



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

DIRECCIÓN DE POSGRADO Y FORMACIÓN CONTINUA

INFORME DE TRABAJO DE TITULACIÓN

**PREVIA LA OBTENCIÓN DEL TÍTULO DE MAGISTER
EN TECNOLOGÍAS DE LA INFORMACIÓN MENCIÓN
REDES Y SISTEMAS DISTRIBUIDOS**

MODALIDAD:

PROYECTO DE INVESTIGACIÓN Y DESARROLLO

TEMA:

**ANÁLISIS DE CIBERSEGURIDAD EN LA ESPAM MFL,
UTILIZANDO LAS METODOLOGÍAS AMFE Y MARISMA**

AUTORES:

**ING. KARINA LISBETH CEDEÑO SANTANA
ING. GINA ELIZABETH LOOR VALENCIA**

TUTORA:

ING. JESSICA MORALES CARRILLO, Mgtr.

CALCETA, AGOSTO 2020

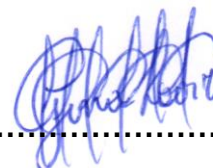
DERECHOS DE AUTORÍA

KARINA LISBETH CEDEÑO SANTANA y GINA ELIZABETH LOOR VALENCIA, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría, que no ha sido previamente presentado para ningún grado o calificación profesional, que se han respetado los derechos de autor de terceros, por lo que asumimos la responsabilidad sobre el contenido del mismo, así como ante la reclamación de terceros, conforme a los artículos 4, 5 y 6 de la Ley de Propiedad Intelectual.

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 en el artículo 46 de la Ley de Propiedad Intelectual y su Reglamento.



.....
ING. KARINA L. CEDEÑO SANTANA



.....
ING. GINA E. LOOR VALENCIA

CERTIFICACIÓN DE LA TUTORA

ING. JESSICA MORALES CARRILLO, Mgtr. certifica haber tutelado el trabajo de titulación **ANÁLISIS DE CIBERSEGURIDAD EN LA ESPAM MFL, UTILIZANDO LAS METODOLOGÍAS AMFE Y MARISMA**, que ha sido desarrollada por **KARINA LISBETH CEDEÑO SANTANA Y GINA ELIZABETH LOOR VALENCIA**, previo a la obtención del título de Magister en Tecnologías de la Información mención Redes y Sistemas Distribuidos, de acuerdo al Reglamento de unidad de Titulación de Posgrado de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López.



.....
ING. JESSICA J. MORALES CARRILLO, Mgtr.

APROBACIÓN DEL TRIBUNAL

Los suscritos integrantes del tribunal correspondiente, declaramos que hemos **APROBADO** el trabajo de titulación **ANÁLISIS DE CIBERSEGURIDAD EN LA ESPAM MFL, UTILIZANDO LAS METODOLOGÍAS AMFE Y MARISMA**, que ha sido propuesto, desarrollado y sustentado por **KARINA LISBETH CEDEÑO SANTANA y GINA ELIZABETH LOOR VALENCIA**, previa la obtención del título de Magíster en Tecnologías de la Información mención Redes y Sistemas Distribuidos, de acuerdo al Reglamento de unidad de Titulación de Posgrado de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López.



Firmado electrónicamente por:
JORGE ANTONIO
PÁRRAGA ÁLAVA

ING. JORGE PÁRRAGA ÁLAVA, PhD.
MIEMBRO

ING. JORGE HERRERA TAPIA, PhD.
MIEMBRO

ING. LUIS CEDEÑO VALAREZO, Mgtr.
PRESIDENTE

AGRADECIMIENTO

A la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, por ser el alma mater, permitiéndonos formarnos en sus aulas;

A los docentes que en cada uno de los módulos demostraron su compromiso hacia el estudiantado, ayudándonos a ser mejores personas y profesionales compartiendo sus vivencias y enseñanzas, ganándose nuestro cariño y respeto;

A nuestros compañeros y amigos con los cuales compartimos anhelos e ilusiones, alcanzándolos con constancia, dedicación y esfuerzo, demostrando que la unión hace la fuerza, ayudándonos los unos a los otros sin malicias, los recordaremos por siempre.

A nuestra tutora la Ing. Jessica Morales Carrillo, gracias por ser la mejor guía que un estudiante puede tener, sembrando el conocimiento en nosotras y el deseo de investigación, por su paciencia y compromiso que nos dio en toda esta etapa de desarrollo de tesis que fueron la base fundamental para poder concluirla con éxito.

LAS AUTORAS

DEDICATORIA

Este trabajo de titulación va dedicado en primer lugar a Dios, y a todas las personas que nos ayudaron a seguir y no desmayar en estos dos años de estudios hasta cumplir con nuestros objetivos.

A nuestros padres, hijos, hermanos, sobrinos, abuelos, tíos, que de una a otra manera fueron parte de este proceso de formación, brindándonos su apoyo y así podernos formar con buenos hábitos y valores, lo cual nos ayudó a seguir adelante en los momentos más difíciles.

A nuestra guía de este proceso Ing. Jessica Morales, sin su apoyo no hubiéramos salido adelante, Ud. posó su confianza en nosotras, permitiéndonos ser parte de sus tutelados.

LAS AUTORAS

CONTENIDO GENERAL

CARÁTULA.....	i
DERECHOS DE AUTORÍA.....	ii
CERTIFICACIÓN DE LA TUTORA	iii
APROBACIÓN DEL TRIBUNAL.....	iv
AGRADECIMIENTO	v
DEDICATORIA	vi
CONTENIDO GENERAL.....	vii
ÍNDICE DE TABLAS Y FIGURAS	ix
RESUMEN.....	x
ABSTRACT.....	xi
CAPÍTULO I. ANTECEDENTES	1
1.1. PLANTEAMIENTO Y FORMULACIÓN DEL PROBLEMA.....	1
1.2. JUSTIFICACIÓN	3
1.3. OBJETIVOS	4
1.3.1. OBJETIVO GENERAL.....	4
1.3.2. OBJETIVOS ESPECÍFICOS.....	4
1.4. HIPÓTESIS, PREMISAS Y/O IDEAS A DEFENDER.....	4
CAPITULO II. REVISIÓN BIBLIOGRÁFICA.....	5
2.1 ESTUDIOS BASADOS EN RIESGOS DE CIBERSEGURIDAD	5
2.1.1 REGISTRO DE INFORMACIÓN DE INSTITUCIONES Y MÉTODOS EMPLEADOS	6
2.1.2 HERRAMIENTAS Y TECNOLOGÍAS DE ANÁLISIS Y DETECCIÓN DE RIESGOS	10
CAPÍTULO III. DESARROLLO METODOLÓGICO.....	14
3.1. FASE 1: IDENTIFICACIÓN DE VARIABLES PARA EL ANÁLISIS EN CIBERSEGURIDAD EN EL ÁREA DE SEGURIDAD DE LA INFORMACIÓN .	14
3.2. FASE 2: DETERMINACIÓN DE LOS CONTROLES A UTILIZAR EN CIBERSEGURIDAD CON LA METODOLOGÍA MARISMA	15
3.3. FASE 3: IMPLEMENTACIÓN DEL PLAN DE GESTIÓN DE RIESGOS EN BASE A LAS METODOLOGÍAS AMFE Y MARISMA.....	16

