | | | | | |
| **A.7** Uso no previsto | 0,05 | 0,40 | 1/10 | Poco frecuente | **0,02** | | | | | |
| **A.11** Acceso no Autorizado | 0,10 | 0,80 | 1/10 | Poco frecuente | **0,08** | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | 0,15 | 0,76 | 1/10 | Poco frecuente | **0,11** | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | 0,05 | 0,83 | 1/10 | Poco frecuente | **0,04** | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | 0,35 | 0,75 | 1 | Normal | **0,26** | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,05 | 0,80 | 1/10 | Poco frecuente | **0,04** | 0,05 | 0,80 | 1/10 | Poco frecuente | **0,04** |
| **A.26** Ataque destructivo | 0,05 | 0,90 | 1/10 | Poco frecuente | **0,05** | 0,05 | 0,90 | 1/10 | Poco frecuente | **0,05** |

| AMENAZAS | CPU | | | | | MONITOR | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | DAÑO EN LA MEMORIA RAM | | | | | | | | | |
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,90 | 1/100 | Muy Poco frecuente | **0,09** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,65 | 1/10 | Poco frecuente | **0,10** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,60 | 1/10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,1 | 0,90 | 1/100 | Muy Poco frecuente | **0,09** | 0,10 | 0,90 | 1/100 | Muy Poco frecuente | **0,09** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,18 | 0,75 | 1/10 | Poco frecuente | **0,14** | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,18 | 0,70 | 1/10 | Poco frecuente | **0,13** | 0,15 | 0,70 | 0,10 | Poco frecuente | **0,11** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,40 | 0,75 | 1 | Normal | **0,30** | 0,08 | 0,45 | 1/10 | Poco frecuente | **0,04** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,30 | 0,60 | 1 | Normal | **0,18** | 0,15 | 0,75 | 1/10 | Poco frecuente | **0,11** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,45 | 0,90 | 1 | Normal | **0,41** | 0,45 | 0,82 | 1 | Normal | **0,37** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,50 | 0,73 | 10 | Frecuente | **0,37** | 0,40 | 0,90 | 10 | Frecuente | **0,36** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,10 | 0,45 | 1/10 | Poco frecuente | **0,05** | 0,10 | 0,45 | 1/10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,60 | 1 | Normal | **0,07** | 0,12 | 0,75 | 1 | Normal | **0,09** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | | | | | | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | | | | | | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | | | | | | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | | | | | | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | | | | | | | | | | |
| **E.25** Pérdida de equipos | 0,45 | 0,80 | 1/10 | Poco frecuente | **0,36** | 0,25 | 0,90 | 1/10 | Poco frecuente | **0,23** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | | | | | | | | | | |
| **A.6** Abuso de Privilegios de Acceso | | | | | | | | | | |
| **A.7** Uso no previsto | | | | | | | | | | |
| **A.11** Acceso no Autorizado | | | | | | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | | | | | | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | | | | | | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | | | | | | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,05 | 0,80 | 1/10 | Poco frecuente | **0,04** | 0,05 | 0,90 | 1/10 | Poco frecuente | **0,05** |
| **A.26** Ataque destructivo | 0,05 | 0,90 | 1/10 | Poco frecuente | **0,05** | 0,05 | 0,90 | 1/10 | Poco frecuente | **0,05** |

| AMENAZAS | SCANNER | | | | | IMPRESORA | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,85 | 1/100 | Muy Poco frecuente | **0,09** | 0,10 | 0,90 | 1/100 | Muy Poco frecuente | **0,09** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,6 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,85 | 1/100 | Muy Poco frecuente | **0,09** | 0,1 | 0,85 | 1/100 | Muy Poco frecuente | **0,09** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,15 | 0,7 | 0,10 | Poco frecuente | **0,11** | 0,15 | 0,70 | 0,10 | Poco frecuente | **0,11** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,25 | 0,75 | 1 | Normal | **0,19** | 0,48 | 0,75 | 10 | Frecuente | **0,36** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** | 0,23 | 0,70 | 1 | Normal | **0,16** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,45 | 0,85 | 1 | Normal | **0,38** | 0,35 | 0,76 | 1 | Normal | **0,27** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,40 | 0,90 | 10 | Frecuente | **0,36** | 0,45 | 0,85 | 10 | Frecuente | **0,38** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 1/10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,75 | 1 | Normal | **0,09** | 0,12 | 0,80 | 1 | Normal | **0,10** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | | | | | | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | | | | | | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | | | | | | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,12 | 0,75 | 1 | Normal | **0,09** | 0,12 | 0,75 | 1 | Normal | **0,09** |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | | | | | | | | | | |
| **E.25** Pérdida de equipos | 0,45 | 0,83 | 1/10 | Poco frecuente | **0,37** | 0,23 | 0,83 | 1/10 | Poco frecuente | **0,19** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | | | | | | | | | | |
| **A.6** Abuso de Privilegios de Acceso | | | | | | | | | | |
| **A.7** Uso no previsto | | | | | | | | | | |
| **A.11** Acceso no Autorizado | | | | | | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | | | | | | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | | | | | | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | | | | | | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,10 | 0,90 | 1/10 | Poco frecuente | **0,09** | 0,07 | 0,90 | 1/10 | Poco frecuente | **0,06** |
| **A.26** Ataque destructivo | 0,05 | 0,90 | 1/10 | Poco frecuente | **0,05** | 0,05 | 0,75 | 1/10 | Poco frecuente | **0,04** |

| AMENAZAS | MOUSE | | | | | TECLADO | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,65 | 1/100 | Muy Poco frecuente | **0,07** | 0,10 | 0,70 | 1/100 | Muy Poco frecuente | **0,07** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,68 | 0,10 | Poco frecuente | **0,11** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,65 | 1/100 | Muy Poco frecuente | **0,07** | 0,10 | 0,70 | 1/100 | Muy Poco frecuente | **0,07** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,16 | 0,68 | 0,10 | Poco frecuente | **0,11** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,10 | 0,50 | 1 | Normal | **0,05** | 0,10 | 0,54 | 1 | Normal | **0,05** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,15 | 0,58 | 1/10 | Poco frecuente | **0,09** | 0,15 | 0,58 | 1/10 | Poco frecuente | **0,09** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,35 | 0,72 | 1 | Normal | **0,25** | 0,35 | 0,76 | 1 | Normal | **0,27** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,70 | 10 | Frecuente | **0,25** | 0,35 | 0,75 | 10 | Frecuente | **0,26** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 1/10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 1/10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,75 | 1 | Normal | **0,09** | 0,12 | 0,80 | 1 | Normal | **0,10** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | | | | | | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | | | | | | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | | | | | | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | | | | | | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | | | | | | | | | | |
| **E.25** Pérdida de equipos | 0,15 | 0,75 | 1/10 | Poco frecuente | **0,11** | 0,15 | 0,80 | 1/10 | Poco frecuente | **0,12** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | | | | | | | | | | |
| **A.6** Abuso de Privilegios de Acceso | | | | | | | | | | |
| **A.7** Uso no previsto | | | | | | | | | | |
| **A.11** Acceso no Autorizado | | | | | | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | | | | | | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | | | | | | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | | | | | | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,07 | 0,65 | 1/10 | Poco frecuente | **0,05** | 0,07 | 0,75 | 1/10 | Poco frecuente | **0,05** |
| **A.26** Ataque destructivo | 0,05 | 0,60 | 1/10 | Poco frecuente | **0,03** | 0,05 | 0,65 | 1/10 | Poco frecuente | **0,03** |

| AMENAZAS | PORTÁTILES | | | | | COMPUTADORAS TODO EN UNO | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,90 | 1/100 | Muy Poco frecuente | **0,09** | 0,10 | 0,90 | 1/100 | Muy Poco frecuente | **0,09** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,88 | 0,10 | Poco frecuente | **0,14** | 0,16 | 0,88 | 0,10 | Poco frecuente | **0,14** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,75 | 0,10 | Poco frecuente | **0,09** | 0,12 | 0,75 | 0,10 | Poco frecuente | **0,09** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,90 | 1/100 | Muy Poco frecuente | **0,09** | 0,10 | 0,90 | 1/100 | Muy Poco frecuente | **0,09** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,16 | 0,88 | 0,10 | Poco frecuente | **0,14** | 0,16 | 0,88 | 0,10 | Poco frecuente | **0,14** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,75 | 0,10 | Poco frecuente | **0,09** | 0,12 | 0,75 | 0,10 | Poco frecuente | **0,09** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,30 | 0,79 | 10 | Frecuente | **0,24** | 0,30 | 0,79 | 10,00 | Frecuente | **0,24** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,15 | 0,58 | 1/10 | Poco frecuente | **0,09** | 0,15 | 0,58 | 1/10 | Poco frecuente | **0,09** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,45 | 0,80 | 1 | Normal | **0,36** | 0,45 | 0,80 | 1 | Normal | **0,36** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,80 | 1 | Normal | **0,28** | 0,35 | 0,80 | 1 | Normal | **0,28** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 1/10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 1/10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,85 | 1 | Normal | **0,10** | 0,12 | 0,85 | 1 | Normal | **0,10** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | 0,12 | 0,88 | 1 | Normal | **0,11** | 0,12 | 0,88 | 1 | Normal | **0,11** |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | 0,08 | 0,60 | 1/10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 1/10 | Poco frecuente | **0,05** |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | | | | | | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,15 | 0,80 | 1/10 | Poco frecuente | **0,12** | 0,15 | 0,80 | 1/10 | Poco frecuente | **0,12** |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | 0,22 | 0,68 | 10 | Frecuente | **0,15** | 0,22 | 0,68 | 10 | Frecuente | **0,15** |
| **E.25** Pérdida de equipos | 0,15 | 0,90 | 1/10 | Poco frecuente | **0,14** | 0,15 | 0,90 | 1/10 | Poco frecuente | **0,14** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | 0,15 | 0,45 | 1/10 | Poco frecuente | **0,07** | 0,15 | 0,45 | 1/10 | Poco frecuente | **0,07** |
| **A.6** Abuso de Privilegios de Acceso | 0,15 | 0,45 | 1/10 | Poco frecuente | **0,07** | 0,15 | 0,45 | 1/10 | Poco frecuente | **0,07** |
| **A.7** Uso no previsto | | | | | | | | | | |
| **A.11** Acceso no Autorizado | | | | | | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | 0,15 | 0,90 | 1/10 | Poco frecuente | **0,14** | 0,15 | 0,90 | 1/10 | Poco frecuente | **0,14** |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | 0,15 | 0,78 | 1/10 | Poco frecuente | **0,12** | 0,15 | 0,78 | 1/10 | Poco frecuente | **0,12** |
| **A.24** Denegación de servicio (Saturación del sistema informático) | 0,15 | 0,72 | 10 | Frecuente | **0,11** | 0,15 | 0,72 | 10 | Frecuente | **0,11** |
| **A.25** Robo (Pérdida de Equipos) | 0,07 | 0,90 | 1/10 | Poco frecuente | **0,06** | 0,07 | 0,90 | 1/10 | Poco frecuente | **0,06** |
| **A.26** Ataque destructivo | 0,05 | 0,65 | 1/10 | Poco frecuente | **0,03** | 0,05 | 0,65 | 1/10 | Poco frecuente | **0,03** |

| AMENAZAS | ROUTERS INALAMBRICOS | | | | | BIOMÉTRICOS | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** | 0,12 | 0,65 | 0,10 | Poco Frecuente | **0,08** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** | 0,15 | 0,75 | 0,10 | Poco Frecuente | **0,11** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** | 0,12 | 0,65 | 0,10 | Poco Frecuente | **0,08** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,15 | 0,60 | 1/10 | Poco frecuente | **0,09** | 0,06 | 0,45 | 1/10 | Poco Frecuente | **0,03** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,30 | 0,75 | 1 | Normal | **0,23** | 0,10 | 0,75 | 1 | Normal | **0,08** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,27 | 0,70 | 1/10 | Poco frecuente | **0,19** | 0,35 | 0,85 | 1 | Normal | **0,30** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,80 | 1 | Normal | **0,28** | 0,35 | 0,75 | 1 | Normal | **0,26** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 1/10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 1/10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,75 | 1 | Normal | **0,09** | 0,35 | 0,78 | 1 | Normal | **0,27** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | 0,12 | 0,88 | 1 | Normal | **0,11** | 0,12 | 0,88 | 1 | Normal | **0,11** |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | 0,08 | 0,60 | 1/10 | Poco frecuente | **0,05** | 0,08 | 0,72 | 1/10 | Poco frecuente | **0,06** |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | 0,10 | 0,62 | 1/10 | Poco frecuente | **0,06** | 0,10 | 0,62 | 1/10 | Poco frecuente | **0,06** |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,15 | 0,65 | 1/10 | Poco frecuente | **0,10** | 0,15 | 0,65 | 1/10 | Poco frecuente | **0,10** |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | 0,22 | 0,68 | 10 | Frecuente | **0,15** | 0,22 | 0,68 | 10 | Frecuente | **0,15** |
| **E.25** Pérdida de equipos | 0,15 | 0,90 | 1/10 | Poco frecuente | **0,14** | 0,15 | 0,80 | 1 | Normal | **0,12** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | 0,15 | 0,65 | 1/10 | Poco frecuente | **0,10** | 0,15 | 0,75 | 1 | Normal | **0,11** |
| **A.6** Abuso de Privilegios de Acceso | 0,15 | 0,45 | 1/10 | Poco frecuente | **0,07** | 0,15 | 0,85 | 1 | Normal | **0,13** |
| **A.7** Uso no previsto | 0,18 | 0,60 | 1/10 | Poco frecuente | **0,11** | 0,18 | 0,60 | 1/10 | Poco frecuente | **0,11** |
| **A.11** Acceso no Autorizado | 0,2 | 0,60 | 1 | Normal | **0,12** | 0,2 | 0,80 | 1 | Normal | **0,16** |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | 0,15 | 0,90 | 1 | Normal | **0,14** | 0,14 | 0,87 | 1 | Normal | **0,12** |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | 0,15 | 0,78 | 1/10 | Poco frecuente | **0,12** | 0,14 | 0,66 | 1 | Normal | **0,09** |
| **A.24** Denegación de servicio (Saturación del sistema informático) | 0,15 | 0,72 | 10 | Frecuente | **0,11** | 0,22 | 0,85 | 1 | Normal | **0,19** |
| **A.25** Robo (Pérdida de Equipos) | 0,07 | 0,90 | 1/10 | Poco frecuente | **0,06** | 0,15 | 0,75 | 1/10 | Poco Frecuente | **0,11** |
| **A.26** Ataque destructivo | 0,05 | 0,65 | 1/10 | Poco frecuente | **0,03** | 0,15 | 0,75 | 1/10 | Poco Frecuente | **0,11** |

**Cuadro 4.2.** Servicio: centro de datos

| AMENAZAS | CPU | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | DAÑO EN EL DISCO DURO | | | | | DAÑO EN LA FUENTE DE PODER | | | | |
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,86 | 0,10 | Poco Frecuente | **0,09** | 0,12 | 0,86 | 0,10 | Poco Frecuente | **0,10** |
| **N.2** Daños por agua (Inundaciones) | 0,15 | 0,84 | 0,10 | Poco Frecuente | **0,13** | 0,12 | 0,8 | 0,10 | Poco Frecuente | **0,10** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,6 | 1/100 | Muy Poco Frecuente | **0,07** | 0,12 | 0,63 | 1/100 | Muy Poco Frecuente | **0,08** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,22 | 0,86 | 0,10 | Poco Frecuente | **0,19** | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,20 | 0,84 | 0,10 | Poco Frecuente | **0,17** | 0,12 | 0,8 | 0,10 | Poco Frecuente | **0,10** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,18 | 0,6 | 1/100 | Muy Poco Frecuente | **0,11** | 0,12 | 0,63 | 1/100 | Muy Poco Frecuente | **0,08** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,18 | 0,45 | 1 | Normal | **0,08** | 0,30 | 0,70 | 1/10 | Poco Frecuente | **0,21** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,12 | 0,55 | 1/10 | Poco Frecuente | **0,07** | 0,12 | 0,6 | 1/10 | Poco Frecuente | **0,07** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,50 | 0,90 | 1 | Normal | **0,45** | 0,28 | 0,45 | 1 | Normal | **0,13** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,25 | 0,75 | 1 | Normal | **0,19** | 0,25 | 0,80 | 1 | Normal | **0,20** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,16 | 0,65 | 1 | Normal | **0,10** | 0,16 | 0,65 | 1 | Normal | **0,10** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,16 | 0,89 | 1 | Normal | **0,14** | 0,16 | 0,89 | 1 | Normal | **0,14** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | 0,45 | 0,9 | 1 | Normal | **0,41** | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | 0,05 | 0,60 | 1 | Normal | **0,03** | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | 0,05 | 0,60 | 1 | Normal | **0,03** | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,25 | 0,80 | 1 | Normal | **0,20** | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | 0,60 | 0,65 | 10 | Frecuente | **0,39** | | | | | |
| **E.25** Pérdida de equipos | 0,15 | 0,85 | 1/10 | Poco Frecuente | **0,13** | 0,15 | 0,75 | 1/10 | Poco Frecuente | **0,11** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | 0,05 | 0,80 | 1/10 | Poco frecuente | **0,04** | | | | | |
| **A.6** Abuso de Privilegios de Acceso | 0,05 | 0,50 | 1/10 | Poco frecuente | **0,03** | | | | | |
| **A.7** Uso no previsto | 0,05 | 0,40 | 1/10 | Poco frecuente | **0,02** | | | | | |
| **A.11** Acceso no Autorizado | 0,15 | 0,75 | 1/10 | Poco Frecuente | **0,11** | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | 0,15 | 0,85 | 1/10 | Poco Frecuente | **0,13** | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | 0,15 | 0,65 | 1/10 | Poco Frecuente | **0,10** | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | 0,15 | 0,85 | 1/10 | Poco Frecuente | **0,13** | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,15 | 0,90 | 1/10 | Poco Frecuente | **0,14** | 0,15 | 0,75 | 1/10 | Poco Frecuente | **0,11** |
| **A.26** Ataque destructivo | 0,20 | 0,85 | 1/10 | Poco Frecuente | **0,17** | 0,20 | 0,78 | 1/10 | Poco Frecuente | **0,16** |

| AMENAZAS | CPU | | | | | MONITOR | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | DAÑO EN LA MEMORIA RAM | | | | | | | | | |
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** |
| **N.2** Daños por agua (Inundaciones) | 0,12 | 0,8 | 0,10 | Poco Frecuente | **0,10** | 0,20 | 0,80 | 0,10 | Poco Frecuente | **0,16** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,63 | 1/100 | Muy Poco Frecuente | **0,08** | 0,20 | 0,65 | 0,10 | Poco Frecuente | **0,13** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,12 | 0,80 | 0,10 | Poco Frecuente | **0,10** | 0,20 | 0,70 | 0,10 | Poco Frecuente | **0,14** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,63 | 1/100 | Muy Poco Frecuente | **0,08** | 0,12 | 0,63 | 1/100 | Muy Poco Frecuente | **0,08** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,30 | 0,80 | 0,10 | Poco Frecuente | **0,24** | 0,08 | 0,70 | 0,10 | Poco Frecuente | **0,06** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,12 | 0,55 | 0,10 | Poco Frecuente | **0,07** | 0,12 | 0,55 | 0,10 | Poco Frecuente | **0,07** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,28 | 0,45 | 1 | Normal | **0,13** | 0,35 | 0,45 | 1 | Normal | **0,16** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,25 | 0,60 | 1 | Normal | **0,15** | 0,28 | 0,45 | 1 | Normal | **0,13** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,16 | 0,65 | 1 | Normal | **0,10** | 0,16 | 0,70 | 1 | Normal | **0,11** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,16 | 0,69 | 1 | Normal | **0,11** | 0,16 | 0,69 | 1 | Normal | **0,11** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | | | | | | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | | | | | | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | | | | | | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | | | | | | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | | | | | | | | | | |
| **E.25** Pérdida de equipos | 0,15 | 0,75 | 0,10 | Poco Frecuente | **0,11** | 0,15 | 0,80 | 0,10 | Poco Frecuente | **0,12** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | | | | | | | | | | |
| **A.6** Abuso de Privilegios de Acceso | | | | | | | | | | |
| **A.7** Uso no previsto | | | | | | | | | | |
| **A.11** Acceso no Autorizado | | | | | | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | | | | | | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | | | | | | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | | | | | | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,15 | 0,75 | 0,10 | Poco Frecuente | **0,11** | 0,15 | 0,80 | 0,10 | Poco Frecuente | **0,12** |
| **A.26** Ataque destructivo | 0,20 | 0,78 | 0,10 | Poco Frecuente | **0,16** | 0,15 | 0,85 | 0,10 | Poco Frecuente | **0,13** |

| AMENAZAS | MOUSE | | | | | TECLADO | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,65 | 1/100 | Muy Poco frecuente | **0,07** | 0,10 | 0,70 | 1/100 | Muy Poco frecuente | **0,07** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,68 | 0,10 | Poco frecuente | **0,11** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,65 | 1/100 | Muy Poco frecuente | **0,07** | 0,10 | 0,70 | 1/100 | Muy Poco frecuente | **0,07** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,16 | 0,68 | 0,1 | Poco frecuente | **0,11** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,10 | 0,50 | 1 | Normal | **0,05** | 0,10 | 0,54 | 1 | Normal | **0,05** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,15 | 0,58 | 0,10 | Poco frecuente | **0,09** | 0,15 | 0,58 | 0,10 | Poco frecuente | **0,09** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,35 | 0,72 | 1 | Normal | **0,25** | 0,35 | 0,76 | 1,00 | Normal | **0,27** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,70 | 10 | Frecuente | **0,25** | 0,35 | 0,75 | 10 | Frecuente | **0,26** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,75 | 1 | Normal | **0,09** | 0,12 | 0,80 | 1 | Normal | **0,10** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | | | | | | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | | | | | | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | | | | | | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | | | | | | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | | | | | | | | | | |
| **E.25** Pérdida de equipos | 0,15 | 0,75 | 0,10 | Poco frecuente | **0,11** | 0,15 | 0,80 | 0,10 | Poco frecuente | **0,12** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | | | | | | | | | | |
| **A.6** Abuso de Privilegios de Acceso | | | | | | | | | | |
| **A.7** Uso no previsto | | | | | | | | | | |
| **A.11** Acceso no Autorizado | | | | | | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | | | | | | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | | | | | | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | | | | | | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,07 | 0,65 | 0,10 | Poco frecuente | **0,05** | 0,07 | 0,75 | 0,10 | Poco frecuente | **0,05** |
| **A.26** Ataque destructivo | 0,05 | 0,60 | 0,10 | Poco frecuente | **0,03** | 0,05 | 0,65 | 0,10 | Poco frecuente | **0,03** |

| AMENAZAS | ROUTERS INALÁMBRICOS | | | | | SWITCH | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** | 0,12 | 0,90 | 0,10 | Poco Frecuente | **0,11** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** | 0,12 | 0,65 | 0,10 | Poco Frecuente | **0,08** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** | 0,15 | 0,90 | 0,10 | Poco Frecuente | **0,14** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** | 0,12 | 0,65 | 0,10 | Poco Frecuente | **0,08** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,15 | 0,60 | 0,10 | Poco frecuente | **0,09** | 0,06 | 0,45 | 0,10 | Poco Frecuente | **0,03** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,15 | 0,75 | 1 | Normal | **0,11** | 0,10 | 0,75 | 1 | Normal | **0,08** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,27 | 0,70 | 0,10 | Poco frecuente | **0,19** | 0,35 | 0,85 | 1 | Normal | **0,30** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,80 | 1 | Normal | **0,28** | 0,35 | 0,82 | 1 | Normal | **0,29** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,75 | 1 | Normal | **0,09** | 0,35 | 0,78 | 1 | Normal | **0,27** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | 0,12 | 0,78 | 1 | Normal | **0,09** | 0,12 | 0,88 | 1 | Normal | **0,11** |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,72 | 0,10 | Poco frecuente | **0,06** |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | 0,10 | 0,62 | 0,10 | Poco frecuente | **0,06** | 0,10 | 0,62 | 0,10 | Poco frecuente | **0,06** |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | 0,22 | 0,68 | 10 | Frecuente | **0,15** | 0,22 | 0,68 | 10 | Frecuente | **0,15** |
| **E.25** Pérdida de equipos | 0,15 | 0,90 | 0,10 | Poco frecuente | **0,14** | 0,15 | 0,85 | 1 | Normal | **0,13** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** | 0,15 | 0,75 | 1 | Normal | **0,11** |
| **A.6** Abuso de Privilegios de Acceso | 0,15 | 0,45 | 0,10 | Poco frecuente | **0,07** | 0,15 | 0,85 | 1 | Normal | **0,13** |
| **A.7** Uso no previsto | 0,18 | 0,60 | 0,10 | Poco frecuente | **0,11** | 0,18 | 0,60 | 0,10 | Poco frecuente | **0,11** |
| **A.11** Acceso no Autorizado | 0,2 | 0,60 | 1 | Normal | **0,12** | 0,2 | 0,80 | 1 | Normal | **0,16** |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | 0,15 | 0,90 | 1 | Normal | **0,14** | 0,14 | 0,87 | 1 | Normal | **0,12** |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | 0,15 | 0,78 | 0,10 | Poco frecuente | **0,12** | 0,14 | 0,66 | 1 | Normal | **0,09** |
| **A.24** Denegación de servicio (Saturación del sistema informático) | 0,15 | 0,72 | 10 | Frecuente | **0,11** | 0,22 | 0,85 | 1 | Normal | **0,19** |
| **A.25** Robo (Pérdida de Equipos) | 0,07 | 0,90 | 0,10 | Poco frecuente | **0,06** | 0,15 | 0,90 | 0,10 | Poco Frecuente | **0,14** |
| **A.26** Ataque destructivo | 0,05 | 0,65 | 0,10 | Poco frecuente | **0,03** | 0,15 | 0,90 | 0,10 | Poco Frecuente | **0,14** |

| AMENAZAS | ACCESS POINT | | | | | BIOMÉTRICOS | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,12 | 0,85 | 0,10 | Poco Frecuente | **0,10** | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** |
| **N.2** Daños por agua (Inundaciones) | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,65 | 0,10 | Poco Frecuente | **0,08** | 0,12 | 0,65 | 0,10 | Poco Frecuente | **0,08** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,15 | 0,85 | 0,10 | Poco Frecuente | **0,13** | 0,15 | 0,75 | 0,10 | Poco Frecuente | **0,11** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,65 | 0,10 | Poco Frecuente | **0,08** | 0,12 | 0,65 | 0,10 | Poco Frecuente | **0,08** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,06 | 0,45 | 0,10 | Poco Frecuente | **0,03** | 0,06 | 0,45 | 0,10 | Poco Frecuente | **0,03** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,10 | 0,75 | 1 | Normal | **0,08** | 0,10 | 0,75 | 1 | Normal | **0,08** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,35 | 0,85 | 1 | Normal | **0,30** | 0,35 | 0,85 | 1 | Normal | **0,30** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,82 | 1 | Normal | **0,29** | 0,35 | 0,75 | 1 | Normal | **0,26** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,35 | 0,78 | 1 | Normal | **0,27** | 0,35 | 0,78 | 1 | Normal | **0,27** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | 0,12 | 0,80 | 1 | Normal | **0,10** | 0,12 | 0,88 | 1 | Normal | **0,11** |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | 0,08 | 0,72 | 0,10 | Poco frecuente | **0,06** | 0,08 | 0,72 | 0,10 | Poco frecuente | **0,06** |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | 0,10 | 0,62 | 0,10 | Poco frecuente | **0,06** | 0,10 | 0,62 | 0,10 | Poco frecuente | **0,06** |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | 0,22 | 0,68 | 10 | Frecuente | **0,15** | 0,22 | 0,68 | 10 | Frecuente | **0,15** |
| **E.25** Pérdida de equipos | 0,15 | 0,85 | 1 | Normal | **0,13** | 0,15 | 0,80 | 1 | Normal | **0,12** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | 0,15 | 0,75 | 1 | Normal | **0,11** | 0,15 | 0,75 | 1 | Normal | **0,11** |
| **A.6** Abuso de Privilegios de Acceso | 0,15 | 0,85 | 1 | Normal | **0,13** | 0,15 | 0,85 | 1 | Normal | **0,13** |
| **A.7** Uso no previsto | 0,18 | 0,60 | 0,10 | Poco frecuente | **0,11** | 0,18 | 0,60 | 0,10 | Poco frecuente | **0,11** |
| **A.11** Acceso no Autorizado | 0,20 | 0,80 | 1 | Normal | **0,16** | 0,20 | 0,80 | 1 | Normal | **0,16** |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | 0,14 | 0,87 | 1 | Normal | **0,12** | 0,14 | 0,87 | 1 | Normal | **0,12** |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | 0,14 | 0,66 | 1 | Normal | **0,09** | 0,14 | 0,66 | 1 | Normal | **0,09** |
| **A.24** Denegación de servicio (Saturación del sistema informático) | 0,22 | 0,85 | 1 | Normal | **0,19** | 0,22 | 0,85 | 1 | Normal | **0,19** |
| **A.25** Robo (Pérdida de Equipos) | 0,15 | 0,85 | 0,10 | Poco Frecuente | **0,13** | 0,15 | 0,75 | 0,10 | Poco Frecuente | **0,11** |
| **A.26** Ataque destructivo | 0,15 | 0,75 | 0,10 | Poco Frecuente | **0,11** | 0,15 | 0,75 | 0,10 | Poco Frecuente | **0,11** |

| AMENAZAS | LAPTOPS | | | | | SERVIDORES | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,90 | 1/100 | Muy Poco frecuente | **0,09** | 0,12 | 0,90 | 0,10 | Poco Frecuente | **0,11** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,88 | 0,10 | Poco frecuente | **0,14** | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,75 | 0,10 | Poco frecuente | **0,09** | 0,12 | 0,65 | 0,10 | Poco Frecuente | **0,08** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,90 | 1/100 | Muy Poco frecuente | **0,09** | 0,15 | 0,90 | 0,10 | Poco Frecuente | **0,14** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,16 | 0,88 | 0,10 | Poco frecuente | **0,14** | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,75 | 0,10 | Poco frecuente | **0,09** | 0,12 | 0,65 | 0,10 | Poco Frecuente | **0,08** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,30 | 0,79 | 10 | Frecuente | **0,24** | 0,06 | 0,55 | 0,10 | Poco Frecuente | **0,03** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,15 | 0,58 | 0,10 | Poco frecuente | **0,09** | 0,23 | 0,75 | 1 | Normal | **0,17** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,45 | 0,82 | 1 | Normal | **0,37** | 0,35 | 0,9 | 1 | Normal | **0,32** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,50 | 1 | Normal | **0,18** | 0,35 | 0,93 | 1 | Normal | **0,33** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,85 | 1 | Normal | **0,10** | 0,35 | 0,78 | 1 | Normal | **0,27** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | 0,12 | 0,88 | 1 | Normal | **0,11** | 0,12 | 0,90 | 1 | Normal | **0,11** |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,12 | 0,75 | 0,10 | Poco frecuente | **0,09** |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | | | | | | 0,15 | 0,62 | 0,10 | Poco frecuente | **0,09** |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,15 | 0,80 | 0,10 | Poco frecuente | **0,12** | 0,15 | 0,75 | 0,10 | Poco frecuente | **0,11** |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | 0,22 | 0,68 | 10 | Frecuente | **0,15** | 0,22 | 0,75 | 10 | Frecuente | **0,17** |
| **E.25** Pérdida de equipos | 0,15 | 0,90 | 0,10 | Poco frecuente | **0,14** | 0,15 | 0,95 | 1 | Normal | **0,14** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | 0,15 | 0,45 | 0,10 | Poco frecuente | **0,07** | 0,15 | 0,75 | 1 | Normal | **0,11** |
| **A.6** Abuso de Privilegios de Acceso | 0,15 | 0,45 | 0,10 | Poco frecuente | **0,07** | 0,15 | 0,85 | 1 | Normal | **0,13** |
| **A.7** Uso no previsto | | | | | | 0,18 | 0,60 | 0,10 | Poco frecuente | **0,11** |
| **A.11** Acceso no Autorizado | | | | | | 0,20 | 0,80 | 1 | Normal | **0,16** |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | 0,15 | 0,90 | 0,10 | Poco frecuente | **0,14** | 0,18 | 0,87 | 1 | Normal | **0,16** |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | 0,15 | 0,78 | 0,10 | Poco frecuente | **0,12** | 0,18 | 0,88 | 1 | Normal | **0,16** |
| **A.24** Denegación de servicio (Saturación del sistema informático) | 0,15 | 0,72 | 10 | Frecuente | **0,11** | 0,22 | 0,85 | 1 | Normal | **0,19** |
| **A.25** Robo (Pérdida de Equipos) | 0,07 | 0,90 | 0,10 | Poco frecuente | **0,06** | 0,15 | 0,95 | 0,10 | Poco Frecuente | **0,14** |
| **A.26** Ataque destructivo | 0,05 | 0,72 | 0,10 | Poco frecuente | **0,04** | 0,15 | 0,90 | 0,10 | Poco Frecuente | **0,14** |

| AMENAZAS | UPS | | | | | DVR | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,12 | 0,90 | 0,10 | Poco Frecuente | **0,11** | 0,12 | 0,80 | 0,10 | Poco Frecuente | **0,10** |
| **N.2** Daños por agua (Inundaciones) | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,65 | 0,10 | Poco Frecuente | **0,08** | 0,12 | 0,65 | 0,10 | Poco Frecuente | **0,08** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,15 | 0,90 | 0,10 | Poco Frecuente | **0,14** | 0,12 | 0,80 | 0,10 | Poco Frecuente | **0,10** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,65 | 0,10 | Poco Frecuente | **0,08** | 0,12 | 0,65 | 0,10 | Poco Frecuente | **0,08** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,06 | 0,65 | 0,10 | Poco Frecuente | **0,04** | 0,06 | 0,45 | 0,10 | Poco Frecuente | **0,03** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,10 | 0,75 | 1 | Normal | **0,08** | 0,10 | 0,75 | 1 | Normal | **0,08** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,35 | 0,85 | 1 | Normal | **0,30** | 0,35 | 0,85 | 1 | Normal | **0,30** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,82 | 1 | Normal | **0,29** | 0,35 | 0,82 | 1 | Normal | **0,29** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,35 | 0,78 | 1 | Normal | **0,27** | 0,35 | 0,78 | 1 | Normal | **0,27** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | | | | | | 0,12 | 0,80 | 1 | Normal | **0,10** |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | | | | | | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | | | | | | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | | | | | | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | 0,22 | 0,68 | 10 | Frecuente | **0,15** | 0,22 | 0,68 | 10 | Frecuente | **0,15** |
| **E.25** Pérdida de equipos | 0,15 | 0,85 | 1 | Normal | **0,13** | 0,15 | 0,85 | 1 | Normal | **0,13** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | | | | | | | | | | |
| **A.6** Abuso de Privilegios de Acceso | | | | | | | | | | |
| **A.7** Uso no previsto | | | | | | | | | | |
| **A.11** Acceso no Autorizado | | | | | | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | | | | | | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | | | | | | 0,14 | 0,66 | 1 | Normal | **0,09** |
| **A.24** Denegación de servicio (Saturación del sistema informático) | 0,22 | 0,85 | 1 | Normal | **0,19** | 0,22 | 0,85 | 1 | Normal | **0,19** |
| **A.25** Robo (Pérdida de Equipos) | 0,15 | 0,90 | 0,10 | Poco Frecuente | **0,14** | 0,15 | 0,90 | 0,10 | Poco Frecuente | **0,14** |
| **A.26** Ataque destructivo | 0,15 | 0,90 | 0,10 | Poco Frecuente | **0,14** | 0,15 | 0,90 | 0,10 | Poco Frecuente | **0,14** |

| AMENAZAS | STORAGE | | | | | TRACYVER (CONVERTIDORES) | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,12 | 0,90 | 0,10 | Poco Frecuente | **0,11** | 0,12 | 0,82 | 0,10 | Poco Frecuente | **0,10** |
| **N.2** Daños por agua (Inundaciones) | 0,12 | 0,80 | 0,10 | Poco Frecuente | **0,10** | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,65 | 0,10 | Poco Frecuente | **0,08** | 0,12 | 0,65 | 0,10 | Poco Frecuente | **0,08** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,15 | 0,90 | 0,10 | Poco Frecuente | **0,14** | 0,15 | 0,82 | 0,10 | Poco Frecuente | **0,12** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,65 | 0,10 | Poco Frecuente | **0,08** | 0,12 | 0,65 | 0,10 | Poco Frecuente | **0,08** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,06 | 0,45 | 0,10 | Poco Frecuente | **0,03** | 0,06 | 0,45 | 0,10 | Poco Frecuente | **0,03** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,16 | 0,75 | 1 | Normal | **0,12** | 0,26 | 0,78 | 1 | Normal | **0,20** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,35 | 0,85 | 1 | Normal | **0,30** | 0,35 | 0,85 | 1 | Normal | **0,30** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,40 | 0,82 | 1 | Normal | **0,33** | 0,35 | 0,82 | 1 | Normal | **0,29** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,35 | 0,78 | 1 | Normal | **0,27** | 0,35 | 0,78 | 1 | Normal | **0,27** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | 0,12 | 0,88 | 1 | Normal | **0,11** | 0,12 | 0,59 | 1 | Normal | **0,07** |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | 0,18 | 0,72 | 0,10 | Poco frecuente | **0,13** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | 0,20 | 0,62 | 0,10 | Poco frecuente | **0,12** | 0,10 | 0,62 | 0,10 | Poco frecuente | **0,06** |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,22 | 0,80 | 0,10 | Poco frecuente | **0,18** | 0,15 | 0,70 | 0,10 | Poco frecuente | **0,11** |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | 0,22 | 0,68 | 10 | Frecuente | **0,15** | 0,22 | 0,68 | 10 | Frecuente | **0,15** |
| **E.25** Pérdida de equipos | 0,15 | 0,90 | 1 | Normal | **0,14** | 0,15 | 0,85 | 1 | Normal | **0,13** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | 0,15 | 0,75 | 1 | Normal | **0,11** | 0,15 | 0,64 | 1 | Normal | **0,10** |
| **A.6** Abuso de Privilegios de Acceso | 0,15 | 0,85 | 1 | Normal | **0,13** | 0,15 | 0,62 | 1 | Normal | **0,09** |
| **A.7** Uso no previsto | 0,18 | 0,60 | 0,10 | Poco frecuente | **0,11** | 0,18 | 0,60 | 0,10 | Poco frecuente | **0,11** |
| **A.11** Acceso no Autorizado | 0,20 | 0,80 | 1 | Normal | **0,16** | 0,20 | 0,80 | 1 | Normal | **0,16** |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | 0,14 | 0,90 | 1 | Normal | **0,13** | 0,14 | 0,87 | 1 | Normal | **0,12** |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | 0,14 | 0,78 | 1 | Normal | **0,11** | 0,14 | 0,66 | 1 | Normal | **0,09** |
| **A.24** Denegación de servicio (Saturación del sistema informático) | 0,22 | 0,85 | 1 | Normal | **0,19** | 0,22 | 0,85 | 1 | Normal | **0,19** |
| **A.25** Robo (Pérdida de Equipos) | 0,15 | 0,90 | 0,10 | Poco Frecuente | **0,14** | 0,15 | 0,90 | 0,10 | Poco Frecuente | **0,14** |
| **A.26** Ataque destructivo | 0,15 | 0,90 | 0,10 | Poco Frecuente | **0,14** | 0,15 | 0,90 | 0,10 | Poco Frecuente | **0,14** |

| AMENAZAS | SYSTEM BLADE C3000 | | | | | BYAS (Cuchillas) | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,12 | 0,85 | 0,10 | Poco Frecuente | **0,10** | 0,12 | 0,85 | 0,10 | Poco Frecuente | **0,10** |
| **N.2** Daños por agua (Inundaciones) | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,65 | 0,10 | Poco Frecuente | **0,08** | 0,12 | 0,65 | 0,10 | Poco Frecuente | **0,08** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,15 | 0,85 | 0,10 | Poco Frecuente | **0,13** | 0,15 | 0,85 | 0,10 | Poco Frecuente | **0,13** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,65 | 0,10 | Poco Frecuente | **0,08** | 0,12 | 0,65 | 0,10 | Poco Frecuente | **0,08** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,06 | 0,45 | 1/10 | Poco Frecuente | **0,03** | 0,06 | 0,45 | 0,10 | Poco Frecuente | **0,03** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,10 | 0,75 | 1 | Normal | **0,08** | 0,10 | 0,75 | 1 | Normal | **0,08** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,35 | 0,85 | 1 | Normal | **0,30** | 0,35 | 0,85 | 1 | Normal | **0,30** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,82 | 1 | Normal | **0,29** | 0,35 | 0,82 | 1 | Normal | **0,29** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,35 | 0,78 | 1 | Normal | **0,27** | 0,35 | 0,78 | 1 | Normal | **0,27** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | 0,12 | 0,88 | 1 | Normal | **0,11** | 0,12 | 0,88 | 1 | Normal | **0,11** |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | | | | | | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | | | | | | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | 0,22 | 0,68 | 10 | Frecuente | **0,15** | 0,22 | 0,68 | 10 | Frecuente | **0,15** |
| **E.25** Pérdida de equipos | 0,15 | 0,85 | 1 | Normal | **0,13** | 0,15 | 0,85 | 1 | Normal | **0,13** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | | | | | | | | | | |
| **A.6** Abuso de Privilegios de Acceso | | | | | | | | | | |
| **A.7** Uso no previsto | | | | | | | | | | |
| **A.11** Acceso no Autorizado | | | | | | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | | | | | | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | 0,14 | 0,66 | 1 | Normal | **0,09** | 0,14 | 0,66 | 1 | Normal | **0,09** |
| **A.24** Denegación de servicio (Saturación del sistema informático) | 0,22 | 0,85 | 1 | Normal | **0,19** | 0,22 | 0,85 | 1 | Normal | **0,19** |
| **A.25** Robo (Pérdida de Equipos) | 0,15 | 0,90 | 0,10 | Poco Frecuente | **0,14** | 0,15 | 0,90 | 0,10 | Poco Frecuente | **0,14** |
| **A.26** Ataque destructivo | 0,15 | 0,75 | 0,10 | Poco Frecuente | **0,11** | 0,15 | 0,75 | 0,10 | Poco Frecuente | **0,11** |

**Cuadro 4.3.** Servicio: Unidad de Producción de Software (UPS)

| AMENAZAS | CPU | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | DAÑO EN EL DISCO DURO | | | | | DAÑO EN LA FUENTE DE PODER | | | | |
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,86 | 0,10 | Poco Frecuente | **0,09** | 0,12 | 0,86 | 0,10 | Poco Frecuente | **0,10** |
| **N.2** Daños por agua (Inundaciones) | 0,15 | 0,84 | 0,10 | Poco Frecuente | **0,13** | 0,12 | 0,80 | 0,10 | Poco Frecuente | **0,10** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,60 | 1/100 | Muy Poco Frecuente | **0,07** | 0,12 | 0,63 | 1/100 | Muy Poco Frecuente | **0,08** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,22 | 0,86 | 0,10 | Poco Frecuente | **0,19** | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,20 | 0,84 | 0,10 | Poco Frecuente | **0,17** | 0,12 | 0,80 | 0,10 | Poco Frecuente | **0,10** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,18 | 0,6 | 1/100 | Muy Poco Frecuente | **0,11** | 0,12 | 0,63 | 1/100 | Muy Poco Frecuente | **0,08** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,18 | 0,45 | 1 | Normal | **0,08** | 0,30 | 0,70 | 0,10 | Poco Frecuente | **0,21** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,12 | 0,55 | 1/10 | Poco Frecuente | **0,07** | 0,12 | 0,6 | 0,10 | Poco Frecuente | **0,07** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,50 | 0,90 | 1 | Normal | **0,45** | 0,28 | 0,45 | 1 | Normal | **0,13** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,25 | 0,75 | 1 | Normal | **0,19** | 0,25 | 0,80 | 1 | Normal | **0,20** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,16 | 0,65 | 1 | Normal | **0,10** | 0,16 | 0,65 | 1 | Normal | **0,10** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,16 | 0,89 | 1 | Normal | **0,14** | 0,16 | 0,89 | 1 | Normal | **0,14** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | 0,45 | 0,9 | 1 | Normal | **0,41** | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | 0,05 | 0,60 | 1 | Normal | **0,03** | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | 0,05 | 0,60 | 1 | Normal | **0,03** | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,25 | 0,80 | 1 | Normal | **0,20** | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | 0,60 | 0,65 | 10 | Frecuente | **0,39** | | | | | |
| **E.25** Pérdida de equipos | 0,15 | 0,85 | 0,10 | Poco Frecuente | **0,13** | 0,15 | 0,75 | 0,10 | Poco Frecuente | **0,11** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** | | | | | |
| **A.6** Abuso de Privilegios de Acceso | 0,05 | 0,50 | 0,10 | Poco frecuente | **0,03** | | | | | |
| **A.7** Uso no previsto | 0,05 | 0,40 | 0,10 | Poco frecuente | **0,02** | | | | | |
| **A.11** Acceso no Autorizado | 0,15 | 0,75 | 0,10 | Poco Frecuente | **0,11** | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | 0,15 | 0,85 | 0,10 | Poco Frecuente | **0,13** | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | 0,15 | 0,65 | 0,10 | Poco Frecuente | **0,10** | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | 0,15 | 0,85 | 0,10 | Poco Frecuente | **0,13** | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,15 | 0,90 | 0,10 | Poco Frecuente | **0,14** | 0,15 | 0,75 | 0,10 | Poco Frecuente | **0,11** |
| **A.26** Ataque destructivo | 0,20 | 0,85 | 0,10 | Poco Frecuente | **0,17** | 0,20 | 0,78 | 0,10 | Poco Frecuente | **0,16** |

| AMENAZAS | CPU<br>DAÑO EN LA MEMORIA RAM | | | | | MONITOR | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** |
| **N.2** Daños por agua (Inundaciones) | 0,12 | 0,80 | 0,10 | Poco Frecuente | **0,10** | 0,20 | 0,80 | 0,10 | Poco Frecuente | **0,16** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,63 | 1/100 | Muy Poco Frecuente | **0,08** | 0,20 | 0,65 | 0,10 | Poco Frecuente | **0,13** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,12 | 0,80 | 0,10 | Poco Frecuente | **0,10** | 0,20 | 0,70 | 0,10 | Poco Frecuente | **0,14** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,63 | 1/100 | Muy Poco Frecuente | **0,08** | 0,12 | 0,63 | 1/100 | Muy Poco Frecuente | **0,08** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,30 | 0,80 | 0,10 | Poco Frecuente | **0,24** | 0,08 | 0,70 | 0,10 | Poco Frecuente | **0,06** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,12 | 0,55 | 0,10 | Poco Frecuente | **0,07** | 0,12 | 0,55 | 0,10 | Poco Frecuente | **0,07** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,28 | 0,45 | 1 | Normal | **0,13** | 0,35 | 0,45 | 1 | Normal | **0,16** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,25 | 0,60 | 1 | Normal | **0,15** | 0,28 | 0,45 | 1 | Normal | **0,13** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,16 | 0,65 | 1 | Normal | **0,10** | 0,16 | 0,70 | 1 | Normal | **0,11** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,16 | 0,69 | 1 | Normal | **0,11** | 0,16 | 0,69 | 1 | Normal | **0,11** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | | | | | | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | | | | | | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | | | | | | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | | | | | | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | | | | | | | | | | |
| **E.25** Pérdida de equipos | 0,15 | 0,75 | 0,10 | Poco Frecuente | **0,11** | 0,15 | 0,80 | 0,10 | Poco Frecuente | **0,12** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | | | | | | | | | | |
| **A.6** Abuso de Privilegios de Acceso | | | | | | | | | | |
| **A.7** Uso no previsto | | | | | | | | | | |
| **A.11** Acceso no Autorizado | | | | | | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | | | | | | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | | | | | | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | | | | | | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,15 | 0,75 | 0,10 | Poco Frecuente | **0,11** | 0,15 | 0,80 | 0,10 | Poco Frecuente | **0,12** |
| **A.26** Ataque destructivo | 0,2 | 0,78 | 0,10 | Poco Frecuente | **0,16** | 0,15 | 0,85 | 0,10 | Poco Frecuente | **0,13** |

| AMENAZAS | MOUSE | | | | | TECLADO | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,65 | 1/100 | Muy Poco frecuente | **0,07** | 0,10 | 0,70 | 1/100 | Muy Poco frecuente | **0,07** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,68 | 0,10 | Poco frecuente | **0,11** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,65 | 1/100 | Muy Poco frecuente | **0,07** | 0,10 | 0,70 | 1/100 | Muy Poco frecuente | **0,07** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,16 | 0,68 | 0,10 | Poco frecuente | **0,11** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,10 | 0,50 | 1 | Normal | **0,05** | 0,10 | 0,54 | 1 | Normal | **0,05** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,15 | 0,58 | 0,10 | Poco frecuente | **0,09** | 0,15 | 0,58 | 0,10 | Poco frecuente | **0,09** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,35 | 0,72 | 1 | Normal | **0,25** | 0,35 | 0,76 | 1 | Normal | **0,27** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,70 | 10 | Frecuente | **0,25** | 0,35 | 0,75 | 10 | Frecuente | **0,26** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,75 | 1 | Normal | **0,09** | 0,12 | 0,80 | 1 | Normal | **0,10** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | | | | | | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | | | | | | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | | | | | | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | | | | | | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | | | | | | | | | | |
| **E.25** Pérdida de equipos | 0,15 | 0,75 | 0,10 | Poco frecuente | **0,11** | 0,15 | 0,80 | 0,10 | Poco frecuente | **0,12** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | | | | | | | | | | |
| **A.6** Abuso de Privilegios de Acceso | | | | | | | | | | |
| **A.7** Uso no previsto | | | | | | | | | | |
| **A.11** Acceso no Autorizado | | | | | | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | | | | | | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | | | | | | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | | | | | | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,07 | 0,65 | 0,10 | Poco frecuente | **0,05** | 0,07 | 0,75 | 0,10 | Poco frecuente | **0,05** |
| **A.26** Ataque destructivo | 0,05 | 0,60 | 0,10 | Poco frecuente | **0,03** | 0,05 | 0,65 | 0,10 | Poco frecuente | **0,03** |

| AMENAZAS | ROUTERS INALAMBRICOS | | | | | SWICTH | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** | 0,12 | 0,90 | 0,10 | Poco Frecuente | **0,11** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** | 0,12 | 0,65 | 0,10 | Poco Frecuente | **0,08** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** | 0,15 | 0,90 | 0,10 | Poco Frecuente | **0,14** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** | 0,12 | 0,65 | 0,10 | Poco Frecuente | **0,08** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,15 | 0,60 | 0,10 | Poco frecuente | **0,09** | 0,06 | 0,45 | 0,10 | Poco Frecuente | **0,03** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,15 | 0,75 | 1 | Normal | **0,11** | 0,10 | 0,75 | 1 | Normal | **0,08** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,27 | 0,70 | 0,10 | Poco frecuente | **0,19** | 0,35 | 0,85 | 1 | Normal | **0,30** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,80 | 1 | Normal | **0,28** | 0,35 | 0,82 | 1 | Normal | **0,29** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,75 | 1 | Normal | **0,09** | 0,35 | 0,78 | 1 | Normal | **0,27** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | 0,12 | 0,78 | 1 | Normal | **0,09** | 0,12 | 0,88 | 1 | Normal | **0,11** |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,72 | 0,10 | Poco frecuente | **0,06** |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | 0,10 | 0,62 | 0,10 | Poco frecuente | **0,06** | 0,10 | 0,62 | 0,10 | Poco frecuente | **0,06** |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | 0,22 | 0,68 | 10 | Frecuente | **0,15** | 0,22 | 0,68 | 10 | Frecuente | **0,15** |
| **E.25** Pérdida de equipos | 0,15 | 0,90 | 0,10 | Poco frecuente | **0,14** | 0,15 | 0,85 | 1 | Normal | **0,13** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** | 0,15 | 0,75 | 1 | Normal | **0,11** |
| **A.6** Abuso de Privilegios de Acceso | 0,15 | 0,45 | 0,10 | Poco frecuente | **0,07** | 0,15 | 0,85 | 1 | Normal | **0,13** |
| **A.7** Uso no previsto | 0,18 | 0,60 | 0,10 | Poco frecuente | **0,11** | 0,18 | 0,60 | 0,10 | Poco frecuente | **0,11** |
| **A.11** Acceso no Autorizado | 0,2 | 0,60 | 1 | Normal | **0,12** | 0,2 | 0,80 | 1 | Normal | **0,16** |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | 0,15 | 0,90 | 1 | Normal | **0,14** | 0,14 | 0,87 | 1 | Normal | **0,12** |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | 0,15 | 0,78 | 1/10 | Poco frecuente | **0,12** | 0,14 | 0,66 | 1 | Normal | **0,09** |
| **A.24** Denegación de servicio (Saturación del sistema informático) | 0,15 | 0,72 | 10 | Frecuente | **0,11** | 0,22 | 0,85 | 1 | Normal | **0,19** |
| **A.25** Robo (Pérdida de Equipos) | 0,07 | 0,90 | 0,10 | Poco frecuente | **0,06** | 0,15 | 0,90 | 0,10 | Poco Frecuente | **0,14** |
| **A.26** Ataque destructivo | 0,05 | 0,65 | 0,10 | Poco frecuente | **0,03** | 0,15 | 0,90 | 0,10 | Poco Frecuente | **0,14** |

| AMENAZAS | BIOMETRICOS | | | | | COMPUTADORAS TODO EN UNO | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** | 0,10 | 0,90 | 1/100 | Muy Poco frecuente | **0,09** |
| **N.2** Daños por agua (Inundaciones) | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** | 0,16 | 0,88 | 0,10 | Poco frecuente | **0,14** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,65 | 0,10 | Poco Frecuente | **0,08** | 0,12 | 0,75 | 0,10 | Poco frecuente | **0,09** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,15 | 0,75 | 0,10 | Poco Frecuente | **0,11** | 0,10 | 0,90 | 1/100 | Muy Poco frecuente | **0,09** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** | 0,16 | 0,88 | 0,10 | Poco frecuente | **0,14** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,65 | 0,10 | Poco Frecuente | **0,08** | 0,12 | 0,75 | 0,10 | Poco frecuente | **0,09** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,06 | 0,45 | 0,10 | Poco Frecuente | **0,03** | 0,30 | 0,79 | 10 | Frecuente | **0,24** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,10 | 0,75 | 1 | Normal | **0,08** | 0,15 | 0,58 | 0,10 | Poco frecuente | **0,09** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,35 | 0,85 | 1 | Normal | **0,30** | 0,45 | 0,80 | 1 | Normal | **0,36** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,75 | 1 | Normal | **0,26** | 0,35 | 0,80 | 1 | Normal | **0,28** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,35 | 0,78 | 1 | Normal | **0,27** | 0,12 | 0,85 | 1 | Normal | **0,10** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | 0,12 | 0,88 | 1 | Normal | **0,11** | 0,12 | 0,88 | 1 | Normal | **0,11** |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | 0,08 | 0,72 | 0,10 | Poco frecuente | **0,06** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | 0,10 | 0,62 | 0,10 | Poco frecuente | **0,06** | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** | 0,15 | 0,80 | 0,10 | Poco frecuente | **0,12** |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | 0,22 | 0,68 | 10 | Frecuente | **0,15** | 0,22 | 0,68 | 10 | Frecuente | **0,15** |
| **E.25** Pérdida de equipos | 0,15 | 0,80 | 1 | Normal | **0,12** | 0,15 | 0,90 | 0,10 | Poco frecuente | **0,14** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | 0,15 | 0,75 | 1 | Normal | **0,11** | 0,15 | 0,45 | 0,10 | Poco frecuente | **0,07** |
| **A.6** Abuso de Privilegios de Acceso | 0,15 | 0,85 | 1 | Normal | **0,13** | 0,15 | 0,45 | 0,10 | Poco frecuente | **0,07** |
| **A.7** Uso no previsto | 0,18 | 0,60 | 0,10 | Poco frecuente | **0,11** | | | | | |
| **A.11** Acceso no Autorizado | 0,2 | 0,80 | 1 | Normal | **0,16** | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | 0,14 | 0,87 | 1 | Normal | **0,12** | 0,15 | 0,90 | 0,10 | Poco frecuente | **0,14** |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | 0,14 | 0,66 | 1 | Normal | **0,09** | 0,15 | 0,78 | 0,10 | Poco frecuente | **0,12** |
| **A.24** Denegación de servicio (Saturación del sistema informático) | 0,22 | 0,85 | 1 | Normal | **0,19** | 0,15 | 0,72 | 10 | Frecuente | **0,11** |
| **A.25** Robo (Pérdida de Equipos) | 0,15 | 0,75 | 0,10 | Poco Frecuente | **0,11** | 0,07 | 0,90 | 0,10 | Poco frecuente | **0,06** |
| **A.26** Ataque destructivo | 0,15 | 0,75 | 0,10 | Poco Frecuente | **0,11** | 0,05 | 0,65 | 0,10 | Poco frecuente | **0,03** |

**Cuadro 4.4.** Servicio: departamento de tecnología

| AMENAZAS | CPU | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | DAÑO EN EL DISCO DURO | | | | | DAÑO EN LA FUENTE DE PODER | | | | |
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,86 | 0,10 | Poco Frecuente | **0,09** | 0,12 | 0,86 | 0,10 | Poco Frecuente | **0,10** |
| **N.2** Daños por agua (Inundaciones) | 0,15 | 0,84 | 0,10 | Poco Frecuente | **0,13** | 0,12 | 0,80 | 0,10 | Poco Frecuente | **0,10** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,60 | 1/100 | Muy Poco Frecuente | **0,07** | 0,12 | 0,63 | 1/100 | Muy Poco Frecuente | **0,08** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,22 | 0,86 | 0,10 | Poco Frecuente | **0,19** | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,20 | 0,84 | 0,10 | Poco Frecuente | **0,17** | 0,12 | 0,80 | 0,10 | Poco Frecuente | **0,10** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,18 | 0,6 | 1/100 | Muy Poco Frecuente | **0,11** | 0,12 | 0,63 | 1/100 | Muy Poco Frecuente | **0,08** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,18 | 0,45 | 1 | Normal | **0,08** | 0,30 | 0,70 | 0,10 | Poco Frecuente | **0,21** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,12 | 0,55 | 0,10 | Poco Frecuente | **0,07** | 0,12 | 0,6 | 0,10 | Poco Frecuente | **0,07** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,50 | 0,90 | 1 | Normal | **0,45** | 0,28 | 0,45 | 1 | Normal | **0,13** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,25 | 0,75 | 1 | Normal | **0,19** | 0,25 | 0,80 | 1 | Normal | **0,20** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,16 | 0,65 | 1 | Normal | **0,10** | 0,16 | 0,65 | 1 | Normal | **0,10** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,16 | 0,89 | 1 | Normal | **0,14** | 0,16 | 0,89 | 1 | Normal | **0,14** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | 0,45 | 0,9 | 1 | Normal | **0,41** | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | 0,05 | 0,60 | 1 | Normal | **0,03** | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | 0,05 | 0,60 | 1 | Normal | **0,03** | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,25 | 0,80 | 1 | Normal | **0,20** | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | 0,60 | 0,65 | 10 | Frecuente | **0,39** | | | | | |
| **E.25** Pérdida de equipos | 0,15 | 0,85 | 0,10 | Poco Frecuente | **0,13** | 0,15 | 0,75 | 0,10 | Poco Frecuente | **0,11** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** | | | | | |
| **A.6** Abuso de Privilegios de Acceso | 0,05 | 0,50 | 0,10 | Poco frecuente | **0,03** | | | | | |
| **A.7** Uso no previsto | 0,05 | 0,40 | 0,10 | Poco frecuente | **0,02** | | | | | |
| **A.11** Acceso no Autorizado | 0,15 | 0,75 | 0,10 | Poco Frecuente | **0,11** | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | 0,15 | 0,85 | 0,10 | Poco Frecuente | **0,13** | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | 0,15 | 0,65 | 0,10 | Poco Frecuente | **0,10** | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | 0,15 | 0,85 | 0,10 | Poco Frecuente | **0,13** | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,15 | 0,90 | 0,10 | Poco Frecuente | **0,14** | 0,15 | 0,75 | 0,10 | Poco Frecuente | **0,11** |
| **A.26** Ataque destructivo | 0,20 | 0,85 | 0,10 | Poco Frecuente | **0,17** | 0,20 | 0,78 | 0,10 | Poco Frecuente | **0,16** |

| AMENAZAS | CPU | | | | | MONITOR | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | DAÑO EN LA MEMORIA RAM | | | | | | | | | |
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** |
| **N.2** Daños por agua (Inundaciones) | 0,12 | 0,80 | 0,10 | Poco Frecuente | **0,10** | 0,20 | 0,80 | 0,10 | Poco Frecuente | **0,16** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,63 | 1/100 | Muy Poco Frecuente | **0,08** | 0,20 | 0,65 | 0,10 | Poco Frecuente | **0,13** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,12 | 0,80 | 0,10 | Poco Frecuente | **0,10** | 0,20 | 0,70 | 0,10 | Poco Frecuente | **0,14** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,63 | 1/100 | Muy Poco Frecuente | **0,08** | 0,12 | 0,63 | 1/100 | Muy Poco Frecuente | **0,08** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,30 | 0,80 | 0,10 | Poco Frecuente | **0,24** | 0,08 | 0,70 | 0,10 | Poco Frecuente | **0,06** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,12 | 0,55 | 0,10 | Poco Frecuente | **0,07** | 0,12 | 0,55 | 0,10 | Poco Frecuente | **0,07** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,28 | 0,45 | 1 | Normal | **0,13** | 0,35 | 0,45 | 1 | Normal | **0,16** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,25 | 0,60 | 1 | Normal | **0,15** | 0,28 | 0,45 | 1 | Normal | **0,13** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,16 | 0,65 | 1 | Normal | **0,10** | 0,16 | 0,70 | 1 | Normal | **0,11** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,16 | 0,69 | 1 | Normal | **0,11** | 0,16 | 0,69 | 1 | Normal | **0,11** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | | | | | | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | | | | | | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | | | | | | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | | | | | | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | | | | | | | | | | |
| **E.25** Pérdida de equipos | 0,15 | 0,75 | 0,10 | Poco Frecuente | **0,11** | 0,15 | 0,80 | 0,10 | Poco Frecuente | **0,12** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | | | | | | | | | | |
| **A.6** Abuso de Privilegios de Acceso | | | | | | | | | | |
| **A.7** Uso no previsto | | | | | | | | | | |
| **A.11** Acceso no Autorizado | | | | | | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | | | | | | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | | | | | | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | | | | | | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,15 | 0,75 | 0,10 | Poco Frecuente | **0,11** | 0,15 | 0,80 | 0,10 | Poco Frecuente | **0,12** |
| **A.26** Ataque destructivo | 0,2 | 0,78 | 0,10 | Poco Frecuente | **0,16** | 0,15 | 0,85 | 0,10 | Poco Frecuente | **0,13** |

| AMENAZAS | MOUSE | | | | | TECLADO | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,65 | 1/100 | Muy Poco frecuente | **0,07** | 0,10 | 0,70 | 1/100 | Muy Poco frecuente | **0,07** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,68 | 0,10 | Poco frecuente | **0,11** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,65 | 1/100 | Muy Poco frecuente | **0,07** | 0,10 | 0,70 | 1/100 | Muy Poco frecuente | **0,07** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,16 | 0,68 | 0,10 | Poco frecuente | **0,11** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,10 | 0,50 | 1 | Normal | **0,05** | 0,10 | 0,54 | 1 | Normal | **0,05** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,15 | 0,58 | 0,10 | Poco frecuente | **0,09** | 0,15 | 0,58 | 0,10 | Poco frecuente | **0,09** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,35 | 0,72 | 1 | Normal | **0,25** | 0,35 | 0,76 | 1 | Normal | **0,27** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,70 | 10 | Frecuente | **0,25** | 0,35 | 0,75 | 10 | Frecuente | **0,26** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,75 | 1 | Normal | **0,09** | 0,12 | 0,80 | 1 | Normal | **0,10** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | | | | | | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | | | | | | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | | | | | | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | | | | | | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | | | | | | | | | | |
| **E.25** Pérdida de equipos | 0,15 | 0,75 | 0,10 | Poco frecuente | **0,11** | 0,15 | 0,80 | 0,10 | Poco frecuente | **0,12** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | | | | | | | | | | |
| **A.6** Abuso de Privilegios de Acceso | | | | | | | | | | |
| **A.7** Uso no previsto | | | | | | | | | | |
| **A.11** Acceso no Autorizado | | | | | | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | | | | | | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | | | | | | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | | | | | | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,07 | 0,65 | 0,10 | Poco frecuente | **0,05** | 0,07 | 0,75 | 0,10 | Poco frecuente | **0,05** |
| **A.26** Ataque destructivo | 0,05 | 0,60 | 0,10 | Poco frecuente | **0,03** | 0,05 | 0,65 | 0,10 | Poco frecuente | **0,03** |

| AMENAZAS | ROUTERS INALAMBRICOS | | | | | SWICTH | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** | 0,12 | 0,90 | 0,10 | Poco Frecuente | **0,11** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** | 0,12 | 0,65 | 0,10 | Poco Frecuente | **0,08** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** | 0,15 | 0,90 | 0,10 | Poco Frecuente | **0,14** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** | 0,12 | 0,65 | 0,10 | Poco Frecuente | **0,08** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,15 | 0,60 | 0,10 | Poco frecuente | **0,09** | 0,06 | 0,45 | 0,10 | Poco Frecuente | **0,03** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,15 | 0,75 | 1 | Normal | **0,11** | 0,10 | 0,75 | 1 | Normal | **0,08** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,27 | 0,70 | 0,10 | Poco frecuente | **0,19** | 0,35 | 0,85 | 1 | Normal | **0,30** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,80 | 1 | Normal | **0,28** | 0,35 | 0,82 | 1 | Normal | **0,29** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,75 | 1 | Normal | **0,09** | 0,35 | 0,78 | 1 | Normal | **0,27** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | 0,12 | 0,78 | 1 | Normal | **0,09** | 0,12 | 0,88 | 1 | Normal | **0,11** |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,72 | 0,10 | Poco frecuente | **0,06** |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | 0,10 | 0,62 | 0,10 | Poco frecuente | **0,06** | 0,10 | 0,62 | 0,10 | Poco frecuente | **0,06** |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | 0,22 | 0,68 | 10 | Frecuente | **0,15** | 0,22 | 0,68 | 10 | Frecuente | **0,15** |
| **E.25** Pérdida de equipos | 0,15 | 0,90 | 0,10 | Poco frecuente | **0,14** | 0,15 | 0,85 | 1 | Normal | **0,13** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** | 0,15 | 0,75 | 1 | Normal | **0,11** |
| **A.6** Abuso de Privilegios de Acceso | 0,15 | 0,45 | 0,10 | Poco frecuente | **0,07** | 0,15 | 0,85 | 1 | Normal | **0,13** |
| **A.7** Uso no previsto | 0,18 | 0,60 | 0,10 | Poco frecuente | **0,11** | 0,18 | 0,60 | 0,10 | Poco frecuente | **0,11** |
| **A.11** Acceso no Autorizado | 0,2 | 0,60 | 1 | Normal | **0,12** | 0,2 | 0,80 | 1 | Normal | **0,16** |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | 0,15 | 0,90 | 1 | Normal | **0,14** | 0,14 | 0,87 | 1 | Normal | **0,12** |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | 0,15 | 0,78 | 0,10 | Poco frecuente | **0,12** | 0,14 | 0,66 | 1 | Normal | **0,09** |
| **A.24** Denegación de servicio (Saturación del sistema informático) | 0,15 | 0,72 | 10 | Frecuente | **0,11** | 0,22 | 0,85 | 1 | Normal | **0,19** |
| **A.25** Robo (Pérdida de Equipos) | 0,07 | 0,90 | 0,10 | Poco frecuente | **0,06** | 0,15 | 0,90 | 0,10 | Poco Frecuente | **0,14** |
| **A.26** Ataque destructivo | 0,05 | 0,65 | 0,10 | Poco frecuente | **0,03** | 0,15 | 0,90 | 0,10 | Poco Frecuente | **0,14** |

| AMENAZAS | IMPRESORAS | | | | | PORTÁTILES | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,90 | 1/100 | Muy Poco frecuente | **0,09** | 0,10 | 0,90 | 1/100 | Muy Poco frecuente | **0,09** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** | 0,16 | 0,88 | 0,10 | Poco frecuente | **0,14** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,75 | 0,10 | Poco frecuente | **0,09** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,85 | 1/100 | Muy Poco frecuente | **0,09** | 0,10 | 0,90 | 1/100 | Muy Poco frecuente | **0,09** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** | 0,16 | 0,88 | 0,10 | Poco frecuente | **0,14** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,15 | 0,70 | 0,10 | Poco frecuente | **0,11** | 0,12 | 0,75 | 0,10 | Poco frecuente | **0,09** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,48 | 0,75 | 10 | Frecuente | **0,36** | 0,30 | 0,79 | 10 | Frecuente | **0,24** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,23 | 0,70 | 1 | Normal | **0,16** | 0,15 | 0,58 | 0,10 | Poco frecuente | **0,09** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,35 | 0,76 | 1 | Normal | **0,27** | 0,45 | 0,80 | 1 | Normal | **0,36** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,45 | 0,85 | 10 | Frecuente | **0,38** | 0,35 | 0,80 | 1 | Normal | **0,28** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,80 | 1 | Normal | **0,10** | 0,12 | 0,85 | 1 | Normal | **0,10** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | | | | | | 0,12 | 0,88 | 1 | Normal | **0,11** |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | | | | | | 0,08 | 0,60 | 1/10 | Poco frecuente | **0,05** |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | | | | | | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,12 | 0,75 | 1 | Normal | **0,09** | 0,15 | 0,80 | 0,10 | Poco frecuente | **0,12** |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | | | | | | 0,22 | 0,68 | 10 | Frecuente | **0,15** |
| **E.25** Pérdida de equipos | 0,23 | 0,83 | 0,10 | Poco frecuente | **0,19** | 0,15 | 0,90 | 0,10 | Poco frecuente | **0,14** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | | | | | | 0,15 | 0,45 | 0,10 | Poco frecuente | **0,07** |
| **A.6** Abuso de Privilegios de Acceso | | | | | | 0,15 | 0,45 | 0,10 | Poco frecuente | **0,07** |
| **A.7** Uso no previsto | | | | | | | | | | |
| **A.11** Acceso no Autorizado | | | | | | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | | | | | | 0,15 | 0,90 | 0,10 | Poco frecuente | **0,14** |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | | | | | | 0,15 | 0,78 | 0,10 | Poco frecuente | **0,12** |
| **A.24** Denegación de servicio (Saturación del sistema informático) | | | | | | 0,15 | 0,72 | 10 | Frecuente | **0,11** |
| **A.25** Robo (Pérdida de Equipos) | 0,07 | 0,90 | 0,10 | Poco frecuente | **0,06** | 0,07 | 0,90 | 0,10 | Poco frecuente | **0,06** |
| **A.26** Ataque destructivo | 0,05 | 0,75 | 0,10 | Poco frecuente | **0,04** | 0,05 | 0,65 | 0,10 | Poco frecuente | **0,03** |

**Cuadro 4.5. Servicio:** sala de docentes

| AMENAZAS | CPU | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | DAÑO EN EL DISCO DURO | | | | | DAÑO EN LA FUENTE DE PODER | | | | |
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,83 | 1/100 | Muy Poco frecuente | **0,08** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,90 | 1/100 | Muy Poco frecuente | **0,09** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,20 | 0,60 | 0,10 | Poco frecuente | **0,12** | 0,20 | 0,70 | 0,10 | Poco frecuente | **0,14** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,25 | 0,55 | 1 | Normal | **0,14** | 0,35 | 0,80 | 1 | Normal | **0,28** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,30 | 0,60 | 1 | Normal | **0,18** | 0,45 | 0,75 | 1 | Normal | **0,34** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,45 | 0,90 | 1 | Normal | **0,41** | 0,45 | 0,90 | 1 | Normal | **0,41** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,50 | 0,80 | 10 | Frecuente | **0,40** | 0,50 | 0,90 | 10 | Frecuente | **0,45** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,10 | 0,45 | 0,10 | Poco frecuente | **0,05** | 0,10 | 0,45 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,60 | 1 | Normal | **0,07** | 0,12 | 0,60 | 1 | Normal | **0,07** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | 0,50 | 0,75 | 1 | Normal | **0,38** | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | 0,05 | 0,60 | 1 | Normal | **0,03** | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | 0,05 | 0,60 | 1 | Normal | **0,03** | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,25 | 0,80 | 1 | Normal | **0,20** | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | 0,60 | 0,65 | 10 | Frecuente | **0,39** | | | | | |
| **E.25** Pérdida de equipos | 0,45 | 0,80 | 0,10 | Poco frecuente | **0,36** | 0,45 | 0,80 | 0,10 | Poco frecuente | **0,36** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** | | | | | |
| **A.6** Abuso de Privilegios de Acceso | 0,05 | 0,50 | 0,10 | Poco frecuente | **0,03** | | | | | |
| **A.7** Uso no previsto | 0,05 | 0,40 | 0,10 | Poco frecuente | **0,02** | | | | | |
| **A.11** Acceso no Autorizado | 0,10 | 0,80 | 0,10 | Poco frecuente | **0,08** | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | 0,15 | 0,76 | 0,10 | Poco frecuente | **0,11** | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | 0,05 | 0,83 | 0,10 | Poco frecuente | **0,04** | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | 0,35 | 0,75 | 1 | Normal | **0,26** | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** |
| **A.26** Ataque destructivo | 0,05 | 0,75 | 0,10 | Poco frecuente | **0,04** | 0,05 | 0,90 | 0,10 | Poco frecuente | **0,05** |

| AMENAZAS | CPU | | | | | MONITOR | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | DAÑO EN LA MEMORIA RAM | | | | | | | | | |
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,65 | 0,10 | Poco frecuente | **0,10** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,90 | 1/100 | Muy Poco frecuente | **0,09** | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,18 | 0,70 | 0,10 | Poco frecuente | **0,13** | 0,15 | 0,60 | 0,10 | Poco frecuente | **0,09** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,40 | 0,75 | 1 | Normal | **0,30** | 0,08 | 0,45 | 0,10 | Poco frecuente | **0,04** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,30 | 0,60 | 1 | Normal | **0,18** | 0,15 | 0,75 | 0,10 | Poco frecuente | **0,11** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,45 | 0,90 | 1 | Normal | **0,41** | 0,45 | 0,70 | 1 | Normal | **0,32** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,50 | 0,73 | 10 | Frecuente | **0,37** | 0,40 | 0,68 | 10 | Frecuente | **0,27** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,10 | 0,45 | 0,10 | Poco frecuente | **0,05** | 0,10 | 0,45 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,60 | 1 | Normal | **0,07** | 0,12 | 0,75 | 1 | Normal | **0,09** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | | | | | | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | | | | | | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | | | | | | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | | | | | | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | | | | | | | | | | |
| **E.25** Pérdida de equipos | 0,45 | 0,80 | 0,10 | Poco frecuente | **0,36** | 0,25 | 0,85 | 0,10 | Poco frecuente | **0,21** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | | | | | | | | | | |
| **A.6** Abuso de Privilegios de Acceso | | | | | | | | | | |
| **A.7** Uso no previsto | | | | | | | | | | |
| **A.11** Acceso no Autorizado | | | | | | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | | | | | | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | | | | | | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | | | | | | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** | 0,05 | 0,85 | 0,10 | Poco frecuente | **0,04** |
| **A.26** Ataque destructivo | 0,05 | 0,90 | 0,10 | Poco frecuente | **0,05** | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** |

| AMENAZAS | IMPRESORA | | | | | MOUSE | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,85 | 1/100 | Muy Poco frecuente | **0,09** | 0,10 | 0,65 | 1/100 | Muy Poco frecuente | **0,07** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** | 0,16 | 0,68 | 0,10 | Poco frecuente | **0,11** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,85 | 1/100 | Muy Poco frecuente | **0,09** | 0,10 | 0,65 | 1/100 | Muy Poco frecuente | **0,07** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** | 0,16 | 0,68 | 0,10 | Poco frecuente | **0,11** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,15 | 0,70 | 0,10 | Poco frecuente | **0,11** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,48 | 0,75 | 10 | Frecuente | **0,36** | 0,10 | 0,50 | 1 | Normal | **0,05** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,23 | 0,70 | 1 | Normal | **0,16** | 0,15 | 0,58 | 0,10 | Poco frecuente | **0,09** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,35 | 0,76 | 1 | Normal | **0,27** | 0,35 | 0,72 | 1 | Normal | **0,25** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,45 | 0,85 | 10 | Frecuente | **0,38** | 0,35 | 0,70 | 10 | Frecuente | **0,25** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,80 | 1 | Normal | **0,10** | 0,12 | 0,75 | 1 | Normal | **0,09** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | | | | | | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | | | | | | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | | | | | | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,12 | 0,75 | 1 | Normal | **0,09** | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | | | | | | | | | | |
| **E.25** Pérdida de equipos | 0,23 | 0,83 | 0,10 | Poco frecuente | **0,19** | 0,15 | 0,75 | 0,10 | Poco frecuente | **0,11** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | | | | | | | | | | |
| **A.6** Abuso de Privilegios de Acceso | | | | | | | | | | |
| **A.7** Uso no previsto | | | | | | | | | | |
| **A.11** Acceso no Autorizado | | | | | | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | | | | | | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | | | | | | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | | | | | | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,07 | 0,85 | 0,10 | Poco frecuente | **0,06** | 0,07 | 0,65 | 0,10 | Poco frecuente | **0,05** |
| **A.26** Ataque destructivo | 0,05 | 0,75 | 0,10 | Poco frecuente | **0,04** | 0,05 | 0,60 | 0,10 | Poco frecuente | **0,03** |

| AMENAZAS | TECLADO | | | | | PORTÁTILES | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,70 | 1/100 | Muy Poco frecuente | **0,07** | 0,10 | 0,85 | 1/100 | Muy Poco frecuente | **0,09** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** | 0,16 | 0,83 | 0,10 | Poco frecuente | **0,13** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,75 | 0,10 | Poco frecuente | **0,09** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,70 | 1/100 | Muy Poco frecuente | **0,07** | 0,10 | 0,85 | 1/100 | Muy Poco frecuente | **0,09** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** | 0,16 | 0,83 | 0,10 | Poco frecuente | **0,13** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,75 | 0,10 | Poco frecuente | **0,09** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,10 | 0,54 | 1 | Normal | **0,05** | 0,30 | 0,79 | 10 | Frecuente | **0,24** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,15 | 0,58 | 0,10 | Poco frecuente | **0,09** | 0,15 | 0,58 | 0,10 | Poco frecuente | **0,09** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,35 | 0,76 | 1 | Normal | **0,27** | 0,45 | 0,80 | 1 | Normal | **0,36** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,75 | 10 | Frecuente | **0,26** | 0,35 | 0,80 | 1 | Normal | **0,28** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,80 | 1 | Normal | **0,10** | 0,12 | 0,85 | 1 | Normal | **0,10** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | | | | | | 0,12 | 0,88 | 1 | Normal | **0,11** |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | | | | | | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | | | | | | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | | | | | | 0,15 | 0,80 | 0,10 | Poco frecuente | **0,12** |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | | | | | | 0,22 | 0,68 | 10 | Frecuente | **0,15** |
| **E.25** Pérdida de equipos | 0,15 | 0,80 | 0,10 | Poco frecuente | **0,12** | 0,15 | 0,85 | 0,10 | Poco frecuente | **0,13** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | | | | | | 0,15 | 0,45 | 0,10 | Poco frecuente | **0,07** |
| **A.6** Abuso de Privilegios de Acceso | | | | | | 0,15 | 0,45 | 0,10 | Poco frecuente | **0,07** |
| **A.7** Uso no previsto | | | | | | | | | | |
| **A.11** Acceso no Autorizado | | | | | | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | | | | | | 0,15 | 0,85 | 0,10 | Poco frecuente | **0,13** |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | | | | | | 0,15 | 0,78 | 0,10 | Poco frecuente | **0,12** |
| **A.24** Denegación de servicio (Saturación del sistema informático) | | | | | | 0,15 | 0,72 | 10 | Frecuente | **0,11** |
| **A.25** Robo (Pérdida de Equipos) | 0,07 | 0,75 | 0,10 | Poco frecuente | **0,05** | 0,07 | 0,85 | 0,10 | Poco frecuente | **0,06** |
| **A.26** Ataque destructivo | 0,05 | 0,65 | 0,10 | Poco frecuente | **0,03** | 0,05 | 0,65 | 0,10 | Poco frecuente | **0,03** |

| AMENAZAS | ROUTERS INALAMBRICOS | | | | | SWITCH | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,15 | 0,60 | 0,10 | Poco frecuente | **0,09** | 0,15 | 0,60 | 0,10 | Poco frecuente | **0,09** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,30 | 0,75 | 1 | Normal | **0,23** | 0,30 | 0,75 | 1 | Normal | **0,23** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,27 | 0,70 | 0,10 | Poco frecuente | **0,19** | 0,27 | 0,70 | 0,10 | Poco frecuente | **0,19** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,80 | 1 | Normal | **0,28** | 0,35 | 0,80 | 1 | Normal | **0,28** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,75 | 1 | Normal | **0,09** | 0,12 | 0,75 | 1 | Normal | **0,09** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | 0,12 | 0,88 | 1 | Normal | **0,11** | 0,12 | 0,88 | 1 | Normal | **0,11** |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | 0,10 | 0,62 | 0,10 | Poco frecuente | **0,06** | 0,10 | 0,62 | 0,10 | Poco frecuente | **0,06** |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | 0,22 | 0,68 | 10 | Frecuente | **0,15** | 0,22 | 0,68 | 10 | Frecuente | **0,15** |
| **E.25** Pérdida de equipos | 0,15 | 0,90 | 0,10 | Poco frecuente | **0,14** | 0,15 | 0,90 | 0,10 | Poco frecuente | **0,14** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** |
| **A.6** Abuso de Privilegios de Acceso | 0,15 | 0,45 | 0,10 | Poco frecuente | **0,07** | 0,15 | 0,45 | 0,10 | Poco frecuente | **0,07** |
| **A.7** Uso no previsto | 0,18 | 0,60 | 0,10 | Poco frecuente | **0,11** | 0,18 | 0,60 | 0,10 | Poco frecuente | **0,11** |
| **A.11** Acceso no Autorizado | 0,2 | 0,60 | 1 | Normal | **0,12** | 0,2 | 0,60 | 1 | Normal | **0,12** |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | 0,15 | 0,90 | 1 | Normal | **0,14** | 0,15 | 0,90 | 1 | Normal | **0,14** |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | 0,15 | 0,78 | 0,10 | Poco frecuente | **0,12** | 0,15 | 0,78 | 0,10 | Poco frecuente | **0,12** |
| **A.24** Denegación de servicio (Saturación del sistema informático) | 0,15 | 0,72 | 10 | Frecuente | **0,11** | 0,15 | 0,72 | 10 | Frecuente | **0,11** |
| **A.25** Robo (Pérdida de Equipos) | 0,07 | 0,90 | 0,10 | Poco frecuente | **0,06** | 0,07 | 0,90 | 0,10 | Poco frecuente | **0,06** |
| **A.26** Ataque destructivo | 0,05 | 0,65 | 0,10 | Poco frecuente | **0,03** | 0,05 | 0,65 | 0,10 | Poco frecuente | **0,03** |

| AMENAZAS | ACCESS POINT | | | | | PROYECTORES | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** | 0,16 | 0,83 | 0,10 | Poco frecuente | **0,13** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** | 0,12 | 0,75 | 0,10 | Poco frecuente | **0,09** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** | 0,16 | 0,83 | 0,10 | Poco frecuente | **0,13** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** | 0,12 | 0,75 | 0,10 | Poco frecuente | **0,09** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,15 | 0,60 | 0,10 | Poco frecuente | **0,09** | 0,30 | 0,79 | 10 | Frecuente | **0,24** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,30 | 0,75 | 1 | Normal | **0,23** | 0,15 | 0,58 | 0,10 | Poco frecuente | **0,09** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,27 | 0,70 | 0,10 | Poco frecuente | **0,19** | 0,45 | 0,80 | 1 | Normal | **0,36** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,80 | 1 | Normal | **0,28** | 0,35 | 0,80 | 1 | Normal | **0,28** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,75 | 1 | Normal | **0,09** | 0,12 | 0,85 | 1 | Normal | **0,10** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | 0,12 | 0,88 | 1 | Normal | **0,11** | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | 0,10 | 0,62 | 0,10 | Poco frecuente | **0,06** | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | 0,22 | 0,68 | 10 | Frecuente | **0,15** | | | | | |
| **E.25** Pérdida de equipos | 0,15 | 0,90 | 0,10 | Poco frecuente | **0,14** | 0,15 | 0,90 | 0,10 | Poco frecuente | **0,14** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** | | | | | |
| **A.6** Abuso de Privilegios de Acceso | 0,15 | 0,45 | 0,10 | Poco frecuente | **0,07** | | | | | |
| **A.7** Uso no previsto | 0,18 | 0,60 | 0,10 | Poco frecuente | **0,11** | | | | | |
| **A.11** Acceso no Autorizado | 0,2 | 0,60 | 1 | Normal | **0,12** | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | 0,15 | 0,90 | 1 | Normal | **0,14** | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | 0,15 | 0,78 | 0,10 | Poco frecuente | **0,12** | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | 0,15 | 0,72 | 10 | Frecuente | **0,11** | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,07 | 0,90 | 0,10 | Poco frecuente | **0,06** | 0,07 | 0,90 | 0,10 | Poco frecuente | **0,06** |
| **A.26** Ataque destructivo | 0,05 | 0,65 | 0,10 | Poco frecuente | **0,03** | 0,05 | 0,75 | 0,10 | Poco frecuente | **0,04** |

| AMENAZAS | BIOMÉTRICOS | | | | |
|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | |
| **N.1** Fuego (Incendios) | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** |
| **N.2** Daños por agua (Inundaciones) | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,65 | 0,10 | Poco Frecuente | **0,08** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | |
| **I.1** Fuego (Incendios) | 0,15 | 0,75 | 0,10 | Poco Frecuente | **0,11** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,65 | 0,10 | Poco Frecuente | **0,08** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,06 | 0,45 | 0,10 | Poco Frecuente | **0,03** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,10 | 0,75 | 1 | Normal | **0,08** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,35 | 0,85 | 1 | Normal | **0,30** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,75 | 1 | Normal | **0,26** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,35 | 0,78 | 1 | Normal | **0,27** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | 0,12 | 0,88 | 1 | Normal | **0,11** |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | |
| **E.2** Errores de Administrador | 0,08 | 0,72 | 0,10 | Poco frecuente | **0,06** |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | 0,10 | 0,62 | 0,10 | Poco frecuente | **0,06** |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | 0,22 | 0,68 | 10 | Frecuente | **0,15** |
| **E.25** Pérdida de equipos | 0,15 | 0,80 | 1 | Normal | **0,12** |
| **ATAQUES INTENCIONADOS (A)** | | | | | |
| **A.5** Suplantación de la identidad del usuario | 0,15 | 0,75 | 1 | Normal | **0,11** |
| **A.6** Abuso de Privilegios de Acceso | 0,15 | 0,85 | 1 | Normal | **0,13** |
| **A.7** Uso no previsto | 0,18 | 0,60 | 0,10 | Poco frecuente | **0,11** |
| **A.11** Acceso no Autorizado | 0,2 | 0,80 | 1 | Normal | **0,16** |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | 0,14 | 0,87 | 1 | Normal | **0,12** |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | 0,14 | 0,66 | 1 | Normal | **0,09** |
| **A.24** Denegación de servicio (Saturación del sistema informático) | 0,22 | 0,85 | 1 | Normal | **0,19** |
| **A.25** Robo (Pérdida de Equipos) | 0,15 | 0,75 | 0,10 | Poco Frecuente | **0,11** |
| **A.26** Ataque destructivo | 0,15 | 0,75 | 0,10 | Poco Frecuente | **0,11** |

**Cuadro 4.6.** Servicio: laboratorios

| AMENAZAS | CPU | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | DAÑO EN EL DISCO DURO | | | | | DAÑO EN LA FUENTE DE PODER | | | | |
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,83 | 1/100 | Muy Poco frecuente | **0,08** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,90 | 1/100 | Muy Poco frecuente | **0,09** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,20 | 0,60 | 0,10 | Poco frecuente | **0,12** | 0,20 | 0,70 | 0,10 | Poco frecuente | **0,14** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,25 | 0,55 | 1 | Normal | **0,14** | 0,35 | 0,80 | 1 | Normal | **0,28** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,30 | 0,60 | 1 | Normal | **0,18** | 0,45 | 0,75 | 1 | Normal | **0,34** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,45 | 0,70 | 1 | Normal | **0,32** | 0,45 | 0,90 | 1 | Normal | **0,41** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,50 | 0,75 | 10 | Frecuente | **0,38** | 0,50 | 0,90 | 10 | Frecuente | **0,45** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,10 | 0,45 | 0,10 | Poco frecuente | **0,05** | 0,10 | 0,45 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,60 | 1 | Normal | **0,07** | 0,12 | 0,60 | 1 | Normal | **0,07** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | 0,50 | 0,75 | 1 | Normal | **0,38** | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | 0,05 | 0,60 | 1 | Normal | **0,03** | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | 0,05 | 0,60 | 1 | Normal | **0,03** | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,25 | 0,80 | 1 | Normal | **0,20** | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | 0,60 | 0,65 | 10 | Frecuente | **0,39** | | | | | |
| **E.25** Pérdida de equipos | 0,45 | 0,80 | 0,10 | Poco frecuente | **0,36** | 0,45 | 0,80 | 0,10 | Poco frecuente | **0,36** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** | | | | | |
| **A.6** Abuso de Privilegios de Acceso | 0,05 | 0,50 | 0,10 | Poco frecuente | **0,03** | | | | | |
| **A.7** Uso no previsto | 0,05 | 0,40 | 0,10 | Poco frecuente | **0,02** | | | | | |
| **A.11** Acceso no Autorizado | 0,10 | 0,80 | 0,10 | Poco frecuente | **0,08** | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | 0,15 | 0,76 | 0,10 | Poco frecuente | **0,11** | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | 0,05 | 0,83 | 0,10 | Poco frecuente | **0,04** | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | 0,35 | 0,75 | 1 | Normal | **0,26** | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** |
| **A.26** Ataque destructivo | 0,05 | 0,75 | 0,10 | Poco frecuente | **0,04** | 0,05 | 0,90 | 0,10 | Poco frecuente | **0,05** |

| AMENAZAS | CPU | | | | | MONITOR | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | DAÑO EN LA MEMORIA RAM | | | | | | | | | |
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,65 | 0,10 | Poco frecuente | **0,10** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,90 | 1/100 | Muy Poco frecuente | **0,09** | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,18 | 0,70 | 0,10 | Poco frecuente | **0,13** | 0,15 | 0,60 | 0,10 | Poco frecuente | **0,09** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,40 | 0,75 | 1 | Normal | **0,30** | 0,08 | 0,45 | 0,10 | Poco frecuente | **0,04** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,30 | 0,60 | 1 | Normal | **0,18** | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,45 | 0,90 | 1 | Normal | **0,41** | 0,45 | 0,70 | 1 | Normal | **0,32** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,50 | 0,73 | 10 | Frecuente | **0,37** | 0,40 | 0,68 | 10 | Frecuente | **0,27** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,10 | 0,45 | 0,10 | Poco frecuente | **0,05** | 0,10 | 0,45 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,60 | 1 | Normal | **0,07** | 0,12 | 0,75 | 1 | Normal | **0,09** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | | | | | | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | | | | | | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | | | | | | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | | | | | | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | | | | | | | | | | |
| **E.25** Pérdida de equipos | 0,45 | 0,80 | 0,10 | Poco frecuente | **0,36** | 0,25 | 0,85 | 0,10 | Poco frecuente | **0,21** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | | | | | | | | | | |
| **A.6** Abuso de Privilegios de Acceso | | | | | | | | | | |
| **A.7** Uso no previsto | | | | | | | | | | |
| **A.11** Acceso no Autorizado | | | | | | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | | | | | | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | | | | | | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | | | | | | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** | 0,05 | 0,85 | 0,10 | Poco frecuente | **0,04** |
| **A.26** Ataque destructivo | 0,05 | 0,90 | 0,10 | Poco frecuente | **0,05** | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** |

| AMENAZAS | COMPUTADORAS TODO EN UNO | | | | | MOUSE | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,85 | 1/100 | Muy Poco frecuente | **0,09** | 0,10 | 0,65 | 1/100 | Muy Poco frecuente | **0,07** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,83 | 0,10 | Poco frecuente | **0,13** | 0,16 | 0,68 | 0,10 | Poco frecuente | **0,11** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,75 | 0,10 | Poco frecuente | **0,09** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,85 | 1/100 | Muy Poco frecuente | **0,09** | 0,10 | 0,65 | 1/100 | Muy Poco frecuente | **0,07** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,16 | 0,83 | 0,10 | Poco frecuente | **0,13** | 0,16 | 0,68 | 0,10 | Poco frecuente | **0,11** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,75 | 0,10 | Poco frecuente | **0,09** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,30 | 0,79 | 10 | Frecuente | **0,24** | 0,10 | 0,50 | 1 | Normal | **0,05** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,15 | 0,58 | 0,10 | Poco frecuente | **0,09** | 0,15 | 0,58 | 0,10 | Poco frecuente | **0,09** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,45 | 0,80 | 1 | Normal | **0,36** | 0,35 | 0,72 | 1 | Normal | **0,25** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,80 | 1 | Normal | **0,28** | 0,35 | 0,70 | 10 | Frecuente | **0,25** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,85 | 1 | Normal | **0,10** | 0,12 | 0,75 | 1 | Normal | **0,09** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | 0,12 | 0,88 | 1 | Normal | **0,11** | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | | | | | | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,15 | 0,80 | 0,10 | Poco frecuente | **0,12** | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | 0,22 | 0,68 | 10 | Frecuente | **0,15** | | | | | |
| **E.25** Pérdida de equipos | 0,15 | 0,90 | 0,10 | Poco frecuente | **0,14** | 0,15 | 0,75 | 0,10 | Poco frecuente | **0,11** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | 0,15 | 0,45 | 0,10 | Poco frecuente | **0,07** | | | | | |
| **A.6** Abuso de Privilegios de Acceso | 0,15 | 0,45 | 0,10 | Poco frecuente | **0,07** | | | | | |
| **A.7** Uso no previsto | | | | | | | | | | |
| **A.11** Acceso no Autorizado | | | | | | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | 0,15 | 0,90 | 0,10 | Poco frecuente | **0,14** | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | 0,15 | 0,78 | 0,10 | Poco frecuente | **0,12** | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | 0,15 | 0,72 | 10 | Frecuente | **0,11** | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,07 | 0,90 | 0,10 | Poco frecuente | **0,06** | 0,07 | 0,65 | 0,10 | Poco frecuente | **0,05** |
| **A.26** Ataque destructivo | 0,05 | 0,65 | 0,10 | Poco frecuente | **0,03** | 0,05 | 0,60 | 0,10 | Poco frecuente | **0,03** |

| AMENAZAS | TECLADO | | | | | PORTÁTILES | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,70 | 1/100 | Muy Poco frecuente | **0,07** | 0,10 | 0,85 | 1/100 | Muy Poco frecuente | **0,09** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** | 0,16 | 0,83 | 0,10 | Poco frecuente | **0,13** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,75 | 0,10 | Poco frecuente | **0,09** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,70 | 1/100 | Muy Poco frecuente | **0,07** | 0,10 | 0,85 | 1/100 | Muy Poco frecuente | **0,09** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** | 0,16 | 0,83 | 0,10 | Poco frecuente | **0,13** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,75 | 0,10 | Poco frecuente | **0,09** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,10 | 0,54 | 1 | Normal | **0,05** | 0,30 | 0,79 | 10 | Frecuente | **0,24** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,15 | 0,58 | 0,10 | Poco frecuente | **0,09** | 0,15 | 0,58 | 0,10 | Poco frecuente | **0,09** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,35 | 0,76 | 1 | Normal | **0,27** | 0,45 | 0,80 | 1 | Normal | **0,36** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,75 | 10 | Frecuente | **0,26** | 0,35 | 0,80 | 1 | Normal | **0,28** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,80 | 1 | Normal | **0,10** | 0,12 | 0,85 | 1 | Normal | **0,10** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | | | | | | 0,12 | 0,88 | 1 | Normal | **0,11** |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | | | | | | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | | | | | | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | | | | | | 0,15 | 0,80 | 0,10 | Poco frecuente | **0,12** |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | | | | | | 0,22 | 0,68 | 10 | Frecuente | **0,15** |
| **E.25** Pérdida de equipos | 0,15 | 0,80 | 0,10 | Poco frecuente | **0,12** | 0,15 | 0,90 | 0,10 | Poco frecuente | **0,14** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | | | | | | 0,15 | 0,45 | 0,10 | Poco frecuente | **0,07** |
| **A.6** Abuso de Privilegios de Acceso | | | | | | 0,15 | 0,45 | 0,10 | Poco frecuente | **0,07** |
| **A.7** Uso no previsto | | | | | | | | | | |
| **A.11** Acceso no Autorizado | | | | | | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | | | | | | 0,15 | 0,85 | 0,10 | Poco frecuente | **0,13** |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | | | | | | 0,15 | 0,78 | 0,10 | Poco frecuente | **0,12** |
| **A.24** Denegación de servicio (Saturación del sistema informático) | | | | | | 0,15 | 0,72 | 10 | Frecuente | **0,11** |
| **A.25** Robo (Pérdida de Equipos) | 0,07 | 0,75 | 0,10 | Poco frecuente | **0,05** | 0,07 | 0,90 | 0,10 | Poco frecuente | **0,06** |
| **A.26** Ataque destructivo | 0,05 | 0,65 | 0,10 | Poco frecuente | **0,03** | 0,05 | 0,75 | 0,10 | Poco frecuente | **0,04** |

| AMENAZAS | ROUTERS INALAMBRICOS | | | | | SWITCH | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,15 | 0,60 | 0,10 | Poco frecuente | **0,09** | 0,15 | 0,60 | 0,10 | Poco frecuente | **0,09** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,30 | 0,75 | 1 | Normal | **0,23** | 0,30 | 0,75 | 1 | Normal | **0,23** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,27 | 0,70 | 0,10 | Poco frecuente | **0,19** | 0,27 | 0,70 | 0,10 | Poco frecuente | **0,19** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,80 | 1 | Normal | **0,28** | 0,35 | 0,80 | 1 | Normal | **0,28** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,75 | 1 | Normal | **0,09** | 0,12 | 0,75 | 1 | Normal | **0,09** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | 0,12 | 0,88 | 1 | Normal | **0,11** | 0,12 | 0,88 | 1 | Normal | **0,11** |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | 0,10 | 0,62 | 0,10 | Poco frecuente | **0,06** | 0,10 | 0,62 | 0,10 | Poco frecuente | **0,06** |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | 0,22 | 0,68 | 10 | Frecuente | **0,15** | 0,22 | 0,68 | 10 | Frecuente | **0,15** |
| **E.25** Pérdida de equipos | 0,15 | 0,90 | 0,10 | Poco frecuente | **0,14** | 0,15 | 0,90 | 0,10 | Poco frecuente | **0,14** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** |
| **A.6** Abuso de Privilegios de Acceso | 0,15 | 0,45 | 0,10 | Poco frecuente | **0,07** | 0,15 | 0,45 | 0,10 | Poco frecuente | **0,07** |
| **A.7** Uso no previsto | 0,18 | 0,60 | 0,10 | Poco frecuente | **0,11** | 0,18 | 0,60 | 0,10 | Poco frecuente | **0,11** |
| **A.11** Acceso no Autorizado | 0,2 | 0,60 | 1 | Normal | **0,12** | 0,2 | 0,60 | 1 | Normal | **0,12** |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | 0,15 | 0,85 | 1 | Normal | **0,13** | 0,15 | 0,90 | 1 | Normal | **0,14** |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | 0,15 | 0,78 | 0,10 | Poco frecuente | **0,12** | 0,15 | 0,78 | 0,10 | Poco frecuente | **0,12** |
| **A.24** Denegación de servicio (Saturación del sistema informático) | 0,15 | 0,72 | 10 | Frecuente | **0,11** | 0,15 | 0,72 | 10 | Frecuente | **0,11** |
| **A.25** Robo (Pérdida de Equipos) | 0,07 | 0,90 | 0,10 | Poco frecuente | **0,06** | 0,07 | 0,90 | 0,10 | Poco frecuente | **0,06** |
| **A.26** Ataque destructivo | 0,05 | 0,65 | 0,10 | Poco frecuente | **0,03** | 0,05 | 0,65 | 0,10 | Poco frecuente | **0,03** |

| AMENAZAS | ACCESS POINT | | | | | PROYECTORES | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** | 0,16 | 0,83 | 0,10 | Poco frecuente | **0,13** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** | 0,12 | 0,75 | 0,10 | Poco frecuente | **0,09** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** | 0,16 | 0,83 | 0,10 | Poco frecuente | **0,13** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** | 0,12 | 0,75 | 0,10 | Poco frecuente | **0,09** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,15 | 0,60 | 0,10 | Poco frecuente | **0,09** | 0,30 | 0,79 | 10 | Frecuente | **0,24** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,30 | 0,75 | 1 | Normal | **0,23** | 0,15 | 0,58 | 0,10 | Poco frecuente | **0,09** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,27 | 0,70 | 0,10 | Poco frecuente | **0,19** | 0,45 | 0,80 | 1 | Normal | **0,36** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,80 | 1 | Normal | **0,28** | 0,35 | 0,80 | 1 | Normal | **0,28** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,75 | 1 | Normal | **0,09** | 0,12 | 0,85 | 1 | Normal | **0,10** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | 0,12 | 0,88 | 1 | Normal | **0,11** | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | 0,10 | 0,62 | 0,10 | Poco frecuente | **0,06** | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | 0,22 | 0,68 | 10 | Frecuente | **0,15** | | | | | |
| **E.25** Pérdida de equipos | 0,15 | 0,90 | 0,10 | Poco frecuente | **0,14** | 0,15 | 0,90 | 0,10 | Poco frecuente | **0,14** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** | | | | | |
| **A.6** Abuso de Privilegios de Acceso | 0,15 | 0,45 | 0,10 | Poco frecuente | **0,07** | | | | | |
| **A.7** Uso no previsto | 0,18 | 0,60 | 0,10 | Poco frecuente | **0,11** | | | | | |
| **A.11** Acceso no Autorizado | 0,2 | 0,60 | 1 | Normal | **0,12** | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | 0,15 | 0,90 | 1 | Normal | **0,14** | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | 0,15 | 0,78 | 0,10 | Poco frecuente | **0,12** | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | 0,15 | 0,72 | 10 | Frecuente | **0,11** | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,07 | 0,90 | 0,10 | Poco frecuente | **0,06** | 0,07 | 0,90 | 0,10 | Poco frecuente | **0,06** |
| **A.26** Ataque destructivo | 0,05 | 0,65 | 0,10 | Poco frecuente | **0,03** | 0,05 | 0,75 | 0,10 | Poco frecuente | **0,04** |

| AMENAZAS | BIOMÉTRICOS | | | | |
|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | |
| **N.1** Fuego (Incendios) | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** |
| **N.2** Daños por agua (Inundaciones) | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,65 | 0,10 | Poco Frecuente | **0,08** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | |
| **I.1** Fuego (Incendios) | 0,15 | 0,75 | 0,10 | Poco Frecuente | **0,11** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,65 | 0,10 | Poco Frecuente | **0,08** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,06 | 0,45 | 0,10 | Poco Frecuente | **0,03** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,10 | 0,75 | 1 | Normal | **0,08** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,35 | 0,85 | 1 | Normal | **0,30** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,75 | 1 | Normal | **0,26** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,35 | 0,78 | 1 | Normal | **0,27** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | 0,12 | 0,88 | 1 | Normal | **0,11** |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | |
| **E.2** Errores de Administrador | 0,08 | 0,72 | 0,10 | Poco frecuente | **0,06** |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | 0,10 | 0,62 | 0,10 | Poco frecuente | **0,06** |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | 0,22 | 0,68 | 10 | Frecuente | **0,15** |
| **E.25** Pérdida de equipos | 0,15 | 0,80 | 1 | Normal | **0,12** |
| **ATAQUES INTENCIONADOS (A)** | | | | | |
| **A.5** Suplantación de la identidad del usuario | 0,15 | 0,75 | 1 | Normal | **0,11** |
| **A.6** Abuso de Privilegios de Acceso | 0,15 | 0,85 | 1 | Normal | **0,13** |
| **A.7** Uso no previsto | 0,18 | 0,60 | 0,10 | Poco frecuente | **0,11** |
| **A.11** Acceso no Autorizado | 0,2 | 0,80 | 1 | Normal | **0,16** |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | 0,14 | 0,87 | 1 | Normal | **0,12** |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | 0,14 | 0,66 | 1 | Normal | **0,09** |
| **A.24** Denegación de servicio (Saturación del sistema informático) | 0,22 | 0,85 | 1 | Normal | **0,19** |
| **A.25** Robo (Pérdida de Equipos) | 0,15 | 0,75 | 0,10 | Poco Frecuente | **0,11** |
| **A.26** Ataque destructivo | 0,15 | 0,75 | 0,10 | Poco Frecuente | **0,11** |