•	GENERACIÓN DE PATRONES PARA EL ANÁLISIS DE RIESGOS (GPRA)17	
•	GENERACIÓN DEL ANÁLISIS Y GESTIÓN DEL RIESGO (GARM)..	18
•	EVENTOS SEGURIDAD (DRM).....	18
3.4.	FASE 4: ANÁLISIS DE LOS PARÁMETROS OBTENIDOS CON AMBAS METODOLOGÍAS.....	19
	CAPÍTULO IV. RESULTADOS Y DISCUSIÓN.....	20
4.1.	RESULTADOS.....	20
4.1.1.	FASE 1: IDENTIFICACIÓN DE VARIABLES A CONSIDERAR EN EL ANÁLISIS EN CIBERSEGURIDAD EN EL ÁREA DE SEGURIDAD DE LA INFORMACIÓN.....	20
4.1.2.	FASE 2: DETERMINACIÓN DE LOS CONTROLES A UTILIZAR EN CIBERSEGURIDAD CON LA METODOLOGÍA MARISMA.....	20
4.1.3.	FASE 3: IMPLEMENTACIÓN DEL PLAN DE GESTIÓN DE RIESGOS EN BASE A LAS METODOLOGÍAS AMFE Y MARISMA.....	21
4.1.3.1.	GENERACIÓN DE PATRONES PARA EL ANÁLISIS DE RIESGOS .	22
4.1.3.2.	GENERACIÓN DEL ANÁLISIS Y GESTIÓN DEL RIESGO.....	22
4.1.3.3.	MANTENIMIENTO DINÁMICO DEL ANÁLISIS DE RIESGOS.....	24
4.1.4.	FASE 4: ANÁLISIS DE LOS PARÁMETROS OBTENIDOS CON AMBAS METODOLOGÍAS.....	25
4.2.	DISCUSIÓN.....	26
	CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES.....	29
5.1.	CONCLUSIONES.....	29
5.2.	RECOMENDACIONES.....	30
	BIBLIOGRAFÍA.....	31
	ANEXOS.....	36

ÍNDICE DE TABLAS Y FIGURAS

TABLAS

Tabla 1. 1. Tabla de resumen de la revisión bibliográfica	7
--	---

FIGURAS

Figura 3. 1. Elementos que componen la herramienta eMarisma y las relaciones.	17
Figura 3. 2. Esquematzación de la estructura de análisis de riesgo.....	18
Figura 4. 3. Cantidad de vulnerabilidades según los patrones de ciberseguridad de acuerdo a las gestiones y dimensiones empleadas en eMarisma.	22
Figura 4. 4. Porcentaje de niveles, impacto y probabilidad generados según las vulnerabilidades de los sistemas de información de la ESPAM MFL de acuerdo a la metodología AMFE.....	23
Figura 4. 5. Porcentaje de probabilidades de ocurrencia y degradación generadas según las vulnerabilidades de los sistemas de información de la ESPAM MFL de acuerdo a la metodología MARISMA.	23
Figura 4. 6. Sondeos por IP, aplicados en eMarisma de acuerdo a las IP de los sistemas de información de la ESPAM MFL.....	24
Figura 4. 7. Cuadro de Mando general de acuerdo a la auditoria de los controles, dominios y objetivos de cada patrón ingresado en eMarisma correspondiente a ciberseguridad dentro de la ESPAM MFL.	24

RESUMEN

El presente trabajo de titulación tuvo como propósito el desarrollo de un Análisis de ciberseguridad en la ESPAM MFL, para evaluar los riesgos encontrados en el área de seguridad de la información mediante el uso de las metodologías AMFE y MARISMA. Para cumplir con la ejecución, fue necesario emplear los métodos: bibliográfico, investigativo-exploratorio y analítico. A través del método bibliográfico se definió la fundamentación de ambas metodologías y la aplicabilidad; con el método investigativo-exploratorio se obtuvo una visión general, que permitió estudiar los riesgos, posteriormente para aplicarlos en el analítico, mediante la implementación de la herramienta *eMarisma*, del cual se identificaron los patrones de seguridad de la información, aplicación y redes, además de los controles empleados en ambas metodologías, y por lo consiguiente el plan de gestión de riesgos de ciberseguridad permitiendo parametrizar criterios de mitigación en base a los resultados obtenidos del mantenimiento dinámico a partir de las vulnerabilidades encontradas en AMFE, en el cual se vincularon aspectos importantes de la norma ISO 27032, 25001 y otras normativas que garantizaron el sustento de los procesos de mitigación de riesgos. El procedimiento antes indicado permitió establecer que en dichos patrones la metodología Marisma es eficiente por el recálculo de datos de activos por amenazas, análisis de riesgo y el plan de tratamiento para llevar a cabo una adecuada gestión del control, análisis de los riesgos de vulnerabilidades y amenazas suscitadas en los sistemas de información, mientras que AMFE brinda una valoración estática de dichos riesgos en ciberseguridad.

PALABRAS CLAVE

Ciberseguridad, ESPAM MFL, gestión de riesgos, AMFE, MARISMA

ABSTRACT

The present work was to develop a Cybersecurity Analysis at ESPAM MFL, to assess the risks found in the area of information security through the use of AMFE and MARISMA methodologies. To comply with the execution, it was necessary to use the methods: bibliographic, investigative-exploratory and analytical. Through the bibliographic method, the foundation of both methodologies and applicability were defined; with the investigative-exploratory method, an overview was obtained, which allowed studying the risks, later to apply them in the analytical one, through the implementation of the eMarisma tool, from which the information, application and network security patterns were identified, in addition of the controls used in both methodologies, and therefore the cybersecurity risk management plan, allowing parameterization of mitigation criteria based on the results obtained from dynamic maintenance based on the vulnerabilities found in AMFE, in which important aspects were linked of ISO 27032, 25001 and other regulations that guaranteed the support of risk mitigation processes. The aforementioned procedure established that in these patterns the Marisma methodology is efficient by recalculating asset data for threats, risk analysis and the treatment plan to carry out adequate control management, vulnerability risk analysis and threats raised in information systems, while AMFE provides a static assessment of these risks in cybersecurity.

KEYWORDS

Cybersecurity, ESPAM MFL, risk management, AMFE, MARISMA.

CAPÍTULO I. ANTECEDENTES

1.1. PLANTEAMIENTO Y FORMULACIÓN DEL PROBLEMA

El mundo cada vez debe adaptarse a nuevas formas de vida y de convivencia, así mismo las empresas a la tecnología, teniendo sus sistemas de información digitalizados, otorgando un fácil acceso, ayudando a mantener la información y sus servicios que ofrecen organizados y disponibles en cualquier momento y lugar, permitiendo una mejor comunicación a nivel empresarial, con los clientes y con demás empresas, utilizando incluso las redes sociales como método de marketing y publicidad de sus productos y servicios (Mena, 2012).

Los sistemas de información modifican profundamente la manera en que una empresa, una industria, un negocio deba ajustarse al impacto digitalizado y los nuevos flujos de información, basados en red de computadoras, son indispensables para realizar las actividades planificadas en cualquier organización (Hamidian-Fernández & Ospino-Sumoza, 2015).

El fácil acceso a la información ofrece oportunidades de negocio, en el comercio electrónico a escala global y prestando servicios en línea; esto ayuda a disminuir costos en comunicación de datos, siendo la internet el medio por el cual ofrece a los usuarios acceder a los recursos y servicios, aumentando las oportunidades de trabajo a distancia; generando riesgos, volviendo vulnerable la información de las organizaciones; viéndose en la necesidad, de implementar técnicas de defensa y análisis de riesgo en ciberseguridad de los activos, para mitigar ataques a la seguridad de la información, que disipen la confidencialidad, integridad de los mismos, causando un impacto negativo en la utilización de los sistemas de información en línea como medio principal de transmisión (Murillo, 2009).

El análisis precedente da a comprender que no solo las compañías grandes o de comercialización, son las únicas que sufren problemas con los sistemas de información; dicho que el tratamiento en ciberseguridad y los riesgo que conlleva estos ataques, también afectan a las instituciones educativas, porque manejan información importante en sus bases de datos, teniendo la obligación de crear mecanismos que aporten a la seguridad de los datos, pero esto no es solo firewall

y software, sino metodología que permitan un análisis de riesgo sistemático, teniendo definidos protocolos de seguridad para determinados eventos, permitiendo dar una respuesta rápida frente a una amenaza, ya que el mal uso y la mala gestión de los riesgos en ciberseguridad, causaría la disminución en la productividad de cualquier organización (Santos *et al.*, 2012) (Kluge & Sambasivam, 2008).

De modo que las metodologías para el análisis de riesgos en las empresas que van de la mano con normas que se determinan por el alcance de la gestión que se realiza, por la línea de negocios o por sus procesos, permitirá generar argumentos sólidos para identificar cuál es la metodología de análisis de riesgos que proporciona una mejor oportunidad de toma de decisiones dentro de una organización que por sus funciones y responsabilidades ayudan a dar cumplimiento con el desempeño de la organización frente a la custodia de la información (Tejena, 2018).

Teniendo en cuenta que en la ESPAM MFL, se empleó en el año 2019, un plan de acción de Ciberseguridad para el departamento de tecnología, que fue propuesto en base a la metodología AMFE y la norma ISO 27032, de acuerdo a los datos obtenidos de las vulnerabilidades de los sistemas distribuidos de aquel entonces, se obtuvo como resultado que la ESPAM MFL arrojaba un promedio de 29% del 100%, en comparación al estudio realizado con las demás Instituciones Públicas de Educación Superior de Manabí, siendo la segunda mayor puntuada; con la necesidad de implementar dicho plan para futuros procesos a ser empleados. Por lo tanto se observó la situación de analizar dicha información con respecto a la gestión de riesgo, para evaluar el cumplimiento frente a una metodología que proporcione una herramienta integral y sistemática, como lo es Marisma.

Por las circunstancias presentadas las autoras del presente trabajo de titulación se plantean la siguiente interrogante:

¿Cómo analizar el impacto de los riesgos en ciberseguridad de la ESPAM MFL?

1.2. JUSTIFICACIÓN

La Ley del Sistema Nacional de Registro de Datos Públicos en el artículo 4 responsabilidad de la información, establece que las instituciones del sector público y privado, y las personas naturales que actualmente o en el futuro administren bases o registros de datos públicos, son responsables de la integridad, protección y control de los registros y bases de datos a su cargo; dichas instituciones responderán por la veracidad, autenticidad, custodia y debida conservación de los registros (Ley del Sistema Nacional de Registro de Datos Públicos, 2018).

La ESPAM MFL, mediante el modelo de Evaluación Institucional de Universidades y Escuelas Politécnicas del Ecuador 2018, presentado por el Consejo de aseguramiento de la calidad de la Educación Superior (CACES), en su criterio 5: Recursos e infraestructura, subcriterio 5.1. Infraestructura, Ítem 5.1.3. Sistemas informáticos, considera que las Instituciones de Educación Superior, apliquen políticas y protocolos de seguridad y gestión de la información, que garantizan la confiabilidad y la confidencialidad de la información.

Por esta razón, se ve la necesidad de implementar una metodología que considere analizar los riesgos en seguridad de tecnologías de la información, que incorpore dentro de la misma una herramienta que proporcione una gestión de los riesgos y vulnerabilidades encontradas, mitigando el impacto, como lo proporciona MARISMA, siendo un mecanismo que permite que los eventos e incidencias que afectan, realimenten el sistema para determinar una buena gestión de las vulnerabilidades en ciberseguridad.

1.3. OBJETIVOS

1.3.1.OBJETIVO GENERAL

Realizar un análisis utilizando las metodologías AMFE y MARISMA, para gestionar y concretar soluciones a los riesgos encontrados en ciberseguridad en la ESPAM MFL.

1.3.2.OBJETIVOS ESPECÍFICOS

- Identificar las variables en el análisis de ciberseguridad de acuerdo a la información obtenida de la metodología AMFE.
- Determinar los controles a utilizar en ciberseguridad mediante la metodología MARISMA.
- Implementar el plan de gestión del riesgo según los datos proporcionados por la metodología MARISMA.
- Analizar los resultados obtenidos con ambas metodologías.

1.4. HIPÓTESIS, PREMISAS Y/O IDEAS A DEFENDER

Mediante un análisis de ciberseguridad empleando las metodologías AMFE y MARISMA, se puede aplicar estrategias de mitigación comprendidas en gestión de riesgos de las vulnerabilidades encontradas en la ESPAM MFL.

CAPITULO II. REVISIÓN BIBLIOGRÁFICA

2.1 ESTUDIOS BASADOS EN RIESGOS DE CIBERSEGURIDAD

Se realizó la investigación bibliográfica en repositorios y revistas científicas, identificando varios documentos referentes al tema planteado, además documentos que contenían información sobre la metodología AMFE y MARISMA; este proceso de revisión sistemática de literatura, garantizó que el trabajo sea representativo, mediante un estudio cronológico de revisiones sistemáticas de literatura en ingeniería de software (Cárdenas *et al.*, 2016).