**Cuadro 4.7**. Servicio: aulas de clases

| AMENAZAS | PROYECTORES | | | | | ROUTERS INALAMBRICOS | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,83 | 0,10 | Poco frecuente | **0,13** | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,75 | 0,10 | Poco frecuente | **0,09** | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,16 | 0,83 | 0,10 | Poco frecuente | **0,13** | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,75 | 0,10 | Poco frecuente | **0,09** | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,30 | 0,79 | 10 | Frecuente | **0,24** | 0,15 | 0,60 | 0,10 | Poco frecuente | **0,09** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,15 | 0,58 | 0,10 | Poco frecuente | **0,09** | 0,30 | 0,75 | 1 | Normal | **0,23** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,45 | 0,80 | 1 | Normal | **0,36** | 0,27 | 0,70 | 0,10 | Poco frecuente | **0,19** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,80 | 1 | Normal | **0,28** | 0,35 | 0,80 | 1 | Normal | **0,28** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,85 | 1 | Normal | **0,10** | 0,12 | 0,75 | 1 | Normal | **0,09** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | | | | | | 0,12 | 0,88 | 1 | Normal | **0,11** |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | | | | | | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | | | | | | 0,10 | 0,62 | 0,10 | Poco frecuente | **0,06** |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | | | | | | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | | | | | | 0,22 | 0,68 | 10 | Frecuente | **0,15** |
| **E.25** Pérdida de equipos | 0,15 | 0,90 | 0,10 | Poco frecuente | **0,14** | 0,15 | 0,90 | 0,10 | Poco frecuente | **0,14** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | | | | | | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** |
| **A.6** Abuso de Privilegios de Acceso | | | | | | 0,15 | 0,45 | 0,10 | Poco frecuente | **0,07** |
| **A.7** Uso no previsto | | | | | | 0,18 | 0,60 | 0,10 | Poco frecuente | **0,11** |
| **A.11** Acceso no Autorizado | | | | | | 0,2 | 0,60 | 1 | Normal | **0,12** |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | | | | | | 0,15 | 0,85 | 1 | Normal | **0,13** |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | | | | | | 0,15 | 0,78 | 0,10 | Poco frecuente | **0,12** |
| **A.24** Denegación de servicio (Saturación del sistema informático) | | | | | | 0,15 | 0,72 | 10 | Frecuente | **0,11** |
| **A.25** Robo (Pérdida de Equipos) | 0,07 | 0,90 | 0,10 | Poco frecuente | **0,06** | 0,07 | 0,90 | 0,10 | Poco frecuente | **0,06** |
| **A.26** Ataque destructivo | 0,05 | 0,75 | 0,10 | Poco frecuente | **0,04** | 0,05 | 0,65 | 0,10 | Poco frecuente | **0,03** |

| AMENAZAS | SWITCH | | | | | ACCESS POINT | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,15 | 0,60 | 0,10 | Poco frecuente | **0,09** | 0,15 | 0,60 | 0,10 | Poco frecuente | **0,09** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,30 | 0,75 | 1 | Normal | **0,23** | 0,30 | 0,75 | 1 | Normal | **0,23** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,27 | 0,70 | 0,10 | Poco frecuente | **0,19** | 0,27 | 0,70 | 0,10 | Poco frecuente | **0,19** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,80 | 1 | Normal | **0,28** | 0,35 | 0,80 | 1 | Normal | **0,28** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,75 | 1 | Normal | **0,09** | 0,12 | 0,75 | 1 | Normal | **0,09** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | 0,12 | 0,88 | 1 | Normal | **0,11** | 0,12 | 0,88 | 1 | Normal | **0,11** |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | 0,10 | 0,62 | 0,10 | Poco frecuente | **0,06** | 0,10 | 0,62 | 0,10 | Poco frecuente | **0,06** |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | 0,22 | 0,68 | 10 | Frecuente | **0,15** | 0,22 | 0,68 | 10 | Frecuente | **0,15** |
| **E.25** Pérdida de equipos | 0,15 | 0,90 | 0,10 | Poco frecuente | **0,14** | 0,15 | 0,90 | 0,10 | Poco frecuente | **0,14** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** |
| **A.6** Abuso de Privilegios de Acceso | 0,15 | 0,45 | 0,10 | Poco frecuente | **0,07** | 0,15 | 0,45 | 0,10 | Poco frecuente | **0,07** |
| **A.7** Uso no previsto | 0,18 | 0,60 | 0,10 | Poco frecuente | **0,11** | 0,18 | 0,60 | 0,10 | Poco frecuente | **0,11** |
| **A.11** Acceso no Autorizado | 0,2 | 0,60 | 1 | Normal | **0,12** | 0,20 | 0,60 | 1 | Normal | **0,12** |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | 0,15 | 0,90 | 1 | Normal | **0,14** | 0,15 | 0,90 | 1 | Normal | **0,14** |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | 0,15 | 0,78 | 0,10 | Poco frecuente | **0,12** | 0,15 | 0,78 | 0,10 | Poco frecuente | **0,12** |
| **A.24** Denegación de servicio (Saturación del sistema informático) | 0,15 | 0,72 | 10 | Frecuente | **0,11** | 0,15 | 0,72 | 10 | Frecuente | **0,11** |
| **A.25** Robo (Pérdida de Equipos) | 0,07 | 0,90 | 0,10 | Poco frecuente | **0,06** | 0,07 | 0,90 | 0,10 | Poco frecuente | **0,06** |
| **A.26** Ataque destructivo | 0,05 | 0,65 | 0,10 | Poco frecuente | **0,03** | 0,05 | 0,65 | 0,10 | Poco frecuente | **0,03** |

| AMENAZAS | BIOMÉTRICOS | | | | |
|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | |
| **N.1** Fuego (Incendios) | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** |
| **N.2** Daños por agua (Inundaciones) | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,65 | 0,10 | Poco Frecuente | **0,08** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | |
| **I.1** Fuego (Incendios) | 0,15 | 0,75 | 0,10 | Poco Frecuente | **0,11** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,65 | 0,10 | Poco Frecuente | **0,08** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,06 | 0,45 | 0,10 | Poco Frecuente | **0,03** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,10 | 0,75 | 1 | Normal | **0,08** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,35 | 0,85 | 1 | Normal | **0,30** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,75 | 1 | Normal | **0,26** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,35 | 0,78 | 1 | Normal | **0,27** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | 0,12 | 0,88 | 1 | Normal | **0,11** |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | |
| **E.2** Errores de Administrador | 0,08 | 0,72 | 0,10 | Poco frecuente | **0,06** |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | 0,10 | 0,62 | 0,10 | Poco frecuente | **0,06** |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | 0,22 | 0,68 | 10 | Frecuente | **0,15** |
| **E.25** Pérdida de equipos | 0,15 | 0,80 | 1 | Normal | **0,12** |
| **ATAQUES INTENCIONADOS (A)** | | | | | |
| **A.5** Suplantación de la identidad del usuario | 0,15 | 0,75 | 1 | Normal | **0,11** |
| **A.6** Abuso de Privilegios de Acceso | 0,15 | 0,85 | 1 | Normal | **0,13** |
| **A.7** Uso no previsto | 0,18 | 0,60 | 0,10 | Poco frecuente | **0,11** |
| **A.11** Acceso no Autorizado | 0,2 | 0,80 | 1 | Normal | **0,16** |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | 0,14 | 0,87 | 1 | Normal | **0,12** |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | 0,14 | 0,66 | 1 | Normal | **0,09** |
| **A.24** Denegación de servicio (Saturación del sistema informático) | 0,22 | 0,85 | 1 | Normal | **0,19** |
| **A.25** Robo (Pérdida de Equipos) | 0,15 | 0,75 | 0,10 | Poco Frecuente | **0,11** |
| **A.26** Ataque destructivo | 0,15 | 0,75 | 0,10 | Poco Frecuente | **0,11** |

**Cuadro 4.8**. Servicio: coordinacion investigacion cientifica, emprendimiento, dirección de planificación, diseño e ingeniería

| AMENAZAS | CPU | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | DAÑO EN EL DISCO DURO | | | | | DAÑO EN LA FUENTE DE PODER | | | | |
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,83 | 1/100 | Muy Poco frecuente | **0,08** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,90 | 1/100 | Muy Poco frecuente | **0,09** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,20 | 0,60 | 0,10 | Poco frecuente | **0,12** | 0,20 | 0,70 | 0,10 | Poco frecuente | **0,14** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,25 | 0,55 | 1 | Normal | **0,14** | 0,35 | 0,80 | 1 | Normal | **0,28** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,30 | 0,60 | 1 | Normal | **0,18** | 0,45 | 0,75 | 1 | Normal | **0,34** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,45 | 0,70 | 1 | Normal | **0,32** | 0,45 | 0,90 | 1 | Normal | **0,41** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,50 | 0,75 | 10 | Frecuente | **0,38** | 0,50 | 0,90 | 10 | Frecuente | **0,45** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,10 | 0,45 | 0,10 | Poco frecuente | **0,05** | 0,10 | 0,45 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,60 | 1 | Normal | **0,07** | 0,12 | 0,60 | 1 | Normal | **0,07** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | 0,50 | 0,75 | 1 | Normal | **0,38** | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | 0,05 | 0,60 | 1 | Normal | **0,03** | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | 0,05 | 0,60 | 1 | Normal | **0,03** | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,25 | 0,80 | 1 | Normal | **0,20** | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | 0,60 | 0,65 | 10 | Frecuente | **0,39** | | | | | |
| **E.25** Pérdida de equipos | 0,45 | 0,80 | 0,10 | Poco frecuente | **0,36** | 0,45 | 0,80 | 0,10 | Poco frecuente | **0,36** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** | | | | | |
| **A.6** Abuso de Privilegios de Acceso | 0,05 | 0,50 | 0,10 | Poco frecuente | **0,03** | | | | | |
| **A.7** Uso no previsto | 0,05 | 0,40 | 0,10 | Poco frecuente | **0,02** | | | | | |
| **A.11** Acceso no Autorizado | 0,10 | 0,80 | 0,10 | Poco frecuente | **0,08** | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | 0,15 | 0,76 | 0,10 | Poco frecuente | **0,11** | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | 0,05 | 0,83 | 0,10 | Poco frecuente | **0,04** | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | 0,35 | 0,75 | 1 | Normal | **0,26** | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** |
| **A.26** Ataque destructivo | 0,05 | 0,75 | 0,10 | Poco frecuente | **0,04** | 0,05 | 0,90 | 0,10 | Poco frecuente | **0,05** |

| AMENAZAS | CPU | | | | | MONITOR | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | DAÑO EN LA MEMORIA RAM | | | | | | | | | |
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,65 | 0,10 | Poco frecuente | **0,10** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,90 | 1/100 | Muy Poco frecuente | **0,09** | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,18 | 0,70 | 0,10 | Poco frecuente | **0,13** | 0,15 | 0,60 | 0,10 | Poco frecuente | **0,09** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,40 | 0,75 | 1 | Normal | **0,30** | 0,08 | 0,45 | 0,10 | Poco frecuente | **0,04** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,30 | 0,60 | 1 | Normal | **0,18** | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,45 | 0,90 | 1 | Normal | **0,41** | 0,45 | 0,70 | 1 | Normal | **0,32** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,50 | 0,73 | 10 | Frecuente | **0,37** | 0,40 | 0,68 | 10 | Frecuente | **0,27** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,10 | 0,45 | 0,10 | Poco frecuente | **0,05** | 0,10 | 0,45 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,60 | 1 | Normal | **0,07** | 0,12 | 0,75 | 1 | Normal | **0,09** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | | | | | | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | | | | | | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | | | | | | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | | | | | | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | | | | | | | | | | |
| **E.25** Pérdida de equipos | 0,45 | 0,80 | 0,10 | Poco frecuente | **0,36** | 0,25 | 0,85 | 0,10 | Poco frecuente | **0,21** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | | | | | | | | | | |
| **A.6** Abuso de Privilegios de Acceso | | | | | | | | | | |
| **A.7** Uso no previsto | | | | | | | | | | |
| **A.11** Acceso no Autorizado | | | | | | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | | | | | | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | | | | | | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | | | | | | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** | 0,05 | 0,85 | 0,10 | Poco frecuente | **0,04** |
| **A.26** Ataque destructivo | 0,05 | 0,90 | 0,10 | Poco frecuente | **0,05** | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** |

| AMENAZAS | COMPUTADORAS TODO EN UNO | | | | | MOUSE | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,85 | 1/100 | Muy Poco frecuente | **0,09** | 0,10 | 0,65 | 1/100 | Muy Poco frecuente | **0,07** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,83 | 0,10 | Poco frecuente | **0,13** | 0,16 | 0,68 | 0,10 | Poco frecuente | **0,11** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,75 | 0,10 | Poco frecuente | **0,09** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,85 | 1/100 | Muy Poco frecuente | **0,09** | 0,10 | 0,65 | 1/100 | Muy Poco frecuente | **0,07** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,16 | 0,83 | 0,10 | Poco frecuente | **0,13** | 0,16 | 0,68 | 0,10 | Poco frecuente | **0,11** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,75 | 0,10 | Poco frecuente | **0,09** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,30 | 0,79 | 10 | Frecuente | **0,24** | 0,10 | 0,50 | 1 | Normal | **0,05** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,15 | 0,58 | 0,10 | Poco frecuente | **0,09** | 0,15 | 0,58 | 0,10 | Poco frecuente | **0,09** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,45 | 0,80 | 1 | Normal | **0,36** | 0,35 | 0,72 | 1 | Normal | **0,25** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,80 | 1 | Normal | **0,28** | 0,35 | 0,70 | 10 | Frecuente | **0,25** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,85 | 1 | Normal | **0,10** | 0,12 | 0,75 | 1 | Normal | **0,09** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | 0,12 | 0,88 | 1 | Normal | **0,11** | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | | | | | | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,15 | 0,80 | 0,10 | Poco frecuente | **0,12** | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | 0,22 | 0,68 | 10 | Frecuente | **0,15** | | | | | |
| **E.25** Pérdida de equipos | 0,15 | 0,90 | 0,10 | Poco frecuente | **0,14** | 0,15 | 0,75 | 0,10 | Poco frecuente | **0,11** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | 0,15 | 0,45 | 0,10 | Poco frecuente | **0,07** | | | | | |
| **A.6** Abuso de Privilegios de Acceso | 0,15 | 0,45 | 0,10 | Poco frecuente | **0,07** | | | | | |
| **A.7** Uso no previsto | | | | | | | | | | |
| **A.11** Acceso no Autorizado | | | | | | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | 0,15 | 0,90 | 0,10 | Poco frecuente | **0,14** | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | 0,15 | 0,78 | 0,10 | Poco frecuente | **0,12** | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | 0,15 | 0,72 | 10 | Frecuente | **0,11** | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,07 | 0,90 | 0,10 | Poco frecuente | **0,06** | 0,07 | 0,65 | 0,10 | Poco frecuente | **0,05** |
| **A.26** Ataque destructivo | 0,05 | 0,65 | 0,10 | Poco frecuente | **0,03** | 0,05 | 0,60 | 0,10 | Poco frecuente | **0,03** |

| AMENAZAS | TECLADO | | | | | ROUTERS INALAMBRICOS | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,70 | 1/100 | Muy Poco frecuente | **0,07** | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,70 | 1/100 | Muy Poco frecuente | **0,07** | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,10 | 0,54 | 1 | Normal | **0,05** | 0,15 | 0,60 | 0,10 | Poco frecuente | **0,09** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,15 | 0,58 | 0,10 | Poco frecuente | **0,09** | 0,30 | 0,75 | 1 | Normal | **0,23** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,35 | 0,76 | 1 | Normal | **0,27** | 0,27 | 0,70 | 0,10 | Poco frecuente | **0,19** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,75 | 10 | Frecuente | **0,26** | 0,35 | 0,80 | 1 | Normal | **0,28** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,80 | 1 | Normal | **0,10** | 0,12 | 0,75 | 1 | Normal | **0,09** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | | | | | | 0,12 | 0,88 | 1 | Normal | **0,11** |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | | | | | | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | | | | | | 0,10 | 0,62 | 0,10 | Poco frecuente | **0,06** |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | | | | | | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | | | | | | 0,22 | 0,68 | 10 | Frecuente | **0,15** |
| **E.25** Pérdida de equipos | 0,15 | 0,80 | 0,10 | Poco frecuente | **0,12** | 0,15 | 0,90 | 0,10 | Poco frecuente | **0,14** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | | | | | | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** |
| **A.6** Abuso de Privilegios de Acceso | | | | | | 0,15 | 0,45 | 0,10 | Poco frecuente | **0,07** |
| **A.7** Uso no previsto | | | | | | 0,18 | 0,60 | 0,10 | Poco frecuente | **0,11** |
| **A.11** Acceso no Autorizado | | | | | | 0,2 | 0,60 | 1 | Normal | **0,12** |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | | | | | | 0,15 | 0,85 | 1 | Normal | **0,13** |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | | | | | | 0,15 | 0,78 | 1/10 | Poco frecuente | **0,12** |
| **A.24** Denegación de servicio (Saturación del sistema informático) | | | | | | 0,15 | 0,72 | 10 | Frecuente | **0,11** |
| **A.25** Robo (Pérdida de Equipos) | 0,07 | 0,75 | 0,10 | Poco frecuente | **0,05** | 0,07 | 0,90 | 0,10 | Poco frecuente | **0,06** |
| **A.26** Ataque destructivo | 0,05 | 0,65 | 0,10 | Poco frecuente | **0,03** | 0,05 | 0,65 | 0,10 | Poco frecuente | **0,03** |

| AMENAZAS | PROYECTORES | | | | | IMPRESORA | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,85 | 1/100 | Muy Poco frecuente | **0,09** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,83 | 0,10 | Poco frecuente | **0,13** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,75 | 0,10 | Poco frecuente | **0,09** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,85 | 1/100 | Muy Poco frecuente | **0,09** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,16 | 0,83 | 0,10 | Poco frecuente | **0,13** | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,75 | 0,10 | Poco frecuente | **0,09** | 0,15 | 0,70 | 0,10 | Poco frecuente | **0,11** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,30 | 0,79 | 10 | Frecuente | **0,24** | 0,48 | 0,75 | 10 | Frecuente | **0,36** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,15 | 0,58 | 0,10 | Poco frecuente | **0,09** | 0,23 | 0,70 | 1 | Normal | **0,16** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,45 | 0,80 | 1 | Normal | **0,36** | 0,35 | 0,76 | 1 | Normal | **0,27** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,80 | 1 | Normal | **0,28** | 0,45 | 0,85 | 10 | Frecuente | **0,38** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,85 | 1 | Normal | **0,10** | 0,12 | 0,80 | 1 | Normal | **0,10** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | | | | | | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | | | | | | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | | | | | | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | | | | | | 0,12 | 0,75 | 1 | Normal | **0,09** |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | | | | | | | | | | |
| **E.25** Pérdida de equipos | 0,15 | 0,90 | 0,10 | Poco frecuente | **0,14** | 0,23 | 0,83 | 0,10 | Poco frecuente | **0,19** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | | | | | | | | | | |
| **A.6** Abuso de Privilegios de Acceso | | | | | | | | | | |
| **A.7** Uso no previsto | | | | | | | | | | |
| **A.11** Acceso no Autorizado | | | | | | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | | | | | | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | | | | | | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | | | | | | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,07 | 0,90 | 0,10 | Poco frecuente | **0,06** | 0,07 | 0,85 | 0,10 | Poco frecuente | **0,06** |
| **A.26** Ataque destructivo | 0,05 | 0,75 | 0,10 | Poco frecuente | **0,04** | 0,05 | 0,75 | 0,10 | Poco frecuente | **0,04** |

**Cuadro 4.9**. Servicio: biblioteca

| AMENAZAS | CPU | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | DAÑO EN EL DISCO DURO | | | | | DAÑO EN LA FUENTE DE PODER | | | | |
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,83 | 1/100 | Muy Poco frecuente | **0,08** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,90 | 1/100 | Muy Poco frecuente | **0,09** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,20 | 0,60 | 0,10 | Poco frecuente | **0,12** | 0,20 | 0,70 | 0,10 | Poco frecuente | **0,14** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,25 | 0,55 | 1 | Normal | **0,14** | 0,35 | 0,80 | 1 | Normal | **0,28** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,30 | 0,60 | 1 | Normal | **0,18** | 0,45 | 0,75 | 1 | Normal | **0,34** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,45 | 0,70 | 1 | Normal | **0,32** | 0,45 | 0,90 | 1 | Normal | **0,41** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,50 | 0,75 | 10 | Frecuente | **0,38** | 0,50 | 0,90 | 10 | Frecuente | **0,45** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,10 | 0,45 | 0,10 | Poco frecuente | **0,05** | 0,10 | 0,45 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,60 | 1 | Normal | **0,07** | 0,12 | 0,60 | 1 | Normal | **0,07** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | 0,50 | 0,75 | 1 | Normal | **0,38** | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | 0,05 | 0,60 | 1 | Normal | **0,03** | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | 0,05 | 0,60 | 1 | Normal | **0,03** | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,25 | 0,80 | 1 | Normal | **0,20** | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | 0,60 | 0,65 | 10 | Frecuente | **0,39** | | | | | |
| **E.25** Pérdida de equipos | 0,45 | 0,80 | 0,10 | Poco frecuente | **0,36** | 0,45 | 0,80 | 0,10 | Poco frecuente | **0,36** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** | | | | | |
| **A.6** Abuso de Privilegios de Acceso | 0,05 | 0,50 | 0,10 | Poco frecuente | **0,03** | | | | | |
| **A.7** Uso no previsto | 0,05 | 0,40 | 0,10 | Poco frecuente | **0,02** | | | | | |
| **A.11** Acceso no Autorizado | 0,10 | 0,80 | 0,10 | Poco frecuente | **0,08** | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | 0,15 | 0,76 | 0,10 | Poco frecuente | **0,11** | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | 0,05 | 0,83 | 0,10 | Poco frecuente | **0,04** | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | 0,35 | 0,75 | 1 | Normal | **0,26** | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** |
| **A.26** Ataque destructivo | 0,05 | 0,75 | 0,10 | Poco frecuente | **0,04** | 0,05 | 0,90 | 0,10 | Poco frecuente | **0,05** |

| AMENAZAS | CPU | | | | | MONITOR | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | DAÑO EN LA MEMORIA RAM | | | | | | | | | |
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,65 | 0,10 | Poco frecuente | **0,10** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,90 | 1/100 | Muy Poco frecuente | **0,09** | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,18 | 0,70 | 0,10 | Poco frecuente | **0,13** | 0,15 | 0,60 | 0,10 | Poco frecuente | **0,09** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,40 | 0,75 | 1 | Normal | **0,30** | 0,08 | 0,45 | 0,10 | Poco frecuente | **0,04** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,30 | 0,60 | 1 | Normal | **0,18** | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,45 | 0,90 | 1 | Normal | **0,41** | 0,45 | 0,70 | 1 | Normal | **0,32** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,50 | 0,73 | 10 | Frecuente | **0,37** | 0,40 | 0,68 | 10 | Frecuente | **0,27** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,10 | 0,45 | 0,10 | Poco frecuente | **0,05** | 0,10 | 0,45 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,60 | 1 | Normal | **0,07** | 0,12 | 0,75 | 1 | Normal | **0,09** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | | | | | | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | | | | | | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | | | | | | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | | | | | | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | | | | | | | | | | |
| **E.25** Pérdida de equipos | 0,45 | 0,80 | 0,10 | Poco frecuente | **0,36** | 0,25 | 0,85 | 0,10 | Poco frecuente | **0,21** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | | | | | | | | | | |
| **A.6** Abuso de Privilegios de Acceso | | | | | | | | | | |
| **A.7** Uso no previsto | | | | | | | | | | |
| **A.11** Acceso no Autorizado | | | | | | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | | | | | | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | | | | | | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | | | | | | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** | 0,05 | 0,85 | 0,10 | Poco frecuente | **0,04** |
| **A.26** Ataque destructivo | 0,05 | 0,90 | 0,10 | Poco frecuente | **0,05** | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** |

| AMENAZAS | MOUSE | | | | | TECLADO | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,65 | 1/100 | Muy Poco frecuente | **0,07** | 0,10 | 0,70 | 1/100 | Muy Poco frecuente | **0,07** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,68 | 0,10 | Poco frecuente | **0,11** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,65 | 1/100 | Muy Poco frecuente | **0,07** | 0,10 | 0,70 | 1/100 | Muy Poco frecuente | **0,07** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,16 | 0,68 | 0,10 | Poco frecuente | **0,11** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,10 | 0,50 | 1 | Normal | **0,05** | 0,10 | 0,54 | 1 | Normal | **0,05** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,15 | 0,58 | 0,10 | Poco frecuente | **0,09** | 0,15 | 0,58 | 0,10 | Poco frecuente | **0,09** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,35 | 0,72 | 1 | Normal | **0,25** | 0,35 | 0,76 | 1 | Normal | **0,27** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,70 | 10 | Frecuente | **0,25** | 0,35 | 0,75 | 10 | Frecuente | **0,26** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,75 | 1 | Normal | **0,09** | 0,12 | 0,80 | 1 | Normal | **0,10** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | | | | | | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | | | | | | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | | | | | | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | | | | | | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | | | | | | | | | | |
| **E.25** Pérdida de equipos | 0,15 | 0,75 | 0,10 | Poco frecuente | **0,11** | 0,15 | 0,80 | 0,10 | Poco frecuente | **0,12** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | | | | | | | | | | |
| **A.6** Abuso de Privilegios de Acceso | | | | | | | | | | |
| **A.7** Uso no previsto | | | | | | | | | | |
| **A.11** Acceso no Autorizado | | | | | | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | | | | | | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | | | | | | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | | | | | | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,07 | 0,65 | 0,10 | Poco frecuente | **0,05** | 0,07 | 0,75 | 0,10 | Poco frecuente | **0,05** |
| **A.26** Ataque destructivo | 0,05 | 0,60 | 0,10 | Poco frecuente | **0,03** | 0,05 | 0,65 | 0,10 | Poco frecuente | **0,03** |

| AMENAZAS | ROUTERS INALAMBRICOS | | | | | SWITCH | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,15 | 0,60 | 0,10 | Poco frecuente | **0,09** | 0,15 | 0,60 | 0,10 | Poco frecuente | **0,09** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,30 | 0,75 | 1 | Normal | **0,23** | 0,30 | 0,75 | 1 | Normal | **0,23** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,27 | 0,70 | 0,10 | Poco frecuente | **0,19** | 0,27 | 0,70 | 0,10 | Poco frecuente | **0,19** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,80 | 1 | Normal | **0,28** | 0,35 | 0,80 | 1 | Normal | **0,28** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,75 | 1 | Normal | **0,09** | 0,12 | 0,75 | 1 | Normal | **0,09** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | 0,12 | 0,88 | 1 | Normal | **0,11** | 0,12 | 0,88 | 1 | Normal | **0,11** |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | 0,10 | 0,62 | 0,10 | Poco frecuente | **0,06** | 0,10 | 0,62 | 0,10 | Poco frecuente | **0,06** |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | 0,22 | 0,68 | 10 | Frecuente | **0,15** | 0,22 | 0,68 | 10 | Frecuente | **0,15** |
| **E.25** Pérdida de equipos | 0,15 | 0,90 | 0,10 | Poco frecuente | **0,14** | 0,15 | 0,90 | 0,10 | Poco frecuente | **0,14** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** |
| **A.6** Abuso de Privilegios de Acceso | 0,15 | 0,45 | 0,10 | Poco frecuente | **0,07** | 0,15 | 0,45 | 0,10 | Poco frecuente | **0,07** |
| **A.7** Uso no previsto | 0,18 | 0,60 | 0,10 | Poco frecuente | **0,11** | 0,18 | 0,60 | 0,10 | Poco frecuente | **0,11** |
| **A.11** Acceso no Autorizado | 0,2 | 0,60 | 1 | Normal | **0,12** | 0,2 | 0,60 | 1 | Normal | **0,12** |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | 0,15 | 0,85 | 1 | Normal | **0,13** | 0,15 | 0,90 | 1 | Normal | **0,14** |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | 0,15 | 0,78 | 1/10 | Poco frecuente | **0,12** | 0,15 | 0,78 | 0,10 | Poco frecuente | **0,12** |
| **A.24** Denegación de servicio (Saturación del sistema informático) | 0,15 | 0,72 | 10 | Frecuente | **0,11** | 0,15 | 0,72 | 10 | Frecuente | **0,11** |
| **A.25** Robo (Pérdida de Equipos) | 0,07 | 0,90 | 0,10 | Poco frecuente | **0,06** | 0,07 | 0,90 | 0,10 | Poco frecuente | **0,06** |
| **A.26** Ataque destructivo | 0,05 | 0,65 | 0,10 | Poco frecuente | **0,03** | 0,05 | 0,65 | 0,10 | Poco frecuente | **0,03** |

| AMENAZAS | ACCESS POINT | | | | | IMPRESORA | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,85 | 1/100 | Muy Poco frecuente | **0,09** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,85 | 1/100 | Muy Poco frecuente | **0,09** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** | 0,15 | 0,70 | 0,10 | Poco frecuente | **0,11** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,15 | 0,60 | 0,10 | Poco frecuente | **0,09** | 0,48 | 0,75 | 10 | Frecuente | **0,36** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,30 | 0,75 | 1 | Normal | **0,23** | 0,23 | 0,70 | 1 | Normal | **0,16** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,27 | 0,70 | 0,10 | Poco frecuente | **0,19** | 0,35 | 0,76 | 1 | Normal | **0,27** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,80 | 1 | Normal | **0,28** | 0,45 | 0,85 | 10 | Frecuente | **0,38** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,75 | 1 | Normal | **0,09** | 0,12 | 0,80 | 1 | Normal | **0,10** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | 0,12 | 0,88 | 1 | Normal | **0,11** | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | 0,10 | 0,62 | 0,10 | Poco frecuente | **0,06** | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** | 0,12 | 0,75 | 1 | Normal | **0,09** |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | 0,22 | 0,68 | 10 | Frecuente | **0,15** | | | | | |
| **E.25** Pérdida de equipos | 0,15 | 0,90 | 0,10 | Poco frecuente | **0,14** | 0,23 | 0,83 | 0,10 | Poco frecuente | **0,19** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** | | | | | |
| **A.6** Abuso de Privilegios de Acceso | 0,15 | 0,45 | 0,10 | Poco frecuente | **0,07** | | | | | |
| **A.7** Uso no previsto | 0,18 | 0,60 | 0,10 | Poco frecuente | **0,11** | | | | | |
| **A.11** Acceso no Autorizado | 0,2 | 0,60 | 1 | Normal | **0,12** | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | 0,15 | 0,90 | 1 | Normal | **0,14** | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | 0,15 | 0,78 | 0,10 | Poco frecuente | **0,12** | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | 0,15 | 0,72 | 10 | Frecuente | **0,11** | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,07 | 0,90 | 0,10 | Poco frecuente | **0,06** | 0,07 | 0,85 | 0,10 | Poco frecuente | **0,06** |
| **A.26** Ataque destructivo | 0,05 | 0,65 | 0,10 | Poco frecuente | **0,03** | 0,05 | 0,75 | 0,10 | Poco frecuente | **0,04** |

**Cuadro 4.10**. Servicio: postgrado y talento humano

| AMENAZAS | CPU | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | DAÑO EN EL DISCO DURO | | | | | DAÑO EN LA FUENTE DE PODER | | | | |
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,83 | 1/100 | Muy Poco frecuente | **0,08** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,90 | 1/100 | Muy Poco frecuente | **0,09** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,20 | 0,60 | 0,10 | Poco frecuente | **0,12** | 0,20 | 0,70 | 0,10 | Poco frecuente | **0,14** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,25 | 0,55 | 1 | Normal | **0,14** | 0,35 | 0,80 | 1 | Normal | **0,28** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,30 | 0,60 | 1 | Normal | **0,18** | 0,45 | 0,75 | 1 | Normal | **0,34** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,45 | 0,70 | 1 | Normal | **0,32** | 0,45 | 0,90 | 1 | Normal | **0,41** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,50 | 0,75 | 10 | Frecuente | **0,38** | 0,50 | 0,90 | 10 | Frecuente | **0,45** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,10 | 0,45 | 0,10 | Poco frecuente | **0,05** | 0,10 | 0,45 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,60 | 1 | Normal | **0,07** | 0,12 | 0,60 | 1 | Normal | **0,07** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | 0,50 | 0,75 | 1 | Normal | **0,38** | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | 0,05 | 0,60 | 1 | Normal | **0,03** | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | 0,05 | 0,60 | 1 | Normal | **0,03** | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,25 | 0,80 | 1 | Normal | **0,20** | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | 0,60 | 0,65 | 10 | Frecuente | **0,39** | | | | | |
| **E.25** Pérdida de equipos | 0,45 | 0,80 | 0,10 | Poco frecuente | **0,36** | 0,45 | 0,80 | 0,10 | Poco frecuente | **0,36** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** | | | | | |
| **A.6** Abuso de Privilegios de Acceso | 0,05 | 0,50 | 0,10 | Poco frecuente | **0,03** | | | | | |
| **A.7** Uso no previsto | 0,05 | 0,40 | 0,10 | Poco frecuente | **0,02** | | | | | |
| **A.11** Acceso no Autorizado | 0,10 | 0,80 | 0,10 | Poco frecuente | **0,08** | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | 0,15 | 0,76 | 0,10 | Poco frecuente | **0,11** | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | 0,05 | 0,83 | 0,10 | Poco frecuente | **0,04** | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | 0,35 | 0,75 | 1 | Normal | **0,26** | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** |
| **A.26** Ataque destructivo | 0,05 | 0,75 | 0,10 | Poco frecuente | **0,04** | 0,05 | 0,90 | 0,10 | Poco frecuente | **0,05** |

| AMENAZAS | CPU | | | | | MONITOR | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | DAÑO EN LA MEMORIA RAM | | | | | | | | | |
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,65 | 0,10 | Poco frecuente | **0,10** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,90 | 1/100 | Muy Poco frecuente | **0,09** | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,18 | 0,70 | 0,10 | Poco frecuente | **0,13** | 0,15 | 0,60 | 0,10 | Poco frecuente | **0,09** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,40 | 0,75 | 1 | Normal | **0,30** | 0,08 | 0,45 | 0,10 | Poco frecuente | **0,04** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,30 | 0,60 | 1 | Normal | **0,18** | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,45 | 0,90 | 1 | Normal | **0,41** | 0,45 | 0,70 | 1 | Normal | **0,32** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,50 | 0,73 | 10 | Frecuente | **0,37** | 0,40 | 0,68 | 10 | Frecuente | **0,27** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,10 | 0,45 | 0,10 | Poco frecuente | **0,05** | 0,10 | 0,45 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,60 | 1 | Normal | **0,07** | 0,12 | 0,75 | 1 | Normal | **0,09** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | | | | | | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | | | | | | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | | | | | | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | | | | | | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | | | | | | | | | | |
| **E.25** Pérdida de equipos | 0,45 | 0,80 | 0,10 | Poco frecuente | **0,36** | 0,25 | 0,85 | 0,10 | Poco frecuente | **0,21** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | | | | | | | | | | |
| **A.6** Abuso de Privilegios de Acceso | | | | | | | | | | |
| **A.7** Uso no previsto | | | | | | | | | | |
| **A.11** Acceso no Autorizado | | | | | | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | | | | | | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | | | | | | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | | | | | | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** | 0,05 | 0,85 | 0,10 | Poco frecuente | **0,04** |
| **A.26** Ataque destructivo | 0,05 | 0,90 | 0,10 | Poco frecuente | **0,05** | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** |

| AMENAZAS | MOUSE | | | | | TECLADO | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,65 | 1/100 | Muy Poco frecuente | **0,07** | 0,10 | 0,70 | 1/100 | Muy Poco frecuente | **0,07** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,68 | 0,10 | Poco frecuente | **0,11** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,65 | 1/100 | Muy Poco frecuente | **0,07** | 0,10 | 0,70 | 1/100 | Muy Poco frecuente | **0,07** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,16 | 0,68 | 0,10 | Poco frecuente | **0,11** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,10 | 0,50 | 1 | Normal | **0,05** | 0,10 | 0,54 | 1 | Normal | **0,05** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,15 | 0,58 | 0,10 | Poco frecuente | **0,09** | 0,15 | 0,58 | 0,10 | Poco frecuente | **0,09** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,35 | 0,72 | 1 | Normal | **0,25** | 0,35 | 0,76 | 1 | Normal | **0,27** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,70 | 10 | Frecuente | **0,25** | 0,35 | 0,75 | 10 | Frecuente | **0,26** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,75 | 1 | Normal | **0,09** | 0,12 | 0,80 | 1 | Normal | **0,10** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | | | | | | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | | | | | | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | | | | | | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | | | | | | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | | | | | | | | | | |
| **E.25** Pérdida de equipos | 0,15 | 0,75 | 0,10 | Poco frecuente | **0,11** | 0,15 | 0,80 | 0,10 | Poco frecuente | **0,12** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | | | | | | | | | | |
| **A.6** Abuso de Privilegios de Acceso | | | | | | | | | | |
| **A.7** Uso no previsto | | | | | | | | | | |
| **A.11** Acceso no Autorizado | | | | | | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | | | | | | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | | | | | | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | | | | | | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,07 | 0,65 | 0,10 | Poco frecuente | **0,05** | 0,07 | 0,75 | 0,10 | Poco frecuente | **0,05** |
| **A.26** Ataque destructivo | 0,05 | 0,60 | 0,10 | Poco frecuente | **0,03** | 0,05 | 0,65 | 0,10 | Poco frecuente | **0,03** |

| AMENAZAS | ACCESS POINT | | | | | IMPRESORA | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,85 | 1/100 | Muy Poco frecuente | **0,09** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,85 | 1/100 | Muy Poco frecuente | **0,09** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** | 0,15 | 0,70 | 0,10 | Poco frecuente | **0,11** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,15 | 0,60 | 0,10 | Poco frecuente | **0,09** | 0,48 | 0,75 | 10 | Frecuente | **0,36** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,30 | 0,75 | 1 | Normal | **0,23** | 0,23 | 0,70 | 1 | Normal | **0,16** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,27 | 0,70 | 0,10 | Poco frecuente | **0,19** | 0,35 | 0,76 | 1 | Normal | **0,27** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,80 | 1 | Normal | **0,28** | 0,45 | 0,85 | 10 | Frecuente | **0,38** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,75 | 1 | Normal | **0,09** | 0,12 | 0,80 | 1 | Normal | **0,10** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | 0,12 | 0,88 | 1 | Normal | **0,11** | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | 0,10 | 0,62 | 0,10 | Poco frecuente | **0,06** | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** | 0,12 | 0,75 | 1 | Normal | **0,09** |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | 0,22 | 0,68 | 10 | Frecuente | **0,15** | | | | | |
| **E.25** Pérdida de equipos | 0,15 | 0,90 | 0,10 | Poco frecuente | **0,14** | 0,23 | 0,83 | 0,10 | Poco frecuente | **0,19** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** | | | | | |
| **A.6** Abuso de Privilegios de Acceso | 0,15 | 0,45 | 0,10 | Poco frecuente | **0,07** | | | | | |
| **A.7** Uso no previsto | 0,18 | 0,60 | 0,10 | Poco frecuente | **0,11** | | | | | |
| **A.11** Acceso no Autorizado | 0,2 | 0,60 | 1 | Normal | **0,12** | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | 0,15 | 0,90 | 1 | Normal | **0,14** | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | 0,15 | 0,78 | 0,10 | Poco frecuente | **0,12** | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | 0,15 | 0,72 | 10 | Frecuente | **0,11** | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,07 | 0,90 | 0,10 | Poco frecuente | **0,06** | 0,07 | 0,85 | 0,10 | Poco frecuente | **0,06** |
| **A.26** Ataque destructivo | 0,05 | 0,65 | 0,10 | Poco frecuente | **0,03** | 0,05 | 0,75 | 0,10 | Poco frecuente | **0,04** |

**Cuadro 4.11**. Servicio: acreditación

| AMENAZAS | CPU | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | DAÑO EN EL DISCO DURO | | | | | DAÑO EN LA FUENTE DE PODER | | | | |
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,83 | 1/100 | Muy Poco frecuente | **0,08** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,90 | 1/100 | Muy Poco frecuente | **0,09** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,20 | 0,60 | 0,10 | Poco frecuente | **0,12** | 0,20 | 0,70 | 0,10 | Poco frecuente | **0,14** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,25 | 0,55 | 1 | Normal | **0,14** | 0,35 | 0,80 | 1 | Normal | **0,28** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,30 | 0,60 | 1 | Normal | **0,18** | 0,45 | 0,75 | 1 | Normal | **0,34** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,45 | 0,70 | 1 | Normal | **0,32** | 0,45 | 0,90 | 1 | Normal | **0,41** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,50 | 0,75 | 10 | Frecuente | **0,38** | 0,50 | 0,90 | 10 | Frecuente | **0,45** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,10 | 0,45 | 0,10 | Poco frecuente | **0,05** | 0,10 | 0,45 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,60 | 1 | Normal | **0,07** | 0,12 | 0,60 | 1 | Normal | **0,07** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | 0,50 | 0,75 | 1 | Normal | **0,38** | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | 0,05 | 0,60 | 1 | Normal | **0,03** | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | 0,05 | 0,60 | 1 | Normal | **0,03** | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,25 | 0,80 | 1 | Normal | **0,20** | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | 0,60 | 0,65 | 10 | Frecuente | **0,39** | | | | | |
| **E.25** Pérdida de equipos | 0,45 | 0,80 | 0,10 | Poco frecuente | **0,36** | 0,45 | 0,80 | 0,10 | Poco frecuente | **0,36** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** | | | | | |
| **A.6** Abuso de Privilegios de Acceso | 0,05 | 0,50 | 0,10 | Poco frecuente | **0,03** | | | | | |
| **A.7** Uso no previsto | 0,05 | 0,40 | 0,10 | Poco frecuente | **0,02** | | | | | |
| **A.11** Acceso no Autorizado | 0,10 | 0,80 | 0,10 | Poco frecuente | **0,08** | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | 0,15 | 0,76 | 0,10 | Poco frecuente | **0,11** | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | 0,05 | 0,83 | 0,10 | Poco frecuente | **0,04** | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | 0,35 | 0,75 | 1 | Normal | **0,26** | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** |
| **A.26** Ataque destructivo | 0,05 | 0,75 | 0,10 | Poco frecuente | **0,04** | 0,05 | 0,90 | 0,10 | Poco frecuente | **0,05** |

| AMENAZAS | CPU | | | | | MONITOR | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | DAÑO EN LA MEMORIA RAM | | | | | | | | | |
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,65 | 0,10 | Poco frecuente | **0,10** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,90 | 1/100 | Muy Poco frecuente | **0,09** | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,18 | 0,70 | 0,10 | Poco frecuente | **0,13** | 0,15 | 0,60 | 0,10 | Poco frecuente | **0,09** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,40 | 0,75 | 1 | Normal | **0,30** | 0,08 | 0,45 | 0,10 | Poco frecuente | **0,04** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,30 | 0,60 | 1 | Normal | **0,18** | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,45 | 0,90 | 1 | Normal | **0,41** | 0,45 | 0,70 | 1 | Normal | **0,32** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,50 | 0,73 | 10 | Frecuente | **0,37** | 0,40 | 0,68 | 10 | Frecuente | **0,27** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,10 | 0,45 | 0,10 | Poco frecuente | **0,05** | 0,10 | 0,45 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,60 | 1 | Normal | **0,07** | 0,12 | 0,75 | 1 | Normal | **0,09** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | | | | | | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | | | | | | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | | | | | | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | | | | | | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | | | | | | | | | | |
| **E.25** Pérdida de equipos | 0,45 | 0,80 | 0,10 | Poco frecuente | **0,36** | 0,25 | 0,85 | 0,10 | Poco frecuente | **0,21** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | | | | | | | | | | |
| **A.6** Abuso de Privilegios de Acceso | | | | | | | | | | |
| **A.7** Uso no previsto | | | | | | | | | | |
| **A.11** Acceso no Autorizado | | | | | | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | | | | | | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | | | | | | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | | | | | | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** | 0,05 | 0,85 | 0,10 | Poco frecuente | **0,04** |
| **A.26** Ataque destructivo | 0,05 | 0,90 | 0,10 | Poco frecuente | **0,05** | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** |

| AMENAZAS | MOUSE | | | | | TECLADO | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,65 | 1/100 | Muy Poco frecuente | **0,07** | 0,10 | 0,70 | 1/100 | Muy Poco frecuente | **0,07** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,68 | 0,10 | Poco frecuente | **0,11** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,65 | 1/100 | Muy Poco frecuente | **0,07** | 0,10 | 0,70 | 1/100 | Muy Poco frecuente | **0,07** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,16 | 0,68 | 0,10 | Poco frecuente | **0,11** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,10 | 0,50 | 1 | Normal | **0,05** | 0,10 | 0,54 | 1 | Normal | **0,05** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,15 | 0,58 | 0,10 | Poco frecuente | **0,09** | 0,15 | 0,58 | 0,10 | Poco frecuente | **0,09** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,35 | 0,72 | 1 | Normal | **0,25** | 0,35 | 0,76 | 1 | Normal | **0,27** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,70 | 10 | Frecuente | **0,25** | 0,35 | 0,75 | 10 | Frecuente | **0,26** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,75 | 1 | Normal | **0,09** | 0,12 | 0,80 | 1 | Normal | **0,10** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | | | | | | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | | | | | | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | | | | | | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | | | | | | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | | | | | | | | | | |
| **E.25** Pérdida de equipos | 0,15 | 0,75 | 0,10 | Poco frecuente | **0,11** | 0,15 | 0,80 | 0,10 | Poco frecuente | **0,12** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | | | | | | | | | | |
| **A.6** Abuso de Privilegios de Acceso | | | | | | | | | | |
| **A.7** Uso no previsto | | | | | | | | | | |
| **A.11** Acceso no Autorizado | | | | | | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | | | | | | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | | | | | | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | | | | | | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,07 | 0,65 | 0,10 | Poco frecuente | **0,05** | 0,07 | 0,75 | 0,10 | Poco frecuente | **0,05** |
| **A.26** Ataque destructivo | 0,05 | 0,60 | 0,10 | Poco frecuente | **0,03** | 0,05 | 0,65 | 0,10 | Poco frecuente | **0,03** |

| AMENAZAS | ACCESS POINT | | | | | ROUTERS INALAMBRICOS | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,15 | 0,60 | 0,10 | Poco frecuente | **0,09** | 0,15 | 0,60 | 0,10 | Poco frecuente | **0,09** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,30 | 0,75 | 1 | Normal | **0,23** | 0,30 | 0,75 | 1 | Normal | **0,23** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,27 | 0,70 | 0,10 | Poco frecuente | **0,19** | 0,27 | 0,70 | 0,10 | Poco frecuente | **0,19** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,80 | 1 | Normal | **0,28** | 0,35 | 0,80 | 1 | Normal | **0,28** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,75 | 1 | Normal | **0,09** | 0,12 | 0,75 | 1 | Normal | **0,09** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | 0,12 | 0,88 | 1 | Normal | **0,11** | 0,12 | 0,88 | 1 | Normal | **0,11** |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | 0,10 | 0,62 | 0,10 | Poco frecuente | **0,06** | 0,10 | 0,62 | 0,10 | Poco frecuente | **0,06** |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | 0,22 | 0,68 | 10 | Frecuente | **0,15** | 0,22 | 0,68 | 10 | Frecuente | **0,15** |
| **E.25** Pérdida de equipos | 0,15 | 0,90 | 0,10 | Poco frecuente | **0,14** | 0,15 | 0,90 | 0,10 | Poco frecuente | **0,14** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** |
| **A.6** Abuso de Privilegios de Acceso | 0,15 | 0,45 | 0,10 | Poco frecuente | **0,07** | 0,15 | 0,45 | 0,10 | Poco frecuente | **0,07** |
| **A.7** Uso no previsto | 0,18 | 0,60 | 0,10 | Poco frecuente | **0,11** | 0,18 | 0,60 | 0,10 | Poco frecuente | **0,11** |
| **A.11** Acceso no Autorizado | 0,2 | 0,60 | 1 | Normal | **0,12** | 0,2 | 0,60 | 1 | Normal | **0,12** |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | 0,15 | 0,90 | 1 | Normal | **0,14** | 0,15 | 0,85 | 1 | Normal | **0,13** |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | 0,15 | 0,78 | 0,10 | Poco frecuente | **0,12** | 0,15 | 0,78 | 0,10 | Poco frecuente | **0,12** |
| **A.24** Denegación de servicio (Saturación del sistema informático) | 0,15 | 0,72 | 10 | Frecuente | **0,11** | 0,15 | 0,72 | 10 | Frecuente | **0,11** |
| **A.25** Robo (Pérdida de Equipos) | 0,07 | 0,90 | 0,10 | Poco frecuente | **0,06** | 0,07 | 0,90 | 0,10 | Poco frecuente | **0,06** |
| **A.26** Ataque destructivo | 0,05 | 0,65 | 0,10 | Poco frecuente | **0,03** | 0,05 | 0,65 | 0,10 | Poco frecuente | **0,03** |

| AMENAZAS | SWITCH | | | | | IMPRESORA | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,85 | 1/100 | Muy Poco frecuente | **0,09** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,85 | 1/100 | Muy Poco frecuente | **0,09** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** | 0,15 | 0,70 | 0,10 | Poco frecuente | **0,11** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,15 | 0,60 | 0,10 | Poco frecuente | **0,09** | 0,48 | 0,75 | 10 | Frecuente | **0,36** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,30 | 0,75 | 1 | Normal | **0,23** | 0,23 | 0,70 | 1 | Normal | **0,16** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,27 | 0,70 | 0,10 | Poco frecuente | **0,19** | 0,35 | 0,76 | 1 | Normal | **0,27** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,80 | 1 | Normal | **0,28** | 0,45 | 0,85 | 10 | Frecuente | **0,38** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,75 | 1 | Normal | **0,09** | 0,12 | 0,80 | 1 | Normal | **0,10** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | 0,12 | 0,88 | 1 | Normal | **0,11** | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | 0,10 | 0,62 | 0,10 | Poco frecuente | **0,06** | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** | 0,12 | 0,75 | 1 | Normal | **0,09** |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | 0,22 | 0,68 | 10 | Frecuente | **0,15** | | | | | |
| **E.25** Pérdida de equipos | 0,15 | 0,90 | 0,10 | Poco frecuente | **0,14** | 0,23 | 0,83 | 0,10 | Poco frecuente | **0,19** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** | | | | | |
| **A.6** Abuso de Privilegios de Acceso | 0,15 | 0,45 | 0,10 | Poco frecuente | **0,07** | | | | | |
| **A.7** Uso no previsto | 0,18 | 0,60 | 0,10 | Poco frecuente | **0,11** | | | | | |
| **A.11** Acceso no Autorizado | 0,2 | 0,60 | 1 | Normal | **0,12** | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | 0,15 | 0,90 | 1 | Normal | **0,14** | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | 0,15 | 0,78 | 0,10 | Poco frecuente | **0,12** | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | 0,15 | 0,72 | 10 | Frecuente | **0,11** | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,07 | 0,90 | 0,10 | Poco frecuente | **0,06** | 0,07 | 0,85 | 0,10 | Poco frecuente | **0,06** |
| **A.26** Ataque destructivo | 0,05 | 0,65 | 0,10 | Poco frecuente | **0,03** | 0,05 | 0,75 | 0,10 | Poco frecuente | **0,04** |