Se identificó los principales estudios sobre riesgos de ciberseguridad realizados en instituciones educativas, pudiendo definir la problemática, en el desarrollo del presente trabajo de titulación se tomó como referencia la revisión sistemática de literatura basada en varios trabajos, haciendo énfasis a tres fases que lo componen para la aplicación (Francischetti *et al.*, 2014) (Kitchenham & Charters, 2007).

Como primer punto se tiene la definición de las preguntas de investigación, efectuada de la siguiente manera:

1. ¿Cuáles son los principales estudios sobre riesgos de ciberseguridad realizados en instituciones de educación superior?

Se investigará los documentos existentes sobre riesgos en ciberseguridad, aplicados en instituciones de educación superior.

2. ¿Cuáles son las herramientas y metodologías utilizadas en el análisis y evaluación de riesgos?

Se realizará un breve resumen de las metodologías similares de análisis de riesgo, además de las planteadas a utilizar.

3. ¿En qué áreas han sido aplicadas las metodologías de gestión de riesgos desarrollados?

Se identifica que instituciones le dan mayor uso a cada metodología de detección de riesgo en base a las vulnerabilidades presentadas en ciberseguridad.

2.1.1 REGISTRO DE INFORMACIÓN DE INSTITUCIONES Y METODOLOGÍAS EMPLEADAS

En la segunda etapa de la revisión bibliográfica, se seleccionó la fuente de datos bibliográficos, utilizando los repositorios de Google Académico, SciELO, Springer, Dialnet, Science Direct, y se emplearon tesis de maestría o doctorado, artículos científicos, libros, etc.

Del cual, es complementada por medio de la investigación-exploratoria, que es llevada a cabo mediante el proceso de la información más relevante para obtener los datos, en donde se profundice las líneas base y se ejecute la resolución de problemas comprendidos en la investigación (Velázquez *et al.*, 2008).

Debido a que los criterios de búsqueda se realizaron por medio de palabras claves como: ciberseguridad, metodologías de análisis de riesgos, empleando como filtro publicaciones desarrolladas en Ecuador y que hayan sido publicados en los últimos 10 años, en la revisión se tomaron como referencia al tema de interés, en los que se obtuvieron como resultado los documentos resumidos en la tabla 1.1.

Tabla 1. 1. Tabla de resumen de la revisión bibliográfica

TABLA DE RESUMEN DE LA REVISIÓN BIBLIOGRÁFICA					
N°	AÑO	TÍTULO	AUTORES	METODOLOGÍA /NORMA ISO	INSTITUCIÓN APLICADA
1	2019	Ciberseguridad y su aplicación en las Instituciones de Educación Superior Públicas de Manabí	Avellán. N, Zambrano. M	AMFE ISO 27032	UNIVERSIDAD DE EDUCACIÓN SUPERIOR PÚBLICAS DE MANABÍ
2	2017	Ciberseguridad en los sistemas de información de las universidades.	Anchundia. C	ISO 27000	UNIVERSIDAD DE CUENCA
3	2017	La evaluación de los riesgos antrópicos en la seguridad corporativa: del Análisis Modal de Fallos y Efectos (AMFE) a un modelo de evaluación integral del riesgo	González. J, Myer, R, Pachón-Muñoz. W.	AMFE	MINISTERIO DE SALUD
4	2007	El análisis modal de Fallos y Efectos (AMFE) ayuda a	Molero. J, Tuset, J	AMFE	MINISTERIO DE SALUD

		aumentar la seguridad en radioterapia			
5	2012	A comparative Study on Information Security Risk Analysis Practice	Shula. N, Kumar. S	CORA – OCTAVE - CRAMM	PYMES
6	2014	Análisis modal de fallos y efectos en las prescripciones farmacológicas informatizadas.	Paredes. A, Aviña. R, González. M	AMFE	MINISTERIO DE SALUD
7	2013	Desarrollando una metodología para gestionar los riesgos de seguridad asociativos y jerárquicos y tasar de forma objetiva los sistemas de la información.	Santos. A, Sánchez. E, Álvarez. E, Fernández. M., Piattini. M.	MAGERIT – OCTAVE – MEHARI, CRAMM, MARISMA	PYMES
8	2015	Desarrollando una metodología de análisis de riesgo para el sector asegurador pueda tasar los riesgos en las PYMES	Santos. A, Fernández. E, Sánchez. E, Piattini. M	MARISMA	PYMES

En la tercera etapa, se definió la información relevante de los documentos obtenidos, alcanzando como resultado que dentro de las búsquedas en Google Académico de riesgos de ciberseguridad en las instituciones del Ecuador se encontraron 1940 resultados filtrando por el año de publicación 2017 a 2019, se hizo un nuevo filtro por instituciones educativas quedando 10 registros, de los cuales al realizar la revisión sistemática de los documentos, los que más se acercaron al tema planteado son dos, "*Ciberseguridad en los sistemas de información de las universidades aplicado en la ciudad de Cuenca en la facultad de ingeniería en sistemas*" realizado en el año 2017, y "*Ciberseguridad y su aplicación en las instituciones de Educación Superior Públicas de Manabí*" desarrollado en el año 2019.

En el objetivo de la primera investigación se revisó el estado actual del conocimiento en ciberseguridad en los sistemas de información en el contexto universitario Ecuatoriano, se obtuvo como resultado que se está produciendo grandes problemas de seguridad y de protección de datos y privacidad con los cuales deben enfrentarse en la actualidad, la universidad está llamada a jugar un papel protagónico en el establecimiento de una necesaria cultura de ciberseguridad que exige una labor de capacitación, además se hizo mención al uso de las normas ISO 27000 (Anchundia, 2017).

El segundo documento se realizó en el año 2019, "*Ciberseguridad y su aplicación en las instituciones de educación superior públicas de Manabí*", utilizando la metodología AMFE y la ISO 27032 aplicadas a las áreas de seguridad de la información, redes y aplicaciones, obteniendo como resultado que las vulnerabilidades encontradas en los sistemas distribuidos representan un promedio en la UTM del 27,33%, ULEAM 14,33%, ESPAM 29% y UNESUM 29,34%, de fallos en los procesos de documentación en el cumplimiento de los diferentes dominios de seguridad de la ISO/IEC 27032. Con respecto a las herramientas de escaneo se comprobó que los sistemas académicos, están expuestos a ataques cibernéticos en un promedio del 20%, debido a la criticidad de las vulnerabilidades, en los riesgos identificados y evaluados con la matriz AMFE (Análisis Modal de Fallos y Efectos), se determinó que el promedio de riesgo crítico en los diferentes dominios de seguridad (información, aplicaciones

y redes) de la UNESUM es del 29,02%, ESPAM MFL el 23,21%, UTM el 20,46% y la ULEAM el 9,09% (Zambrano & Zambrano, 2019).