**Cuadro 4.12.** Servicio: jefatura de almacén, vicerrectorado de extensión y bienestar politécnico, vinculación y coordinación de cultura

| AMENAZAS | CPU | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | DAÑO EN EL DISCO DURO | | | | | DAÑO EN LA FUENTE DE PODER | | | | |
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,83 | 1/100 | Muy Poco frecuente | **0,08** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,90 | 1/100 | Muy Poco frecuente | **0,09** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,20 | 0,60 | 0,10 | Poco frecuente | **0,12** | 0,20 | 0,70 | 0,10 | Poco frecuente | **0,14** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,25 | 0,55 | 1 | Normal | **0,14** | 0,35 | 0,80 | 1 | Normal | **0,28** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,30 | 0,60 | 1 | Normal | **0,18** | 0,45 | 0,75 | 1 | Normal | **0,34** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,45 | 0,70 | 1 | Normal | **0,32** | 0,45 | 0,90 | 1 | Normal | **0,41** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,50 | 0,75 | 10 | Frecuente | **0,38** | 0,50 | 0,90 | 10 | Frecuente | **0,45** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,10 | 0,45 | 0,10 | Poco frecuente | **0,05** | 0,10 | 0,45 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,60 | 1 | Normal | **0,07** | 0,12 | 0,60 | 1 | Normal | **0,07** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | 0,50 | 0,75 | 1 | Normal | **0,38** | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | 0,05 | 0,60 | 1 | Normal | **0,03** | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | 0,05 | 0,60 | 1 | Normal | **0,03** | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,25 | 0,80 | 1 | Normal | **0,20** | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | 0,60 | 0,65 | 10 | Frecuente | **0,39** | | | | | |
| **E.25** Pérdida de equipos | 0,45 | 0,80 | 0,10 | Poco frecuente | **0,36** | 0,45 | 0,80 | 0,10 | Poco frecuente | **0,36** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** | | | | | |
| **A.6** Abuso de Privilegios de Acceso | 0,05 | 0,50 | 0,10 | Poco frecuente | **0,03** | | | | | |
| **A.7** Uso no previsto | 0,05 | 0,40 | 0,10 | Poco frecuente | **0,02** | | | | | |
| **A.11** Acceso no Autorizado | 0,10 | 0,80 | 0,10 | Poco frecuente | **0,08** | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | 0,15 | 0,76 | 0,10 | Poco frecuente | **0,11** | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | 0,05 | 0,83 | 0,10 | Poco frecuente | **0,04** | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | 0,35 | 0,75 | 1 | Normal | **0,26** | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** |
| **A.26** Ataque destructivo | 0,05 | 0,75 | 0,10 | Poco frecuente | **0,04** | 0,05 | 0,90 | 0,10 | Poco frecuente | **0,05** |

| AMENAZAS | CPU | | | | | MONITOR | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | DAÑO EN LA MEMORIA RAM | | | | | | | | | |
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,65 | 0,10 | Poco frecuente | **0,10** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,90 | 1/100 | Muy Poco frecuente | **0,09** | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,18 | 0,70 | 0,10 | Poco frecuente | **0,13** | 0,15 | 0,60 | 0,10 | Poco frecuente | **0,09** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,40 | 0,75 | 1 | Normal | **0,30** | 0,08 | 0,45 | 0,10 | Poco frecuente | **0,04** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,30 | 0,60 | 1 | Normal | **0,18** | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,45 | 0,90 | 1 | Normal | **0,41** | 0,45 | 0,70 | 1 | Normal | **0,32** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,50 | 0,73 | 10 | Frecuente | **0,37** | 0,40 | 0,68 | 10 | Frecuente | **0,27** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,10 | 0,45 | 0,10 | Poco frecuente | **0,05** | 0,10 | 0,45 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,60 | 1 | Normal | **0,07** | 0,12 | 0,75 | 1 | Normal | **0,09** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | | | | | | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | | | | | | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | | | | | | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | | | | | | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | | | | | | | | | | |
| **E.25** Pérdida de equipos | 0,45 | 0,80 | 0,10 | Poco frecuente | **0,36** | 0,25 | 0,85 | 0,10 | Poco frecuente | **0,21** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | | | | | | | | | | |
| **A.6** Abuso de Privilegios de Acceso | | | | | | | | | | |
| **A.7** Uso no previsto | | | | | | | | | | |
| **A.11** Acceso no Autorizado | | | | | | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | | | | | | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | | | | | | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | | | | | | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** | 0,05 | 0,85 | 0,10 | Poco frecuente | **0,04** |
| **A.26** Ataque destructivo | 0,05 | 0,90 | 0,10 | Poco frecuente | **0,05** | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** |

| AMENAZAS | MOUSE | | | | | TECLADO | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,65 | 1/100 | Muy Poco frecuente | **0,07** | 0,10 | 0,70 | 1/100 | Muy Poco frecuente | **0,07** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,68 | 0,10 | Poco frecuente | **0,11** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,65 | 1/100 | Muy Poco frecuente | **0,07** | 0,10 | 0,70 | 1/100 | Muy Poco frecuente | **0,07** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,16 | 0,68 | 0,10 | Poco frecuente | **0,11** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,10 | 0,50 | 1 | Normal | **0,05** | 0,10 | 0,54 | 1 | Normal | **0,05** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,15 | 0,58 | 0,10 | Poco frecuente | **0,09** | 0,15 | 0,58 | 0,10 | Poco frecuente | **0,09** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,35 | 0,72 | 1 | Normal | **0,25** | 0,35 | 0,76 | 1 | Normal | **0,27** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,70 | 10 | Frecuente | **0,25** | 0,35 | 0,75 | 10 | Frecuente | **0,26** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,75 | 1 | Normal | **0,09** | 0,12 | 0,80 | 1 | Normal | **0,10** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | | | | | | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | | | | | | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | | | | | | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | | | | | | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | | | | | | | | | | |
| **E.25** Pérdida de equipos | 0,15 | 0,75 | 0,10 | Poco frecuente | **0,11** | 0,15 | 0,80 | 0,10 | Poco frecuente | **0,12** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | | | | | | | | | | |
| **A.6** Abuso de Privilegios de Acceso | | | | | | | | | | |
| **A.7** Uso no previsto | | | | | | | | | | |
| **A.11** Acceso no Autorizado | | | | | | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | | | | | | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | | | | | | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | | | | | | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,07 | 0,65 | 0,10 | Poco frecuente | **0,05** | 0,07 | 0,75 | 0,10 | Poco frecuente | **0,05** |
| **A.26** Ataque destructivo | 0,05 | 0,60 | 0,10 | Poco frecuente | **0,03** | 0,05 | 0,65 | 0,10 | Poco frecuente | **0,03** |

| AMENAZAS | ACCESS POINT | | | | | ROUTERS INALAMBRICOS | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,15 | 0,60 | 0,10 | Poco frecuente | **0,09** | 0,15 | 0,60 | 0,10 | Poco frecuente | **0,09** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,30 | 0,75 | 1 | Normal | **0,23** | 0,30 | 0,75 | 1 | Normal | **0,23** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,27 | 0,70 | 0,10 | Poco frecuente | **0,19** | 0,27 | 0,70 | 0,10 | Poco frecuente | **0,19** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,80 | 1 | Normal | **0,28** | 0,35 | 0,80 | 1 | Normal | **0,28** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,75 | 1 | Normal | **0,09** | 0,12 | 0,75 | 1 | Normal | **0,09** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | 0,12 | 0,88 | 1 | Normal | **0,11** | 0,12 | 0,88 | 1 | Normal | **0,11** |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | 0,10 | 0,62 | 0,10 | Poco frecuente | **0,06** | 0,10 | 0,62 | 0,10 | Poco frecuente | **0,06** |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | 0,22 | 0,68 | 10 | Frecuente | **0,15** | 0,22 | 0,68 | 10 | Frecuente | **0,15** |
| **E.25** Pérdida de equipos | 0,15 | 0,90 | 0,10 | Poco frecuente | **0,14** | 0,15 | 0,90 | 0,10 | Poco frecuente | **0,14** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** |
| **A.6** Abuso de Privilegios de Acceso | 0,15 | 0,45 | 0,10 | Poco frecuente | **0,07** | 0,15 | 0,45 | 0,10 | Poco frecuente | **0,07** |
| **A.7** Uso no previsto | 0,18 | 0,60 | 0,10 | Poco frecuente | **0,11** | 0,18 | 0,60 | 0,10 | Poco frecuente | **0,11** |
| **A.11** Acceso no Autorizado | 0,2 | 0,60 | 1 | Normal | **0,12** | 0,2 | 0,60 | 1 | Normal | **0,12** |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | 0,15 | 0,90 | 1 | Normal | **0,14** | 0,15 | 0,85 | 1 | Normal | **0,13** |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | 0,15 | 0,78 | 0,10 | Poco frecuente | **0,12** | 0,15 | 0,78 | 0,10 | Poco frecuente | **0,12** |
| **A.24** Denegación de servicio (Saturación del sistema informático) | 0,15 | 0,72 | 10 | Frecuente | **0,11** | 0,15 | 0,72 | 10 | Frecuente | **0,11** |
| **A.25** Robo (Pérdida de Equipos) | 0,07 | 0,90 | 0,10 | Poco frecuente | **0,06** | 0,07 | 0,90 | 0,10 | Poco frecuente | **0,06** |
| **A.26** Ataque destructivo | 0,05 | 0,65 | 0,10 | Poco frecuente | **0,03** | 0,05 | 0,65 | 0,10 | Poco frecuente | **0,03** |

| AMENAZAS | IMPRESORA | | | | |
|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,85 | 1/100 | Muy Poco frecuente | **0,09** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,85 | 1/100 | Muy Poco frecuente | **0,09** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,15 | 0,70 | 0,10 | Poco frecuente | **0,11** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,48 | 0,75 | 10 | Frecuente | **0,36** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,23 | 0,70 | 1 | Normal | **0,16** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,35 | 0,76 | 1 | Normal | **0,27** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,45 | 0,85 | 10 | Frecuente | **0,38** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,80 | 1 | Normal | **0,10** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | |
| **E.2** Errores de Administrador | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,12 | 0,75 | 1 | Normal | **0,09** |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | | | | | |
| **E.25** Pérdida de equipos | 0,23 | 0,83 | 0,10 | Poco frecuente | **0,19** |
| **ATAQUES INTENCIONADOS (A)** | | | | | |
| **A.5** Suplantación de la identidad del usuario | | | | | |
| **A.6** Abuso de Privilegios de Acceso | | | | | |
| **A.7** Uso no previsto | | | | | |
| **A.11** Acceso no Autorizado | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,07 | 0,85 | 0,10 | Poco frecuente | **0,06** |
| **A.26** Ataque destructivo | 0,05 | 0,75 | 0,10 | Poco frecuente | **0,04** |

**Cuadro 4.13**. Servicio:FEPAM

| AMENAZAS | CPU | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | DAÑO EN EL DISCO DURO | | | | | DAÑO EN LA FUENTE DE PODER | | | | |
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,83 | 1/100 | Muy Poco frecuente | **0,08** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,90 | 1/100 | Muy Poco frecuente | **0,09** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,20 | 0,60 | 0,10 | Poco frecuente | **0,12** | 0,20 | 0,70 | 0,10 | Poco frecuente | **0,14** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,25 | 0,55 | 1 | Normal | **0,14** | 0,35 | 0,80 | 1 | Normal | **0,28** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,30 | 0,60 | 1 | Normal | **0,18** | 0,45 | 0,75 | 1 | Normal | **0,34** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,45 | 0,70 | 1 | Normal | **0,32** | 0,45 | 0,90 | 1 | Normal | **0,41** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,50 | 0,75 | 10 | Frecuente | **0,38** | 0,50 | 0,90 | 10 | Frecuente | **0,45** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,10 | 0,45 | 0,10 | Poco frecuente | **0,05** | 0,10 | 0,45 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,60 | 1 | Normal | **0,07** | 0,12 | 0,60 | 1 | Normal | **0,07** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | 0,50 | 0,75 | 1 | Normal | **0,38** | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | 0,05 | 0,60 | 1 | Normal | **0,03** | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | 0,05 | 0,60 | 1 | Normal | **0,03** | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,25 | 0,80 | 1 | Normal | **0,20** | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | 0,60 | 0,65 | 10 | Frecuente | **0,39** | | | | | |
| **E.25** Pérdida de equipos | 0,45 | 0,80 | 0,10 | Poco frecuente | **0,36** | 0,45 | 0,80 | 0,10 | Poco frecuente | **0,36** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** | | | | | |
| **A.6** Abuso de Privilegios de Acceso | 0,05 | 0,50 | 0,10 | Poco frecuente | **0,03** | | | | | |
| **A.7** Uso no previsto | 0,05 | 0,40 | 0,10 | Poco frecuente | **0,02** | | | | | |
| **A.11** Acceso no Autorizado | 0,10 | 0,80 | 0,10 | Poco frecuente | **0,08** | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | 0,15 | 0,76 | 0,10 | Poco frecuente | **0,11** | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | 0,05 | 0,83 | 0,10 | Poco frecuente | **0,04** | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | 0,35 | 0,75 | 1 | Normal | **0,26** | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** |
| **A.26** Ataque destructivo | 0,05 | 0,75 | 0,10 | Poco frecuente | **0,04** | 0,05 | 0,90 | 0,10 | Poco frecuente | **0,05** |

| AMENAZAS | CPU | | | | | MONITOR | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | DAÑO EN LA MEMORIA RAM | | | | | | | | | |
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,65 | 0,10 | Poco frecuente | **0,10** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,90 | 1/100 | Muy Poco frecuente | **0,09** | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,18 | 0,70 | 0,10 | Poco frecuente | **0,13** | 0,15 | 0,60 | 0,10 | Poco frecuente | **0,09** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,40 | 0,75 | 1 | Normal | **0,30** | 0,08 | 0,45 | 0,10 | Poco frecuente | **0,04** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,30 | 0,60 | 1 | Normal | **0,18** | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,45 | 0,90 | 1 | Normal | **0,41** | 0,45 | 0,70 | 1 | Normal | **0,32** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,50 | 0,73 | 10 | Frecuente | **0,37** | 0,40 | 0,68 | 10 | Frecuente | **0,27** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,10 | 0,45 | 0,10 | Poco frecuente | **0,05** | 0,10 | 0,45 | 1/10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,60 | 1 | Normal | **0,07** | 0,12 | 0,75 | 1 | Normal | **0,09** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | | | | | | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | | | | | | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | | | | | | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | | | | | | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | | | | | | | | | | |
| **E.25** Pérdida de equipos | 0,45 | 0,80 | 0,10 | Poco frecuente | **0,36** | 0,25 | 0,85 | 0,10 | Poco frecuente | **0,21** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | | | | | | | | | | |
| **A.6** Abuso de Privilegios de Acceso | | | | | | | | | | |
| **A.7** Uso no previsto | | | | | | | | | | |
| **A.11** Acceso no Autorizado | | | | | | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | | | | | | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | | | | | | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | | | | | | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** | 0,05 | 0,85 | 0,10 | Poco frecuente | **0,04** |
| **A.26** Ataque destructivo | 0,05 | 0,90 | 0,10 | Poco frecuente | **0,05** | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** |

| AMENAZAS | MOUSE | | | | | TECLADO | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,65 | 1/100 | Muy Poco frecuente | **0,07** | 0,10 | 0,70 | 1/100 | Muy Poco frecuente | **0,07** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,68 | 0,10 | Poco frecuente | **0,11** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,65 | 1/100 | Muy Poco frecuente | **0,07** | 0,10 | 0,70 | 1/100 | Muy Poco frecuente | **0,07** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,16 | 0,68 | 0,10 | Poco frecuente | **0,11** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,10 | 0,50 | 1 | Normal | **0,05** | 0,10 | 0,54 | 1 | Normal | **0,05** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,15 | 0,58 | 0,10 | Poco frecuente | **0,09** | 0,15 | 0,58 | 0,10 | Poco frecuente | **0,09** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,35 | 0,72 | 1 | Normal | **0,25** | 0,35 | 0,76 | 1 | Normal | **0,27** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,70 | 10 | Frecuente | **0,25** | 0,35 | 0,75 | 10 | Frecuente | **0,26** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,75 | 1 | Normal | **0,09** | 0,12 | 0,80 | 1 | Normal | **0,10** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | | | | | | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | | | | | | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | | | | | | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | | | | | | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | | | | | | | | | | |
| **E.25** Pérdida de equipos | 0,15 | 0,75 | 0,10 | Poco frecuente | **0,11** | 0,15 | 0,80 | 0,10 | Poco frecuente | **0,12** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | | | | | | | | | | |
| **A.6** Abuso de Privilegios de Acceso | | | | | | | | | | |
| **A.7** Uso no previsto | | | | | | | | | | |
| **A.11** Acceso no Autorizado | | | | | | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | | | | | | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | | | | | | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | | | | | | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,07 | 0,65 | 0,10 | Poco frecuente | **0,05** | 0,07 | 0,75 | 0,10 | Poco frecuente | **0,05** |
| **A.26** Ataque destructivo | 0,05 | 0,60 | 0,10 | Poco frecuente | **0,03** | 0,05 | 0,65 | 0,10 | Poco frecuente | **0,03** |

| AMENAZAS | ROUTERS INALAMBRICOS | | | | | IMPRESORA | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,85 | 1/100 | Muy Poco frecuente | **0,09** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,85 | 1/100 | Muy Poco frecuente | **0,09** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** | 0,15 | 0,70 | 0,10 | Poco frecuente | **0,11** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,15 | 0,60 | 0,10 | Poco frecuente | **0,09** | 0,48 | 0,75 | 10 | Frecuente | **0,36** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,30 | 0,75 | 1 | Normal | **0,23** | 0,23 | 0,70 | 1 | Normal | **0,16** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,27 | 0,70 | 0,10 | Poco frecuente | **0,19** | 0,35 | 0,76 | 1 | Normal | **0,27** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,80 | 1 | Normal | **0,28** | 0,45 | 0,85 | 10 | Frecuente | **0,38** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,75 | 1 | Normal | **0,09** | 0,12 | 0,80 | 1 | Normal | **0,10** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | 0,12 | 0,88 | 1 | Normal | **0,11** | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | 0,10 | 0,62 | 0,10 | Poco frecuente | **0,06** | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** | 0,12 | 0,75 | 1 | Normal | **0,09** |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | 0,22 | 0,68 | 10 | Frecuente | **0,15** | | | | | |
| **E.25** Pérdida de equipos | 0,15 | 0,90 | 0,10 | Poco frecuente | **0,14** | 0,23 | 0,83 | 0,10 | Poco frecuente | **0,19** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** | | | | | |
| **A.6** Abuso de Privilegios de Acceso | 0,15 | 0,45 | 0,10 | Poco frecuente | **0,07** | | | | | |
| **A.7** Uso no previsto | 0,18 | 0,60 | 0,10 | Poco frecuente | **0,11** | | | | | |
| **A.11** Acceso no Autorizado | 0,2 | 0,60 | 1 | Normal | **0,12** | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | 0,15 | 0,85 | 1 | Normal | **0,13** | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | 0,15 | 0,78 | 0,10 | Poco frecuente | **0,12** | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | 0,15 | 0,72 | 10 | Frecuente | **0,11** | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,07 | 0,90 | 0,10 | Poco frecuente | **0,06** | 0,07 | 0,85 | 0,10 | Poco frecuente | **0,06** |
| **A.26** Ataque destructivo | 0,05 | 0,65 | 0,10 | Poco frecuente | **0,03** | 0,05 | 0,75 | 0,10 | Poco frecuente | **0,04** |

**Cuadro 4.14.** Servicio: dirección administrativa y financiera

| AMENAZAS | CPU | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | DAÑO EN EL DISCO DURO | | | | | DAÑO EN LA FUENTE DE PODER | | | | |
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,83 | 1/100 | Muy Poco frecuente | **0,08** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,90 | 1/100 | Muy Poco frecuente | **0,09** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,20 | 0,60 | 0,10 | Poco frecuente | **0,12** | 0,20 | 0,70 | 0,10 | Poco frecuente | **0,14** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,25 | 0,55 | 1 | Normal | **0,14** | 0,35 | 0,80 | 1 | Normal | **0,28** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,30 | 0,60 | 1 | Normal | **0,18** | 0,45 | 0,75 | 1 | Normal | **0,34** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,45 | 0,70 | 1 | Normal | **0,32** | 0,45 | 0,90 | 1 | Normal | **0,41** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,50 | 0,75 | 10 | Frecuente | **0,38** | 0,50 | 0,90 | 10 | Frecuente | **0,45** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,10 | 0,45 | 0,10 | Poco frecuente | **0,05** | 0,10 | 0,45 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,60 | 1 | Normal | **0,07** | 0,12 | 0,60 | 1 | Normal | **0,07** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | 0,50 | 0,75 | 1 | Normal | **0,38** | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | 0,05 | 0,60 | 1 | Normal | **0,03** | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | 0,05 | 0,60 | 1 | Normal | **0,03** | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,25 | 0,80 | 1 | Normal | **0,20** | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | 0,60 | 0,65 | 10 | Frecuente | **0,39** | | | | | |
| **E.25** Pérdida de equipos | 0,45 | 0,80 | 0,10 | Poco frecuente | **0,36** | 0,45 | 0,80 | 0,10 | Poco frecuente | **0,36** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** | | | | | |
| **A.6** Abuso de Privilegios de Acceso | 0,05 | 0,50 | 0,10 | Poco frecuente | **0,03** | | | | | |
| **A.7** Uso no previsto | 0,05 | 0,40 | 0,10 | Poco frecuente | **0,02** | | | | | |
| **A.11** Acceso no Autorizado | 0,10 | 0,80 | 0,10 | Poco frecuente | **0,08** | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | 0,15 | 0,76 | 0,10 | Poco frecuente | **0,11** | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | 0,05 | 0,83 | 0,10 | Poco frecuente | **0,04** | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | 0,35 | 0,75 | 1 | Normal | **0,26** | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** |
| **A.26** Ataque destructivo | 0,05 | 0,75 | 0,10 | Poco frecuente | **0,04** | 0,05 | 0,90 | 0,10 | Poco frecuente | **0,05** |

| AMENAZAS | CPU | | | | | MONITOR | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | DAÑO EN LA MEMORIA RAM | | | | | | | | | |
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,65 | 0,10 | Poco frecuente | **0,10** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,90 | 1/100 | Muy Poco frecuente | **0,09** | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,18 | 0,70 | 0,10 | Poco frecuente | **0,13** | 0,15 | 0,60 | 0,10 | Poco frecuente | **0,09** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,40 | 0,75 | 1 | Normal | **0,30** | 0,08 | 0,45 | 0,10 | Poco frecuente | **0,04** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,30 | 0,60 | 1 | Normal | **0,18** | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,45 | 0,90 | 1 | Normal | **0,41** | 0,45 | 0,70 | 1 | Normal | **0,32** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,50 | 0,73 | 10 | Frecuente | **0,37** | 0,40 | 0,68 | 10 | Frecuente | **0,27** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,10 | 0,45 | 0,10 | Poco frecuente | **0,05** | 0,10 | 0,45 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,60 | 1 | Normal | **0,07** | 0,12 | 0,75 | 1 | Normal | **0,09** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | | | | | | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | | | | | | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | | | | | | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | | | | | | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | | | | | | | | | | |
| **E.25** Pérdida de equipos | 0,45 | 0,80 | 0,10 | Poco frecuente | **0,36** | 0,25 | 0,85 | 0,10 | Poco frecuente | **0,21** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | | | | | | | | | | |
| **A.6** Abuso de Privilegios de Acceso | | | | | | | | | | |
| **A.7** Uso no previsto | | | | | | | | | | |
| **A.11** Acceso no Autorizado | | | | | | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | | | | | | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | | | | | | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | | | | | | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** | 0,05 | 0,85 | 0,10 | Poco frecuente | **0,04** |
| **A.26** Ataque destructivo | 0,05 | 0,90 | 0,10 | Poco frecuente | **0,05** | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** |

| AMENAZAS | MOUSE | | | | | TECLADO | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,65 | 1/100 | Muy Poco frecuente | **0,07** | 0,10 | 0,70 | 1/100 | Muy Poco frecuente | **0,07** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,68 | 0,10 | Poco frecuente | **0,11** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,65 | 1/100 | Muy Poco frecuente | **0,07** | 0,10 | 0,70 | 1/100 | Muy Poco frecuente | **0,07** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,16 | 0,68 | 0,10 | Poco frecuente | **0,11** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,10 | 0,50 | 1 | Normal | **0,05** | 0,10 | 0,54 | 1 | Normal | **0,05** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,15 | 0,58 | 0,10 | Poco frecuente | **0,09** | 0,15 | 0,58 | 0,10 | Poco frecuente | **0,09** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,35 | 0,72 | 1 | Normal | **0,25** | 0,35 | 0,76 | 1 | Normal | **0,27** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,70 | 10 | Frecuente | **0,25** | 0,35 | 0,75 | 10 | Frecuente | **0,26** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,75 | 1 | Normal | **0,09** | 0,12 | 0,80 | 1 | Normal | **0,10** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | | | | | | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | | | | | | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | | | | | | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | | | | | | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | | | | | | | | | | |
| **E.25** Pérdida de equipos | 0,15 | 0,75 | 1/10 | Poco frecuente | **0,11** | 0,15 | 0,80 | 0,10 | Poco frecuente | **0,12** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | | | | | | | | | | |
| **A.6** Abuso de Privilegios de Acceso | | | | | | | | | | |
| **A.7** Uso no previsto | | | | | | | | | | |
| **A.11** Acceso no Autorizado | | | | | | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | | | | | | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | | | | | | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | | | | | | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,07 | 0,65 | 0,10 | Poco frecuente | **0,05** | 0,07 | 0,75 | 0,10 | Poco frecuente | **0,05** |
| **A.26** Ataque destructivo | 0,05 | 0,60 | 0,10 | Poco frecuente | **0,03** | 0,05 | 0,65 | 0,10 | Poco frecuente | **0,03** |

| AMENAZAS | ACCESS POINT | | | | | IMPRESORA | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,85 | 1/100 | Muy Poco frecuente | **0,09** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,85 | 1/100 | Muy Poco frecuente | **0,09** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** | 0,15 | 0,70 | 0,10 | Poco frecuente | **0,11** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,15 | 0,60 | 1/10 | Poco frecuente | **0,09** | 0,48 | 0,75 | 10 | Frecuente | **0,36** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,30 | 0,75 | 1 | Normal | **0,23** | 0,23 | 0,70 | 1 | Normal | **0,16** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,27 | 0,70 | 1/10 | Poco frecuente | **0,19** | 0,35 | 0,76 | 1 | Normal | **0,27** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,80 | 1 | Normal | **0,28** | 0,45 | 0,85 | 10 | Frecuente | **0,38** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,75 | 1 | Normal | **0,09** | 0,12 | 0,80 | 1 | Normal | **0,10** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | 0,12 | 0,88 | 1 | Normal | **0,11** | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | 0,10 | 0,62 | 0,10 | Poco frecuente | **0,06** | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** | 0,12 | 0,75 | 1 | Normal | **0,09** |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | 0,22 | 0,68 | 10 | Frecuente | **0,15** | | | | | |
| **E.25** Pérdida de equipos | 0,15 | 0,90 | 0,10 | Poco frecuente | **0,14** | 0,23 | 0,83 | 0,10 | Poco frecuente | **0,19** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** | | | | | |
| **A.6** Abuso de Privilegios de Acceso | 0,15 | 0,45 | 0,10 | Poco frecuente | **0,07** | | | | | |
| **A.7** Uso no previsto | 0,18 | 0,60 | 0,10 | Poco frecuente | **0,11** | | | | | |
| **A.11** Acceso no Autorizado | 0,2 | 0,60 | 1 | Normal | **0,12** | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | 0,15 | 0,90 | 1 | Normal | **0,14** | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | 0,15 | 0,78 | 0,10 | Poco frecuente | **0,12** | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | 0,15 | 0,72 | 10 | Frecuente | **0,11** | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,07 | 0,90 | 0,10 | Poco frecuente | **0,06** | 0,07 | 0,85 | 0,10 | Poco frecuente | **0,06** |
| **A.26** Ataque destructivo | 0,05 | 0,65 | 0,10 | Poco frecuente | **0,03** | 0,05 | 0,75 | 0,10 | Poco frecuente | **0,04** |

**Cuadro 4.15**. Servicio:Rectorado y Jurídico

| AMENAZAS | CPU | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | DAÑO EN EL DISCO DURO | | | | | DAÑO EN LA FUENTE DE PODER | | | | |
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,83 | 1/100 | Muy Poco frecuente | **0,08** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,90 | 1/100 | Muy Poco frecuente | **0,09** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,20 | 0,60 | 0,10 | Poco frecuente | **0,12** | 0,20 | 0,70 | 0,10 | Poco frecuente | **0,14** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,25 | 0,55 | 1 | Normal | **0,14** | 0,35 | 0,80 | 1 | Normal | **0,28** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,30 | 0,60 | 1 | Normal | **0,18** | 0,45 | 0,75 | 1 | Normal | **0,34** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,45 | 0,70 | 1 | Normal | **0,32** | 0,45 | 0,90 | 1 | Normal | **0,41** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,50 | 0,75 | 10 | Frecuente | **0,38** | 0,50 | 0,90 | 10 | Frecuente | **0,45** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,10 | 0,45 | 0,10 | Poco frecuente | **0,05** | 0,10 | 0,45 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,60 | 1 | Normal | **0,07** | 0,12 | 0,60 | 1 | Normal | **0,07** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | 0,50 | 0,75 | 1 | Normal | **0,38** | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | 0,05 | 0,60 | 1 | Normal | **0,03** | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | 0,05 | 0,60 | 1 | Normal | **0,03** | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,25 | 0,80 | 1 | Normal | **0,20** | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | 0,60 | 0,65 | 10 | Frecuente | **0,39** | | | | | |
| **E.25** Pérdida de equipos | 0,45 | 0,80 | 0,10 | Poco frecuente | **0,36** | 0,45 | 0,80 | 0,10 | Poco frecuente | **0,36** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** | | | | | |
| **A.6** Abuso de Privilegios de Acceso | 0,05 | 0,50 | 0,10 | Poco frecuente | **0,03** | | | | | |
| **A.7** Uso no previsto | 0,05 | 0,40 | 0,10 | Poco frecuente | **0,02** | | | | | |
| **A.11** Acceso no Autorizado | 0,10 | 0,80 | 0,10 | Poco frecuente | **0,08** | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | 0,15 | 0,76 | 0,10 | Poco frecuente | **0,11** | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | 0,05 | 0,83 | 0,10 | Poco frecuente | **0,04** | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | 0,35 | 0,75 | 1 | Normal | **0,26** | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** |
| **A.26** Ataque destructivo | 0,05 | 0,75 | 0,10 | Poco frecuente | **0,04** | 0,05 | 0,90 | 0,10 | Poco frecuente | **0,05** |

| AMENAZAS | CPU | | | | | MONITOR | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | DAÑO EN LA MEMORIA RAM | | | | | | | | | |
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,65 | 0,10 | Poco frecuente | **0,10** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,90 | 1/100 | Muy Poco frecuente | **0,09** | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,18 | 0,70 | 0,10 | Poco frecuente | **0,13** | 0,15 | 0,60 | 0,10 | Poco frecuente | **0,09** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,40 | 0,75 | 1 | Normal | **0,30** | 0,08 | 0,45 | 0,10 | Poco frecuente | **0,04** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,30 | 0,60 | 1 | Normal | **0,18** | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,45 | 0,90 | 1 | Normal | **0,41** | 0,45 | 0,70 | 1 | Normal | **0,32** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,50 | 0,73 | 10 | Frecuente | **0,37** | 0,40 | 0,68 | 10 | Frecuente | **0,27** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,10 | 0,45 | 0,10 | Poco frecuente | **0,05** | 0,10 | 0,45 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,60 | 1 | Normal | **0,07** | 0,12 | 0,75 | 1 | Normal | **0,09** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | | | | | | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | | | | | | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | | | | | | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | | | | | | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | | | | | | | | | | |
| **E.25** Pérdida de equipos | 0,45 | 0,80 | 0,10 | Poco frecuente | **0,36** | 0,25 | 0,85 | 0,10 | Poco frecuente | **0,21** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | | | | | | | | | | |
| **A.6** Abuso de Privilegios de Acceso | | | | | | | | | | |
| **A.7** Uso no previsto | | | | | | | | | | |
| **A.11** Acceso no Autorizado | | | | | | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | | | | | | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | | | | | | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | | | | | | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** | 0,05 | 0,85 | 0,10 | Poco frecuente | **0,04** |
| **A.26** Ataque destructivo | 0,05 | 0,90 | 0,10 | Poco frecuente | **0,05** | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** |

| AMENAZAS | MOUSE | | | | | TECLADO | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,65 | 1/100 | Muy Poco frecuente | **0,07** | 0,10 | 0,70 | 1/100 | Muy Poco frecuente | **0,07** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,68 | 0,10 | Poco frecuente | **0,11** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,65 | 1/100 | Muy Poco frecuente | **0,07** | 0,10 | 0,70 | 1/100 | Muy Poco frecuente | **0,07** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,16 | 0,68 | 0,10 | Poco frecuente | **0,11** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,10 | 0,50 | 1 | Normal | **0,05** | 0,10 | 0,54 | 1 | Normal | **0,05** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,15 | 0,58 | 0,10 | Poco frecuente | **0,09** | 0,15 | 0,58 | 0,10 | Poco frecuente | **0,09** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,35 | 0,72 | 1 | Normal | **0,25** | 0,35 | 0,76 | 1 | Normal | **0,27** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,70 | 10 | Frecuente | **0,25** | 0,35 | 0,75 | 10 | Frecuente | **0,26** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 1/10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,75 | 1 | Normal | **0,09** | 0,12 | 0,80 | 1 | Normal | **0,10** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | | | | | | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | | | | | | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | | | | | | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | | | | | | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | | | | | | | | | | |
| **E.25** Pérdida de equipos | 0,15 | 0,75 | 0,10 | Poco frecuente | **0,11** | 0,15 | 0,80 | 0,10 | Poco frecuente | **0,12** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | | | | | | | | | | |
| **A.6** Abuso de Privilegios de Acceso | | | | | | | | | | |
| **A.7** Uso no previsto | | | | | | | | | | |
| **A.11** Acceso no Autorizado | | | | | | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | | | | | | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | | | | | | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | | | | | | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,07 | 0,65 | 0,10 | Poco frecuente | **0,05** | 0,07 | 0,75 | 0,10 | Poco frecuente | **0,05** |
| **A.26** Ataque destructivo | 0,05 | 0,60 | 0,10 | Poco frecuente | **0,03** | 0,05 | 0,65 | 0,10 | Poco frecuente | **0,03** |

| AMENAZAS | ACCESS POINT | | | | | IMPRESORA | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,85 | 1/100 | Muy Poco frecuente | **0,09** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,85 | 1/100 | Muy Poco frecuente | **0,09** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,16 | 0,78 | 0,10 | Poco frecuente | **0,12** | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,65 | 0,10 | Poco frecuente | **0,08** | 0,15 | 0,70 | 0,10 | Poco frecuente | **0,11** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,15 | 0,60 | 0,10 | Poco frecuente | **0,09** | 0,48 | 0,75 | 10 | Frecuente | **0,36** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,30 | 0,75 | 1 | Normal | **0,23** | 0,23 | 0,70 | 1 | Normal | **0,16** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,27 | 0,70 | 0,10 | Poco frecuente | **0,19** | 0,35 | 0,76 | 1 | Normal | **0,27** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,80 | 1 | Normal | **0,28** | 0,45 | 0,85 | 10 | Frecuente | **0,38** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,75 | 1 | Normal | **0,09** | 0,12 | 0,80 | 1 | Normal | **0,10** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | 0,12 | 0,88 | 1 | Normal | **0,11** | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | 0,10 | 0,62 | 0,10 | Poco frecuente | **0,06** | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** | 0,12 | 0,75 | 1 | Normal | **0,09** |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | 0,22 | 0,68 | 10 | Frecuente | **0,15** | | | | | |
| **E.25** Pérdida de equipos | 0,15 | 0,90 | 0,10 | Poco frecuente | **0,14** | 0,23 | 0,83 | 0,10 | Poco frecuente | **0,19** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** | | | | | |
| **A.6** Abuso de Privilegios de Acceso | 0,15 | 0,45 | 0,10 | Poco frecuente | **0,07** | | | | | |
| **A.7** Uso no previsto | 0,18 | 0,60 | 0,10 | Poco frecuente | **0,11** | | | | | |
| **A.11** Acceso no Autorizado | 0,2 | 0,60 | 1 | Normal | **0,12** | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | 0,15 | 0,90 | 1 | Normal | **0,14** | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | 0,15 | 0,78 | 0,10 | Poco frecuente | **0,12** | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | 0,15 | 0,72 | 10 | Frecuente | **0,11** | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,07 | 0,90 | 0,10 | Poco frecuente | **0,06** | 0,07 | 0,85 | 0,10 | Poco frecuente | **0,06** |
| **A.26** Ataque destructivo | 0,05 | 0,65 | 0,10 | Poco frecuente | **0,03** | 0,05 | 0,75 | 0,10 | Poco frecuente | **0,04** |

**Cuadro 4.16.** Servicio:audiovisuales

| AMENAZAS | CPU | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | DAÑO EN EL DISCO DURO | | | | | DAÑO EN LA FUENTE DE PODER | | | | |
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,83 | 1/100 | Muy Poco frecuente | **0,08** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,90 | 1/100 | Muy Poco frecuente | **0,09** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,20 | 0,60 | 0,10 | Poco frecuente | **0,12** | 0,20 | 0,70 | 0,10 | Poco frecuente | **0,14** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,25 | 0,55 | 1 | Normal | **0,14** | 0,35 | 0,80 | 1 | Normal | **0,28** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,30 | 0,60 | 1 | Normal | **0,18** | 0,45 | 0,75 | 1 | Normal | **0,34** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,45 | 0,70 | 1 | Normal | **0,32** | 0,45 | 0,90 | 1 | Normal | **0,41** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,50 | 0,75 | 10 | Frecuente | **0,38** | 0,50 | 0,90 | 10 | Frecuente | **0,45** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,10 | 0,45 | 0,10 | Poco frecuente | **0,05** | 0,10 | 0,45 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,60 | 1 | Normal | **0,07** | 0,12 | 0,60 | 1 | Normal | **0,07** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | 0,50 | 0,75 | 1 | Normal | **0,38** | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | 0,05 | 0,60 | 1 | Normal | **0,03** | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | 0,05 | 0,60 | 1 | Normal | **0,03** | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,25 | 0,80 | 1 | Normal | **0,20** | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | 0,60 | 0,65 | 10 | Frecuente | **0,39** | | | | | |
| **E.25** Pérdida de equipos | 0,45 | 0,80 | 0,10 | Poco frecuente | **0,36** | 0,45 | 0,80 | 0,10 | Poco frecuente | **0,36** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** | | | | | |
| **A.6** Abuso de Privilegios de Acceso | 0,05 | 0,50 | 0,10 | Poco frecuente | **0,03** | | | | | |
| **A.7** Uso no previsto | 0,05 | 0,40 | 0,10 | Poco frecuente | **0,02** | | | | | |
| **A.11** Acceso no Autorizado | 0,10 | 0,80 | 0,10 | Poco frecuente | **0,08** | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | 0,15 | 0,76 | 0,10 | Poco frecuente | **0,11** | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | 0,05 | 0,83 | 0,10 | Poco frecuente | **0,04** | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | 0,35 | 0,75 | 1 | Normal | **0,26** | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** |
| **A.26** Ataque destructivo | 0,05 | 0,75 | 0,10 | Poco frecuente | **0,04** | 0,05 | 0,90 | 0,10 | Poco frecuente | **0,05** |

| AMENAZAS | CPU | | | | | MONITOR | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | DAÑO EN LA MEMORIA RAM | | | | | | | | | |
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,65 | 0,10 | Poco frecuente | **0,10** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,90 | 1/100 | Muy Poco frecuente | **0,09** | 0,10 | 0,75 | 1/100 | Muy Poco frecuente | **0,08** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** | 0,18 | 0,75 | 0,10 | Poco frecuente | **0,14** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,18 | 0,70 | 0,10 | Poco frecuente | **0,13** | 0,15 | 0,60 | 0,10 | Poco frecuente | **0,09** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,40 | 0,75 | 1 | Normal | **0,30** | 0,08 | 0,45 | 0,10 | Poco frecuente | **0,04** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,30 | 0,60 | 1 | Normal | **0,18** | 0,15 | 0,65 | 1/10 | Poco frecuente | **0,10** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,45 | 0,90 | 1 | Normal | **0,41** | 0,45 | 0,70 | 1 | Normal | **0,32** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,50 | 0,73 | 10 | Frecuente | **0,37** | 0,40 | 0,68 | 10 | Frecuente | **0,27** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,10 | 0,45 | 0,10 | Poco frecuente | **0,05** | 0,10 | 0,45 | 1/10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,60 | 1 | Normal | **0,07** | 0,12 | 0,75 | 1 | Normal | **0,09** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | | | | | | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | | | | | | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | | | | | | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | | | | | | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | | | | | | | | | | |
| **E.25** Pérdida de equipos | 0,45 | 0,80 | 0,10 | Poco frecuente | **0,36** | 0,25 | 0,85 | 0,10 | Poco frecuente | **0,21** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | | | | | | | | | | |
| **A.6** Abuso de Privilegios de Acceso | | | | | | | | | | |
| **A.7** Uso no previsto | | | | | | | | | | |
| **A.11** Acceso no Autorizado | | | | | | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | | | | | | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | | | | | | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | | | | | | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** | 0,05 | 0,85 | 0,10 | Poco frecuente | **0,04** |
| **A.26** Ataque destructivo | 0,05 | 0,90 | 0,10 | Poco frecuente | **0,05** | 0,05 | 0,80 | 0,10 | Poco frecuente | **0,04** |

| AMENAZAS | MOUSE | | | | | TECLADO | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,65 | 1/100 | Muy Poco frecuente | **0,07** | 0,10 | 0,70 | 1/100 | Muy Poco frecuente | **0,07** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,68 | 0,10 | Poco frecuente | **0,11** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,65 | 1/100 | Muy Poco frecuente | **0,07** | 0,10 | 0,70 | 1/100 | Muy Poco frecuente | **0,07** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,16 | 0,68 | 0,10 | Poco frecuente | **0,11** | 0,16 | 0,75 | 0,10 | Poco frecuente | **0,12** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** | 0,12 | 0,60 | 0,10 | Poco frecuente | **0,07** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,10 | 0,50 | 1 | Normal | **0,05** | 0,10 | 0,54 | 1 | Normal | **0,05** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,15 | 0,58 | 0,10 | Poco frecuente | **0,09** | 0,15 | 0,58 | 0,10 | Poco frecuente | **0,09** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,35 | 0,72 | 1 | Normal | **0,25** | 0,35 | 0,76 | 1 | Normal | **0,27** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,70 | 10 | Frecuente | **0,25** | 0,35 | 0,75 | 10 | Frecuente | **0,26** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,75 | 1 | Normal | **0,09** | 0,12 | 0,80 | 1 | Normal | **0,10** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | | | | | | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | | | | | | |
| **E.2** Errores de Administrador | | | | | | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | | | | | | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | | | | | | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | | | | | | | | | | |
| **E.25** Pérdida de equipos | 0,15 | 0,75 | 0,10 | Poco frecuente | **0,11** | 0,15 | 0,80 | 0,10 | Poco frecuente | **0,12** |
| **ATAQUES INTENCIONADOS (A)** | | | | | | | | | | |
| **A.5** Suplantación de la identidad del usuario | | | | | | | | | | |
| **A.6** Abuso de Privilegios de Acceso | | | | | | | | | | |
| **A.7** Uso no previsto | | | | | | | | | | |
| **A.11** Acceso no Autorizado | | | | | | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | | | | | | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | | | | | | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | | | | | | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,07 | 0,65 | 0,10 | Poco frecuente | **0,05** | 0,07 | 0,75 | 0,10 | Poco frecuente | **0,05** |
| **A.26** Ataque destructivo | 0,05 | 0,60 | 0,10 | Poco frecuente | **0,03** | 0,05 | 0,65 | 0,10 | Poco frecuente | **0,03** |

| AMENAZAS | PROYECTORES | | | | |
|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | |
| **N.1** Fuego (Incendios) | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** |
| **N.2** Daños por agua (Inundaciones) | 0,16 | 0,83 | 0,10 | Poco frecuente | **0,13** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,75 | 0,10 | Poco frecuente | **0,09** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | |
| **I.1** Fuego (Incendios) | 0,10 | 0,80 | 1/100 | Muy Poco frecuente | **0,08** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,16 | 0,83 | 0,10 | Poco frecuente | **0,13** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,75 | 0,10 | Poco frecuente | **0,09** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,30 | 0,79 | 10 | Frecuente | **0,24** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,15 | 0,58 | 0,10 | Poco frecuente | **0,09** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,45 | 0,80 | 1 | Normal | **0,36** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,80 | 1 | Normal | **0,28** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,12 | 0,85 | 1 | Normal | **0,10** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | | | | | |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | |
| **E.2** Errores de Administrador | | | | | |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | | | | | |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | | | | | |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | | | | | |
| **E.25** Pérdida de equipos | 0,15 | 0,90 | 0,10 | Poco frecuente | **0,14** |
| **ATAQUES INTENCIONADOS (A)** | | | | | |
| **A.5** Suplantación de la identidad del usuario | | | | | |
| **A.6** Abuso de Privilegios de Acceso | | | | | |
| **A.7** Uso no previsto | | | | | |
| **A.11** Acceso no Autorizado | | | | | |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | | | | | |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | | | | | |
| **A.24** Denegación de servicio (Saturación del sistema informático) | | | | | |
| **A.25** Robo (Pérdida de Equipos) | 0,07 | 0,90 | 0,10 | Poco frecuente | **0,06** |
| **A.26** Ataque destructivo | 0,05 | 0,75 | 0,10 | Poco frecuente | **0,04** |

**Cuadro 4.17.** Servicio: control de acceso

| AMENAZAS | BIOMÉTRICOS | | | | |
|---|---|---|---|---|---|
| | PROBABILIDAD | IMPACTO | FRECUENCIA | | RIESGO |
| **DESASTRES NATURALES (N)** | | | | | |
| **N.1** Fuego (Incendios) | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** |
| **N.2** Daños por agua (Inundaciones) | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** |
| **N.*** Desastres naturales (Otros incidentes que se producen sin intervención humana) | 0,12 | 0,65 | 0,10 | Poco Frecuente | **0,08** |
| **DE ORIGEN INDUSTRIAL (I)** | | | | | |
| **I.1** Fuego (Incendios) | 0,15 | 0,75 | 0,10 | Poco Frecuente | **0,11** |
| **I.2** Daños por agua (Escape, fugas, inundaciones) | 0,12 | 0,75 | 0,10 | Poco Frecuente | **0,09** |
| **I.*** Desastres Industriales (Otros desastres debido a la actividad humana) | 0,12 | 0,65 | 0,10 | Poco Frecuente | **0,08** |
| **I.3** Contaminación mecánica (Vibraciones, polvo, suciedad) | 0,06 | 0,45 | 0,10 | Poco Frecuente | **0,03** |
| **I.4** Contaminación electromagnética (Interferencias de radios, campos magnéticos, luz ultravioleta,...) | 0,10 | 0,75 | 1 | Normal | **0,08** |
| **I.5** Avería de origen físico o lógico (Fallos de los equipos o fallos en los programas) | 0,35 | 0,85 | 1 | Normal | **0,30** |
| **I.6** Corte de suministro eléctrico (Cese de la alimentación de potencia) | 0,35 | 0,75 | 1 | Normal | **0,26** |
| **I.7** Condiciones inadecuadas de temperatura o humedad (Climatización) | 0,08 | 0,60 | 0,10 | Poco frecuente | **0,05** |
| **I.8** Fallo de Servicios de comunicaciones (Destrucción o detección Física) | 0,35 | 0,78 | 1 | Normal | **0,27** |
| **I.11** Emanaciones electromagnéticas (Fuga de información) | 0,12 | 0,88 | 1 | Normal | **0,11** |
| **ERRORES Y FALLOS NO INTENCIONADOS (E)** | | | | | |
| **E.2** Errores de Administrador | 0,08 | 0,72 | 0,10 | Poco frecuente | **0,06** |
| **E.9** Errores de [re-] encaminamiento (Ruta incorrecta de envío) | 0,10 | 0,62 | 0,10 | Poco frecuente | **0,06** |
| **E.23** Errores de Mantenimiento / Actualización de Equipos Hardware | 0,15 | 0,65 | 0,10 | Poco frecuente | **0,10** |
| **E.24** Caída del sistema por agotamiento de Recursos (Saturación del Sistema Informático) | 0,22 | 0,68 | 10 | Frecuente | **0,15** |
| **E.25** Pérdida de equipos | 0,15 | 0,80 | 1 | Normal | **0,12** |
| **ATAQUES INTENCIONADOS (A)** | | | | | |
| **A.5** Suplantación de la identidad del usuario | 0,15 | 0,75 | 1 | Normal | **0,11** |
| **A.6** Abuso de Privilegios de Acceso | 0,15 | 0,85 | 1 | Normal | **0,13** |
| **A.7** Uso no previsto | 0,18 | 0,60 | 0,10 | Poco frecuente | **0,11** |
| **A.11** Acceso no Autorizado | 0,2 | 0,80 | 1 | Normal | **0,16** |
| **A.12** Análisis de tráfico (Monitorización de tráfico) | 0,14 | 0,87 | 1 | Normal | **0,12** |
| **A.23** Manipulación de los Equipos (Alteración intensionada del Funcionamiento de los programas) | 0,14 | 0,66 | 1 | Normal | **0,09** |
| **A.24** Denegación de servicio (Saturación del sistema informático) | 0,22 | 0,85 | 1 | Normal | **0,19** |
| **A.25** Robo (Pérdida de Equipos) | 0,15 | 0,75 | 0,10 | Poco Frecuente | **0,11** |
| **A.26** Ataque destructivo | 0,15 | 0,75 | 0,10 | Poco Frecuente | **0,11** |

Por consiguiente, una vez realizadas las matrices de riesgos se continuó con la elaboración del cuestionario de incidencias informáticas, con la finalidad de conocer los inconvenientes mas relevantes que presenta la institución. A continuación se describen los resultados obtenidos por cada una de las interrogantes efectuadas:

| DATOS GENERALES | | | |
|---|---|---|---|
| **¿CUÁLES DE LOS SIGUIENTES INCIDENTES INFORMÁTICOS SE PRESENTAN A MENUDO EN SU DEPARTAMENTO?** | | | |
| **INCIDENTES** | **POBLACIÓN** | **TOTAL** | **%** |
| **1.** PROBLEMAS CON FUEGO (INCENDIOS) | 26 | **0** | 0,00% |
| **2.** DAÑOS EN LOS EQUIPOS POR AGUA (ESCAPE, FUGAS, INUNDACIONES) | 26 | **1** | 3,85% |
| **3**. PRESENCIA DE DESASTRES INDUSTRIALES (DEBIDO A LA ACTIVIDAD HUMANA) | 26 | **2** | 7,69% |
| **4.** ROBO DE EQUIPOS INFORMÁTICOS | 26 | **4** | 15,38% |
| **5**. CORTE DE SUMINISTRO ELÉCTRICO | 26 | **6** | 23,08% |
| **6.** DENEGACIÓN DEL SERVICIO (SATURACIÓN DEL SISTEMA INFORMÁTICO) | 26 | **11** | 42,31% |
| **7**. FALLO DEL SERVICIO DE COMUNICACIÓN (PROBLEMAS CON LA CONEXIÓN A INTERNET) | 26 | **24** | 92,31% |
| **8.** INCONVENIENTES CON EL SERVICIO DE CORREO ELECTRÓNICO DE LA INSTITUCIÓN | 26 | **19** | 73,08% |
| **9.** PROBLEMAS POR SUMINISTRO DE COMPONENTES A COMPUTADORAS DE ESCRITORIO | 26 | **12** | 46,15% |
| **10.** DEPERFECTOS DE HARDWARE (COMPONENTES INTERNOS DEL CPU) | 26 | **9** | 34,62% |
| **11.** PROBLEMAS DE VIDEO (PROYECTORES, PANTALLAS O MONITORES) | 26 | **5** | 19,23% |
| **12.** PROBLEMAS POR VIRUS EN LAS COMPUTADORAS | 26 | **20** | 76,92% |
| **13.** REINICIO CONSTANTE DE LAS COMPUTADORAS | 26 | **12** | 46,15% |
| **14.** PROBLEMAS AL ACTUALIZAR PROGRAMAS (SOFTWARE) | 26 | **9** | 34,62% |
| **15.** PROBLEMAS AL EJECUTAR PROGRAMAS (ABREN LENTOS O NO SE EJECUTAN) | 26 | **12** | 46,15% |
| **16.** ALERTA POR LICENCIAMIENTO DE PROGRAMAS (PIRATAS) | 26 | **12** | 46,15% |
| **17.** FALTA DE MANTENIMIENTO PREVENTIVO | 26 | **21** | 80,77% |
| **18.** FALTA DE MANTENIMIENTO CORRECTIVO | 26 | **25** | 96,15% |
| **19.** DAÑOS EN LAS IMPRESORAS MULTIFUNCIÓN | 26 | **14** | 53,85% |
| **20.** PROBLEMAS POR CAMBIO DE SUMINISTRO A LOS EQUIPOS DE IMPRESIÓN | 26 | **20** | 76,92% |
| **21.** DAÑOS EN EL HARDWARE DE SCANNER | 26 | **1** | 3,85% |

**Cuadro 4.18.** Total de incidentes informáticos que se presentan en la ESPAM-MFL

1. Problemas con fuego (incendios).

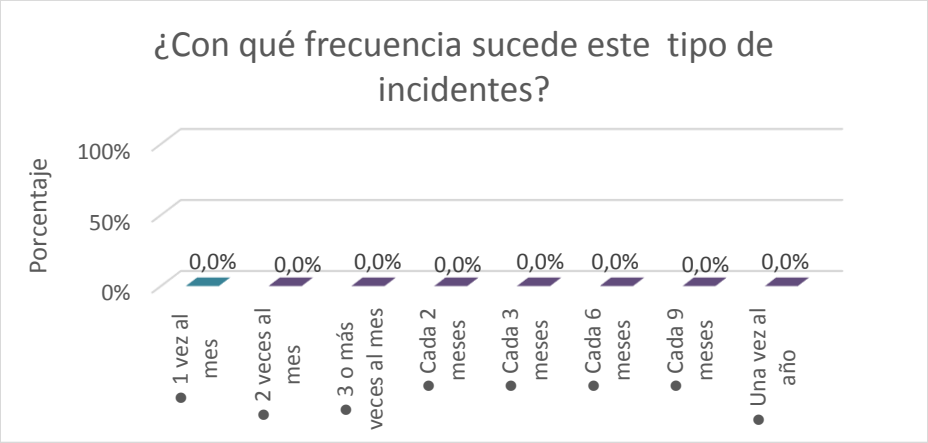



**Gráfico 4.15.** Frecuencia de incidentes con fuego

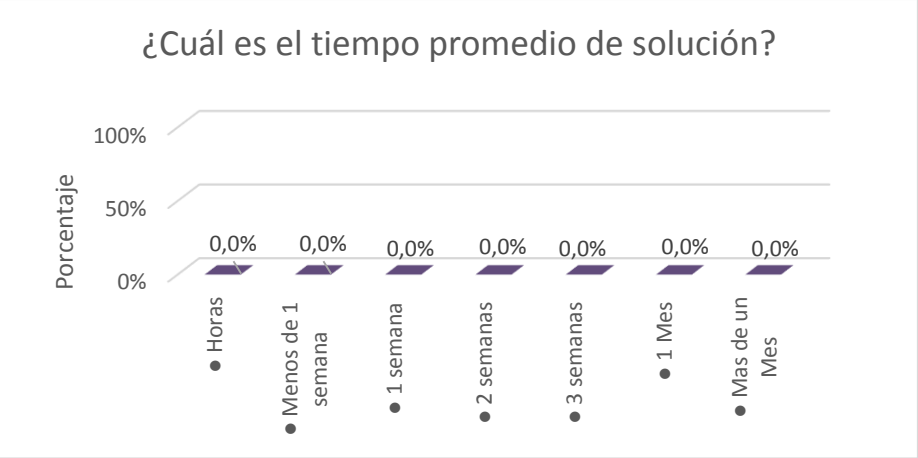



**Gráfico 4.16.** Tiempo promedio de solución a incidentes con fuego

Los resultados obtenidos muestran que la institución no ha sufrido ningún inconveniente con respecto a incendios y otros referentes con el fuego.

2. Daños en los equipos por agua ( escape, fugas e inundaciones).

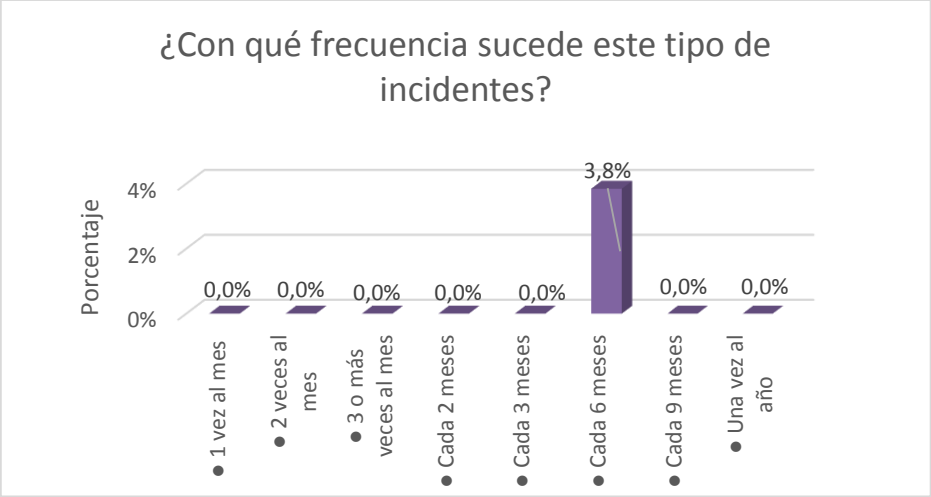



**Gráfico 4.17.** Frecuencia de incidentes con agua

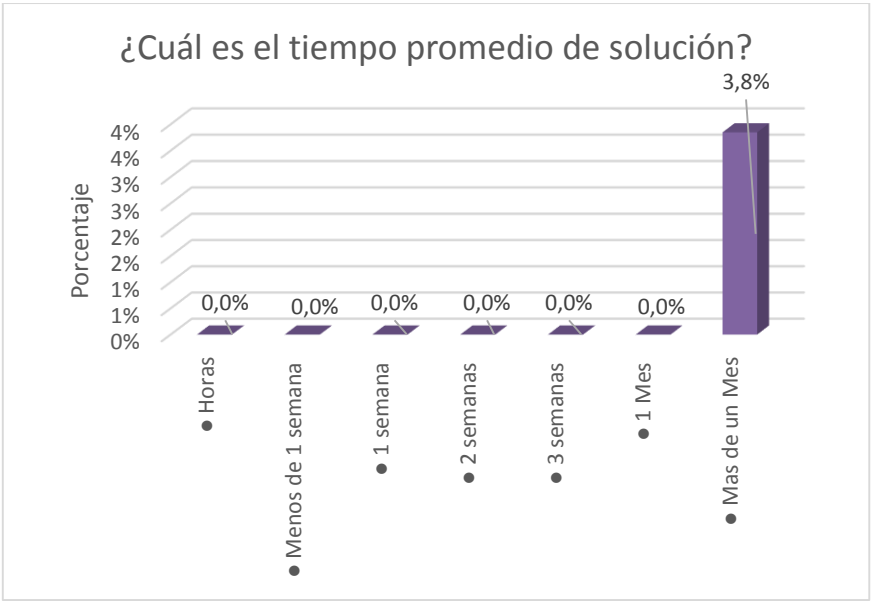



**Gráfico 4.18.** Tiempo promedio de solución a incidentes con agua

El 3.8% de la población manifiesta haber sufrido incidentes con agua en una frecuencia de seis meses, por lo consiguiente, el tiempo promedio de solución es de mas de un mes, consiguiendo así un 96.2% de la población que no presenta este tipo de incidencia en su departamento.

3. Presencia de desastres industriales (debido a la actividad humana).

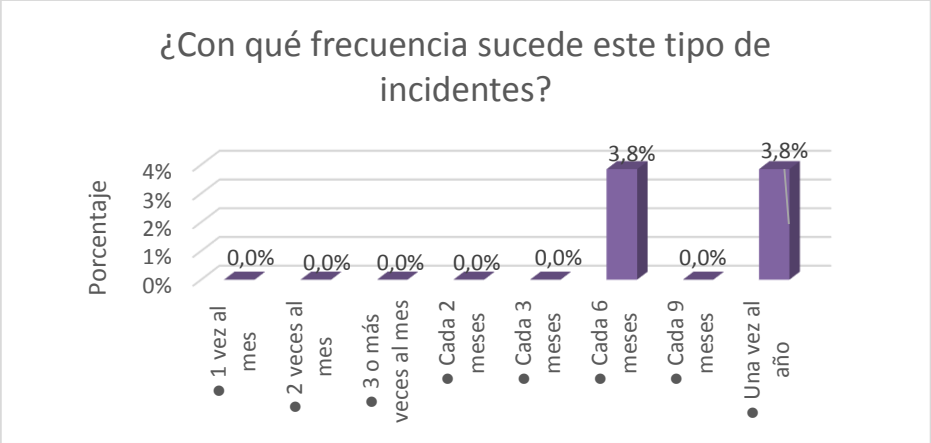



**Gráfico 4.19.** Frecuencia de desastres industriales

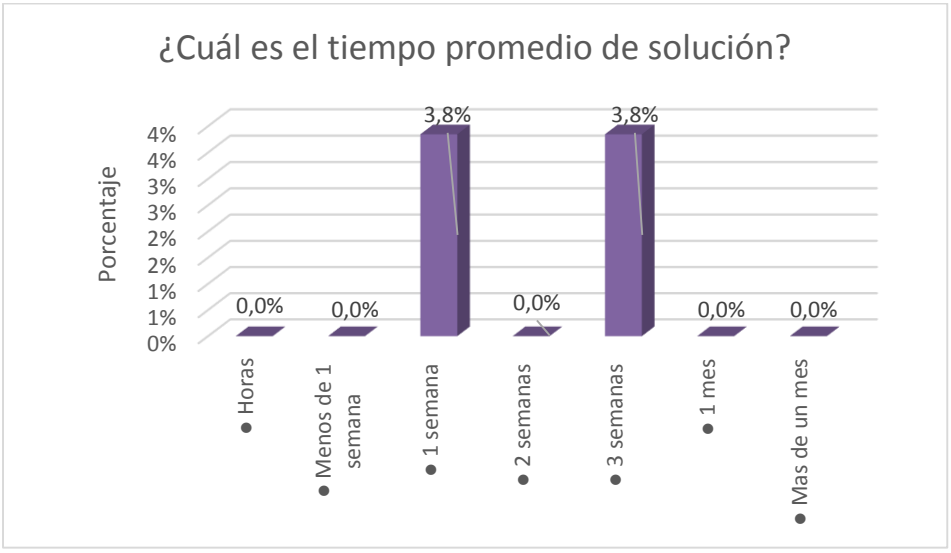



**Gráfico 4.20.** Tiempo promedio de solución a desastres industriales

El 7,69% de personas encuestadas declaran haber presentado desastres industriales y que afectaron a los equipos informáticos de la institución, la misma que se manifiesta cada seis meses y una vez al año en un 3.8%, además se presenta el tiempo promedio de solución a la incidencia en una semana con un 3.8% y el mismo porcentaje para 3 semanas, tomando en cuenta, que el 92.31% notificaron no presentar este tipo de incidencias.

4. Robo de equipos informáticos.

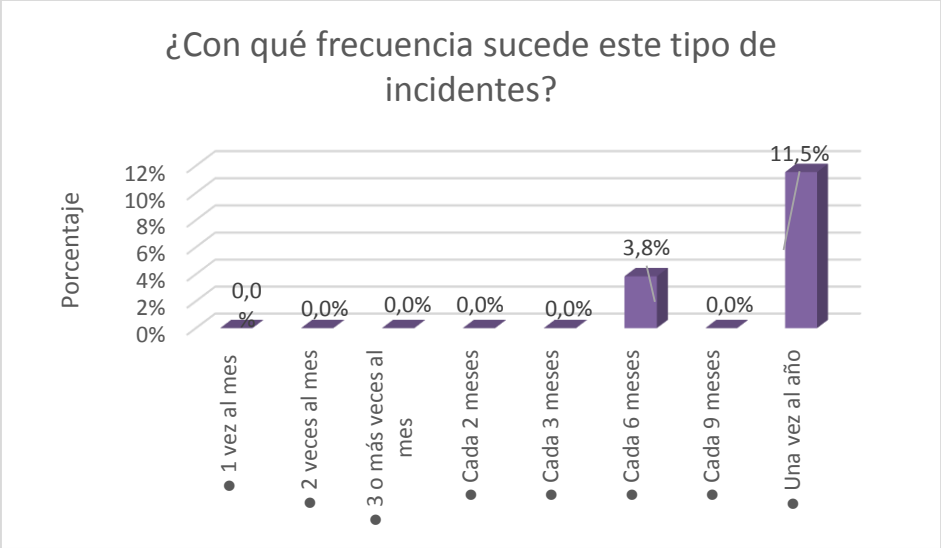



**Gráfico 4.21.** Frecuencia de robos de equipos informáticos

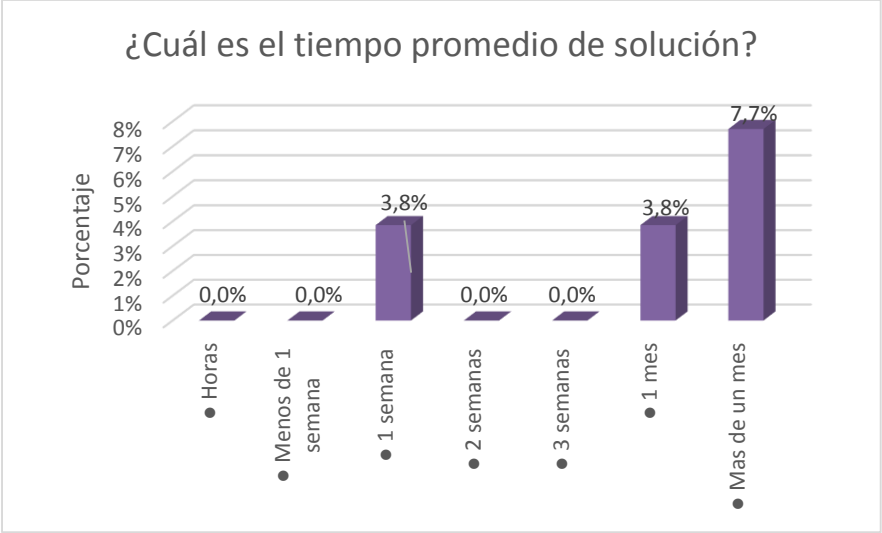



**Gráfico 4.22.** Tiempo promedio de solución a robo de equipos informáticos

Como se pudo observar, se han sucitado en la instirución robos de los equipos informáticos en una medida de 15,38%, para lo cual, la frecuencia es de cada seis meses y una vez al año, en porcentajes del 3.8% y 11.5% respectivamente. Además, el tiempo promedio para dar solución es del 3.8% para una semana y un mes, y del 7.7% para mas de un mes. Se agrega a esto, que el 84.62% notifica no haber presentado este tipo de incidencia

5. Corte de suministro eléctrico.

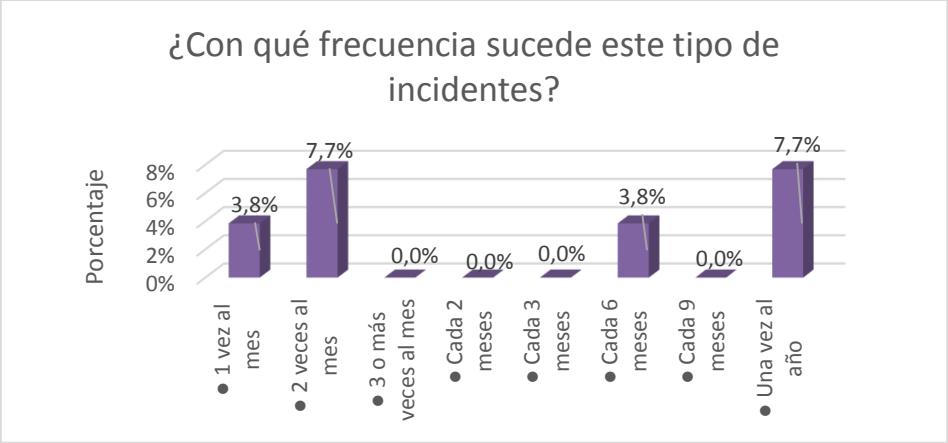



**Gráfico 4.23.** Frecuencia de cortes de suministro eléctrico

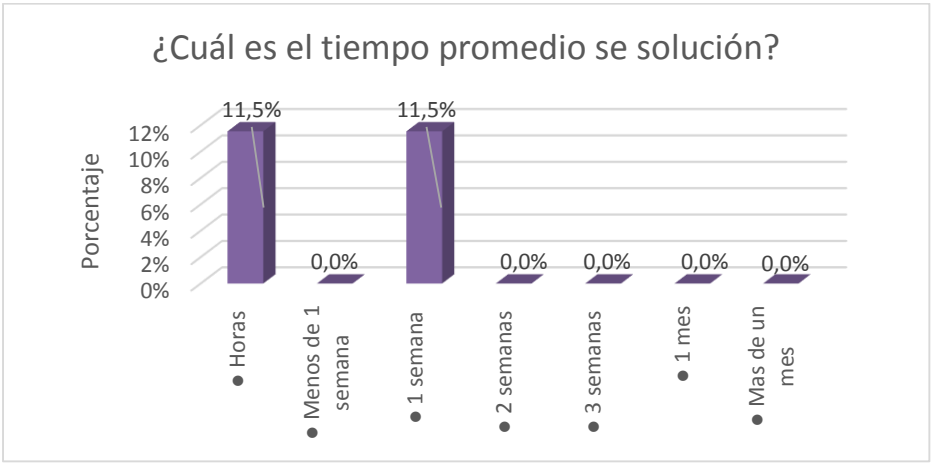



**Gráfico 4.24.** Tiempo promedio de solución a cortes de suministro eléctrico

En concordancia con los datos mostrados, el 23.08% de la población indica haber presenciado cortes de suministro eléctrico, con una frecuencia del 3.8% una vez al mes y cada seis meses, mientras que el 7.7% tenían esta incidencia una vez al año; el tiempo promedio de solución según los resultados es por horas y en una semana en un 11.5%, acotando que el 76.92% de encuentados no han presentado la incidencia.

6. Denegación del servicio (saturación del sistema informático).

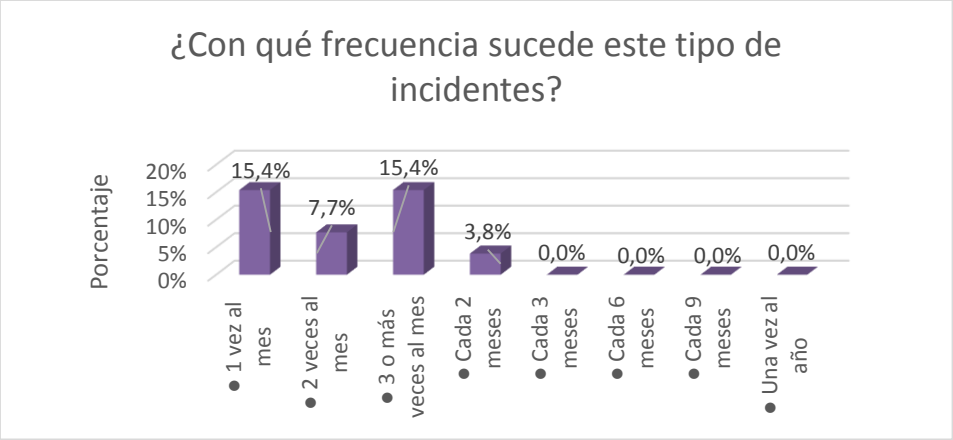



**Gráfico 4.25.** Frecuencia de denegación del servicio

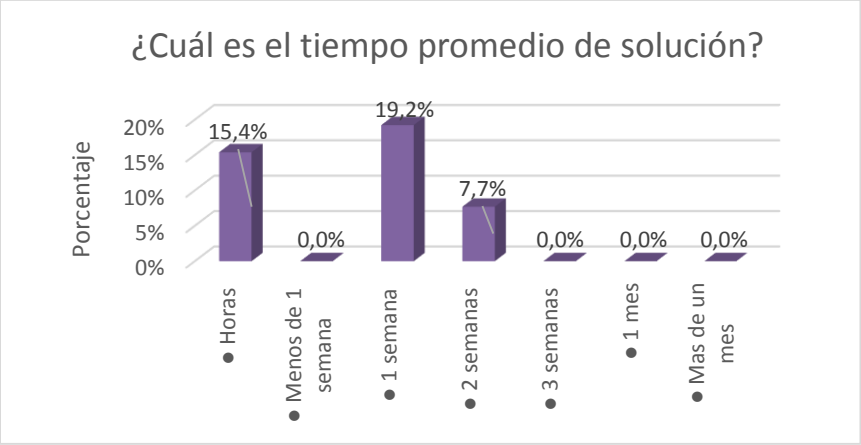



**Gráfico 4.26.** Tiempo promedio de solución a denegación del servicio

El 42.31% de la población presenta inconvenientes con la saturación del sistema informatico, en una frecuencia del 7.7% dos veces al mes, el 15.4% una vez al mes y tres o mas veces al mes, y el 3.8% cada dos meses; mientras que su tiempo promedio de solución es por horas en un 15.4%, una semana el 19.2% y en dos semanas el 7.7%, notificando que el 57.69% no presentan este tipo de incidencias.

7. Fallo del servicio de comunicación (problemas con la conexión a internet).

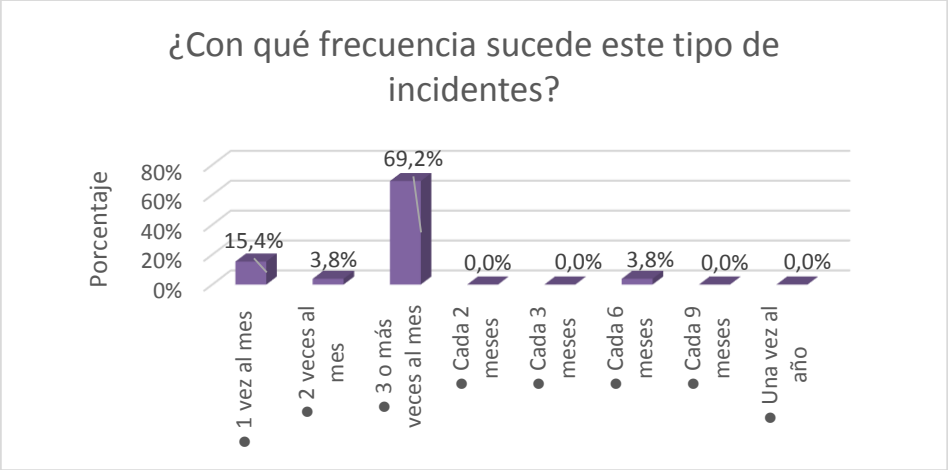



**Gráfico 4.27.** Frecuencia de problemas con la conexión de internet

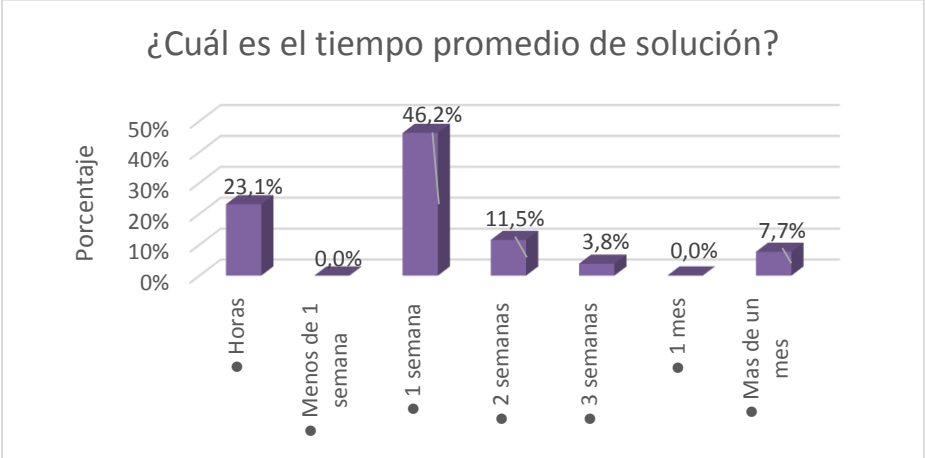



**Gráfico 4.28.** Tiempo promedio de solución a problemas con la conexión de internet

Según las ilustraciones, el 92.31% de la población posee problemas con la conexión a internet, consiguiendo así, una frecuencia del 69.2% cada tres o mas veces al mes, mientras que el 15.4% presenta inconveniente una vez al mes y el 3.8% cada 2 veces al mes y cada 6 meses. Además, el porcentaje en tiempo promedio de solución es del 46.2% para una semana, el 23.1% notificaba que se soluciona en horas, mientras que el 11.5% indica que tarda dos semanas y el 7.7% de la población manifiesta que se soluciona en mas de un mes; agregando, que el 7.69% de personas encuestadas no señalaron presentar la incidencia.

Para lo cual, se puntializa que los fallos con el servicio de comunicación es el mayor problema que posee la institución.

8. Inconvenientes con el servicio de correo electrónico de la institución.

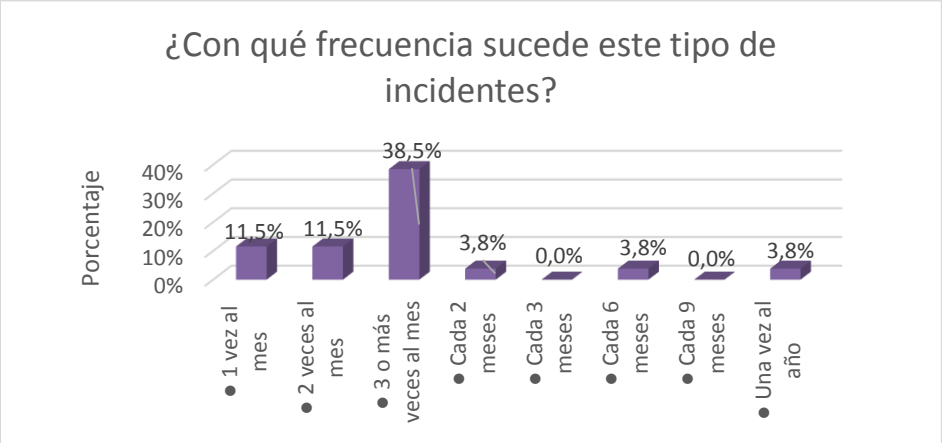



**Gráfico 4.29**. Frecuencia de inconvenientes con el correo electrónico institucional

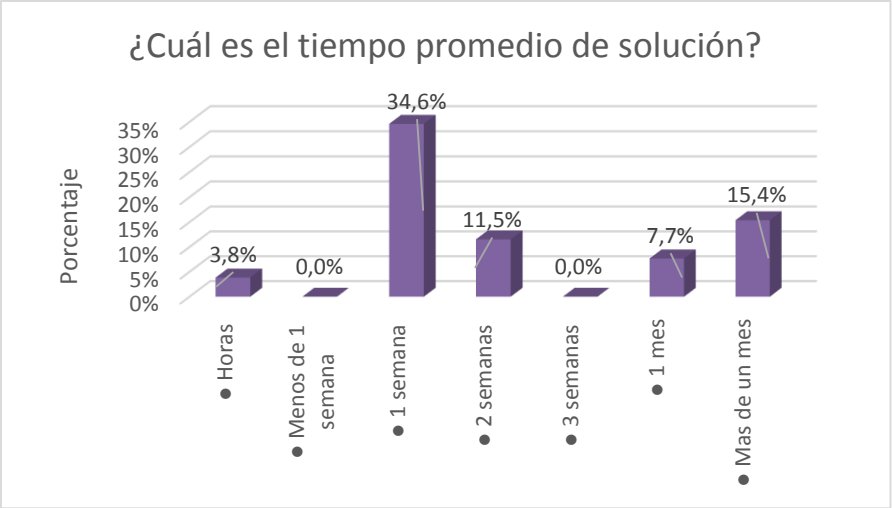



**Gráfico 4.30.** Tiempo promedio de solución a inconvenientes con el correo electrónico institucional

El 73. 08% de la población tiene problemas con el correo electrónico de la institución; de los cuales, el 38.5% presenta el inconveniente tres o mas veces al mes, el 11.5% menciona que el incidente se da una vez y cada dos veces al mes, mientras que el 3.8% notifica tener el inconveniente cada dos meses, seis meses y una vez al año. Agregando, que su tiempo promedio de solución es del

34.6% durante una semana, el 15.4% mas de un mes, del 11.5% en 2 semanas, el 7.7% en un mes y el 3.8% en horas. Adicionalmente, se complementa que el 26.92% no presenta este tipo de incidencia en su departamento.

9. Problemas por suministro de componentes a computadoras de escritorio como son: mouse, teclado y parlantes

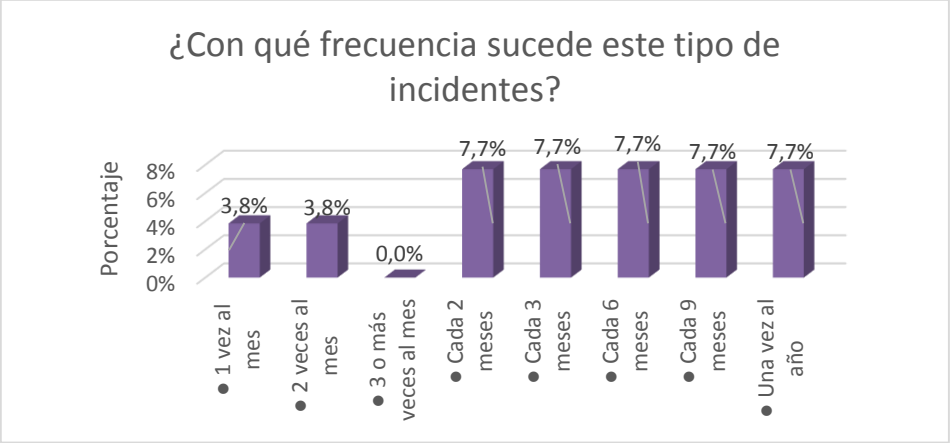



**Gráfico 4.31.** Frecuencia de problemas por suministro de componentes a computadoras de escritorio

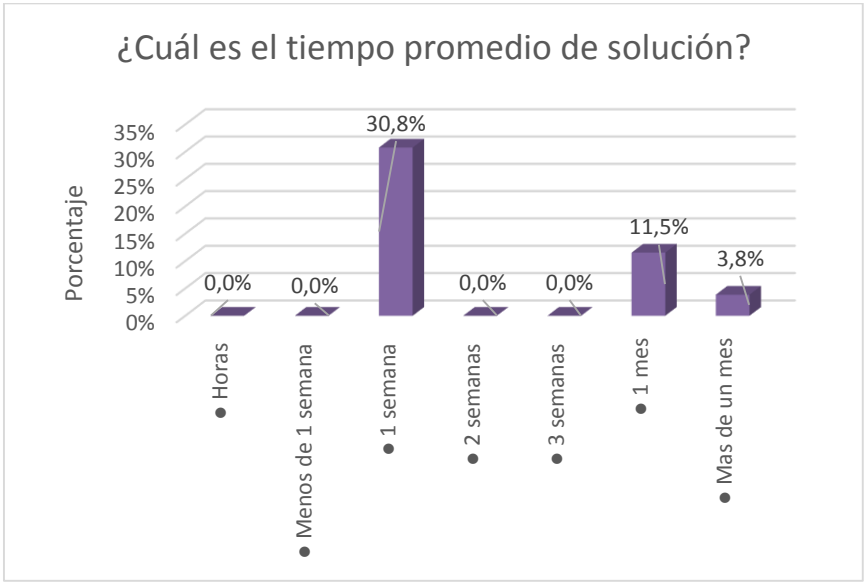



**Gráfico 4.32.** Tiempo promedio de solución a problemas por suminstro de componentes a computadoras de escritorio

El 46.15% de la población presenta inconvenientes por suministro de componentes a computadoras de escritorio, tal que, el 7.7% presenta el

inconveniente cada dos, tres, seis y nueve meses, y una vez al año; mientras que el 3.8% presenta el incidente una o dos veces al mes. Para lo cual, el 30.8% indica que su tiempo promedio de solución es en una semana, el 11.5% en un mes y el 3.8% mas de un mes. Mencionando, que el 53.85% no presenta esta incidencia.

10. Deperfectos de hardware (componentes internos del CPU).

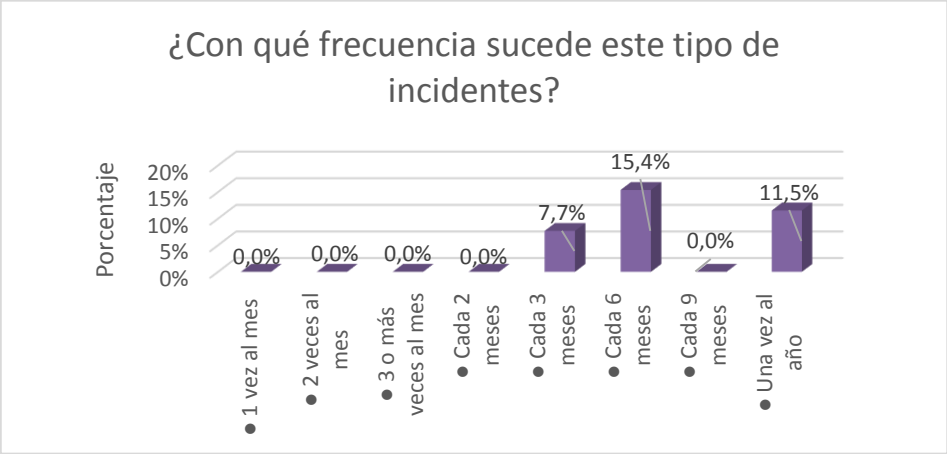



**Gráfico 4.33.** Frecuencia de incidentes con deperfectos de hardware

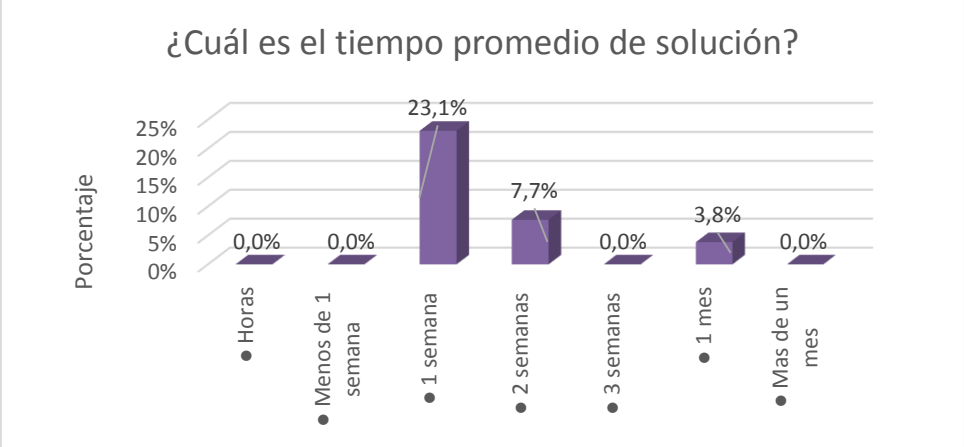



**Gráfico 4.34.** Tiempo promedio de solución a incidentes de deperfectos de hardware

La información recolectada muestra que el 34.62% de la población tiene problemas con los componentes internos del CPU, de los cuales se dan en un 15.4% cada 6 meses, el 11.5% una vez al año y el 7.7% cada tres meses; teniendo un tiempo promedio de solución de una semana con el 23.1%, el 7.7%

se soluciona en dos semanas y el 3.8% en un mes. Sumando a ellos, que el 65.38% notificaron no presentar la incidencia.

11. Problemas de video (proyectores, pantallas o monitores).

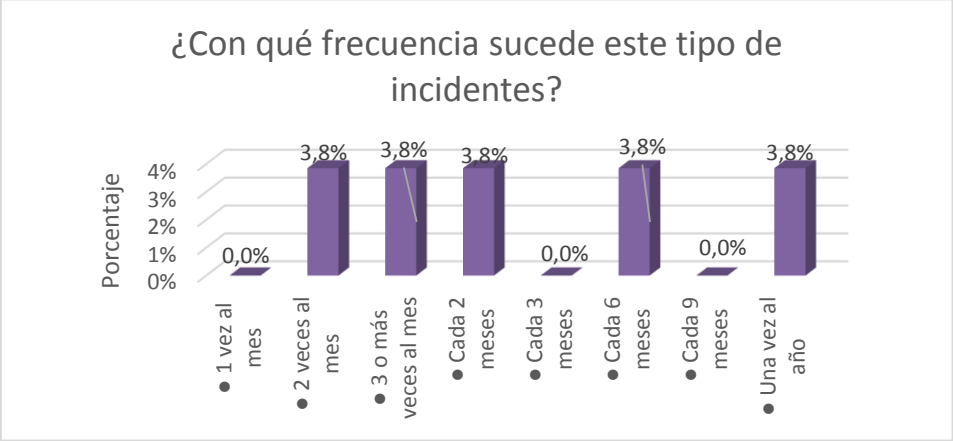



**Gráfico 4.35.** Frecuencia de problemas de video

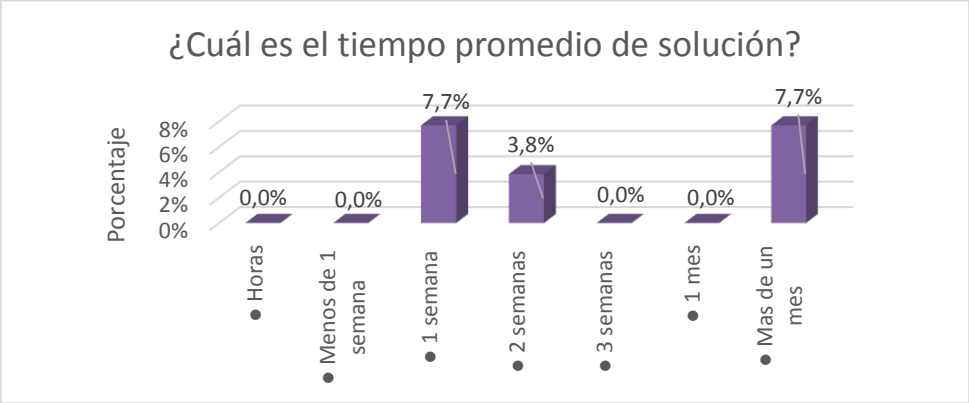



**Gráfico 4.36.** Tiempo promedio de solución a problemas de video

Los gráficos muestran que el 19.23% posee inconvenientes con los proyectores, pantallas o monitores; el 3.8% manifiestan que suceden dos veces, tres o mas veces, cada dos y seis veces al mes, y una vez al año. Su tiempo promedio de solución es del 7.7% para una semana y mas de un mes, y el 3.8% se resuelve en dos semanas. Agregando que el 80.77% no notificaron presentar la incidencia.

12. Problemas por virus en las computadoras.

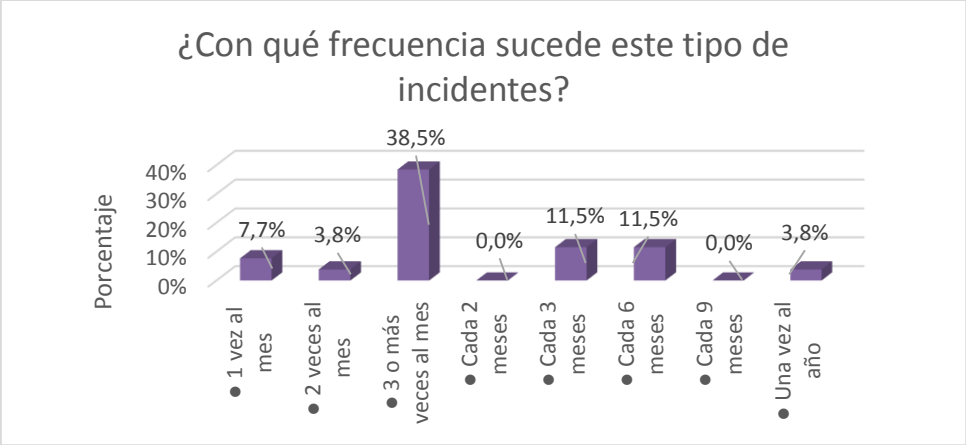



**Gráfico 4.37.** Frecuencia de problemas por virus en las computadoras

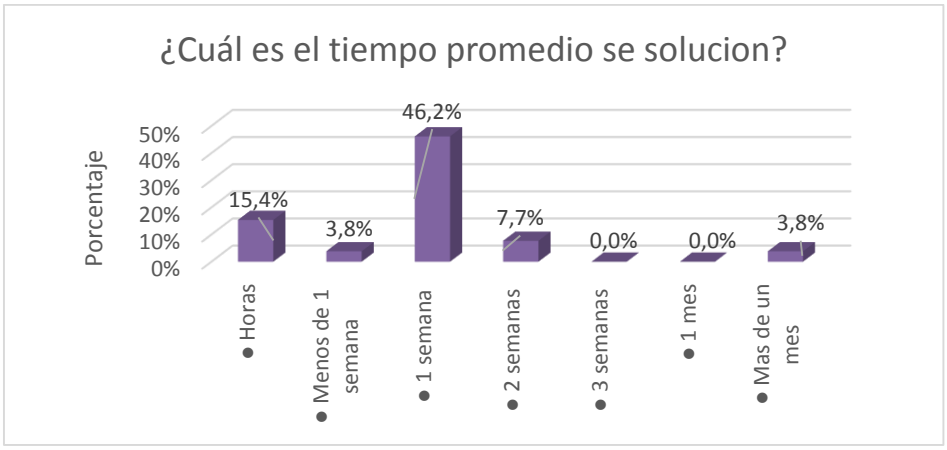



**Gráfico 4.38.** Tiempo promedio de solución a problemas por virus en las computadoras

El 76.92% de las personas encuentadas manifestaron tener problemas por virus en las computadoras; de las cuales, el 38.5% los presenta 3 o mas veces al mes, el 11.5% cada tres y seis meses, el 7.7% una vez al mes y el 3.8% dos veces al mes y una vez al año. Además, su tiempo promedio de solución es del 46.5% en una semana, el 15.4% en horas, el 7.7% en dos semanas y el 3.8% menos de una semana y mas de un mes. El 23.08% de las personas que se les aplicó el cuestionario, no mencionó este incidente.

13. Reinicio constante de las computadoras.

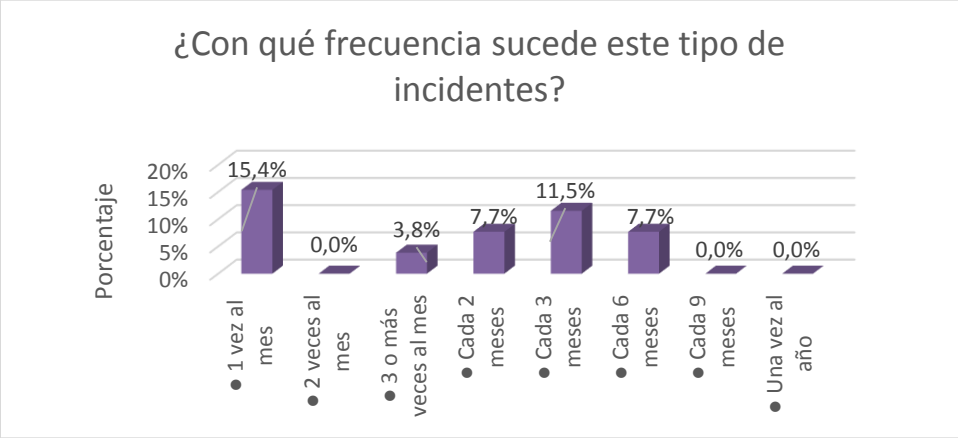



**Gráfico 4.39.** Frecuencia de incidentes por reinicio de computadoras

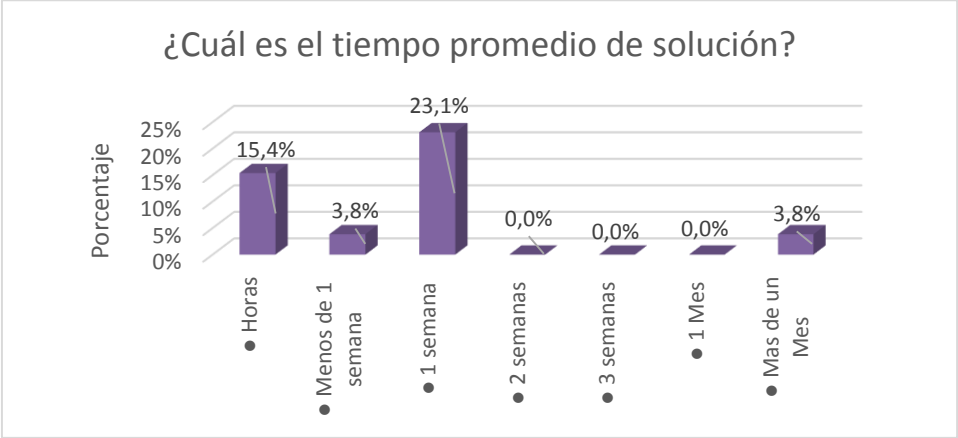



**Gráfico 4.40.** Tiempo promedio de solución de incidentes por reinicio de computadoras

De acuerdo a los graficos expuestos, el 46.15% de la población presenta inconvenientes por el reinicio constante de las computadoras. La frecuencia en que sucede este tipo de incidente es una vez al mes en un 15.4%, el 11.5% cada tres meses, el 7.7% cada dos y seis meses y el 3.8% tres o mas veces al mes; para lo cual, el tiempo promedio de solución es de una semana en un 23.1%, el 15.4% se resuelve en horas y el 3.8% en menos de una semana y mas de un mes. Adicionalmente, el 53.85% no mencionó la incidencia.