2.1.2 HERRAMIENTAS Y TECNOLOGÍAS DE ANÁLISIS Y DETECCIÓN DE RIESGOS

Dentro de las herramientas y tecnologías de análisis y detección de riesgos en la búsqueda se encontraron 1008 documentos, de los cuales, filtrados por año y metodologías de mayor utilización dentro de la detección de riesgos, los más utilizados en ciberseguridad de mayor relevancia fueron:

- MAGERIT (Metodología de análisis y Gestión de Riesgo de los sistemas de información)(Lucero & Valverde, 2017)
- AMFE (Análisis modal de fallos y efecto), encontrando un estudio realizado en las universidades de Manabí, una de ellas es la universidad en la cual se va a desarrollar el análisis de riesgos en ciberseguridad (Liu *et al.*, 2017).
- CIRA (Análisis de riesgo de incentivos conflictivos) (Shukla & Kumar, 2012).
- CORA (Construcción de plataforma para el análisis de riesgo crítico de seguridad) (Montalvo, 2017).
- ISRAM (método de análisis de riesgo de seguridad de la información) (Tubío *et al.*, 2019).
- MEHARI (metodología de gestión de riesgos en el dominio de la seguridad de la información) (El Fray, 2012).
- OCTAVE (Evaluación crítica de las amenazas, activos y vulnerabilidades) (Espinosa *et al.*, 2014).
- MARISMA (Análisis de Riesgo sistemático basado en modelos asociativos inteligentes), este último permite gestionar de forma dinámica la evolución de los riesgos de manera sencilla y óptima mediante sus funcionalidades, por medio de Check auditoria, análisis de riesgos, plan de tratamiento, e incidencias, de todos los documentos investigados sobre esta metodología (Santos *et al.*, 2015).

Otro de los artículos citados es *“Desarrollando una metodología de análisis de riesgos para que el sector asegurador pueda tasar los riesgos en las PYMES”*, como resultado en esta investigación aplicando MARISMA como marco de trabajo se pudo establecer la importancia que tiene la gestión y el análisis de los riesgos sobre la seguridad de los sistemas de información en el desempeño sostenible de toda institución para alcanzar sus objetivos y mantener la evolución sostenible de las empresas, de igual forma el artículo *“Desarrollando una metodología para gestionar los riesgos de seguridad asociativos y jerárquicos y tasar de forma objetiva los sistemas de información”*, hace un análisis de todas las metodologías y estándares de análisis de riesgos más usados y que mejor resultados obtenga, determinando la utilización de MARISMA, como la mejor dentro de su gama para el análisis de riesgos, porque aporta un marco de trabajo que permite la tasación objetiva de un sistema de información y la generación de un análisis de riesgos objetivo que tenga en cuenta aspectos asociativos y jerárquicos y sea de bajo coste en su generación y mantenimiento (Parra *et al.*, 2013).

Dentro de las instituciones que utilizaron herramientas y metodologías de análisis de riesgo el criterio de búsqueda fue AMFE y MARISMA, encontrando 163 resultados en Springer de los cuales se filtró por artículos científicos publicados en los últimos años, se analizaron varios artículos seleccionando tres de estos para su estudio: *“Análisis modal de Fallos y Efectos (AMFE) ayuda a aumentar la seguridad en radioterapia”* (Govindarajan *et al.*, 2007), *“Análisis modal de fallos y efectos en las prescripciones farmacológicas informatizadas”* (Paredes-Atenciano *et al.*, 2015) y *“La evaluación de los riesgos antrópicos en la seguridad corporativa del análisis modal fallos y efectos (AMFE) a un modelo de evaluación integral del riesgo”* (González *et al.*, 2017) (Gómez, 2017).

Estos tres documentos utilizaron AMFE como metodología de análisis riesgos y detección de fallos, de los cuales el ámbito de mayor aplicación de AMFE es la medicina y MARISMA es dedicado a procesos empresariales de medianas y grandes empresas, pudiendo destacarse en control de procesos (Santos *et al.*, 2015).

Debido a los riesgos presentados, las Instituciones están llamadas a jugar un papel protagónico en el establecimiento de una necesaria cultura de ciberseguridad que exige una labor de capacitación de todos los sectores de la sociedad; las instituciones universitarias no pueden quedarse ajenas y deben participar en el proceso, contribuyendo a crear un ciberespacio universitario seguro y liderando el arraigo de una cultura de ciberseguridad, puesto que están produciendo grandes problemas de seguridad si no se controlan adecuadamente (Betancourt, 2017) (Torres, 2015).

MARISMA además de ser una herramienta de análisis de riesgo permite realizar auditoria inicial del estado, generación de mapa y tratamiento, gestión de incidencias, monitorización y auditoria del riesgo, por lo que es de mayor uso en procesos de tecnologías de la información para la detección de vulnerabilidades.

Dado que los servicios ofrecidos por esta herramienta permiten la adecuada gestión de la ciberseguridad basadas en componentes tecnológicos, que continuamente están en evolución y actualización de acuerdo a la demanda significativa dentro del impacto de la administración de activos, asegurando la calidad y seguridad de información en las empresas (Destinonegocio, 2015) (Gómez-Suarez, 2019).

Se puede además combinar metodologías y herramientas para obtener resultados que permiten una mayor eficacia al momento de localizar algún tipo de riesgos presentados en el ciberespacio, de manera que se mitiga algún tipo de eventualidad a la hora de efectuar un análisis de ciberseguridad, por lo que así se podrá encontrar el riesgo y determinar la prioridad para la respectiva toma de decisiones y mejora dentro de los procesos tecnológicos. Dada la importancia que tiene la seguridad y el análisis de riesgos de la información sobre el desempeño de las empresas.

Concluyendo de esta manera, que mediante un análisis de ciberseguridad en las instituciones, se puede comprobar efectivamente las vulnerabilidades que se presentan en información, aplicación y redes, que mediante el uso de herramientas óptimas en tiempo real se logra evaluar y comprobar los riesgos presentados en el ciberespacio, debido que en AMFE los riesgos son calculados

de manera estática, pero que si bien al ser vinculados con MARISMA son dinámicos y más operativos en cuestión de precisión, ayudando de esta manera a promover la mitigación de dichos riesgos y brindando alternativas estratégicas que avalen la protección de los recursos tecnológicos de la Institución.

CAPÍTULO III. DESARROLLO METODOLÓGICO

En el presente trabajo se utilizó el método bibliográfico para la recolección de información sobre los riesgos en Ciberseguridad y las metodologías de análisis de riesgo existente y aplicado en las Instituciones Educativas (Roussos, 2011).