14. Problemas al actualizar programas (software).

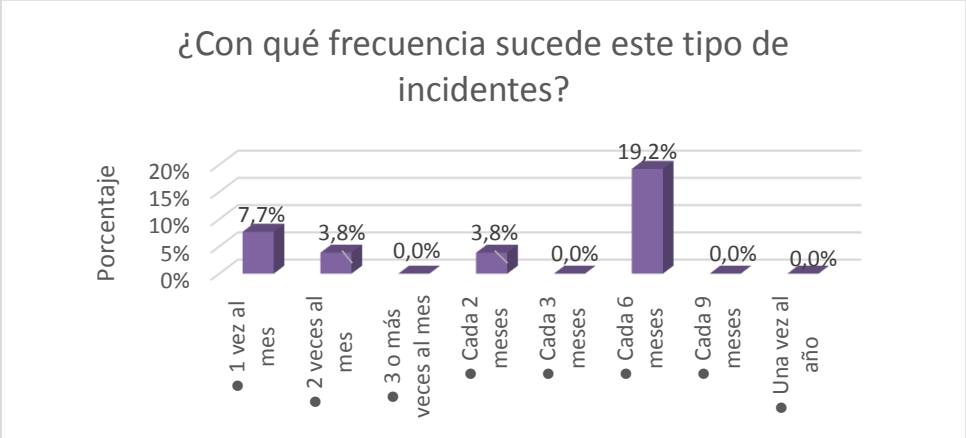



**Gráfico 4.41.** Frecuencia de problemas al actualizar programas

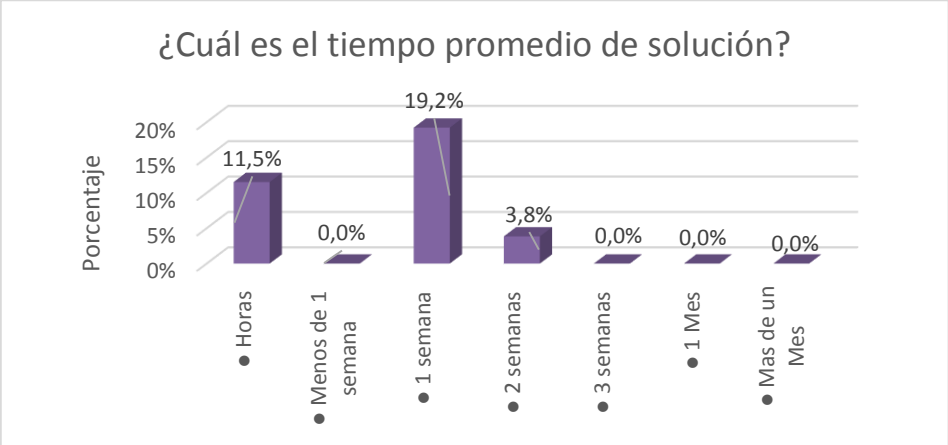



**Gráfico 4.42.** Tiempo promedio de solución de problemas al actualizar programas

El 34.62% de las personas encuestadas manifiestan tener problemas con la actualización de programas; de las cuales el 19.2% se dan cada 6 meses, el 7.7% una vez al mes y el 3.8% dos veces al mes y cada dos meses; con su respectivo tiempo promedio de solución de 19.2 % en una semana, el 11.5% se resuelve en horas y el 3.8% en dos semanas. Además, el 65.38% no presenta este inconveniente.

15. Problemas al ejecutar los programas (abren lentos o no se ejecutan)

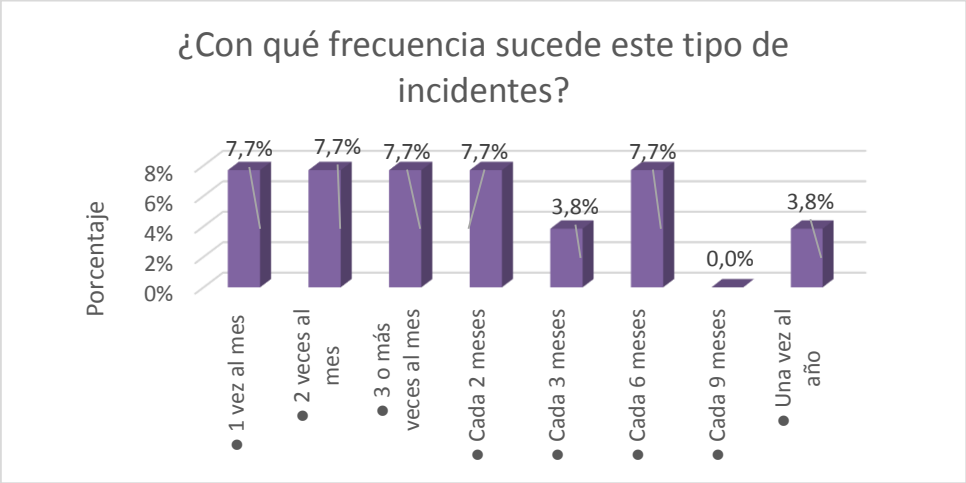



**Gráfico 4.43.** Frecuencia de problemas al ejecutar los programas

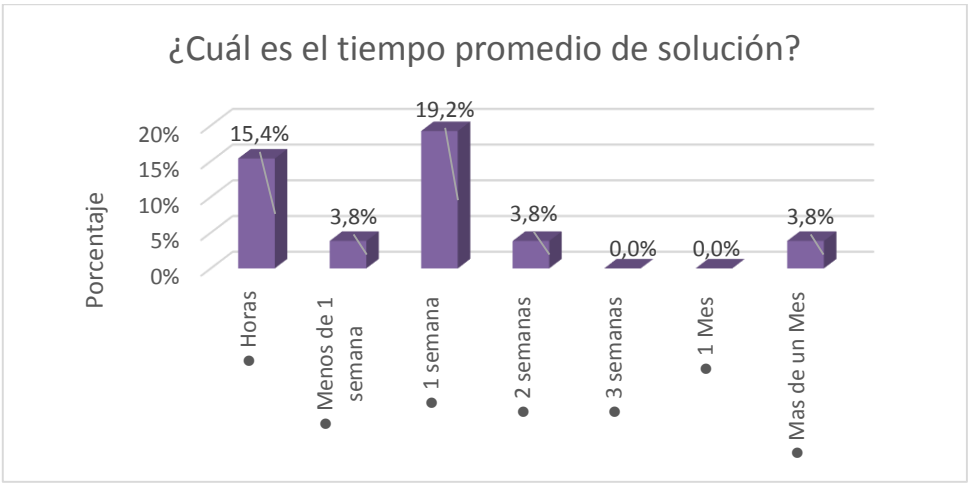



**Gráfico 4.44.** Tiempo promedio de solución a problemas al ejecutar los programas

Según los gráficos presentados el 46.15% de la población presenta inconvenientes al ejecutar los programas; el 7.7% manifiesta que estos inconvenientes suceden una vez, dos veces, tres o mas veces al mes, cada dos meses y cada seis meses, mientras que el 3.8% indica que se presenta cada 3 meses y una vez al año. Para lo cual, el tiempo promedio de solución es del 19.2% en una semana, el 15.4% por horas y el 3.8% se resuelve en menos de una semana, en dos semanas y mas de un mes. A esto se acota que el 53.85% mencionaron no presentar la incidencia.

16. Alerta por licenciamiento de programas (piratas).

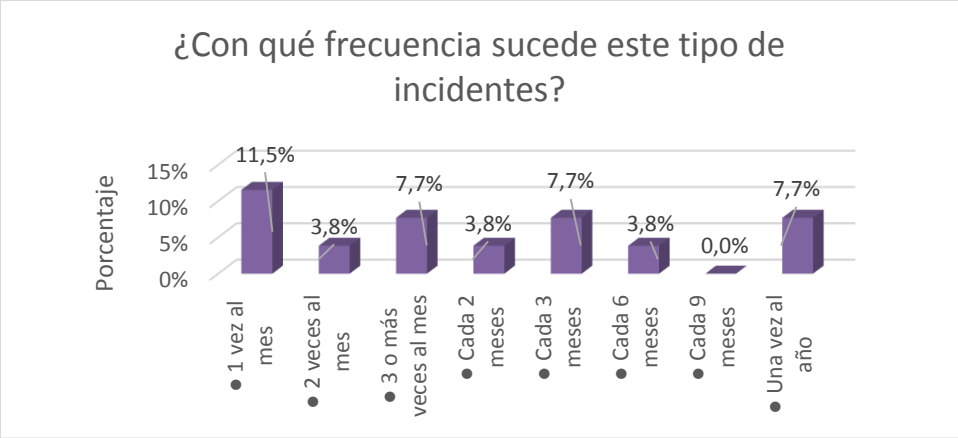



**Gráfico 4.45.** Frecuencia de alertas por licenciamiento de programas

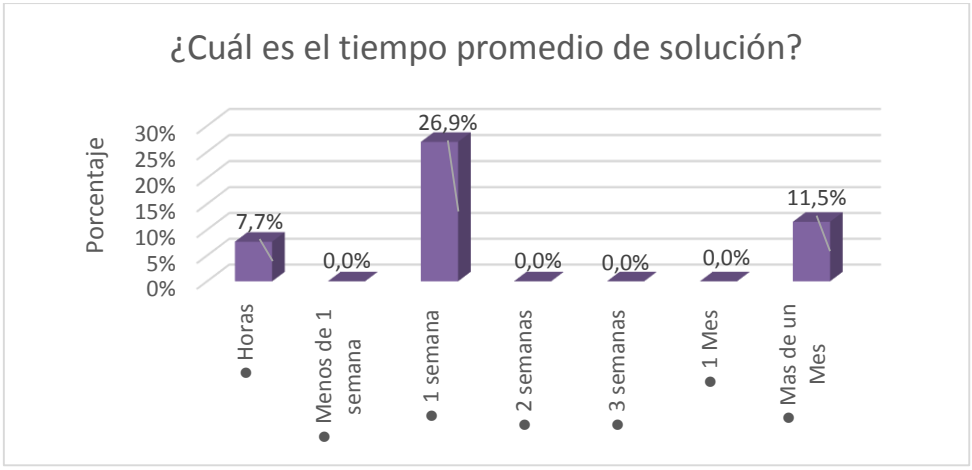



**Gráfico 4.46.** Tiempo promedio de solución de alertas por licenciamiento de programas

El 46.15% de la población indicó tener inconvenientes con programas piratas; de los cuales, el 11.5% manifestó que el incidente sucede una vez al mes; el 7.7% tres o mas veces al mes, cada tres meses y una vez al año, y el 3.8% indicó que sucede dos veces al mes, cada dos y seis meses. Su tiempo promedio de solución es del 26.9% en una semana, el 11.5% mas de un mes y el 7.7% se resuelve en horas; tomando en cuenta que el 53.85% no mostraba este incidente en su departamento.

17. Falta de mantenimiento preventivo.

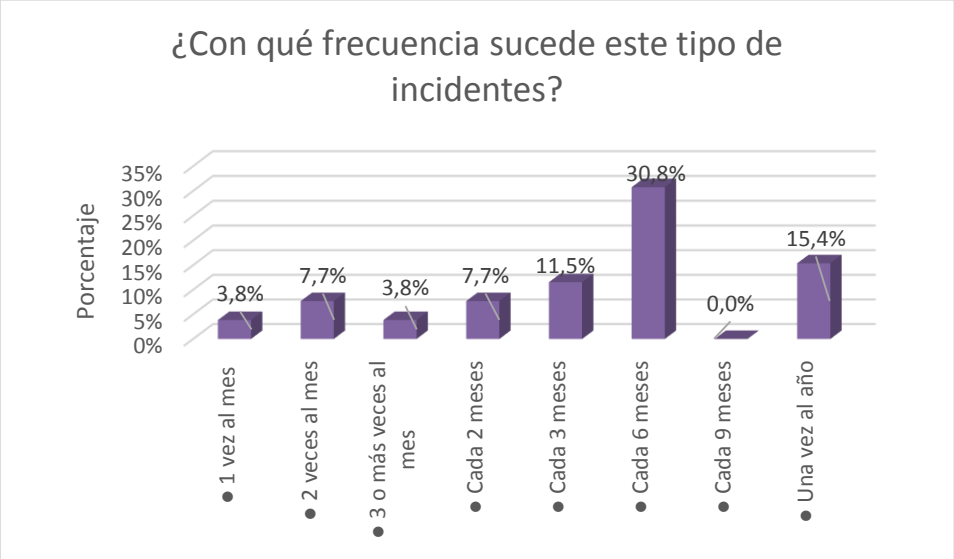



**Gráfico 4.47.** Frecuencia de incidentes referentes a la falta de mantenimiento preventivo

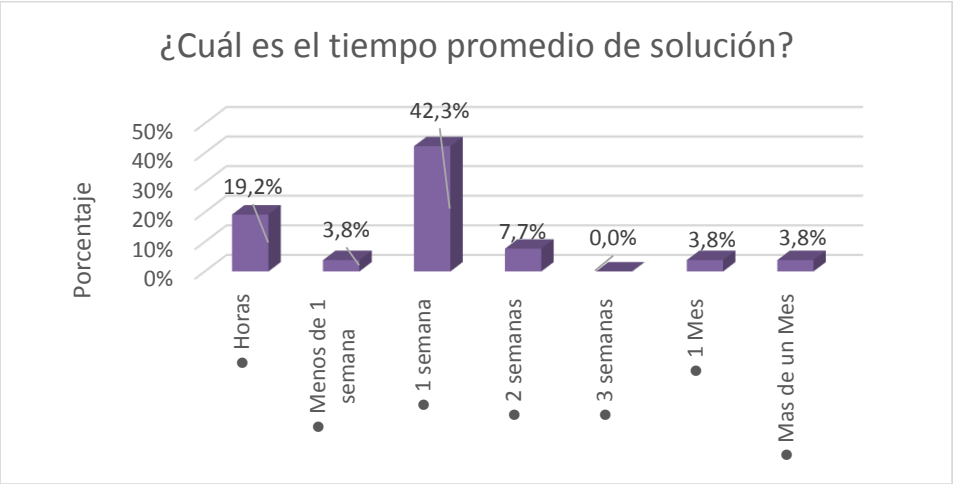



**Gráfico 4.48.** Tiempo promedio de solución a la falta de mantenimiento preventivo

El 80.77% de la población registró la falta de mantemiento preventivo en las instalaciones de la ESPAM – MFL. La frecuencia con la que se requeria este servicio era en un 30.8% cada seis meses, el 15.4% una vez al año, el 11.5% cada tres meses, el 7.7% dos veces al mes y cada dos meses, el 3.8% una vez y tres o mas veces al mes. Para lo cual, su tiempo promedio de solución es del 42.3% en una semana, 19.2% por horas, el 7.7% en dos semanas, el 3.8% en menos de una semana, en un mes y mas de un mes. Agregandole a ello, el 19.23% no solicitaba el servicio.

18. Falta de mantenimiento correctivo.

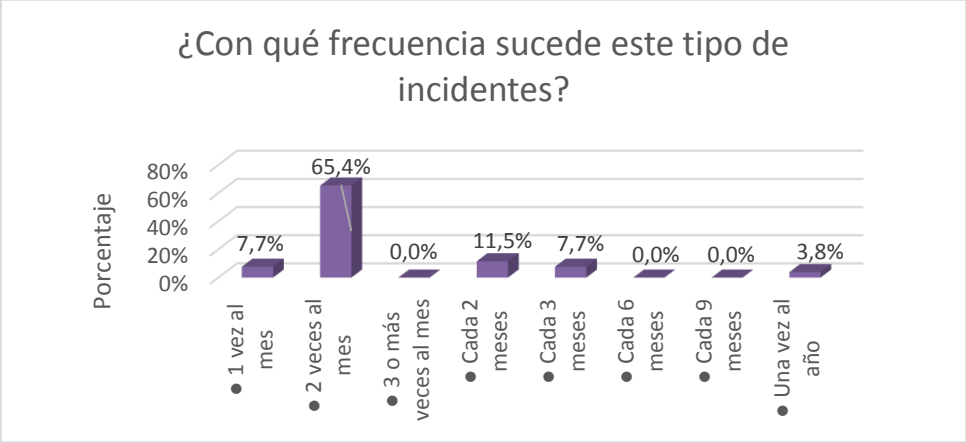



**Gráfico 4.49.** Frecuencia de la falta de mantenimiento correctivo

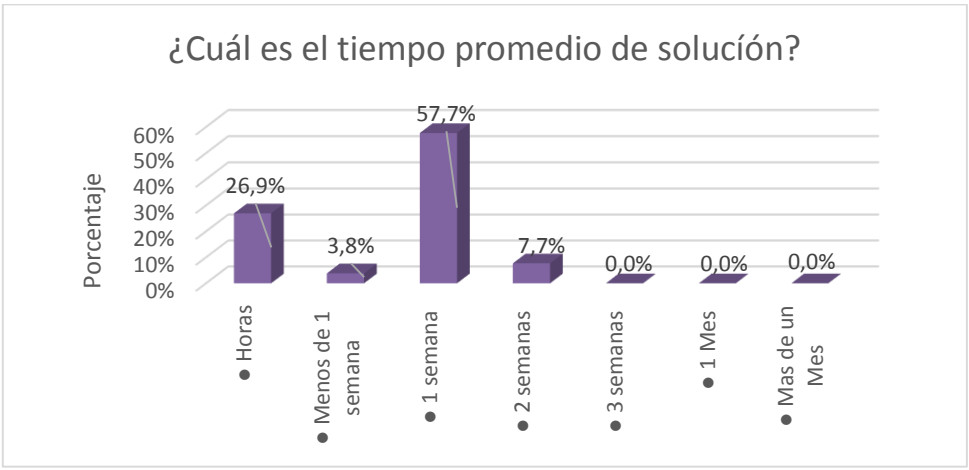



**Gráfico 4.50.** Tiempo promedio de solución a la falta de mantenimiento correctivo

El 96.15% de la población manifestó los problemas por la falta de mantenimiento correctivo; la frecuencia en la que se presenta es del 65.4% dos veces al mes, el 11.5% cada dos meses, el 7.7% una vez al mes y cada tres meses, y el 3.8% una vez al año. Para lo cual, el tiempo promedio de solución es del 57.7% en una semana, el 26.9% en horas, el 7.7% en dos semanas y el 3.8% en menos de una semana. Adicionalmente, el 3.85% no mencionó este incidente.

19. Daños en las impresoras multinfunción.

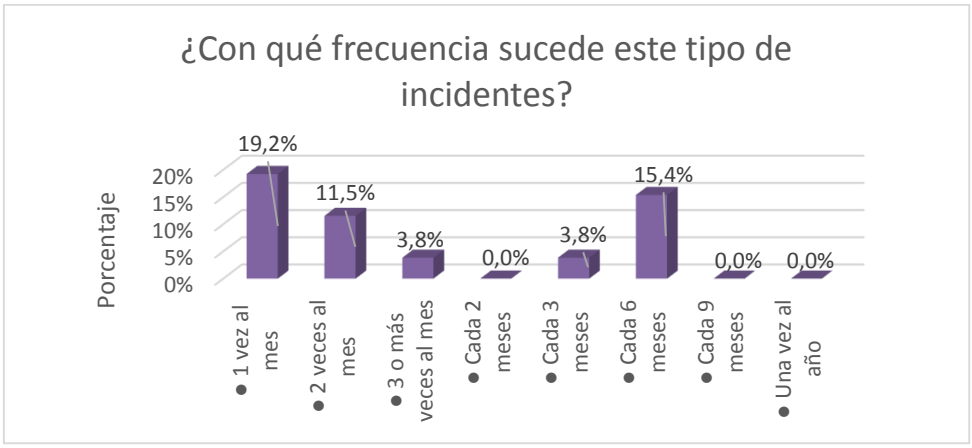



**Gráfico 4.51.** Frecuencia de daños en las impresoras multifunción

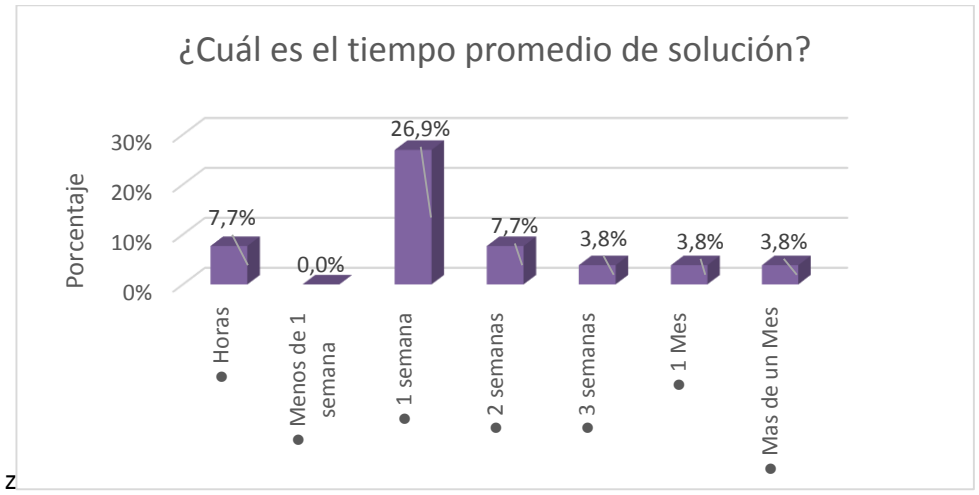



**Gráfico 4.52.** Tiempo promedio de solución a daños en las impresoras multifunción

Un total de 53.85% de las personas encuestadas, notificó los daños en las impresoras multifunción, los mismos que ocurren una vez al mes en un porcentaje del 19.2%, el 15.4% cada seis meses, el 11.5% dos veces al mes y el 3.8% tres o mas veces al mes y cada tres meses. Su tiempo promedio de solución es del 26.9% en una semana, del 7.7% en horas y dos semanas, y el 3.8% es de tres semanas, un mes y mas de un mes. Además, el 46.15% no mencionó presentar esta incidencia en su departamento.

20. Problemas por cambio de suministros a los equipos de impresión.

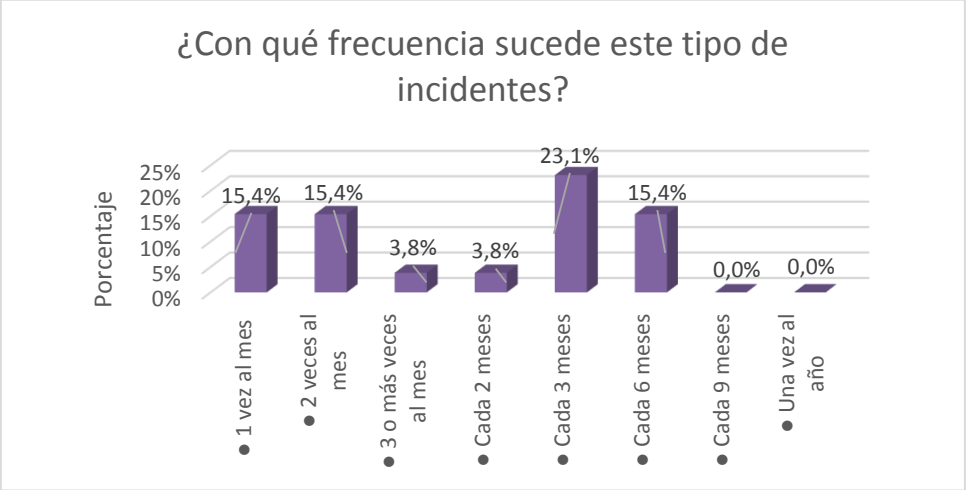



**Gráfico 4.53.** Frecuencia de incidentes por cambio de suministros a los equipos de impresión

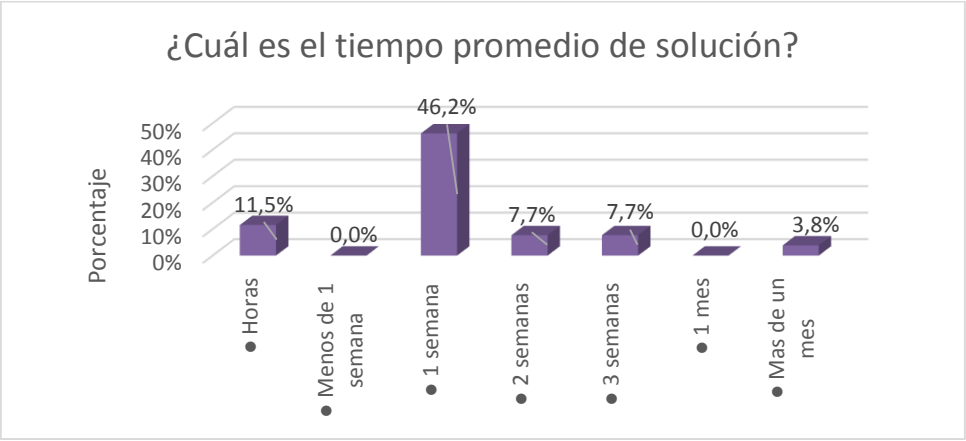



**Gráfico 4.54.** Tiempo promedio de solución a incidentes por cambio de suministros a los equipos de impresión

El 76.92% de la población presenta problemas por cambio de suministros a equipos de impresión; en la cual, su frecuencia es del 23.1% cada tres meses, del 15.4% una vez al mes, dos veces al mes y cada seis meses, y el 3.8% tres o mas veces al mes y cada dos meses. Por consiguiente, su tiempo promedio de solución es del 46.2% en una semana, el 11.5% en horas, el 3.8% mas de un mes y el 7.7% entre dos y tres semanas. Adicionalmente, el 23.08% no registraron esta incidencia, pero algunos hicieron énfasis, en la prestación de impresiones entre los departamentos de la institución, para continuar con las actividades diarias.

21. Daños en el hardware de scanner.

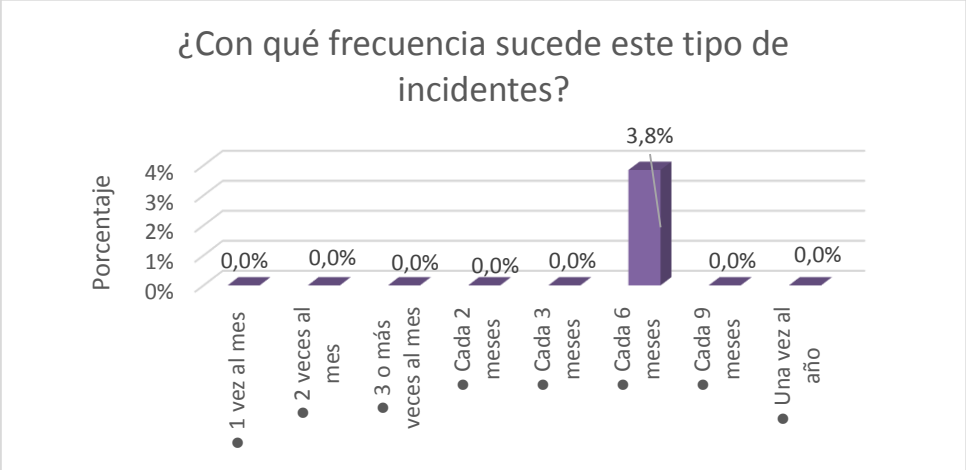



**Gráfico 4.55.** Frecuencia de daños en el hardware de scanner

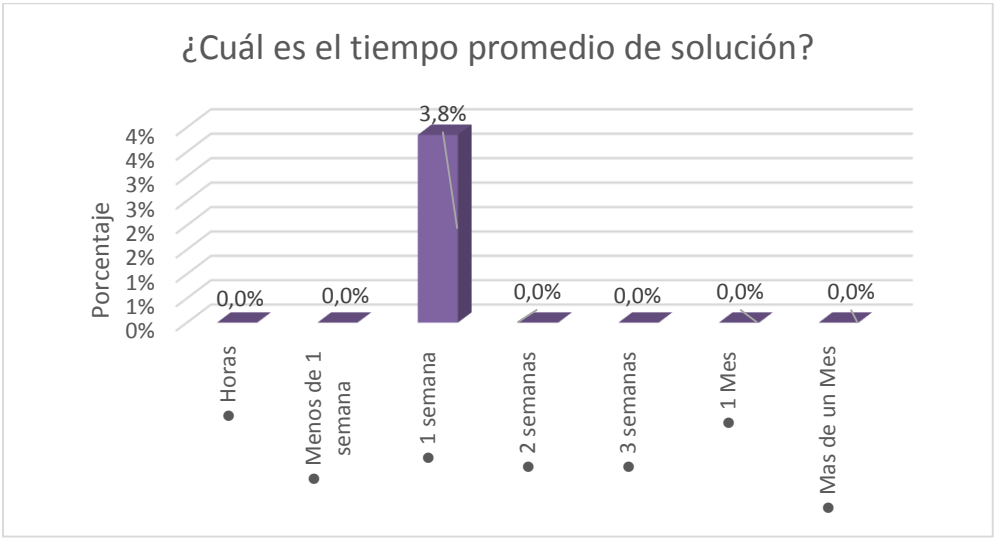



**Gráfico 4.56.** Tiempo promedio de solución a daños en el hardware de scanner

El 3.85% de la población manifestó los incidentes provocados por daños en el hardware de scanner; el mismo que tiene una frecuencia del 3.8% cada seis meses y su tiempo promedio de solución es de una semana con un 3.8%. Adicional a ello, el 96.15% no presenta este inconveniente.

El cuestionario incluía además, el registro de la persona que notifica el incidente en cada uno de los departamentos y carreras de la institución y los efectos que se derivan de los mismos. Para lo cual, los resultados obtenidos indican que la mayoría de los incidentes se anuncian al jefe del departamento o director de carrera, quien se encarga a su vez de comunicar al coodinador del departamento de tecnología, para la respectiva asignación del técnico encargado en brindar la asistencia. Asi también, en un 69.23% el usuario notifica la incidencia directamente al coordinador del departamento de tecnología, en caso de no encontrarse en su lugar de trabajo el jefe inmediato.

A continuación se muestran los principales efectos derivados del sucedo de un incidente informático:

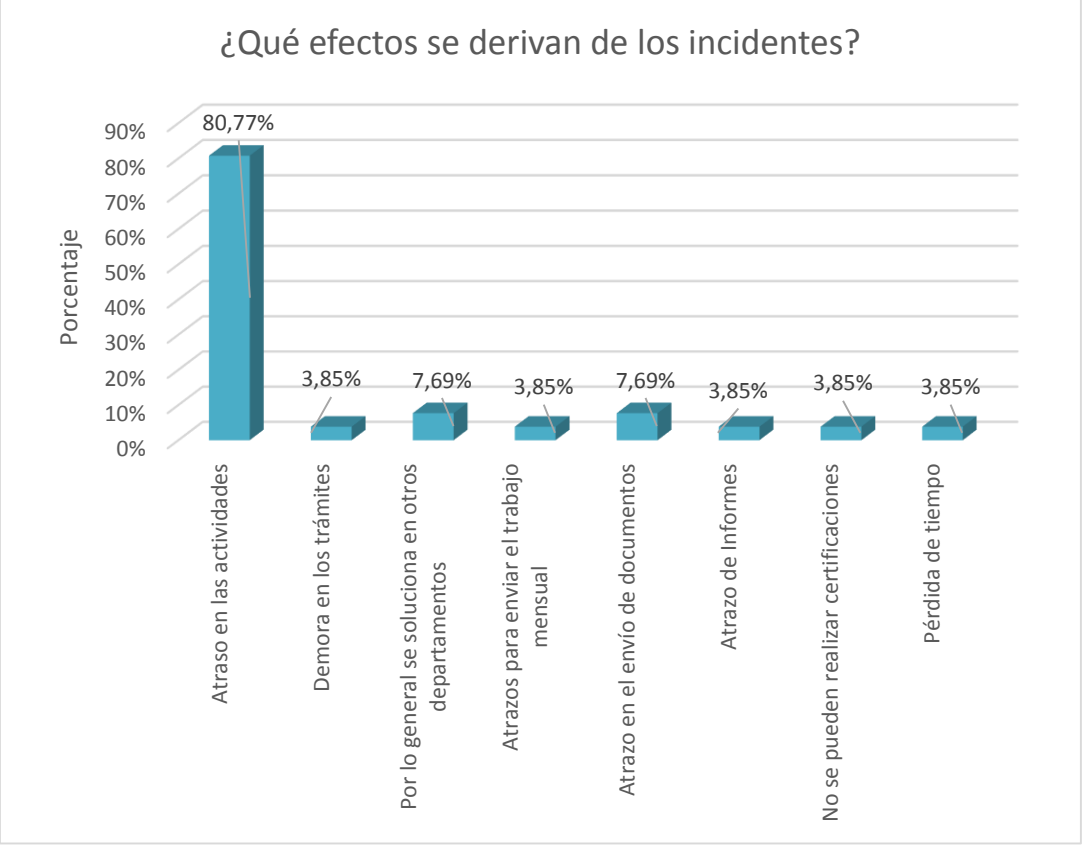



**Gráfico 4.57.** Efectos que se derivan de los incidentes

Como se puede observar en el gráfico anterior, el efecto principal que se deriva cuando ocurre un incidente, es el atraso en las actividades regulares de la

institución, el cual alcanza el 80.77%. Sumando, que otros de los inconvenientes que se presentan, es la falta de UPS en el laboratorio de Quimica General.

### 4.1.2. CLASIFICACIÓN DE LOS INCIDENTES INFORMÁTICOS

Lo realizado para determinar las incidencias informáticas que transcurren en las instalaciones de la ESPAM-MFL, permitió elaborar una clasificación de los principales inconvenientes ocurridos, estabeciendo en número y porcentaje el total de incidentes registrados mediante la aplicación del cuestionario.

| TIPOLOGÍA DE INCIDENTES | N° | % |
|---|---|---|
| **Incidentes de red** | **43** | **17,99%** |
| Fallo del servicio de comunicación (Problemas con la conexión a internet) | 24 | **10,04%** |
| Inconvenientes con el servício de correo electrónico de la institución | 19 | **7,95%** |
| **Incidentes de software** | **38** | **15,90%** |
| Problemas de video (proyectores, pantallas o monitores) | 5 | **2,09%** |
| Problemas al actualizar programas | 9 | **3,77%** |
| Problemas al ejecutar programas (abren lentos o no se ejecutan) | 12 | **5,02%** |
| Alerta por licenciamiento de programas | 12 | **5,02%** |
| **Incidentes de hardware** | **22** | **9,21%** |
| Problemas por suministro de componentes a computadoras de escritorio | 12 | **5,02%** |
| Desperfectos de hardware (componentes internos del CPU) | 9 | **3,77%** |
| Daños en el hardware de scanner | 1 | **0,42%** |
| **Incidentes de impresoras** | **34** | **14,23%** |
| Daños en las impresoras multifunción | 14 | **5,86%** |
| Problemas por cambio de suministro a los equipos de impresión | 20 | **8,37%** |
| **Incidentes que implican software y hardware** | **89** | **37,24%** |
| Reinicio constante de las computadoras | 12 | **5,02%** |
| Problemas por virus en las computadoras | 20 | **8,37%** |
| Falta de mantenimiento preventivo | 21 | **8,79%** |
| Falta de mantenimiento correctivo | 25 | **10,46%** |
| Denegación del servicio (saturación del sistema informático) | 11 | **4,60%** |
| **Incidentes de origen natural y humano (accidental o deliberado)** | **13** | **5,44%** |
| Problemas con fuego (incendios) | 0 | **0,00%** |
| Daños en los equipos por agua (escape, fugas e inundaciones) | 1 | **0,42%** |
| Presencia de desastres industriales (Debido a la actividad humana) | 2 | **0,84%** |
| Corte de suministro eléctrico | 6 | **2,51%** |
| Robo de equipos informáticos | 4 | **1,67%** |
| **TOTAL DE INCIDENCIAS** | **239** | **100,00%** |

**Cuadro 4.19.** Tipología de incidentes informáticos

Como se observa en el cuadro 4.19, las incidencias más relevantes en relación al total de las mismas son aquellas que implican software y hardware, las cuales

alcanzan un 37,24%; mientras que los incidentes de red se encuentran en un 17,99%. Por consiguiente, las menos relevantes son las de origen natural y humano con un 5.44%, debido a su probabilidad y frecuencia de ocurrencia.

## 4.1.3. DIAGNÓSTICO Y RESOLUCIÓN

### 4.1.3.1. METODOLOGÍA ITIL – GESTIÓN DE SERVICIOS

Una vez definidos los problemas más relevantes, se procedió a elaborar un catálogo mediante el cual se definieron los servicios tecnológicos disponibles en la institución y que son brindados por el departamento de tecnología, los mismos que se detallan a continuación:

| CATÁLOGO DE SERVICIOS TECNOLÓGICOS | | | |
|---|---|---|---|
| **GRUPOS DE SERVICIOS** | **SERVICIO TECNOLÓGICO** | **DESCRIPCIÓN DEL SERVICIO** | **REQUERIMIENTOS SOBRE LOS SERVICIOS** |
| **Servicios Estándar** Son los servicios tecnológicos que por defecto cualquier servidor de la institución recibe y tiene acceso, estos son: computador personal, correo electrónico e impresión. | **Computadoras Personales de Escritorio y Portátiles** | Habilitación y soporte de computadoras personales de escritorio y portátiles para los servidores (funcionarios) de la institución. Incluye hardware, software base, acceso a la red, Intranet, cuenta de correo electrónico interno y mensajería instantanea. (ATENCION DEL DIA A DIA). | 1. Soporte Tecnico Hardware y Software |
| | | | 2. Acceso a Internet |
| | | | 3. Acceso a red inalámbrica |
| | | | 4. Soporte Ofimatico |
| | | | 5. Instalacion de hardware para equipos de escritorio |
| | | | 6. Aplicación de garantías de hardware |
| | | | 7. Asignación de equipos informáticos |
| | | | 8. Instalación de software base |
| | | | 9. Instalación de software adicional |
| | | | 10. Movilización / retiro de estación de trabajo |
| | | | 11. Gestión de usuario |
| | | | 12. Respaldo de Información |
| | | | 13. Mantenimiento Preventivo |
| | **Correo Electrónico** | Permite el envió y recepción electrónica de mensajes y documentos para facilitar el intercambio de información entre los servidores (funcionarios) a través de funcionalidades como las de compartir: agenda, libreta de direcciones, carpetas públicas, etc. | 1. Gestión de Usuario |
| | | | 2. Entrega y recepción de correo |
| | | | 3. Gestión del funcionamiento del servidor |

| | | | |
|---|---|---|---|
| | **Impresión y digitalizacion** | Servicio de impresión, fotocopiado, digitalización de documentos en equipos de impresión multifunción. | 1. Actualización de hardware para equipos de escritorio<br>2. Asignación y/o movilización de impresora o escáner<br>3. Configuración de impresora y/o escáner<br>4. Retiro de impresora y/o escáner<br>5. Cambio de suministros para impresoras/copiadoras<br>6. Configuracion De Impresión via Wireless para laptops.<br>7. Asignacion de IP estaticas en cada impresora<br>8. Asignacion de claves para Impresoras auditadas |
| **Servicios Por Demanda**<br>Son aquellos servicios que se prestan de forma temporal o definitiva pero que no son de libre acceso para todos los servidores de la institución. | **Gestión de Redes y Conectividad** | Permite la conexión de computadoras personales y dispositivos en general propios de la institución o de terceros a la red interna de manera local o por medio de una conexión remota VPN desde Internet. | 1. Análisis del desempeño de equipos<br>2. Restricción de red a telefonos celulares personales<br>3. Habilitación de conectividad inalámbrica móvil (módems)<br>4. Requerimiento de información técnica de redes y conectividad<br>5. Gestión de sostenibilidad<br>6. Inventario de Equipos de Comunicación<br>7. Instalacion de Punto de Red |
| **Servicios para la Gestión Documental**<br>Son servicios basados en aplicaciones que apoyan y automatizan los procesos de Gestion Documental en la que se inmiscuyen todas las Direcciones de la institución. | **Intranet Insititucional** | Es un servicio tecnológico que está dirigido a todos los Servidores de la institución, con contenido informativo y servicios Insitucionales. | 1. Configuracion de acceso a Portal Intranet<br>2. Carga de Procedimientos<br>3. Soporte técnico especializado sobre las aplicaciones |
| | **Pagina Web** | Soporte Funcional, acerca de plugins y complementos adicionales , no incluidos en el diseño. | 1. Instalacion de Herramientas Adicionales<br>2. Mantenimiento especializado sobre las aplicaciones |

**Cuadro 4.20.** Catálogo de Servicios tecnológicos de la ESPAM-MFL

La definición del catálogo, se encuentra desarrollada considerando las buenas practicas, de prestación de servicios. En su caracterización por cada uno de los servicios, se desarrolló el acuerdo de servicios (SLA) entre las autoridades y el departamento de tecnología, en el cual, se establecen y organizan cada una de las actividades, dependiendo de la prioridad, urgencia e impacto. Se especifica además, el escalado jerárquico, las responsabilidades de los miembros del departamento de tecnología y los tiempos de respuesta y solución al incidente.

El acuerdo de servicios, se convertirá en el instrumento en el que consten las normas y procedimientos, que propendan a gestionar de manera eficaz y eficiente ante los incidentes informáticos, con la finalidad de definir el proceso que se lleva desde su notificación hasta el cierre del mismo, tal como se muestra a continuación:

# ACUERDO DE NIVEL DE SERVICIOS DEL DEPARTAMENTO DE TECNOLOGÍA DE LA ESPAM – MFL

# CONTENIDO

1. INTRODUCCIÓN ..... 175
2. DATOS GENERALES DEL DEPARTAMENTO DE TECNOLOGÍA..... 176
2.1. MISIÓN ..... 176
2.2. VISIÓN..... 176
2.3. OBJETIVOS..... 176
3. DEFINICIÓN ..... 178
3.1. PARTES DEL ACUERDO..... 178
3.2. ACUERDO DE EXCLUSIVIDAD..... 178
3.3. DISPONIBILIDAD DEL SERVICIO ..... 178
3.4. MODIFICACIONES DE LOS SERVICIOS ..... 179
4. MONITORIZACIÓN E INFORMES ..... 180
4.1. SERVICIOS ESTÁNDAR..... 181
4.1.1. COMPUTADORAS PERSONALES DE ESCRITORIO Y PORTÁTILES..... 181
4.1.2. CORREO ELECTRÓNICO..... 183
4.1.3. IMPRESIÓN Y DIGITALIZACIÓN ..... 184
4.2. SERVICIOS POR DEMANDA..... 185
4.2.1. GESTIÓN DE REDES Y CONECTIVIDAD..... 185
4.3. SERVICIOS PARA LA GESTIÓN DOCUMENTAL ..... 186
4.3.1. INTRANET INSTITUCIONAL ..... 186
4.3.2. PÁGINA WEB..... 187
5. ESTRUCTURA ORGÁNICA DEL DEPARTAMENTO..... 188
6. RESPONSABLES DE LOS INCIDENTES INFORMÁTICOS..... 189
7. PROCESO DE UN INCIDENTE INFORMÁTICO..... 190
8. PRIORIDADES DE LOS INCIDENTES INFORMÁTICOS ..... 191
9. GARANTÍAS ..... 192

9.1. CALIDAD DEL SERVICIO ..... 192

9.2. SEGURIDAD DE LOS SERVICIOS ..... 192

10. FINALIZACIÓN DEL ACUERDO ..... 193

# 1. INTRODUCCIÓN

En los últimos años se ha llegado a reconocer el creciente valor de la información, hasta el punto que es considerada el recurso más importante y estratégico que cualquier organización tiene que manejar. La clave para el análisis, la producción y la distribución de la información dentro de una institución viene definida por la calidad de los sistemas de tecnología de la información que atienden a la organización.

En las instituciones sean públicas o privadas, es necesario brindar a los usuarios soluciones agiles a inconvenientes que se presentan con los servicios de Tecnología de la Información, por lo que es preciso fijar políticas y procedimientos para estandarizar los tiempos que permitan a las personas encargadas de prestar el soporte a las incidencias, acudir eficazmente al llamado de los usuarios.

Por ello, el presente acuerdo tiene como finalidad agilitar los servicios que brinda el Departamento de Tecnología de la ESPAM-MFL, mediante normas que rijan tiempos previamente establecidos, con el fin de llegar a un consenso entre las autoridades y los miembros del departamento de tecnología, garantizando disponibilidad y una mejor calidad en los servicios que se brindan.

# 2. DATOS GENERALES DEL DEPARTAMENTO DE TECNOLOGÍA

## 2.1. MISIÓN

Contribuir con el crecimiento institucional de manera integral mediante un plan de trabajo coordinado que incorpore recursos, políticas y estrategias con el fin de implementar una infraestructura tecnológica que satisfaga las necesidades administrativas, académicas, operativas e investigativas de nuestra Escuela Politécnica en la consecución eficiente de los objetivos institucionales.

## 2.2. VISIÓN

Coadyuvar al desarrollo de la Institución como una entidad de gestión tecnológica con calidad, solidez y eficacia en el cumplimiento de sus funciones orientadas al mejoramiento de los servicios y productos de las unidades administrativas, académicas e investigativas de nuestra Institución.

## 2.3. OBJETIVOS

- Brindar apoyo en la consecución de los objetivos estratégicos de la Institución mediante una infraestructura tecnológica consistente y sólida.
- Implementar un Plan de trabajo de Tecnología que responda eficazmente a las necesidades tecnológicas de las diferentes áreas de la institución.
- Ofrecer un servicio de calidad y eficiencia en la automatización de funciones administrativas, académicas, operativas e investigativas.
- Mantener los servicios tecnológicos integrados y consistentes para la comunidad Politécnica.
- Optimizar el uso y mantenimiento de la infraestructura tecnológica en procura de reflejar una relación costo-beneficio, que aporte eficiencia a la institución.

- Participar de forma activa en la ejecución de las actividades inherentes en la adquisición e implementación de nuevas tecnologías para el desarrollo tecnológico de la Institución.
- Proyectar a la Universidad como una institución líder en avances tecnológicos constituyéndose en un aporte constante en la búsqueda de soluciones a las necesidades de información y tecnología.

# 3. DEFINICIÓN

Este acuerdo de nivel de servicios define los términos y condiciones en función de una serie de parámetros objetivos, bajo las cuales el Departamento de Tecnología de la ESPAM-MFL proporciona su ayuda a la comunidad universitaria. Mediante el mismo, se refleja contractualmente el nivel operativo de funcionamiento, sus responsabilidades, confiabilidad, calidad y garantía de la asistencia que se brinda, beneficiando a los usuarios y brindando estabilidad a la hora de realizar las actividades diarias.

## 3.1. PARTES DEL ACUERDO

El acuerdo está relacionado directamente entre los miembros del Departamento tecnológico y cada uno de los coordinadores de los departamentos que conforman la ESPAM – MFL, conjuntamente con las autoridades que dirigen la misma.

## 3.2. ACUERDO DE EXCLUSIVIDAD

Este acuerdo garantiza al Departamento Tecnológico de la ESPAM-MFL derechos exclusivos de uso y manipulación del servicio que brindan los equipos informáticos de la institución.

## 3.3. DISPONIBILIDAD DEL SERVICIO

El departamento de tecnología de la ESPAM-MFL, está disponible de lunes a viernes en horarios de 8:00 am hasta las 17:00 pm, para atender cada uno de los inconvenientes que se presentan con los servicios tecnológicos en la institución y de esta manera garantizan un servicio de calidad.

De esta manera se puede sugerir que los técnicos encargados de atender los inconvenientes en cada uno de los departamentos puedan turnarse en la noche de lunes a viernes y los fines de semanas, para atender cualquier incidencia que se pueda presentar en los equipos informáticos de la institución.

## 3.4. MODIFICACIONES DE LOS SERVICIOS

Cualquiera de las partes podrá disponer modificaciones en el ámbito, naturaleza, disponibilidad, tiempo de respuesta, etc. De mutuo acuerdo, las partes deberán aprobar los cambios propuestos, incluyendo los gastos que se deriven de estos.

# 4. MONITORIZACIÓN E INFORMES

Cada uno de los servicios del presente acuerdo serán monitoreados a través del registro de las incidencias y el oficio del departamento que lo solicita. A continuación se muestra la ficha mediante la cual se procederá a registrar las incidencias informáticas:

**ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ**

## REGISTRO DE INCIDENCIAS INFORMÁTICAS

| № DE INCIDENCIA | NOMBRE DEL DEPARTAMENTO | FECHA DE REGISTRO | HORA DE REGISTRO | TIPO DE INCIDENCIA | DESCRIPCIÓN | TÉCNICO ENCARGADO | FECHA DE SOLUCIÓN | HORA DE SOLUCION | FIRMA DEL COORDINADOR DEL DEPARTAMENTO |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## 4.1. SERVICIOS ESTÁNDAR

Son los servicios tecnológicos que por defecto cualquier servidor de la institución recibe y tiene acceso, estos son: computador personal, correo electrónico e impresión.

### 4.1.1. COMPUTADORAS PERSONALES DE ESCRITORIO Y PORTÁTILES

| DESCRIPCIÓN | INCIDENCIAS | TIEMPO DE RESPUESTA A LA INCIDENCIA | TIEMPO MÁXIMO DE SOLUCIÓN | ESCALADO FUNCIONAL | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | 1er ESCALAM. | 2do ESCALAM. | 3ero ESCALAM. | 4to ESCALAM. | 5to ESCALAM. |
| Habilitación y soporte de computadoras personales de escritorio y portátiles para los servidores (funcionarios) de la institución. Incluye hardware, software base, acceso a la red, Intranet, cuenta de correo electrónico interno y mensajería instantánea. (ATENCION DEL DIA A DIA) | Soporte Técnico Hardware y Software | 1 hora | 3 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |
| | Acceso a Internet | 30 minutos | 3 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |
| | Acceso a red inalámbrica | 30 minutos | 2 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |
| | Soporte Ofimático | 1 hora | 6 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |
| | Instalación de hardware para equipos de escritorio | 1 hora | 12 horas laborables | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | Autoridades de la Institución |
| | Aplicación de garantías de hardware | 1 hora | 4 días laborables | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | Autoridades de la Institución |
| | Asignación de equipos informáticos | 1 hora | 3 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | Autoridades de la Institución |

| DESCRIPCIÓN | INCIDENCIAS | TIEMPO DE RESPUESTA A LA INCIDENCIA | TIEMPO MÁXIMO DE SOLUCIÓN | ESCALADO FUNCIONAL | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | 1er ESCALAM. | 2do ESCALAM. | 3ero ESCALAM. | 4to ESCALAM. | 5to ESCALAM. |
| Habilitación y soporte de computadoras personales de escritorio y portátiles para los servidores (funcionarios) de la institución. Incluye hardware, software base, acceso a la red, Intranet, cuenta de correo electrónico interno y mensajería instantánea. (ATENCION DEL DIA A DIA) | Instalación de software adicional | 1 hora | 6 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |
| | Instalación de software base | 1 hora | 6 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |
| | Movilización / retiro de estación de trabajo | 1 hora | 12 horas laborables | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | Autoridades de la Institución |
| | Gestión de usuario | 1 hora | 6 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |
| | Respaldo de Información | 1 hora | 10 horas laborales | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |
| | Mantenimiento Preventivo | 1 hora | 3 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |

## 4.1.2. CORREO ELECTRÓNICO

| DESCRIPCIÓN | INCIDENCIAS | TIEMPO DE RESPUESTA A LA INCIDENCIA | TIEMPO MÁXIMO DE SOLUCIÓN | ESCALADO FUNCIONAL | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | 1er ESCALAM. | 2do ESCALAM. | 3ero ESCALAM. | 4to ESCALAM. | 5to ESCALAM. |
| Permite el envío y recepción electrónica de mensajes y documentos para facilitar el intercambio de información entre los servidores (funcionarios) a través de funcionalidades como las de compartir: agenda, libreta de direcciones, carpetas públicas, etc. | Gestión de Usuario | 30 minutos | 2 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |
| | Entrega y recepción de correo | 30 minutos | 2 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |
| | Gestión del funcionamiento del servidor | 30 minutos | 6 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | Autoridades de la Institución |

## 4.1.3. IMPRESIÓN Y DIGITALIZACIÓN

| DESCRIPCIÓN | INCIDENCIAS | TIEMPO DE RESPUESTA A LA INCIDENCIA | TIEMPO MÁXIMO DE SOLUCIÓN | ESCALADO FUNCIONAL | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | 1er ESCALAM. | 2do ESCALAM. | 3ero ESCALAM. | 4to ESCALAM. | 5to ESCALAM. |
| Servicio de impresión, fotocopiado, digitalización de documentos en equipos de impresión multifunción | Actualización de hardware para equipos de escritorio | 1 hora | 10 horas laborables | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | Autoridades de la Institución |
| | Asignación y/o movilización de impresora o escáner | 1 hora | 12 horas laborables | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | Autoridades de la Institución |
| | Configuración de impresora y/o escáner | 1 hora | 2 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |
| | Retiro de impresora y/o escáner | 1 hora | 2 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |
| | Cambio de suministros para impresoras/copiadoras | 1 hora | 2 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | Autoridades de la Institución |
| | Configuración De Impresión vía Wireless para laptops. | 1 hora | 2 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |
| | Asignación de IP estáticas en cada impresora | 1 hora | 2 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |
| | Asignación de claves para Impresoras auditadas | 1 hora | 2 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |

## 4.2. SERVICIOS POR DEMANDA

Son aquellos servicios que se prestan de forma temporal o definitiva pero que no son de libre acceso para todos los servidores de la institución.