La ejecución del presente trabajo fue mediante consecución de objetivos específicos, en donde se indica el establecimiento de los patrones de análisis de ciberseguridad: la seguridad de la información, seguridad de aplicación y seguridad de redes; como objeto de estudio se consideró la Unidad de Tecnología de la Escuela Superior Politécnica Agropecuaria de Manabí “ESPAM MFL”, en donde se realiza un análisis con la metodología AMFE y MARISMA, que permitió identificar las amenazas existentes mediante auditorias de riesgos basadas en aspectos de ciberseguridad, para el debido proceso del cumplimiento de la investigación.

A continuación se puede apreciar el desarrollo de cada una de las fases empleadas en el trabajo de titulación.

3.1. FASE 1: IDENTIFICACIÓN DE VARIABLES PARA EL ANÁLISIS EN CIBERSEGURIDAD EN EL ÁREA DE SEGURIDAD DE LA INFORMACIÓN

Se realizó el levantamiento de información en el área de tecnologías de la información, solicitando que se facilite la información necesaria para la recolección de la información, tales como: El plan de acción de Ciberseguridad efectuado anteriormente con la metodología AMFE y la ISO 270032 (Avellán y Zambrano, 2019), que también se encuentran en el repositorio de la Biblioteca de la ESPAM MFL de fácil acceso y a disposición de los estudiantes de dicha universidad, reportes de monitoreo de vulnerabilidades por parte del departamento, investigaciones relacionadas a los temas, normativas o políticas y demás información relevante al mismo.

Además, se solicitó por medio de correo electrónico a la empresa SICAMAN, las credenciales para el uso de la herramienta MARISMA, para fines académicos, dado que el administrador una vez aceptada la solicitud procedió a dar el permiso

para el uso del sistema en este trabajo, otorgando las credenciales administrativas, para que esta importante herramienta y metodología de análisis y gestión de riesgos en ciberseguridad se dé a conocer.

Una vez obtenida las credenciales, se realizó el estudio de la metodología MARISMA, para realizar el funcionamiento que permitiera identificar los hallazgos de las diferentes causas de riesgos, precisando prioridades en cuestión del nivel de riesgo y cómo proponer mejoras y acciones de mitigación para encontrar una óptima solución en ciberseguridad para la ESPAM MFL, que posteriormente se procedió a determinar parámetros considerados en dicha gestión, para adaptarlo a sus debidas configuraciones.

3.2. FASE 2: DETERMINACIÓN DE LOS CONTROLES A UTILIZAR EN CIBERSEGURIDAD CON LA METODOLOGÍA MARISMA

En esta fase se procedió a determinar los controles que se utilizaron en ciberseguridad mediante la información obtenida en la fase 1, se ingresó los parámetros que establecía la Metodología MARISMA en la herramienta, dentro de estos los controles que destacan los dominios, objetivos y Checklists, que fueron ligados a gestión de activos, control de amenazas, y administración de consultas correspondientemente por los respectivos patrones considerados como las antes indicadas variables de análisis.

- **Dominios:** En esta opción los dominios por cada uno de los patrones son ingresados, así como un conjunto de controles para la gestión del dominio que se encuentran almacenados en el repositorio de patrones y un conjunto de elementos (tipos de activos, amenazas, vulnerabilidades y criterios de riesgo) necesarios para la elaboración del análisis de riesgos.
- **Objetivos:** En esta parte, funciona correctamente planteadas en el alcance las metas propuestas por la dirección de los dominios.
- **Rangos:** Permite ingresar aquellos intervalos en donde se le va a dar valor por medio de la escala Bajo mayor a 0 y menor a 25, Medio mayor a 25 y menor a 50 y Alta mayor a 50 hasta 100, de acuerdo a una semaforización establecida previamente para identificarlos una vez que

se pongan en ejecución según la metodología de riesgos de Sistemas de Información.

- **Controles:** Permiten establecer medidas que se van a tomar para controlar algún riesgo subsistido en ciberseguridad, de manera que todo se proyecte uniformemente en lo que se pretende conocer mediante estos controles aplicados a todos los patrones.
- **Checklist:** En esta parte se procede a ingresar los datos para la creación de un cuestionario en base a los datos ya establecidos con autoridad en el sistema con respecto al patrón seguridad de la información, en donde se debe completar y relacionar al checklist levantado en investigaciones anteriores, y con ello así sucesivamente hasta que se completen para todos los demás patrones ingresados respectivamente.

3.3. FASE 3: IMPLEMENTACIÓN DEL PLAN DE GESTIÓN DE RIESGOS EN BASE A LAS METODOLOGÍAS AMFE Y MARISMA.

Se implementó el plan de gestión de riesgos mediante el uso de las metodologías AMFE y MARISMA en el sistema eMarisma, en donde se logró determinar el control de activos, análisis de riesgo de ciberseguridad y plan de tratamiento, conforme la información fue ingresada se procedía generar los resultados para proporcionar las acciones de mejora para la Unidad de Tecnología de la ESPAM MFL.

Cabe indicar que dicho plan fue modelado según los riesgos preventivos y correctivos existente, mediante un informe técnico basado en las auditorias y reportes de eMarisma, para ser tomadas se consideraron en corto, mediano y largo plazo.

Finalmente se efectuó una categorización de los resultados y se priorizó según la semaforización de riesgos obtenidos de cada una, en el cual se realizó una matriz dándose a conocer los procesos que son prioridad según los criterios (Rojo: Alto, Naranja: Medio, Azul: Bajo) acompañados de las directrices de la escala de Likert para más precisión en caso de alguna eventualidad y coordinar

la sincronización de información para los resultados de la investigación, conforme sean las vulnerabilidades o amenazas presentadas en los resultados, del cual MARISMA asocia el análisis y la gestión del riesgo a los controles necesarios para poder realizar un análisis de riesgos dinámico expresado en tres procesos que comprende el sistema, del cual en la figura 3.1, se puede apreciar esquemáticamente el funcionamiento de cada proceso comprendido en eMarisma. Se observa de forma resumida los tres procesos que la componen y cómo intercambian información entre ellos. Los datos generados en el proceso GPRA será utilizada por los otros dos procesos. De igual forma, la información generada en el proceso GARM será necesaria para el proceso DRM. Esto no implica que siempre se deban ejecutar los tres procesos para obtener un resultado, sino que debe existir un Patrón generado previamente por el proceso GPRA para que se pueda ejecutar el GARM.