### 4.2.1. GESTIÓN DE REDES Y CONECTIVIDAD

| DESCRIPCIÓN | INCIDENCIAS | TIEMPO DE RESPUESTA A LA INCIDENCIA | TIEMPO MÁXIMO DE SOLUCIÓN | ESCALADO FUNCIONAL | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | 1er ESCALAM. | 2do ESCALAM. | 3ero ESCALAM. | 4to ESCALAM. | 5to ESCALAM. |
| Permite la conexión de computadoras personales y dispositivos en general propios de la institución o de terceros a la red interna de manera local o por medio de una conexión remota VPN desde Internet | Análisis del desempeño de equipos | 1 hora | 2 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |
| | Restricción de red a teléfonos celulares personales | 1 hora | 2 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |
| | Habilitación de conectividad inalámbrica móvil (módems) | 1 hora | 2 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | Autoridades de la Institución |
| | Requerimiento de información técnica de redes y conectividad | 1 hora | 2 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |
| | Gestión de sostenibilidad | 1 hora | 2 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | Autoridades de la Institución |
| | Inventario de Equipos de Comunicación | 1 hora | 2 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |
| | Instalación de Punto de Red | 1 hora | 2 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |

## 4.3. SERVICIOS PARA LA GESTIÓN DOCUMENTAL

Son servicios basados en aplicaciones que apoyan y automatizan los procesos de Gestión Documental en la que se inmiscuyen todas las Direcciones de la institución.

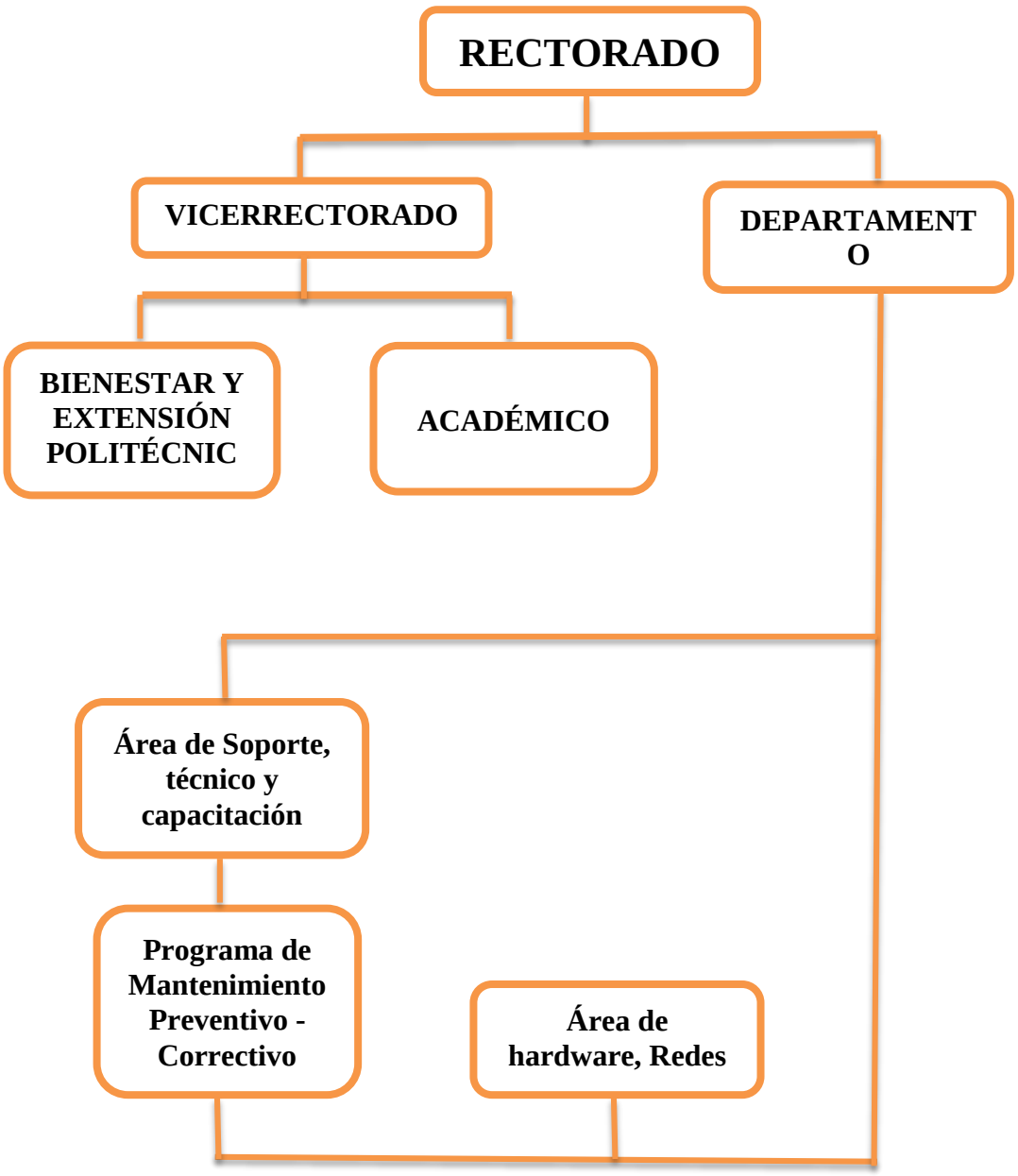
### 4.3.1. INTRANET INSTITUCIONAL

| DESCRIPCIÓN | INCIDENCIAS | TIEMPO DE RESPUESTA A LA INCIDENCIA | TIEMPO MÁXIMO DE SOLUCIÓN | ESCALADO FUNCIONAL | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | 1er ESCALAM. | 2do ESCALAM. | 3ero ESCALAM. | 4to ESCALAM. | 5to ESCALAM. |
| Es un servicio tecnológico que está dirigido a todos los Servidores de la institución, con contenido informativo y servicios Institucionales. | Configuración de acceso a Portal Intranet | 1 hora | 2 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |
| | Carga de Procedimientos | 1 hora | 5 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |
| | Soporte técnico especializado sobre las aplicaciones | 1 hora | 6 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | Autoridades de la Institución |

### 4.3.2. PÁGINA WEB

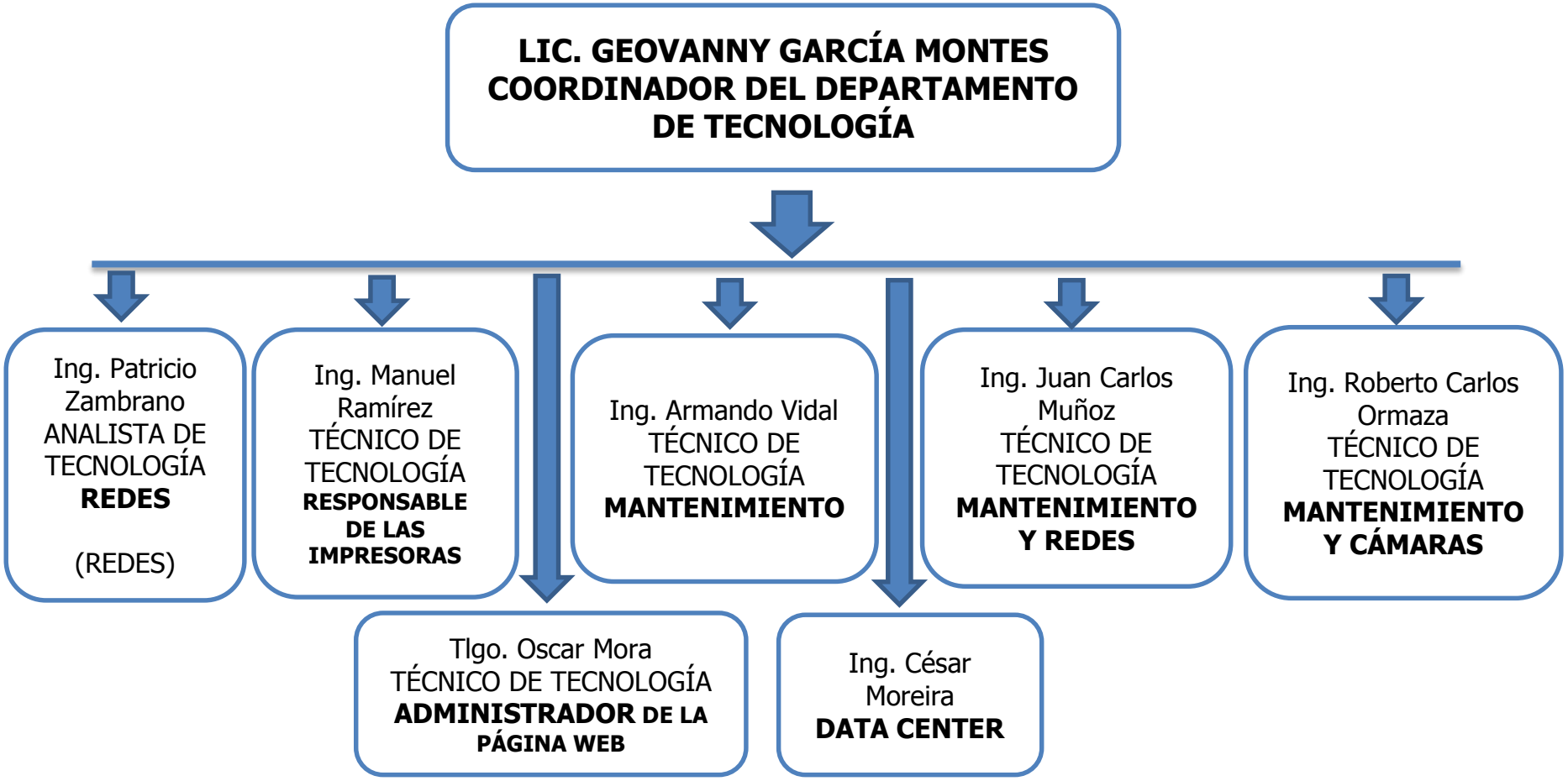
| DESCRIPCIÓN | INCIDENCIAS | TIEMPO DE RESPUESTA A LA INCIDENCIA | TIEMPO MÁXIMO DE SOLUCIÓN | ESCALADO FUNCIONAL | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | 1er ESCALAM. | 2do ESCALAM. | 3ero ESCALAM. | 4to ESCALAM. | 5to ESCALAM. |
| Soporte Funcional, acerca de plugins y complementos adicionales, no incluidos en el diseño. | Instalación de Herramientas Adicionales | 1 hora | 8 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |
| | Mantenimiento especializado sobre las aplicaciones | 1 hora | 8 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | Autoridades de la Institución |

# 5. ESTRUCTURA ORGÁNICA DEL DEPARTAMENTO

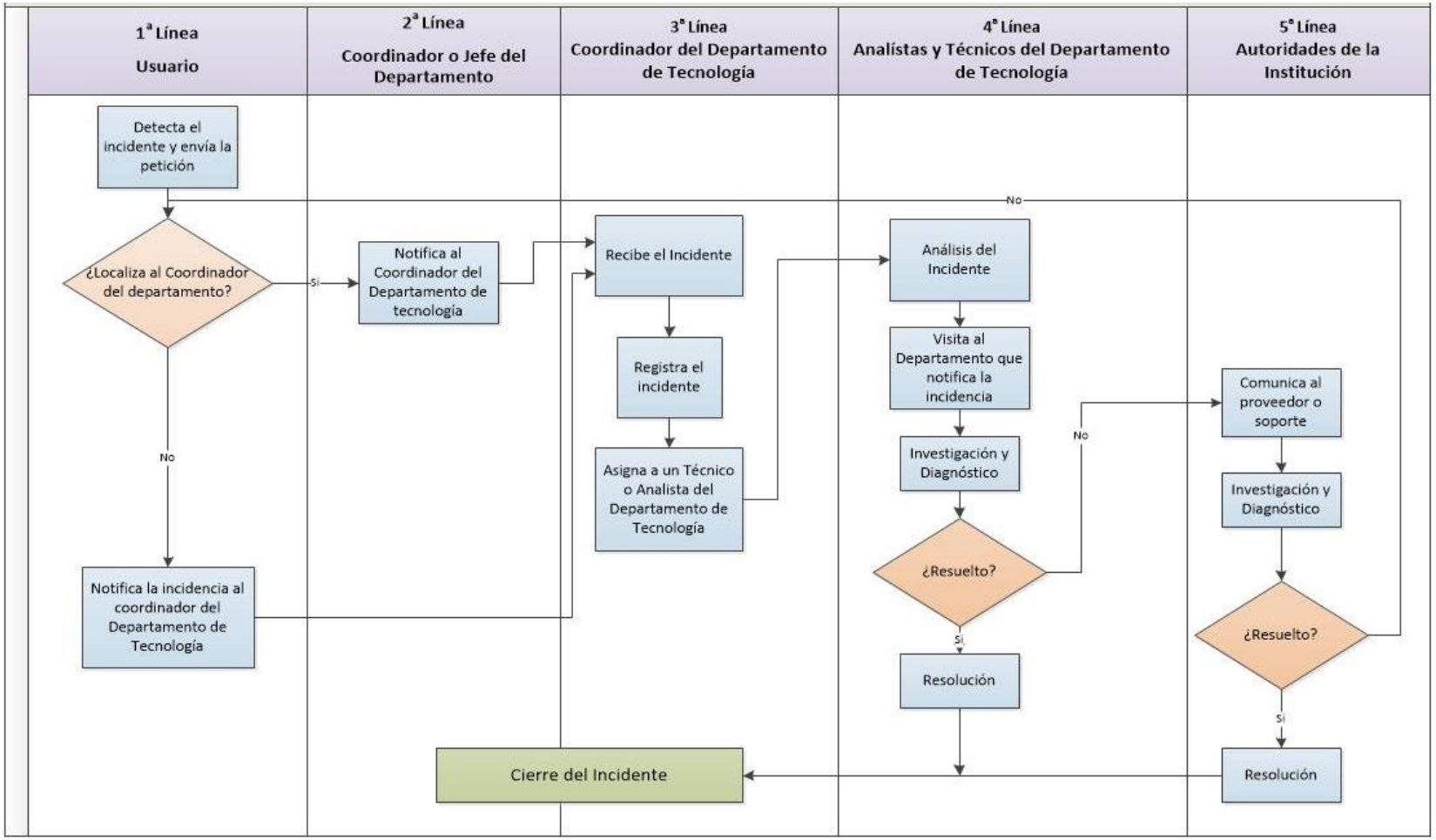


# 6. RESPONSABLES DE LOS INCIDENTES INFORMÁTICOS

El siguiente organigrama muestra las funciones y responsabilidades de cada uno de los entes que conforman el Departamento de Tecnología:



# 7. PROCESO DE UN INCIDENTE INFORMÁTICO



# 8. PRIORIDADES DE LOS INCIDENTES INFORMÁTICOS

| PRIORIDAD | APLICACIÓN DEL INCIDENTE INFORMÁTICO |
|---|---|
| Crítica | **INCIDENTES DE RED**<br>❖ Fallo del servicio de comunicación (Problemas con la conexión a internet)<br>❖ Inconvenientes con el servicio de correo electrónico de la Institución.<br>**INCIDENTES DE ORIGEN NATURAL Y HUMANO (Accidental o deliberado)**<br>❖ Problemas con Fuego (Incendios)<br>❖ Daños en los equipos por agua (escape, fugas e inundaciones)<br>❖ Presencia de desastres industriales (Debido a la actividad humana)<br>❖ Corte de suministro eléctrico<br>❖ Robo de equipos informáticos<br>**INCIDENTES DE HARDWARE**<br>❖ Desperfectos de hardware (componentes internos del CPU) |
| Alta | **INCIDENTES DE SOFTWARE**<br>❖ Problemas de video (proyectores, pantallas o monitores).<br>**INCIDENTES QUE IMPLICAN SOFTWARE Y HARDWARE**<br>❖ Problemas por virus en las computadoras.<br>❖ Reinicio constante de las computadoras.<br>❖ Falta de mantenimiento correctivo. |
| Media | **INCIDENTES DE SOFTWARE**<br>❖ Problemas al actualizar programas.<br>❖ Alerta por licenciamiento de programas.<br>**INCIDENTES DE HARDWARE**<br>❖ Problemas por suministro de componentes a computadoras de escritorio.<br>**INCIDENTES DE IMPRESORAS**<br>❖ Daños en las impresoras multifunción.<br>❖ Problemas por cambio de suministro a los equipos de impresión.<br>**INCIDENTES QUE IMPLICAN SOFTWARE Y HARDWARE**<br>❖ Falta de mantenimiento preventivo.<br>❖ Denegación del servicio (saturación del sistema informático). |
| Baja | **INCIDENTES DE SOFTWARE**<br>❖ Problemas al ejecutar programas (abren lentos o no se ejecutan).<br>**INCIDENTES DE HARDWARE**<br>❖ Daños en el hardware de scanner. |

# 9. GARANTÍAS

## 9.1. CALIDAD DEL SERVICIO

El departamento de Tecnología garantiza realizar un mantenimiento preventivo cada 3 meses a los equipos informáticos de la institución, así como también, cumplirá según los tiempos establecidos con el mantenimiento correctivo, considerando que se debe brindar un servicio de buena calidad.

## 9.2. SEGURIDAD DE LOS SERVICIOS

- **ACCESO LÓGICO**

El acceso a los sistemas y base de datos de la institución, van a ser exclusivamente de los empleados involucrados directamente y las personas autorizadas por las autoridades de la misma, debido a que la información que se maneja es confidencial y debe estar resguardada.

- **ACCESO FÍSICO**

Los responsables de dar mantenimiento, actualización y modificación a los sistemas y equipos informáticos son el coordinador y los técnicos del departamento de tecnología de la ESPAM – MFL. Adicional a esto, si las autoridades deciden contratar proveedores encargados de diversas funciones relacionadas a estos equipos, podrán tener acceso, con la debida documentación acerca del servicio prestado.

- **RECUPERACIÓN DE DESASTRES**

Si llegaran a presentarse desastres naturales y que afecten directamente a los equipos informáticos de la ESPAM-MFL, las autoridades optaran las decisiones adecuadas para restaurar cada uno de los servicios que prestan los equipos.

# 10. FINALIZACIÓN DEL ACUERDO

El presente acuerdo de servicios establece niveles pactados que permitirán atender cada una de las incidencias informáticas que se puedan presentar en las instalaciones de la ESPAM – MFL, con el fin de coordinar y ejecutar actividades para entregar una asistencia de calidad. Además, detalla los servicios tecnológicos que se brindan, presentando sus prioridades y los responsables de atender cada uno de los inconvenientes.

Ninguna de las partes asignará o transferirá los servicios o tareas definidas en éste acuerdo sin el consentimiento de la otra parte.

Los cambios a este acuerdo deben ser justificados por escrito entre las personas autorizadas. Cualquiera de las partes puede dar por concluido el acuerdo previo aviso por escrito.

| | |
|---|---|
| Econ. Miriam Félix López<br>**RECTORA DE LA ESPAM – MFL** | Lic. Geovanny García Montes<br>**COORDINADOR DEL DEPARTAMENTO DE TECNOLOGÍA** |

Ing. Patricio Zambrano
**ANALISTA DE TECNOLOGÍA**

Seguidamente, se presenta el plan de gestión de incidentes informáticos (**Anexo 6**), en el que se definen actividades y procedimientos para dar respuesta a tales sucesos en la ESPAM-MFL, de la cual los puntos mas relevantes se detallan a continuación:

1. Alcance y objetivos
2. Marco legal
3. Respuesta a incidentes y limitaciones
4. Equipo de respuesta a incidentes y responsabilidades
5. Pasos del proceso de notificación
6. Medidas de evaluación de daños
7. Proceso de declaración de las incidencias
8. Proceso de escalamiento
9. Decisión de poner en marcha actividades de emergencia adicionales
10. Revisión del plan y mejora continua

La correcta gestión de incidentes informáticos mitiga debilidades en los procedimientos que se llevan a cabo mediante el uso de tecnologías de la información y comunicación, permitiendo así, reducir amenazas que puedan causar daños a los sistemas de información.

Para ello, se debe determinar una frecuencia de revisión de los servicios tecnológicos disponibles en la institución, con el fin de llevar una actualización periódica que permita servir de mejor manera a la comunidad politécnica. Así mismo, se tienen que coordinar y ejecutar actividades que permitan entregar los servicios con los niveles previamente establecidos. Tomando en cuenta, que la velocidad con la que se reconozca, analice y responda a un incidente, limitará daños y disminuirá costos de reparación.

Es de gran importancia que las instituciones cuenten con una herramienta que permita mantener el control sobre este tipo de inconvenientes, con el fin de minimizar los periodos de fuera de servicio y registrar información relevante de todas las incidencias . Por ello, las autoras de la presente investigación sugieren la implementación de una solución de software Open Source que permita la

gestión de incidentes informáticos y sirva como un mecanismo para facilitar la correcta administración de los recursos informáticos en la ESPAM-MFL.

Para lo cual, se analizó el software GLPI de origen francés (Gestionnaire Libre de Parc Informatique, que en español significa: Administrador Libre de Equipos de Cómputo) el cual permite realizar inventarios de los equipos y a la vez, registrar y controlar los incidentes de seguridad informática que ocurren en una organización.

## 4.2. DISCUSIÓN

Para el desarrollo del plan de gestión de incidentes que afectan a los equipos informáticos de la ESPAM – MFL se aplicó la metodología ITIL, tomando como referencia el apartado gestión de incidentes, la cual establecía conceptos básicos, procesos y actividades sobre la gestión de incidentes, con el objetivo de restaurar el servicio tan pronto como sea posible y minimizar los impactos adversos de las interrupciones generadas. Esta metodología comprendía las siguientes actividades: registro, clasificación, diagnóstico y resolución, mediante las cuales, las autoras ejecutaron el trabajo de investigación.

En comparación con otros trabajos investigativos, con la finalidad de descubrir procedimientos, estructuras y características en común referente a la investigación planteada, se analizaron varias tesis de grado sobre gestión de Incidentes informáticos, dentro de las cuales se puede mencionar la Implantación de los procesos de gestión de incidentes y gestión de problemas según itil v3.0 en el área de tecnologías de información de una entidad financiera de la Pontificia Universidad Católica del Perú, del autor, Jesús Rafael Gómez Álvarez (Gómez, 2012), el cual realizó su investigación utilizando la metodología ITIL para determinar cada una de las actividades y procesos que intervienen en la gestión de servicios y por ende en el proceso de gestión de incidentes de seguridad informática.

Por lo cual, se coincide que es indispensable que las instituciones lleven un control y registro adecuado de los incidentes informáticos, definiendo correctamente cada uno de los procesos . Además, se deben utilizar lineamientos estratégicos para la problemática presentada.

Así mismo, se analizó el trabajo de investigación titulado Análisis, diseño e implementación de un sistema de administración de incidentes en atención al cliente para una empresa de telecomunicaciones de la Pontificia Universidad Católica del Perú, de la autora, Rocío Olinda Vega Bustamante (Vega, 2009), en la cual, se detallan los procedimientos para determinar niveles de prioridad y

tipos de escalamiento que se pueden utilizar para tratar incidentes de seguridad informática.

Luego de realizar el análisis respectivo, las autoras coinciden en que la metodología idónea para sustentar la respuesta a incidentes informáticos en la ESPAM-MFL es la gestión de incidentes de seguridad informática, basada en ITIL, además, se concuerda que para clasificar las incidencias es necesario establecer niveles de prioridad según su función y jerarquía, así como también, se deben instaurar procesos de escalamiento para definir tiempos de atención a cada uno de los incidentes.

Adicionalmente, se acuerda que por medio del plan de respuesta a incidentes se detallan todas las políticas y reglamentos que deben ser tomadas en encuenta al momento de notificar un incidente y todo el proceso que lleva desde que sucede hasta el cierre del mismo.

# CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

## 5.1. CONCLUSIONES

Finalizado el plan de gestión de incidentes que afectan a los equipos informáticos de la ESPAM-MFL, las autoras concluyen lo siguiente:

- ✓ Con el registro de los equipos informáticos pertenecientes a la ESPAM-MFL, se recopiló información relevante, como era el inventario de los mismos, logrando así establecer su disponibilidad, además identificar las tareas o actividades que brindan y los riesgos a los que están expuestos cada uno de ellos.

- ✓ A través de la evaluación de los incidentes informáticos se permitió documentarlos y clasificarlos dependiendo de su prioridad y escalado, con el propósito de desarrollar actividades y procesos que faciliten responder ante ellos.

- ✓ Mediante la elaboración de un catálogo de servicos y definiendo acuerdos para su correcta gestión, se estructura el nivel habitual del funcionamiento de los servicios en cuanto a calidad y disponibliidad entre el personal que labora en el departamento de tecnología y las autoridades .de la institución.

- ✓ El desarrollo de un plan que gestione los incidentes informáticos, permite establecer procedimientos de resolución a inconvenientes que se presentan a diario en la institución, con el fin de tratarlos de forma correcta y en el tiempo establecido.

## 5.2. RECOMENDACIONES

Concluido el plan de gestión de incidentes que afectan a los equipos informáticos de la ESPAM-MFL, las autoras recomiendan lo siguiente:

- ✓ Inventariar continuamente los equipos informáticos de la institución, es clave para la correcta administración y gestión de los mismos, ya que constituyen uno de los elementos fundamentales de toda organización y permiten lograr el nivel de servicio adecuado para satisfacer las necesidades de los usuarios.

- ✓ Documentar información relevante de los incidentes y clasificarlos, con el fin de prevenir nuevas ocurrencias, ya que una interrupción en los servicios que brindan los equipos informáticos reduce la productividad de los usuarios y genera perdida de dinero.

- ✓ La correcta administración de incidentes informáticos no es solamente un asunto de tecnología, es una necesidad del negocio; Del mismo modo, los encargados de dar solución a este tipo de incidentes, deben enfocarse en la detección, no únicamente en la protección o reccuperación.

- ✓ Todas las acciones técnicas y procedimentales utilizadas para tal fin, deben tener en cuenta las consideraciones regulatorias que se apliquen a la institución por su sector y ámbito, y que requieran ser tomadas en cuenta en el proceso de resolución de incidentes, en especial en la toma de evidencias que se derivan.

# BIBLIOGRAFÍA

Acuerdo Nº 166. 2013. Esquema Gubernamental de Seguridad de la Información (EGSI). San Francisco de Quito, EC. 19 de sept.

Amutio, M. s.f. MAGERIT version 3. (En línea). Consultado, 13 de feb. 2015. Formato HTML. Disponible en http://administracionelectronica.gob.es/ctt/magerit#.VO4HNCuUeMI.

APN (Administración de Parques Nacionales). 2010. Guía para la elaboración de planes de gestión de áreas protegidas. (En línea). AR. Consultado, 01 de jul. 2014. Formato PDF. Disponible en http://unrn.edu.ar/blogs/maydt/files/2013/08/Guia-Plan-Gesti%C3%B3n-APN-Arg-2010.pdf.

Aquino, R; Chávez, J; Vidal, L; Ferreyro, L; Álvez, A y Corazo, E. 2011. Manual: Gestión de Incidentes de Seguridad Informática. (En línea). Consultado, 28 de jun. 2014. Formato PDF. Disponible en http://es.slideshare.net/cxocommunity/proyecto-amparo-gestin-de-incidentes-de-seguridad-informtica.

Arancibia, M: Paz, C y Contreras, P. 2010. Concepciones del Profesor sobre el uso educativo de las Tecnologías de la Información y la Comunicación (TIC) asociadas a procesos de enseñanza-aprendizaje en el aula escolar. CH. Estudios Pedagógicos. Vol. 36. n. 1. p 23-51.

Arcilla, M; Ruíz, E; Cerrada, C; Gómez, G; Calvo, J; San Feliu, T y Sánchez, A. 2007. Una propuesta organizativa de los procesos de SD y SS en ITIL. Madrid, ES. REICIS. Revista Española de Innovación, Calidad e Ingeniería del Software. Vol. 3. n. 2. p 6-20.

CAES S.A. (Consulting & Education Services). s.f. ¿Qué es un Incidente Informático? (En línea). CR. Consultado, 03 de jul. 2014. Formato HTML. Disponible en http://www.caescr.com/index.php/capacitacion/tecnologia/investigacion-de-delitos-informaticos-en-bases-de-datos-data-base-forensics-descripcion.html.

Carrasco, A. 2013. Conceptos de seguridad informática y su reflejo en la cámara de cuentas de Andalucía. Sevilla, ES. Revista Auditoría Pública. n. 61. p 11-117.

Cayssials, A. 2006. ¿Subjetividad en un cuestionario? Buenos Aires, AR. Subjetividad y Procesos Cognitivos. n. 8. p 80-87.

Cuello, P y Vizcaya, M. 2002. Uso de técnicas de enseñanza para desarrollar el potencial creativo de los estudiantes del programa de educación integral de la UPEL-IPB. Caracas, VE. Investigación y Postgrado. Vol. 17. n. 1. p 83-113.

De Freitas, V. 2009. Análisis y evaluación del riesgo de la información: caso de estudio Universidad Simón Bolívar. Maracaibo, VE. Enlace. Vol. 6. n. 1. p 43-55.

Del Castillo, A y Sardi, N. 2012. Las normas ISO y el concepto de calidad aplicado a los servicios médicos en anestesiología. Bogotá, CO. Revista Colombiana de Anestesiología. Vol. 40. n. 1. p 14-16.

Dussan, C. 2006.Políticas de seguridad informática. Cali, CO. Entramado. Vol. 2. n. 1. p 86-92.

EAR/PILAR - Entorno de Análisis de Riesgos. s.f. MAGERIT versión 3. (En línea). Consultado, 20 de dic. 2014. Formato HTML. Disponible en https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/.

Gerbrandy, G y Hoogendam, P. 1998. Aguas y Acequias: los derechos del agua y la gestión campesina de riesgo en los Andes Bolivarianos. Centro de Información para el Desarrollo-CID. Bolivia. Plural Editores. p 237.

Gómez, A. 2012. Implantación de los procesos de gestión de incidentes y gestión de problemas según itil v3.0 en el área de tecnologías de información de una entidad financiera. (En línea). Consultado, 20 de feb. 2015. Formato HTML. Disponible en http://tesis.pucp.edu.pe/repositorio/handle/123456789/1433

Graniel, G. 2011. La Tecnología de la Información como factor competitivo: Un estudio en el APL Cosecha Metal-Mecánico Santa Rosa/Horizontina RS, Brazil. Miguel Lanus, AR. Visión de futuro. Vol. 15. n. 1.

Hernández, N; Yelandy, M y Cuza, B. 2013. Modelos causales para la Gestión de Riesgos. La Habana, CU. Revista Cubana de Ciencias Informáticas. Vol. 7. n. 4.

Hitpass, B. 2012. Business Process Management Fundamentos y Conceptos de Implementación. 3 ed. Chile. BHH Ltda. p 303.

Jiménez, J. 2008. La seguridad informática y el usuario final. Ciudad Universitaria, MX. Revista Digital Universitaria. Vol. 9. n. 4. p. 4.

Kolthof, A; Pieper, M; Bon, J. 2012. Fundamentos de Gestión de Servicios TI basada en ITIL. 2 ed. Holanda. Van Haren Publishing. p 33.

León, B y Rosero, M. 2014. Recomendaciones para contratar servicios en la 'nube'. Tunja-Boyacá, CO. Facultad de Ingeniería. Vol. 23. n. 37. p 93-108.

Marrero, Y. 2003. La criptografía como elemento de la seguridad informática. La Habana, CU. ACIMED. Vol. 11. n. 6.

Mesquida, A; Mas, A y Amengual, E. 2009. La madurez de los servicios TI. Madrid, ES. REICIS. Revista Española de Innovación, Calidad e Ingeniería del Software. Vol. 5. n. 2. p 77-87.

Monterroso, E. s.f. Normas ISO: Generalidades. (En línea). Consultado, 20 de dic. 2014. Formato HTML. Disponible en http://www.unlu.edu.ar/~ope20156/normasiso.htm.

Montesino, R; Baluja, W y Porvén, J. 2013. Gestión automatizada e integrada de controles de seguridad informática. La Habana, CU. Ingeniería Electrónica, Automática y Comunicaciones. Vol. 34. n. 1. 40-58.

Morlanes, G. 2012. Seguridad Informática, Matanzas, CU. Revista de Arquitectura e Ingeniería. Vol. 6. n. 2. p 1-14.

Nacipucha, E. 2013. Gestión de incidentes y problemas en el área de sistemas con metodología ITIL, para mejorar la utilización de los recursos de la organización. Tesis. Ing. Informática. Universidad Tecnológica Israel. Cuenca. EC. p 99.

Ocampo, C; Moreno, R y Caicedo, S. 2009. Implementación de modelo de procesos de gestión de servicios con ITIL. Pereira, CO. Scientia Et Technica. Vol. 15. n. 41. p 215-220.

Ocaña, H. 2012. Dirección Estratégica de los Negocios. 1 ed. Argentina. Dunken. p 400.

Ochoa, K. s.f. Manual de GPLI. (En línea). Consultado, 09 de jun. 2015. Formato PDF. Disponible en http://www.finanzas.gob.ec/wp-content/uploads/downloads/2014/02/Manual-Usuario-final-v2-GLPI.pdf

Ortiz, P y Hoyos, A. 2005. ITIL: Una nueva alternativa en el aprovechamiento de los recursos informáticos para las empresas colombianas. Medellín, CO. Revista Ingenierías Universidad de Medellín. Vol. 4. n. 6. p 25-39.

Ortiz, S y Pedroza, A. 2006. ¿Qué es la gestión de la innovación y la tecnología (GInnT)? Jalisco, MX. Journal of Technology Management & Innovation. Vol. 1. n. 2. p 64-82.

OSIATIS S.A. s.f. ITIL Gestión de Servícios TI: Fundamentos de la Gestión TI. (En línea). Consultado, 09 de jun. 2014. Formato PHP. Disponible en http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/gestion_de_incidentes/vision_general_gestion_de_incidentes/vision_general_gestion_de_incidentes.php.

OVERTI (Consultoría y Soluciones para la Gestión de Servicios TI). c2011. Gestión de Incidencias. (En línea). Consultado, 09 de jun. 2014. Formato HTML. Disponible en http://www.overti.es/procesos-itsm/gestion-incidencias-itil-v3.aspx.

Pacheco, F y Jara, H. 2012. Ethical Hacking: Gestión de Incidentes. 1 ed. Argentina. Fox Andina; DÁLAGA. p 352.

Piattini, M; Del Peso, E.; Del Peso, M. 2008. Auditoria de Tecnologías y Sistemas de Información. 4ed. Madrid, ES. RA-MAl. Vol. 1378. p 38.

Prieto, V; Quiñones, I; Ramírez, G; Fuentes, Z; Labrada, T; Pérez, O y Montero, M. 2011. Impacto de las tecnologías de la información y las comunicaciones en la educación y nuevos paradigmas del enfoque educativo. La Habana, CU. Educaciín Médica Superior. Vol. 25. n.1. p 95-102.

Puello, O. 2012. Gerencia Informática: Operación del Servicio. (En línea). Consultado, 14 de nov. 2014. Formato PDF. Disponible en http://manglar.uninorte.edu.co/bitstream/handle/10584/2209/Operaci%F3n%20del%20servicio.pdf;jsessionid=F2253D0E76F5F08FEBCD8B91118993F8?sequence=1.

Rabinowitz, P. c2014. ¿Qué es un plan de gestión? (En línea). Consultado, 18 de jul. 2014. Formato HTML. Disponible en http://ctb.ku.edu/es/tabla-de-contenidos/liderazgo/administracion-efectiva/plan-de-gestion/principal.

Ramos, M. 2002. La seguridad de los datos. Madrid, ES. Revista Ingenlum. Vol. 28. p. 6.

Sanchis, R; Poler, R y Ortiz, A. 2009. Técnicas para el Modelado de Procesos de Negocio en Cadenas de Suministro. La Serena, CH. Información Tecnológica. Vol. 20. n. 2. p 29-40.

Teopanta, D. 2006. Aspectos generales de Seguridad Informática. (En línea). Consultado, 25 de jul. 2014. Formato PDF. Disponible en http://repositorio.utc.edu.ec/bitstream/27000/536/1/T-UTC-1052(1).pdf.

Toro, F. 2013. Administración de proyectos de informática. 1 ed. Bogotá-Colombia. Ecoe. p 236.

Velasco, M y Arean, H. 2008. El Derecho Informático y la gestión de la seguridad de la información una perspectiva con base en la norma ISO 27001. Barranquilla, CO. Revista de derecho. n. 29. p 333-366.

Valdés, M. 1996. Las normar ISO relacionadas con la documentación y la información. La Habana, CU. ACIMED. Vol. 4. n. 3. p 33-37.

Vega, R. 2009. Análisis, diseño e implementación de un sistema de administración de incidentes en atención al cliente para una empresa de telecomunicaciones de la Pontificia Universidad Católica del Perú. (En línea). PE. Consultado, 03 de jul. 2014. Formato PDF. Disponible en http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/334/VEGA_ROC%C3%8DO_AN%C3%81LISIS_DISE%C3%91O_E_IMPLEMENTACI%C3%93N_DE_UN_SISTEMA_DE_ADMINISTRACI%C3%93N_DE_INCIDENTES_EN_ATENCI%C3%93N_AL_CLIENTE_PARA_UNA_EMPRESA_DE_TELECOMUNICACIONES.pdf?sequence=1

VenCERT (Sistema Nacional de Gestión de Incidentes Telemáticos). 2008. ¿Qué es un incidente? (En línea). VE. Consultado, 03 de jul. 2014. Formato HTML. Disponible en http://vencert.gob.ve/index.php/vencert/faqs/90-que-es-un-incidente.

Vera, R. 2009. Análisis, diseño e implementación de un sistema de administración de incidentes en atención al cliente para una empresa de telecomunicaciones. (En línea). Consultado, 20 de feb. 2015. Formato HTML. Disponible en http://tesis.pucp.edu.pe/repositorio/handle/123456789/334

# ANEXOS

# ANEXO 1
# OFICIO DE AUTORIZACIÓN DEL RECTOR DE LA ESPAM-MFL

**ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ**

REPÚBLICA DEL ECUADOR

ESPAM MFL
CARRERA DE INFORMÁTICA

Oficio Nº ESPAM MFL - CI – 2014- 266-OF
Calceta, 09 de octubre de 2014

Ingeniero
Leonardo Félix López
**RECTOR ESPAM MFL**
En su despacho.-

De mi consideración:

Por medio del presente reciba un cordial y afectuoso saludo de quienes conformamos la Carrera de Informática de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López ESPAM - MFL.

Nuestra institución dentro de su malla curricular contempla la realización de tesis de tercer nivel que tienen que efectuar todos los estudiantes con la finalidad de obtener el título de Ingeniero en Informática y, dentro de estas, las Instituciones públicas o privadas.

Con estos antecedentes, solicito a usted de la manera más cordial, se les brinde la facilidad en la toma de datos requeridos para la elaboración del PLAN DE GESTIÓN DE INCIDENTES INFORMÁTICOS EN LA ESPAM en la institución que acertadamente usted dirige; por parte de las señoritas: **CUZME ROMERO MARÍA GABRIEL y PINARGOTE ANCHUNDIA ROXANNA ELIZABETH**, estudiantes de décimo semestre de la Carrera de Informática ESPAM – MFL, para tal efecto es necesario contar con el apoyo requerido brindándole las facilidades pertinentes.

Esperando favorable acogida a la presente quedo de usted agradecida

Atentamente,

Ing. Jéssica Morales Carrillo
**DIRECTORA CARRERA DE INFORMÁTICA ESPAM – MFL**

JM/jb

ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ "MANUEL FÉLIX LÓPEZ" ESPAM "MFL"
RECIBIDO
Fecha: 14-10-2014
Hora: 16:45
RECEPCIÓN

**ANEXO 2**
**CERTIFICACIÓN EMITIDA POR EL JEFE DE ALMACÉN**

**ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ**
**MANUEL FÉLIX LÓPEZ**

*Calceta, 17 de Noviembre de 2014*

WWW.ESPAM.EDU.EC

# *CERTIFICACIÓN*

*Yo, Héctor Jhon Macías Moreira, Jefe de Almacén de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, mediante el presente documento certifico que proporcioné la información de los bienes informáticos requerida para el desarrollo de la Tesis de Grado "Plan de Gestión de Incidentes que Afectan a los Equipos Informáticos de la ESPAM MFL", la misma que fue desarrollada por las estudiantes de la Carrera de Informática Pinargote Anchundia Roxanna y Cuzme Romero Gabriela.*

*Es todo cuanto puedo certificar en honor a la verdad, las mencionadas estudiantes pueden hacer uso de la presente certificación para los fines correspondientes.*

*Atentamente,*

*Ing. Héctor Jhon Macías Moreira*
***JEFE DE ALMACÉN ESPAM MFL***

**Dirección: Av.10 de AGOSTO Nº 82 y GRANDA CENTENO. Telefaxes 593-052 685 134/156/035/048**
**CALCETA - ECUADOR**

**ANEXO 3**
**FICHA DE REGISTRO DE EQUIPOS INFORMÁTICOS**

**ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ**

## FICHA DE REGISTRO DE EQUIPOS INFORMÁTICOS

**Carrera**: **Fecha:**

**Sección:** **Área:**

| CÓDIGO | DESCRIPCIÓN | TIPO | RESPONSABLE | LOCALIZACIÓN |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

**ANEXO 4**
**CUESTIONARIO DE INCIDENCIAS INFORMÁTICAS**

## CUESTIONARIO DE INCIDENTES INFORMÁTICOS

**Objetivo:** Determinar los incidentes informáticos que se presentan en las carreras y departamentos de la ESPAM MFL.

**Departamento: _____**
**Área: _____ Fecha: _____**

**¿CUÁLES DE LOS SIGUIENTES INCIDENTES INFORMÁTICOS SE PRESENTAN A MENUDO EN SU DEPARTAMENTO?**

- **Problemas con fuego (incendios)** ☐

| **¿Con qué frecuencia sucede este tipo de incidentes?** | **¿Cuál es el tiempo promedio de solución?** |
|---|---|
| ○ 1 vez al mes<br>○ 2 veces al mes<br>○ 3 o más veces al mes<br>○ Cada 2 meses<br>○ Cada 3 meses<br>○ Cada seis meses<br>○ Cada 9 meses<br>○ Una vez al año | ○ 1 semana<br>○ 2 semanas<br>○ 3 semanas<br>○ 1 mes<br>○ Más de un Mes |

- **Daños en los equipos por agua (escape, fugas, inundaciones)** ☐

| **¿Con qué frecuencia sucede este tipo de incidentes?** | **¿Cuál es el tiempo promedio de solución?** |
|---|---|
| ○ 1 vez al mes<br>○ 2 veces al mes<br>○ 3 o más veces al mes<br>○ Cada 2 meses<br>○ Cada 3 meses<br>○ Cada seis meses<br>○ Cada 9 meses<br>○ Una vez al año | ○ 1 semana<br>○ 2 semanas<br>○ 3 semanas<br>○ 1 mes<br>○ Más de un Mes |

| | |
|---|---|
| • **Presencia de desastres industriales (debido a la actividad humana)** ☐ | |
| **¿Con qué frecuencia sucede este tipo de incidentes?**<br>○ 1 vez al mes<br>○ 2 veces al mes<br>○ 3 o más veces al mes<br>○ Cada 2 meses<br>○ Cada 3 meses<br>○ Cada seis meses<br>○ Cada 9 meses<br>○ Una vez al año | **¿Cuál es el tiempo promedio de solución?**<br>○ 1 semana<br>○ 2 semanas<br>○ 3 semanas<br>○ 1 mes<br>○ Más de un Mes |
| • **Robo de equipos informáticos** ☐ | |
| **¿Con qué frecuencia sucede este tipo de incidentes?**<br>○ 1 vez al mes<br>○ 2 veces al mes<br>○ 3 o más veces al mes<br>○ Cada 2 meses<br>○ Cada 3 meses<br>○ Cada seis meses<br>○ Cada 9 meses<br>○ Una vez al año | **¿Cuál es el tiempo promedio de solución?**<br>○ 1 semana<br>○ 2 semanas<br>○ 3 semanas<br>○ 1 mes<br>○ Más de un Mes |
| • **Corte de suministro eléctrico** ☐ | |
| **¿Con qué frecuencia sucede este tipo de incidentes?**<br>○ 1 vez al mes<br>○ 2 veces al mes<br>○ 3 o más veces al mes<br>○ Cada 2 meses<br>○ Cada 3 meses<br>○ Cada seis meses<br>○ Cada 9 meses<br>○ Una vez al año | **¿Cuál es el tiempo promedio de solución?**<br>○ 1 semana<br>○ 2 semanas<br>○ 3 semanas<br>○ 1 mes<br>○ Más de un Mes |

<table>
<tr><td colspan="2">• Denegación del servicio (saturación del sistema informático) ☐</td></tr>
<tr><td>¿Con qué frecuencia sucede este tipo de incidentes?<br>○ 1 vez al mes<br>○ 2 veces al mes<br>○ 3 o más veces al mes<br>○ Cada 2 meses<br>○ Cada 3 meses<br>○ Cada seis meses<br>○ Cada 9 meses<br>○ Una vez al año</td><td>¿Cuál es el tiempo promedio de solución?<br>○ 1 semana<br>○ 2 semanas<br>○ 3 semanas<br>○ 1 mes<br>○ Más de un Mes</td></tr>
<tr><td colspan="2">• Fallo del servicio de comunicación (Problemas con la conexión a internet) ☐</td></tr>
<tr><td>¿Con qué frecuencia sucede este tipo de incidentes?<br>○ 1 vez al mes<br>○ 2 veces al mes<br>○ 3 o más veces al mes<br>○ Cada 2 meses<br>○ Cada 3 meses<br>○ Cada seis meses<br>○ Cada 9 meses<br>○ Una vez al año</td><td>¿Cuál es el tiempo promedio de solución?<br>○ 1 semana<br>○ 2 semanas<br>○ 3 semanas<br>○ 1 mes<br>○ Más de un Mes</td></tr>
<tr><td colspan="2">• Inconvenientes con el servicio de correo electrónico de la institución ☐</td></tr>
<tr><td>¿Con qué frecuencia sucede este tipo de incidentes?<br>○ 1 vez al mes<br>○ 2 veces al mes<br>○ 3 o más veces al mes<br>○ Cada 2 meses<br>○ Cada 3 meses<br>○ Cada seis meses<br>○ Cada 9 meses<br>○ Una vez al año</td><td>¿Cuál es el tiempo promedio de solución?<br>○ 1 semana<br>○ 2 semanas<br>○ 3 semanas<br>○ 1 mes<br>○ Más de un Mes</td></tr>
</table>

<table>
<tr><td colspan="2">• Problemas por suministro de componentes a computadoras de escritorio ☐</td></tr>
<tr><td>¿Con qué frecuencia sucede este tipo de incidentes?<br>○ 1 vez al mes<br>○ 2 veces al mes<br>○ 3 o más veces al mes<br>○ Cada 2 meses<br>○ Cada 3 meses<br>○ Cada seis meses<br>○ Cada 9 meses<br>○ Una vez al año</td><td>¿Cuál es el tiempo promedio de solución?<br>○ 1 semana<br>○ 2 semanas<br>○ 3 semanas<br>○ 1 mes<br>○ Más de un Mes</td></tr>
<tr><td colspan="2">• Desperfectos de hardware (componentes internos del CPU) ☐<br>○ Disco Duro<br>○ Memoria RAM<br>○ Fuente de Poder<br>○ Mainboard<br>○ Otros _____</td></tr>
<tr><td>¿Con qué frecuencia sucede este tipo de incidentes?<br>○ 1 vez al mes<br>○ 2 veces al mes<br>○ 3 o más veces al mes<br>○ Cada 2 meses<br>○ Cada 3 meses<br>○ Cada seis meses<br>○ Cada 9 meses<br>○ Una vez al año</td><td>¿Cuál es el tiempo promedio de solución?<br>○ 1 semana<br>○ 2 semanas<br>○ 3 semanas<br>○ 1 mes<br>○ Más de un Mes</td></tr>
<tr><td colspan="2">• Problemas de video (proyectores, pantallas o monitores) ☐</td></tr>
<tr><td>¿Con qué frecuencia sucede este tipo de incidentes?<br>○ 1 vez al mes<br>○ 2 veces al mes<br>○ 3 o más veces al mes<br>○ Cada 2 meses<br>○ Cada 3 meses<br>○ Cada seis meses<br>○ Cada 9 meses<br>○ Una vez al año</td><td>¿Cuál es el tiempo promedio de solución?<br>○ 1 semana<br>○ 2 semanas<br>○ 3 semanas<br>○ 1 mes<br>○ Más de un Mes</td></tr>
</table>

| | |
|---|---|
| • **Problemas por virus en las computadoras** ☐ | |
| **¿Con qué frecuencia sucede este tipo de incidentes?**<br>○ 1 vez al mes<br>○ 2 veces al mes<br>○ 3 o más veces al mes<br>○ Cada 2 meses<br>○ Cada 3 meses<br>○ Cada seis meses<br>○ Cada 9 meses<br>○ Una vez al año | **¿Cuál es el tiempo promedio de solución?**<br>○ 1 semana<br>○ 2 semanas<br>○ 3 semanas<br>○ 1 mes<br>○ Más de un Mes |
| • **Reinicio constante de las computadoras** ☐ | |
| **¿Con qué frecuencia sucede este tipo de incidentes?**<br>○ 1 vez al mes<br>○ 2 veces al mes<br>○ 3 o más veces al mes<br>○ Cada 2 meses<br>○ Cada 3 meses<br>○ Cada seis meses<br>○ Cada 9 meses<br>○ Una vez al año | **¿Cuál es el tiempo promedio de solución?**<br>○ 1 semana<br>○ 2 semanas<br>○ 3 semanas<br>○ 1 mes<br>○ Más de un Mes |
| • **Problemas al actualizar programas (software)** ☐ | |
| **¿Con qué frecuencia sucede este tipo de incidentes?**<br>○ 1 vez al mes<br>○ 2 veces al mes<br>○ 3 o más veces al mes<br>○ Cada 2 meses<br>○ Cada 3 meses<br>○ Cada seis meses<br>○ Cada 9 meses<br>○ Una vez al año | **¿Cuál es el tiempo promedio de solución?**<br>○ 1 semana<br>○ 2 semanas<br>○ 3 semanas<br>○ 1 mes<br>○ Más de un Mes |