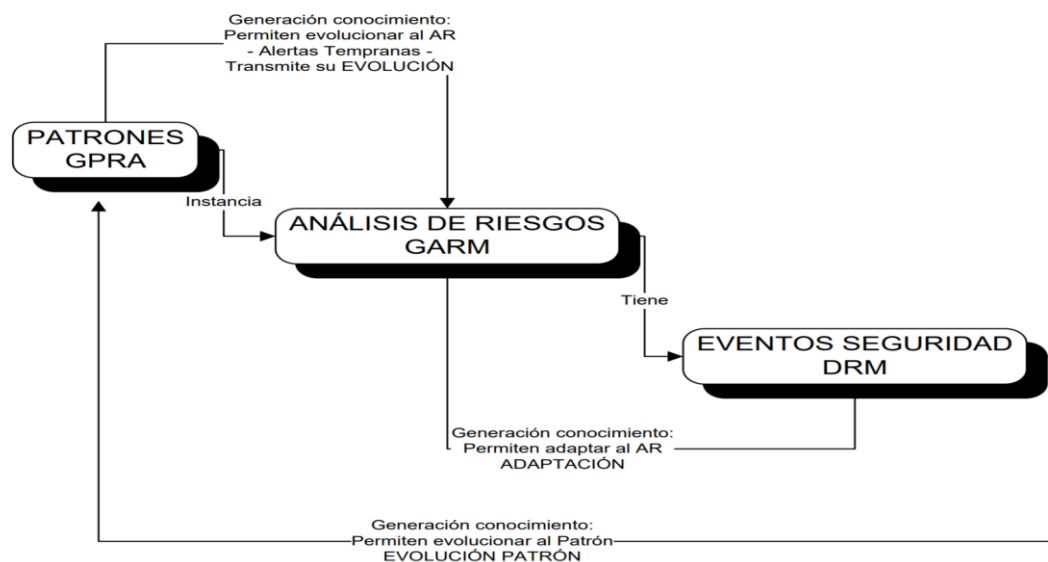


Figura 3. 1. Elementos que componen la herramienta eMarisma y las relaciones.

Fuente: (MARISMA, 2018)

Dentro de las herramientas que componen eMarisma se definen a continuación:

- **GENERACIÓN DE PATRONES PARA EL ANÁLISIS DE RIESGOS (GPRA)**

Se establece una estructura de relaciones entre los diferentes elementos involucrados en el análisis del riesgo y los controles necesarios para gestionar

los riesgos, mediante el conocimiento adquirido del estudio realizado con AMFE en las diferentes implantaciones, siendo almacenado en una estructura denominada patrón en la herramienta eMARISMA para ser reutilizado y aplicado dependiendo los eventos que se produzcan, según indica la estructura de los elementos que la componen como se muestra a continuación:

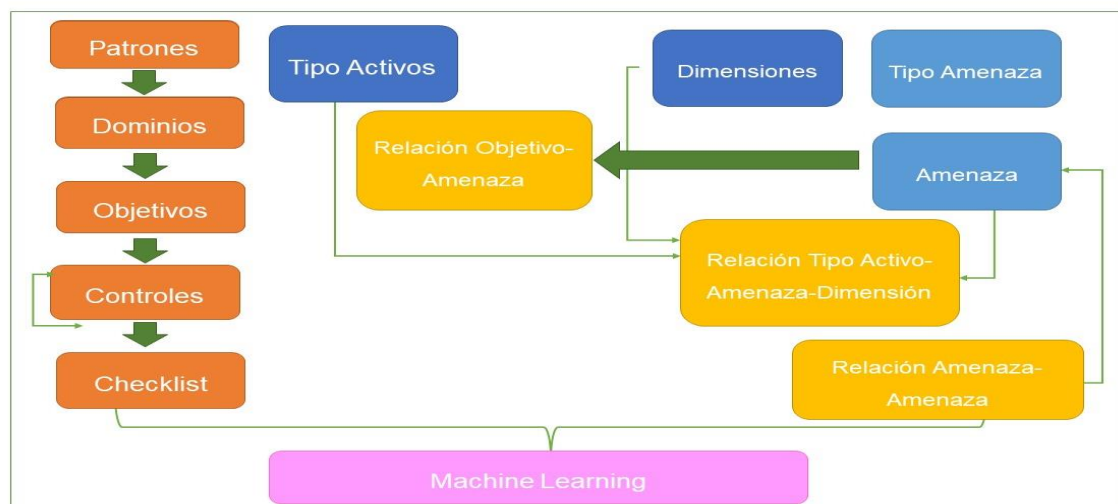


Figura 3. 2. Esquematación de la estructura de análisis de riesgo.

Fuente: Propia.

- **GENERACIÓN DEL ANÁLISIS Y GESTIÓN DEL RIESGO (GARM)**

A partir de la selección de los patrones y controles, se lleva a cabo la identificación de los principales activos examinados en AMFE, en donde se obtiene un esquema de la situación actual del análisis del riesgo, teniendo en cuenta que al ingresar la información de riesgo proporcionada por AMFE, la herramienta eMarisma valida dichos datos por varios filtros de verificación que son estipulados por la ISO 25001, para obtener las auditorías específicas por cada proceso permitido en el sistema, condensando de esta forma dicha información, para generar los informes respectivos para proceder analizar.

- **EVENTOS SEGURIDAD (DRM)**

Mediante la utilización de las matrices generadas, que relacionan los diferentes activos de la institución, el sistema irá recalculando el análisis de riesgos según

se produzcan los eventos, dependiendo del fallo de las métricas definidas, detectando la no autorización en los controles.

3.4. FASE 4: ANÁLISIS DE LOS PARÁMETROS OBTENIDOS CON AMBAS METODOLOGÍAS

El análisis de ambas metodologías permitieron mostrar los resultados obtenidos en MARISMA y los constatados en AMFE, por lo cual se elaboró un análisis de parámetros de riesgos, en donde se indicó los resultados comparativos entre metodologías de gestión de Ciberseguridad, además se estableció tiempos previos de pruebas con intervalos de días, de acuerdo a cada parámetro de información hallado dentro de la plataforma eMarisma, luego se condensó todo para proceder a las conclusiones de la auditoría y reportes comprendida en los tres patrones: seguridad de la información, seguridad de aplicaciones y seguridad de redes, de esta manera proceder a la adecuada interpretación y evaluación de los riesgos de ciberseguridad en la Institución.

CAPÍTULO IV. RESULTADOS Y DISCUSIÓN

4.1. RESULTADOS

En este capítulo se procedió a efectuar cuatro fases basadas en el cumplimiento de los objetivos planteados, que se llevaron a cabalidad en los resultados conforme cada proceso efectuado dentro de la investigación.

4.1.1. FASE 1: IDENTIFICACIÓN DE VARIABLES A CONSIDERAR EN EL ANÁLISIS EN CIBERSEGURIDAD EN EL ÁREA DE SEGURIDAD DE LA INFORMACIÓN

Mediante el levantamiento de la información posterior al análisis de ciberseguridad en la ESPAM MFL (Anexo 1), se procedió como punto de partida la identificación de las variables correspondientes al área de seguridad de la información, de la cual se tomó como referencia la información recopilada de la matriz AMFE (Anexo 2), correspondiente a las vulnerabilidades suscitadas en ciberseguridad con respecto a los sistemas de información alojados en la infraestructura tecnológica de la Institución.