<table>
<tr><td colspan="2">• Problemas al ejecutar programas (abren lentos o no se ejecutan) ☐</td></tr>
<tr><td>¿Con qué frecuencia sucede este tipo de incidentes?<br>○ 1 vez al mes<br>○ 2 veces al mes<br>○ 3 o más veces al mes<br>○ Cada 2 meses<br>○ Cada 3 meses<br>○ Cada seis meses<br>○ Cada 9 meses<br>○ Una vez al año</td><td>¿Cuál es el tiempo promedio de solución?<br>○ 1 semana<br>○ 2 semanas<br>○ 3 semanas<br>○ 1 mes<br>○ Más de un Mes</td></tr>
<tr><td colspan="2">• Alerta por licenciamiento de programas (piratas) ☐</td></tr>
<tr><td>¿Con qué frecuencia sucede este tipo de incidentes?<br>○ 1 vez al mes<br>○ 2 veces al mes<br>○ 3 o más veces al mes<br>○ Cada 2 meses<br>○ Cada 3 meses<br>○ Cada seis meses<br>○ Cada 9 meses<br>○ Una vez al año</td><td>¿Cuál es el tiempo promedio de solución?<br>○ 1 semana<br>○ 2 semanas<br>○ 3 semanas<br>○ 1 mes<br>○ Más de un Mes</td></tr>
<tr><td colspan="2">• Falta de mantenimiento preventivo ☐</td></tr>
<tr><td>¿Con qué frecuencia sucede este tipo de incidentes?<br>○ 1 vez al mes<br>○ 2 veces al mes<br>○ 3 o más veces al mes<br>○ Cada 2 meses<br>○ Cada 3 meses<br>○ Cada seis meses<br>○ Cada 9 meses<br>○ Una vez al año</td><td>¿Cuál es el tiempo promedio de solución?<br>○ 1 semana<br>○ 2 semanas<br>○ 3 semanas<br>○ 1 mes<br>○ Más de un Mes</td></tr>
</table>

<table>
<tr><td colspan="2">

- **Falta de mantenimiento correctivo** ☐

</td></tr>
<tr><td>

**¿Con qué frecuencia sucede este tipo de incidentes?**

- ○ 1 vez al mes
- ○ 2 veces al mes
- ○ 3 o más veces al mes
- ○ Cada 2 meses
- ○ Cada 3 meses
- ○ Cada seis meses
- ○ Cada 9 meses
- ○ Una vez al año

</td><td>

**¿Cuál es el tiempo promedio de solución?**

- ○ 1 semana
- ○ 2 semanas
- ○ 3 semanas
- ○ 1 mes
- ○ Más de un Mes

</td></tr>
<tr><td colspan="2">

- **Daños en las impresoras multifuncion** ☐

</td></tr>
<tr><td>

**¿Con qué frecuencia sucede este tipo de incidentes?**

- ○ 1 vez al mes
- ○ 2 veces al mes
- ○ 3 o más veces al mes
- ○ Cada 2 meses
- ○ Cada 3 meses
- ○ Cada seis meses
- ○ Cada 9 meses
- ○ Una vez al año

</td><td>

**¿Cuál es el tiempo promedio de solución?**

- ○ 1 semana
- ○ 2 semanas
- ○ 3 semanas
- ○ 1 mes
- ○ Más de un Mes

</td></tr>
<tr><td colspan="2">

- **Problemas por cambio de suministro a los equipos de impresión** ☐

- ○ Tóner
- ○ Cartuchos b/n
- ○ Cartuchos a Color
- ○ Resmas de papel

</td></tr>
<tr><td>

**¿Con qué frecuencia sucede este tipo de incidentes?**

- ○ 1 vez al mes
- ○ 2 veces al mes
- ○ 3 o más veces al mes
- ○ Cada 2 meses
- ○ Cada 3 meses
- ○ Cada seis meses
- ○ Cada 9 meses
- ○ Una vez al año

</td><td>

**¿Cuál es el tiempo promedio de solución?**

- ○ 1 semana
- ○ 2 semanas
- ○ 3 semanas
- ○ 1 mes
- ○ Más de un Mes

</td></tr>
</table>

- **Daños en el hardware de scanner** ☐

| **¿Con qué frecuencia sucede este tipo de incidentes?** | **¿Cuál es el tiempo promedio de solución?** |
|---|---|
| ○ 1 vez al mes<br>○ 2 veces al mes<br>○ 3 o más veces al mes<br>○ Cada 2 meses<br>○ Cada 3 meses<br>○ Cada seis meses<br>○ Cada 9 meses<br>○ Una vez al año | ○ 1 semana<br>○ 2 semanas<br>○ 3 semanas<br>○ 1 mes<br>○ Más de un Mes |

**¿Qué persona notifica el incidente?**

_____
_____
_____
_____

**¿A quién se le comunica?**

_____
_____
_____
_____

**¿Qué efectos se derivan de los mismos?**

_____
_____
_____
_____
_____

**OTROS INCIDENTES**

_____
_____
_____
_____

**ANEXO 5**
**FICHA DE REGISTRO DE INCIDENTES INFORMÁTICOS**

**ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ**

**REGISTRO DE INCIDENCIAS INFORMÁTICAS**

| № DE INCIDENCIA | NOMBRE DEL DEPARTAMENTO | FECHA DE REGISTRO | HORA DE REGISTRO | TIPO DE INCIDENCIA | DESCRIPCIÓN | TÉCNICO ENCARGADO | FECHA DE SOLUCIÓN | HORA DE SOLUCION | FIRMA DEL COORDINADOR DEL DEPARTAMENTO |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

# ANEXO 6
# PLAN DE GESTIÓN DE INCIDENTES QUE AFECTAN A LOS EQUIPOS INFORMÁTICOS DE LA ESPAM-MFL

# PLAN DE GESTIÓN DE INCIDENTES INFORMÁTICOS DE LA ESPAM-MFL

# CONTENIDO

1. ALCANCE Y OBJETIVOS....228
1.1. ALCANCE....228
1.2. OBJETIVOS....228
2. MARCO LEGAL....229
3. RESPUESTA A INCIDENTES Y LIMITACIONES....230
3.1. RESPUESTA A INCIDENTES....230
3.1.1. SERVICIOS ESTÁNDAR....230
3.1.1.1. COMPUTADORAS PERSONALES DE ESCRITORIO Y PORTÁTILES 230
3.1.1.2. CORREO ELECTRÓNICO....232
3.1.1.3. IMPRESIÓN Y DIGITALIZACIÓN....233
3.1.2. SERVICIOS POR DEMANDA....234
3.1.2.1. GESTIÓN DE REDES Y CONECTIVIDAD....234
3.1.3. SERVICIOS PARA LA GESTIÓN DOCUMENTAL....235
3.1.3.1. INTRANET INSTITUCIONAL....235
3.1.3.2. PÁGINA WEB....236
3.2. LIMITACIONES....237
4. EQUIPO DE RESPUESTA A INCIDENTES Y RESPONSABILIDADES....241
4.1. EQUIPO DE RESPUESTA A INCIDENTES....241
4.2. RESPONSABILIDADES....243
5. PASOS DEL PROCESO DE NOTIFICACIÓN....244
6. MEDIDAS DE EVALUACIÓN DE DAÑOS....245
6.1. RESPUESTA DE POST-ACCIONES....246
7. PROCESO DE DECLARACIÓN DE INCIDENCIAS....247
8. PROCESO DE ESCALAMIENTO....248

9. DECISIÓN DE PONER EN MARCHA ACTIVIDADES DE EMERGENCIA ADICIONALES .....249

9.1. LISTADO DE AMENAZAS ..... 249

9.1.1. DESASTRES NATURALES (N) ..... 249

9.1.2. DE ORIGEN INDUSTRIAL (I) ..... 249

9.1.3. ERRORES Y FALLOS NO INTENCIONADOS (E)..... 250

9.1.4. ATAQUES INTENCIONADOS (A) ..... 250

9.2. CONSEJOS PARA EVITAR AMENAZAS QUE AFECTEN A LOS EQUIPOS INFORMATICOS. ..... 251

10. REVISIÓN DEL PLAN Y MEJORA CONTINUA.....253

ANEXOS .....254

ANEXO 1. FICHA DE REGISTRO DE INCIDENCIAS INFORMÁTICAS..... 255

# 1. ALCANCE Y OBJETIVOS

## 1.1. ALCANCE

Agilizar y monitorizar los servicios que brinda el departamento de tecnología de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López.

## 1.2. OBJETIVOS

- Establecer lineamientos que permitan gestionar los incidentes informáticos que se presentan en la ESPAM-MFL, con el fin de limitar el impacto de los mismos.
- Coordinar actividades que permitan al Departamento de Tecnología entregar servicios de calidad.
- Gestionar los incidentes informáticos de forma correcta y según los tiempos establecidos.
- Recuperar la calidad y disponibilidad de los servicios que brindan los equipos informáticos.

# 2. MARCO LEGAL

La Constitución de la República determina en el artículo 227 que la Administración Pública constituye un servicio a la colectividad que se rige en principios de eficacia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia y evaluación, por lo que es de vital importancia adoptar políticas y procedimientos necesarios para mantener la seguridad de la información que se genera y custodia en diferentes medios y formatos de las entidades de la Administración Pública.

Al mismo tiempo, en el segundo suplemento del registro oficial número 88 del 05 de septiembre de 2013, la secretaría nacional de la administración pública considera que las Tecnologías de la Información y Comunicación son herramientas imprescindibles para el cumplimiento de la gestión institucional e inter-institucional de la Administración pública en virtud tal, deben cumplir con estándares de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la información.

Conjuntamente, en su primer artículo declara: “Disponer a las entidades de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva el uso obligatorio de la Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la información”.

El plan de gestión está enfocado a tratar los incidentes que provoquen interrupción en los servicios que brindan los equipos informáticos, permitiendo la calidad y continuidad de las actividades regulares de la institución.

# 3. RESPUESTA A INCIDENTES Y LIMITACIONES

## 3.1. RESPUESTA A INCIDENTES

### 3.1.1. SERVICIOS ESTÁNDAR

Son los servicios tecnológicos que por defecto cualquier servidor de la institución recibe y tiene acceso, estos son: computador personal, correo electrónico e impresión.

#### 3.1.1.1. COMPUTADORAS PERSONALES DE ESCRITORIO Y PORTÁTILES

| DESCRIPCIÓN | INCIDENCIAS | TIEMPO DE RESPUESTA A LA INCIDENCIA | TIEMPO MÁXIMO DE SOLUCIÓN | ESCALADO FUNCIONAL | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | 1er ESCALAM. | 2do ESCALAM. | 3ero ESCALAM. | 4to ESCALAM. | 5to ESCALAM. |
| Habilitación y soporte de computadoras personales de escritorio y portátiles para los servidores (funcionarios) de la institución. Incluye hardware, software base, acceso a la red, Intranet, cuenta de correo electrónico interno y mensajería instantánea. (ATENCION DEL DIA A DIA) | Soporte Técnico Hardware y Software | 1 hora | 3 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |
| | Acceso a Internet | 30 minutos | 3 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |
| | Acceso a red inalámbrica | 30 minutos | 2 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |
| | Soporte Ofimático | 1 hora | 6 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |
| | Instalación de hardware para equipos de escritorio | 1 hora | 12 horas laborables | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | Autoridades de la Institución |
| | Aplicación de garantías de hardware | 1 hora | 4 días laborables | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | Autoridades de la Institución |
| | Asignación de equipos informáticos | 1 hora | 3 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | Autoridades de la Institución |

| DESCRIPCIÓN | INCIDENCIAS | TIEMPO DE RESPUESTA A LA INCIDENCIA | TIEMPO MÁXIMO DE SOLUCIÓN | ESCALADO FUNCIONAL | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | 1er ESCALAM. | 2do ESCALAM. | 3ero ESCALAM. | 4to ESCALAM. | 5to ESCALAM. |
| Habilitación y soporte de computadoras personales de escritorio y portátiles para los servidores (funcionarios) de la institución. Incluye hardware, software base, acceso a la red, Intranet, cuenta de correo electrónico interno y mensajería instantánea. (ATENCION DEL DIA A DIA) | Instalación de software adicional | 1 hora | 6 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |
| | Instalación de software base | 1 hora | 6 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |
| | Movilización / retiro de estación de trabajo | 1 hora | 12 horas laborables | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | Autoridades de la Institución |
| | Gestión de usuario | 1 hora | 6 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |
| | Respaldo de Información | 1 hora | 10 horas laborales | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |
| | Mantenimiento Preventivo | 1 hora | 3 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |

### 3.1.1.2. CORREO ELECTRÓNICO

| DESCRIPCIÓN | INCIDENCIAS | TIEMPO DE RESPUESTA A LA INCIDENCIA | TIEMPO MÁXIMO DE SOLUCIÓN | ESCALADO FUNCIONAL | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | 1er ESCALAM. | 2do ESCALAM. | 3ero ESCALAM. | 4to ESCALAM. | 5to ESCALAM. |
| Permite el envío y recepción electrónica de mensajes y documentos para facilitar el intercambio de información entre los servidores (funcionarios) a través de funcionalidades como las de compartir: agenda, libreta de direcciones, carpetas públicas, etc. | Gestión de Usuario | 30 minutos | 2 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |
| | Entrega y recepción de correo | 30 minutos | 2 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |
| | Gestión del funcionamiento del servidor | 30 minutos | 6 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | Autoridades de la Institución |

### 3.1.1.3. IMPRESIÓN Y DIGITALIZACIÓN

| DESCRIPCIÓN | INCIDENCIAS | TIEMPO DE RESPUESTA A LA INCIDENCIA | TIEMPO MÁXIMO DE SOLUCIÓN | ESCALADO FUNCIONAL | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | 1er ESCALAM. | 2do ESCALAM. | 3ero ESCALAM. | 4to ESCALAM. | 5to ESCALAM. |
| Servicio de impresión, fotocopiado, digitalización de documentos en equipos de impresión multifunción | Actualización de hardware para equipos de escritorio | 1 hora | 10 horas laborables | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | Autoridades de la Institución |
| | Asignación y/o movilización de impresora o escáner | 1 hora | 12 horas laborables | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | Autoridades de la Institución |
| | Configuración de impresora y/o escáner | 1 hora | 2 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |
| | Retiro de impresora y/o escáner | 1 hora | 2 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |
| | Cambio de suministros para impresoras/copiadoras | 1 hora | 2 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | Autoridades de la Institución |
| | Configuración De Impresión vía Wireless para laptops. | 1 hora | 2 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |
| | Asignación de IP estáticas en cada impresora | 1 hora | 2 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |
| | Asignación de claves para Impresoras auditadas | 1 hora | 2 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |

### 3.1.2. SERVICIOS POR DEMANDA

Son aquellos servicios que se prestan de forma temporal o definitiva pero que no son de libre acceso para todos los servidores de la institución.

#### 3.1.2.1. GESTIÓN DE REDES Y CONECTIVIDAD

| DESCRIPCIÓN | INCIDENCIAS | TIEMPO DE RESPUESTA A LA INCIDENCIA | TIEMPO MÁXIMO DE SOLUCIÓN | ESCALADO FUNCIONAL | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | 1er ESCALAM. | 2do ESCALAM. | 3ero ESCALAM. | 4to ESCALAM. | 5to ESCALAM. |
| Permite la conexión de computadoras personales y dispositivos en general propios de la institución o de terceros a la red interna de manera local o por medio de una conexión remota VPN desde Internet | Análisis del desempeño de equipos | 1 hora | 2 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |
| | Restricción de red a teléfonos celulares personales | 1 hora | 2 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |
| | Habilitación de conectividad inalámbrica móvil (módems) | 1 hora | 2 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | Autoridades de la Institución |
| | Requerimiento de información técnica de redes y conectividad | 1 hora | 2 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |
| | Gestión de sostenibilidad | 1 hora | 2 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | Autoridades de la Institución |
| | Inventario de Equipos de Comunicación | 1 hora | 2 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |
| | Instalación de Punto de Red | 1 hora | 2 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |

### 3.1.3. SERVICIOS PARA LA GESTIÓN DOCUMENTAL

Son servicios basados en aplicaciones que apoyan y automatizan los procesos de Gestión Documental en la que se inmiscuyen todas las Direcciones de la institución.

#### 3.1.3.1. INTRANET INSTITUCIONAL

| DESCRIPCIÓN | INCIDENCIAS | TIEMPO DE RESPUESTA A LA INCIDENCIA | TIEMPO MÁXIMO DE SOLUCIÓN | ESCALADO FUNCIONAL | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | 1er ESCALAM. | 2do ESCALAM. | 3ero ESCALAM. | 4to ESCALAM. | 5to ESCALAM. |
| Es un servicio tecnológico que está dirigido a todos los Servidores de la institución, con contenido informativo y servicios Institucionales. | Configuración de acceso a Portal Intranet | 1 hora | 2 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |
| | Carga de Procedimientos | 1 hora | 5 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |
| | Soporte técnico especializado sobre las aplicaciones | 1 hora | 6 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | Autoridades de la Institución |

### 3.1.3.2. PÁGINA WEB

| DESCRIPCIÓN | INCIDENCIAS | TIEMPO DE RESPUESTA A LA INCIDENCIA | TIEMPO MÁXIMO DE SOLUCIÓN | ESCALADO FUNCIONAL | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | 1er ESCALAM. | 2do ESCALAM. | 3ero ESCALAM. | 4to ESCALAM. | 5to ESCALAM. |
| Soporte Funcional, acerca de plugins y complementos adicionales, no incluidos en el diseño. | Instalación de Herramientas Adicionales | 1 hora | 8 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | |
| | Mantenimiento especializado sobre las aplicaciones | 1 hora | 8 horas | Coordinador del Departamento | Coordinador del Departamento de Tecnología | Analista de Tecnología | Técnicos | Autoridades de la Institución |

## 3.2. LIMITACIONES

El presente plan de gestión de incidentes tiene como finalidad agilizar los servicios que brindan los equipos informáticos de la ESPAM-MFL, así como también, permite dar soporte y verificar que estos equipos funcionen correctamente, consiguiendo gestionar de forma acertada los incidentes que ocasionan interrupción en los servicios que se brindan. El siguiente listado muestra los equipos informáticos sujetos a revisión para tal fin.

**Periféricos de entrada:**

- Teclado
- Mouse
- Scanners

**Periféricos de salida:**

- Proyector
- Monitor
- Pantalla LCD
- Impresoras

**Periféricos de almacenamiento:**

- CPU
- DVR
- Storage

**Equipos de comunicación de la red de datos:**

- Routers Inalámbricos
- Switch
- Access Point

**Equipos Fijos:**

- Portátiles
- Servidores
- Computadoras Todo en uno

**Tableros de Transferencia**

- UPS

**Sistemas de Acceso**

- Biométricos

Mediante esta clasificación, se consiguió determinar los principales incidentes que afectan a la calidad de los servicios que se brindan en la institución, logrando modelar por cada incidencia la urgencia y el impacto generado si llegara a suceder, lo cual permitió establecer prioridades de resolución de las mismas.

| Incidentes de red | URGENCIA | IMPACTO | PRIORIDAD |
|---|---|---|---|
| Fallo del servicio de comunicación (Problemas con la conexión a internet) | Crítica | Alto | **Crítica** |
| Inconvenientes con el servicio de correo electrónico de la institución | Crítica | Alto | **Crítica** |
| **Incidentes de software** | | | |
| Problemas de video (proyectores, pantallas o monitores) | Alta | Alto | **Alta** |
| Problemas al actualizar programas | Media | Alto | **Media** |
| Problemas al ejecutar programas (abren lentos o no se ejecutan) | Media | Bajo | **Baja** |
| Alerta por licenciamiento de programas | Media | Medio | **Media** |
| **Incidentes de hardware** | | | |
| Problemas por suministro de componentes a computadoras de escritorio | Alta | Medio | **Media** |
| Desperfectos de hardware (componentes internos del CPU) | Alta | Crítico | **Crítica** |
| Daños en el hardware de scanner | Baja | Bajo | **Baja** |

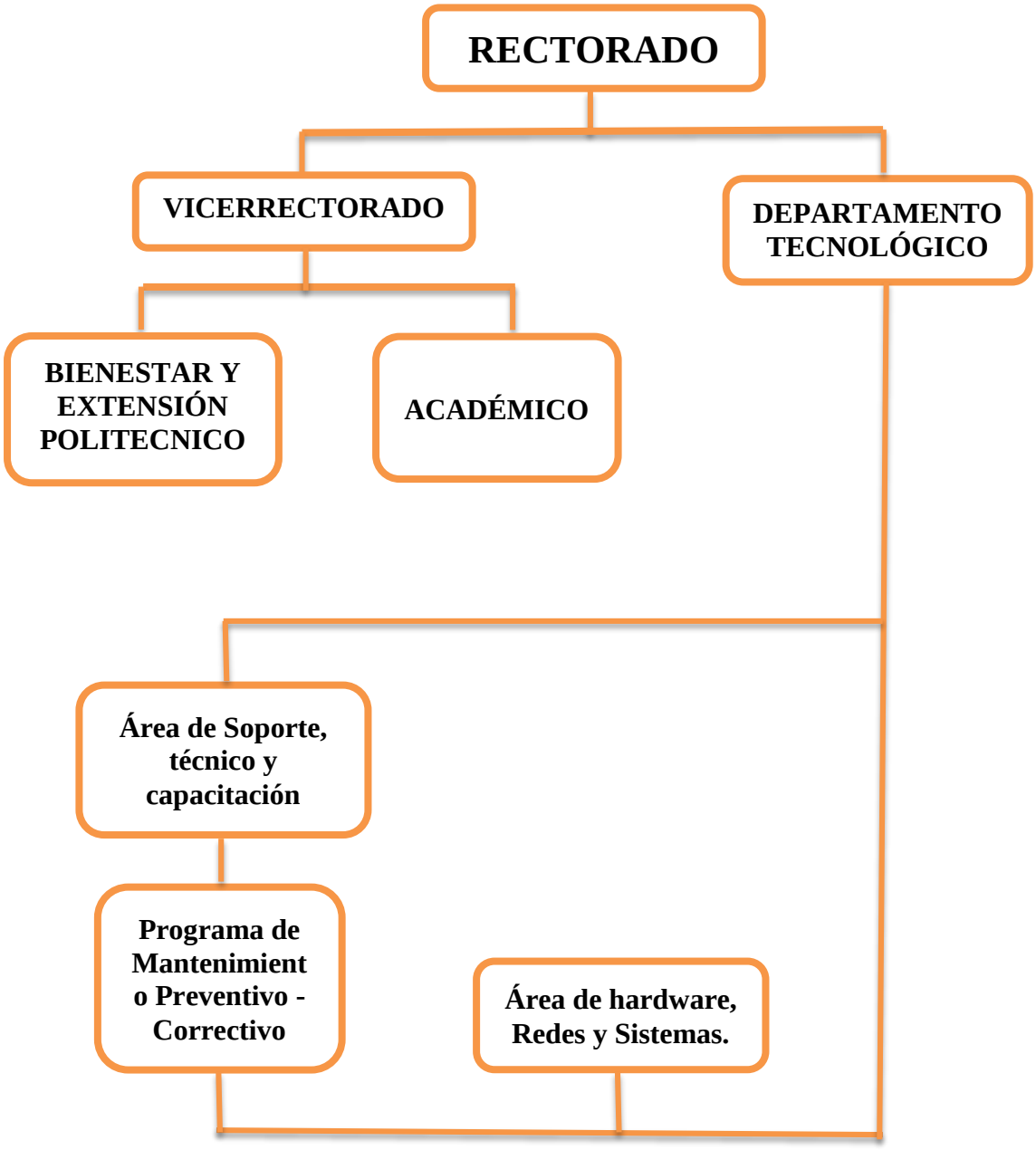
| **Incidentes de impresoras** | | | |
|---|---|---|---|
| Daños en las impresoras multifunción | Alta | Medio | **Media** |
| Problemas por cambio de suministro a los equipos de impresión | Alta | Medio | **Media** |
| **Incidentes que implican software y hardware** | **URGENCIA** | **IMPACTO** | **PRIORIDAD** |
| Reinicio constante de las computadoras | Alta | Alto | **Alta** |
| Problemas por virus en las computadoras | Alta | Alto | **Alta** |
| Falta de mantenimiento preventivo | Baja | Alto | **Media** |
| Falta de mantenimiento correctivo | Alta | Alto | **Alta** |
| Denegación del servicio (saturación del sistema informático) | Media | Medio | **Media** |
| **Incidentes de origen natural y humano (accidental o deliberado)** | | | |
| Problemas con fuego (incendios) | Alta | Crítico | **Crítica** |
| Daños en los equipos por agua (escape, fugas e inundaciones) | Alta | Crítico | **Crítica** |
| Presencia de desastres industriales (Debido a la actividad humana) | Alta | Crítico | **Crítica** |
| Corte de suministro eléctrico | Alta | Crítico | **Crítica** |
| Robo de equipos informáticos | Alta | Crítico | **Crítica** |

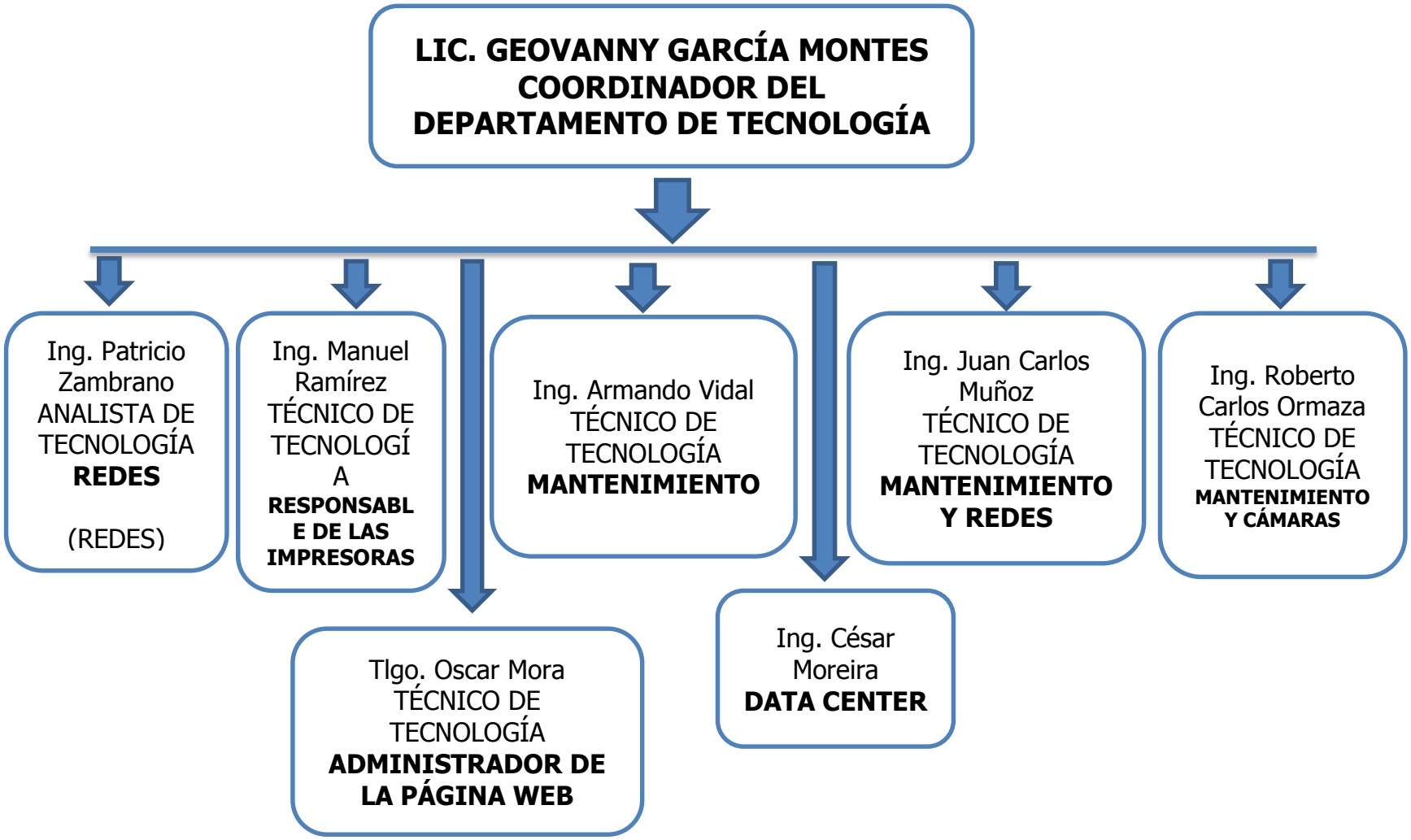
| PRIORIDAD | APLICACIÓN DEL INCIDENTE INFORMÁTICO |
|---|---|
| Crítica | **INCIDENTES DE RED**<br>❖ Fallo del servicio de comunicación (Problemas con la conexión a internet)<br>❖ Inconvenientes con el servicio de correo electrónico de la Institución.<br>**INCIDENTES DE ORIGEN NATURAL Y HUMANO (Accidental o deliberado)**<br>❖ Problemas con Fuego (Incendios)<br>❖ Daños en los equipos por agua (escape, fugas e inundaciones)<br>❖ Presencia de desastres industriales (Debido a la actividad humana)<br>❖ Corte de suministro eléctrico<br>❖ Robo de equipos informáticos<br>**INCIDENTES DE HARDWARE**<br>❖ Desperfectos de hardware (componentes internos del CPU) |
| Alta | **INCIDENTES DE SOFTWARE**<br>❖ Problemas de video (proyectores, pantallas o monitores).<br>**INCIDENTES QUE IMPLICAN SOFTWARE Y HARDWARE**<br>❖ Problemas por virus en las computadoras.<br>❖ Reinicio constante de las computadoras.<br>❖ Falta de mantenimiento correctivo. |
| Media | **INCIDENTES DE SOFTWARE**<br>❖ Problemas al actualizar programas.<br>❖ Alerta por licenciamiento de programas.<br>**INCIDENTES DE HARDWARE**<br>❖ Problemas por suministro de componentes a computadoras de escritorio.<br>**INCIDENTES DE IMPRESORAS**<br>❖ Daños en las impresoras multifunción.<br>❖ Problemas por cambio de suministro a los equipos de impresión.<br>**INCIDENTES QUE IMPLICAN SOFTWARE Y HARDWARE**<br>❖ Falta de mantenimiento preventivo.<br>❖ Denegación del servicio (saturación del sistema informático). |
| Baja | **INCIDENTES DE SOFTWARE**<br>❖ Problemas al ejecutar programas (abren lentos o no se ejecutan).<br>**INCIDENTES DE HARDWARE**<br>❖ Daños en el hardware de scanner. |

# 4. EQUIPO DE RESPUESTA A INCIDENTES Y RESPONSABILIDADES

## 4.1. EQUIPO DE RESPUESTA A INCIDENTES

Los siguientes diagramas, muestra la jerarquía de las personas vinculadas con el proceso de resolución de incidentes.




LIC. GEOVANNY GARCÍA MONTES
COORDINADOR DEL
DEPARTAMENTO DE TECNOLOGÍA
Ing. Patricio Zambrano
ANALISTA DE TECNOLOGÍA
REDES
(REDES)
Ing. Manuel Ramírez
TÉCNICO DE TECNOLOGÍA
RESPONSABLE DE LAS IMPRESORAS
Tlgo. Oscar Mora
TÉCNICO DE TECNOLOGÍA
ADMINISTRADOR DE LA PÁGINA WEB
Ing. Armando Vidal
TÉCNICO DE TECNOLOGÍA
MANTENIMIENTO
Ing. César Moreira
DATA CENTER
Ing. Juan Carlos Muñoz
TÉCNICO DE TECNOLOGÍA
MANTENIMIENTO Y REDES
Ing. Roberto Carlos Ormaza
TÉCNICO DE TECNOLOGÍA
MANTENIMIENTO Y CÁMARAS

## 4.2. RESPONSABILIDADES

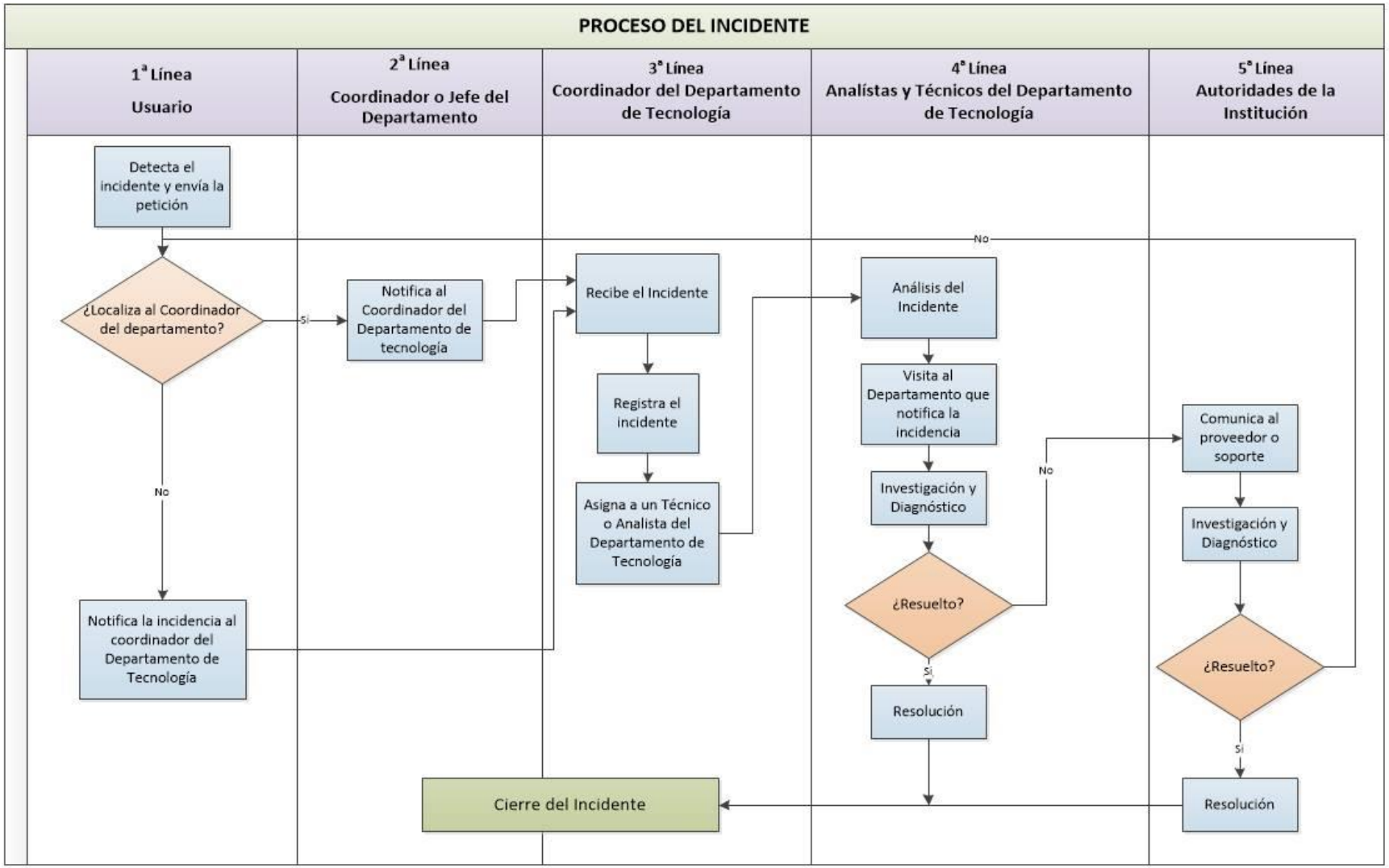
El Coordinador del Departamento de Tecnología es responsable de:

- Habilitar los recursos necesarios que permitan gestionar los incidentes informáticos de forma apropiada, asignando el recurso responsable para dar solución a cada una de las incidencias.
- Transmitir el presente plan de gestión a todos los miembros del departamento de tecnología independientemente de la función que desempeñe.
- Asegurar el mantenimiento tanto preventivo, como correctivo, de los equipos informáticos en cada uno de los departamentos de la ESPAM – MFL.
- Administrar y cerciorar la disponibilidad de las redes, comunicación, servidores y estaciones de trabajo.
- Instalar aplicaciones desarrolladas por el servicio a todo equipo nuevo o reparado.
- Recepción de fallas de hardware en servidores, PC e impresoras.

Todo el personal del Departamento de Tecnología es responsable de:

- Implementar el presente Plan de Gestión de incidentes independientemente del cargo que desempeñe.
- Registrar las incidencias informáticas que se presenten siguiendo los procedimientos establecidos para tal fin.

# 5. PASOS DEL PROCESO DE NOTIFICACIÓN



# 6. MEDIDAS DE EVALUACIÓN DE DAÑOS

La estimación de emergencia a un incidente, se realizará mediante una evaluación al mismo, siendo concretos y adoptando las acciones necesarias dependiendo del equipo informático que se vea afectado, permitiendo determinar cuáles de estas tuvieron éxito y cuáles fracasaron, a fin de mejorar la respuesta a incidentes futuros.

Inmediatamente después que el siniestro ha concluido, se deberá evaluar la magnitud del daño, los sistemas afectados, que equipos han quedado no operativos, cuales se pueden recuperar, y en qué tiempo.

Para la evaluación de los daños, se realizarán las preguntas o indagaciones necesarias al equipo encargado de la vigilancia o supervisión del área en donde se produjo el siniestro. El objetivo de establecer esta evaluación es que los encargados de cada área puedan reconocer el tipo de desastre que se produjo, sea este en el ámbito físico o lógico.

Si se tratase de un desastre en el ámbito lógico se deben verificar los siguientes puntos:

- La calidad e integridad de la información de respaldo.
- En lo posible volver al estado original de la información antes del desastre.

Si se tratase de un desastre en el ámbito físico se deben verificar los siguientes puntos:

- Por una Suspensión o caída del suministro eléctrico, el estado del hardware (Equipos de cómputo, Equipos de telecomunicaciones, entre otros).

Si se tratara de siniestros de fuerza mayor como: incendios, inundaciones, maremotos, tornados, robo a la institución; se deben seguir los lineamientos para desastres de gran magnitud.

## 6.1. RESPUESTA DE POST-ACCIONES

El Director del departamento Tecnológico en conjunto con las autoridades de la institución son los responsables de los organismos de apoyo intervinientes en la emergencia, de un informe de Post-Acciones para documentar el incidente y las acciones a desarrollar.

# 7. PROCESO DE DECLARACIÓN DE INCIDENCIAS

El presente manual, permite gestionar la movilización, el uso eficiente y eficaz de los recursos necesarios para cumplir con las operaciones de emergencia, incluyendo la respuesta a inconvenientes que se presentan en la vida diaria.

En la gestión de cada incidente o evento existe un conjunto de acciones o funciones, de carácter principal. El proceso que se debe tomar en cuenta para la resolución de los incidentes informáticos es el siguiente:

1. Registro del incidente.- Permite detallar el departamento en que sucede el incidente, la fecha, hora y el personal encargado de dar solución al mismo **(Anexo 1).**

2. Clasificación.- Es necesario realizar la respectiva categorización de los incidentes para determinar su prioridad en función de la urgencia y el impacto que tendría en la organización.

3. Diagnóstico y resolución.- Mediante la respectiva evaluación del incidente y tomando en cuenta el nivel de prioridad correspondiente, se continua con la asignación de la persona encargada de resolver el mismo.

4. Cierre del incidente.- Luego que el técnico visita el departamento y soluciona el inconveniente notificado, se procede a realizar el informe del mismo en una bitácora de incidentes.

# 8. PROCESO DE ESCALAMIENTO

| NIVEL DE LLAMADO | CRITERIO DE CLASIFICACIÓN |
|---|---|
| **Primer Nivel** | **COORDINADOR O JEFE DEL DEPARTAMENTO** |
| **Segundo Nivel** | **COORDINADOR DEL DEPARTAMENTO DE TECNOLOGÍA**<br>Lic. Geovanny García Montes |
| **Tercer Nivel** | **ANALISTAS DE TECNOLOGIA**<br>Ing. Patricio Zambrano |
| **Cuarto Nivel** | **TÉCNICOS DEL DEPARTAMENTO DE TECNOLOGÍA**<br>Ing. Manuel Ramírez<br>Ing. Armando Vidal<br>Ing. Juan Carlos Muñoz<br>Ing. Roberto Ormaza<br>Ing. Oscar Mora<br>Ing. Cesar Moreira |
| **Quinto Nivel** | **AUTORIDADES DE LA INSTITUCIÓN**<br>Econ. Miriam Félix López **RECTORA DE LA ESPAM**<br>Ing. Lorena Carreño **VICERECTORA ACADEMICA DE LA ESPAM**<br>Lcda. Maryuri Zamora **VICERECTORA DE BIENESTAR POLITECNICO** |

# 9. DECISIÓN DE PONER EN MARCHA ACTIVIDADES DE EMERGENCIA ADICIONALES

Para resolver un incidente y tomar las medidas adecuadas después de un desastre (sea natural o provocado por el hombre) que afecte directamente los servicios que brindan los equipos informáticos, se deben tomar en cuenta las amenazas dependiendo del medio donde se encuentra ubicada la institución.

Para tal efecto, se muestra un listado de amenazas que afectan a los equipos informáticos según lo establece la Metodología de Análisis y Gestión de Riesgos (MAGERIT – Versión 3), en su Catálogo de elementos.

## 9.1. LISTADO DE AMENAZAS

### 9.1.1. DESASTRES NATURALES (N)

**N.1** FUEGO (Incendios).

**N.2** DAÑOS POR AGUA (Inundaciones).

**N*** DESASTRES NATURALES (Otros incidentes que se producen sin intervención humana).

### 9.1.2. DE ORIGEN INDUSTRIAL (I)

**I.1** FUEGO (Incendios).

**I.2** DAÑOS POR AGUA (Escape, fugas, inundaciones).

**I*** DESASTRES INDUSTRIALES (Otros desastres debido a la actividad humana).

**I.3** CONTAMINACIÓN MECÁNICA (Vibraciones, polvo, suciedad).

**I.4** CONTAMINACIÓN ELECTROMAGNÉTICA (interferencias de radios, campos magnéticos, luz ultravioleta,…)

**I.5** AVERÍA DE ORIGEN FÍSICO O LÓGICO (Fallos en los equipos o fallos en los programas).

**I.6** CORTE DE SUMINISTRO ELÉCTRICO (Cese de la alimentación de potencia).

**I.7** CONDICIONES INADECUADAS DE TEMPERATURA O HUMEDAD (Climatización).

**I.8** FALLO DE SERVÍCIOS DE COMUNICACIONES (Destrucción o detención física).

**I.11** EMANACIONES ELECTROMAGNÉTICAS (Fuga de información).

### 9.1.3. ERRORES Y FALLOS NO INTENCIONADOS (E)

**E.2** ERRORES DEL ADMINISTRADOR.

**E.9** ERRORES DE [RE-] ENCAMINAMIENTO (Ruta incorrecta de envío).

**E.23** ERRORES DE MANTENIMIENTO/ ACTUALIZACIÓN DE EQUIPOS HARDWARE.

**E.24** CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS.

**E.25** PÉRDIDA DE EQUIPOS.

### 9.1.4. ATAQUES INTENCIONADOS (A)

**A.5** SUPLANTACIÓN DE LA IDENTIDAD DEL USUARIO.

**A.6** ABUSO DE PRIVILEGIOS DE ACCESO.

**A.7** USO NO PREVISTO.

**A.11** ACCESO NO AUTORIZADO.

**A.12** ANÁLISIS DE TRÁFICO (Monitorización de tráfico).

**A.23** MANIPULACIÓN DE LOS EQUIPOS (Alteración intencionada del funcionamiento de los programas).

**A.24** DENEGACIÓN DE SERVICIO (Saturación del sistema informático).

**A.25** ROBO.

**A.26** ATAQUE DESTRUCTIVO.

## 9.2. CONSEJOS PARA EVITAR AMENAZAS QUE AFECTEN A LOS EQUIPOS INFORMATICOS.

Para cada una de las amenazas presentadas anteriormente, como medida de respuesta para su posterior solución se presentan las siguientes sugerencias:

- Ubicar y revisar periódicamente, que se encuentren en buen estado las instalaciones de agua, y sistema eléctrico.
- Evitar colocar cada uno de los equipos en espacios donde se pueda filtrar agua.
- No se deben realizar demasiadas conexiones en contactos múltiples, para evitar la sobre carga de los circuitos eléctricos.
- Procurar que las conexiones eléctricas estén en buen estado.
- Tener en un lugar visible y accesible un extintor contra incendios.
- Tener una climatización adecuada en el lugar donde se encuentran cada uno de los equipos informáticos.
- Realizar e implementar una política de respaldo de la información que se maneje en cada uno de los departamentos, para evitar pérdidas en caso que se dañen los equipos.
- Actualizar constantemente las aplicaciones.
- Tener mayor vigilancia en los laboratorios e instalaciones en donde se maneje información confidencial, evitando la fuga de datos y robo intencionado de equipos informáticos.
- Al entrar y salir de las instalaciones se deberá observar previamente de que no exista ningún individuo sospechoso.
- Queda prohibido dar información personal de los empleados o información confidencial de la institución.
- Se deberá realizar una señalización o etiquetado de los Computadores de acuerdo a la importancia de su contenido, para ser priorizados en caso de evacuación.

- Los servidores de archivos no deben ser accesible físicamente a cualquier persona.
- Es conveniente que exista un espacio físico donde se ubiquen los servidores, con acceso restringido al personal autorizado, y que cumpla con los requisitos adecuados para su funcionamiento, como temperatura ambiental adecuada, aislado del polvo y plagas dañinas.
- Habilitar un sistema que evite ingresos desde redes internas y externas.

.

# 10. REVISIÓN DEL PLAN Y MEJORA CONTINUA

Las actividades que se exponen en el plan de gestión de incidentes informáticos deben actualizarse anualmente, debido a nuevas incidencias que se puedan presentar y que afecten directamente a los equipos, consiguiendo así adoptar las medidas de seguridad necesarias para proteger los equipos informáticos y que permitan brindar un mejor servicio a la institución. Además, las autoridades de la ESPAM - MFL en conjunto con el coordinador y los miembros del departamento de tecnología deben cumplir con lo establecido en este plan, el cual debe estar sujeto a constante revisión.

| | |
|---|---|
| Econ. Miriam Félix López<br>**RECTORA DE LA ESPAM – MFL** | Lic. Geovanny García Montes<br>**COORDINADOR DEL DEPARTAMENTO DE TECNOLOGÍA** |

# ANEXOS

## ANEXO 1. FICHA DE REGISTRO DE INCIDENCIAS INFORMÁTICAS

**ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ**

**REGISTRO DE INCIDENCIAS INFORMÁTICAS**

| № DE INCIDENCIA | NOMBRE DEL DEPARTAMENTO | FECHA DE REGISTRO | HORA DE REGISTRO | TIPO DE INCIDENCIA | DESCRIPCIÓN | TÉCNICO ENCARGADO | FECHA DE SOLUCIÓN | HORA DE SOLUCION | FIRMA DEL COORDINADOR DEL DEPARTAMENTO |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

**ANEXO 7**
**CERTIFICADO DEL TUTOR**

Calceta, 07 de Julio de 2015

Ingeniero
Daniel Mera Martínez
**PRESIDENTE DEL TRIBUNAL DE TESIS DE HARDWARE**

En su despacho.-

De mi consideración:

Por medio del presente me dirijo a usted, deseándole el mayor de los éxitos en cada una de sus labores diarias, y a la vez exponerle que he revisado y corregido la tesis y el artículo científico titulado: **"PLAN DE GESTIÓN DE INCIDENTES QUE AFECTAN A LOS EQUIPOS INFORMÁTICOS DE LA ESPAM MFL"** de las postulantes Cuzme Romero María Gabriela y Pinargote Anchundia Roxanna Elizabeth.

Para los fines pertinentes y sin otro particular, me suscribo.

Atentamente

Ing. Sergio Intriago Briones

**ANEXO 8**
**CERTIFICACIÓN DEL CENTRO DE IDIOMAS**

**ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ**
**MANUEL FÉLIX LÓPEZ**

REPÚBLICA DEL ECUADOR

CENTRO DE IDIOMAS

## CENTRO DE IDIOMAS

Calceta, 17 de julio de 2015

OFICIO 235 - 15

Ing. Jessica Morales

**DIRECTORA DE LA CARRERA DE INFORMATICA**

De mi consideración:

Certifico la revisión del abstract cuyo tema es **PLAN DE GESTIÓN DE INCIDENTES QUE AFECTAN A LOS EQUIPOS INFORMÁTICOS DE LA ESPAM MFL** , que ha sido propuesto, desarrollado y planteado por las estudiantes: MARÍA GABRIELA CUZME ROMERO y ROXANNA ELIZABETH PINARGOTE ANCHUNDIA.


**ABSTRACT**

The Plan for the incidents management that affect the computing equipment at ESPAM-MFL, allowed to analyze incidents and establish procedures to mitigate the impact caused by disruptions of services that the computer equipment provide, for this, the Incidents Management of the ITIL methodology was used, which divides the incident management into four phases: registration, it included the determination of the computing equipment, in which the risks that each of the teams are exposed were identified and classified, by proceeding to perform the respective evaluation, forming judgments of probability, occurrence and impact, according to what it is established in the MAGERIT (version 3.0) methodology, and it concluded with the registration of computing incidents; the classification phase allowed to set levels of priority for each incident according to the urgency and impact criterion; through the stages of diagnosis and resolution, service agreements between the staff responsible for IT and the teams responsible for each department and career ESPAM-MFL, were carried out. Based on the results obtained through the Plan for Incidents Management, the impact of such events was limited by the assignment of responsibility for managing team, a situation that is checked with the service agreements made, therefore, it is concluded that when response procedures to incidents are run, it can contain and mitigate them, for this reason, it is appropriate to adopt effective security measures to protect the information assets of the institution.


KEY WORDS: Management, Management Plan, IT incidents, ITIL

REVISADO POR

LUIS ALBERTO ORTEGA ARCIA

COORDINADOR CENTRO DE IDIOMAS

**Dirección:** Campus Politécnico "El Limón". **Teléfono:** (05)3023903
**Email:** languagecenterespam@hotmail.com
**CALCETA - ECUADOR**