Seguidamente se pudo conocer que existían vulnerabilidades en dichos dominios comprendidos en el área de tecnologías de la información, para ello una vez estudiada dicha información, se procedió a identificar los patrones denominados: Seguridad de Información, Aplicación y Redes, que fueron tomados en cuenta como patrones prioritarios dentro de eMarisma, que fue creado para efectuar el ingreso de información teniendo como referencia los campos que contiene cada patrón del aplicativo, en el que se considera vulnerabilidades para conocer o direccionar a los posibles riesgos o fallos que se podrían presentar mediante la aplicación de esta metodología.

4.1.2. FASE 2: DETERMINACIÓN DE LOS CONTROLES A UTILIZAR EN CIBERSEGURIDAD CON LA METODOLOGÍA MARISMA

Luego de haber identificado las variables para el respectivo análisis de ciberseguridad, se procedió a determinar los controles por medio de la metodología de análisis de riesgo dentro del sistema eMarisma, en este caso

correspondieron a todo aquello que ayude a mejorar la incidencia de riesgos en Ciberseguridad, de manera que fueron ingresados para obtener la información de acuerdo a lo indicado en las normas ISO 27032, 25001 y otros estándares plasmados en matrices e informes de levantamiento de información (Anexo 3).

Posteriormente en eMarisma, se pudo apreciar que dichos controles estaban ligados a la comprensión de análisis en tiempo real, de manera que los controles: Dominios, Objetivos, Controles, Checklist, se vincularon a los activos comprendidos a físicos, información, servicios y personal que permitieron conocer el tipo de patrón en el momento de sacar las matrices de dimensión que se ingresan en el control de amenazas y activo, además se llevó acabo comprendiendo las denominaciones en Seguridad de la Información, Seguridad de las Aplicaciones y Seguridad de las Redes de acuerdo a tipos de activos Personales, Activo Físicos, Activos Información y Activos de servicios, que son los nombres que se le otorgaron en el sistema eMarisma para su identificación de activos.

4.1.3. FASE 3: IMPLEMENTACIÓN DEL PLAN DE GESTIÓN DE RIESGOS EN BASE A LAS METODOLOGÍAS AMFE Y MARISMA.

Por medio de la elaboración de un plan de gestión de riesgos en ciberseguridad en la Unidad de Tecnología de la ESPAM MFL, se pudo brindar las directrices necesarias basadas en la metodología AMFE y MARISMA como mecanismos preventivos y correctivos en caso de suscitar algún tipo de riesgo de vulnerabilidad o amenaza presentados en el ciberespacio, motivo por el cual da a conocer en su contenido diversas estrategias de acción y mitigación para llevar a cabo un adecuado control del seguimiento constante y administración de los recursos de información dentro de la Institución (Anexo 4).

Se adaptaron todos los aspectos relacionados con la gestión de los riesgos y bajo la condición de que cualquier análisis de gestión de riesgo realizado con eMarisma es válido para utilizarlo en otras compañías, esta herramienta trabaja con tres procesos muy importantes:

- **Proceso 1:** Generación de Patrones para el Análisis de Riesgos (GPRA).
- **Proceso 2:** Generación del Análisis y Gestión del Riesgo (GARM).

- **Proceso 3:** Mantenimiento Dinámico del Análisis de Riesgos (DRM).

De manera que se lleva una operatividad sistemática y con los procesos ingresados se puede visualizar constantemente los reportes según sea la auditoria que se desea consultar de riesgos presentados en ciberseguridad.

4.1.3.1. GENERACIÓN DE PATRONES PARA EL ANÁLISIS DE RIESGOS

Una vez creada la denominación de los patrones para el análisis de riesgos se pudo completar la información en eMarisma, vinculando y clasificando en matrices los controles de vulnerabilidades en base a la gestión y dimensiones, para la obtención oportuna de resultados comprendidos en ciberseguridad, de acuerdo a las áreas empleadas respectivamente (figura 4.2).

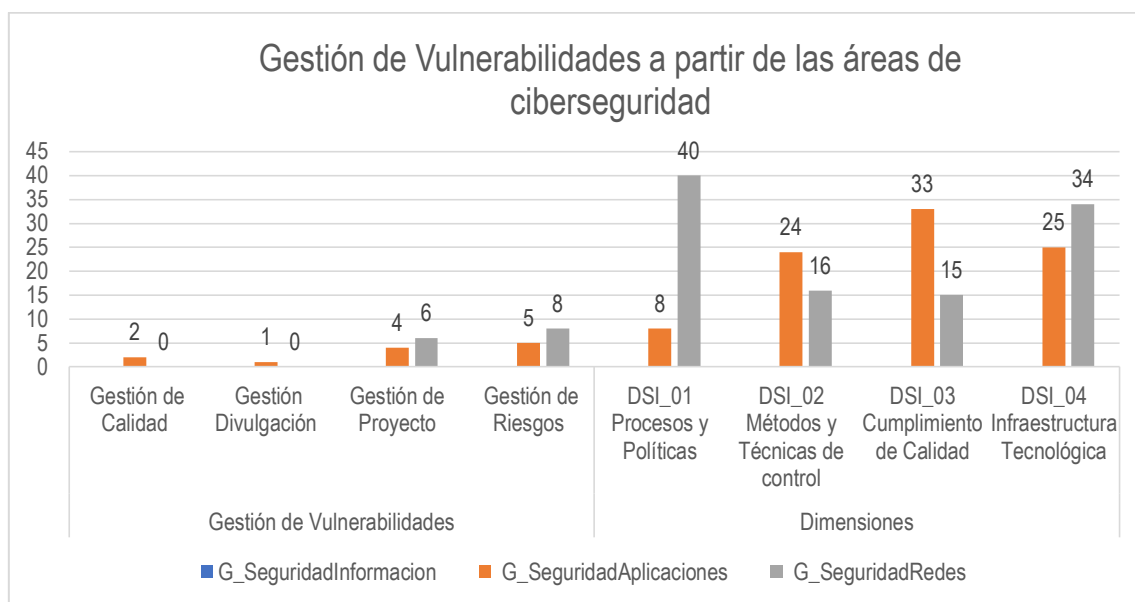


Figura 4. 3. Cantidad de vulnerabilidades según los patrones de ciberseguridad de acuerdo a las gestiones y dimensiones empleadas en eMarisma.

Elaboración: Propia.

4.1.3.2. GENERACIÓN DEL ANÁLISIS Y GESTIÓN DEL RIESGO

Luego de conocer la situación actual por medio de la identificación de patrones de ciberseguridad, se obtuvo de manera óptima el análisis y gestión de riesgos que fueron resultados de la implementación de las metodologías AMFE (figura 4.3) y MARISMA (figura 4.4), en donde conllevó al estudio y comprensión de los datos para llegar a las conclusiones y recomendaciones de evaluación de la

auditoria aplicada a gestión de riesgos en ciberseguridad conforme los resultados del sondeo IP (figura 4.5) y cuadro de mando (figura 4.6).

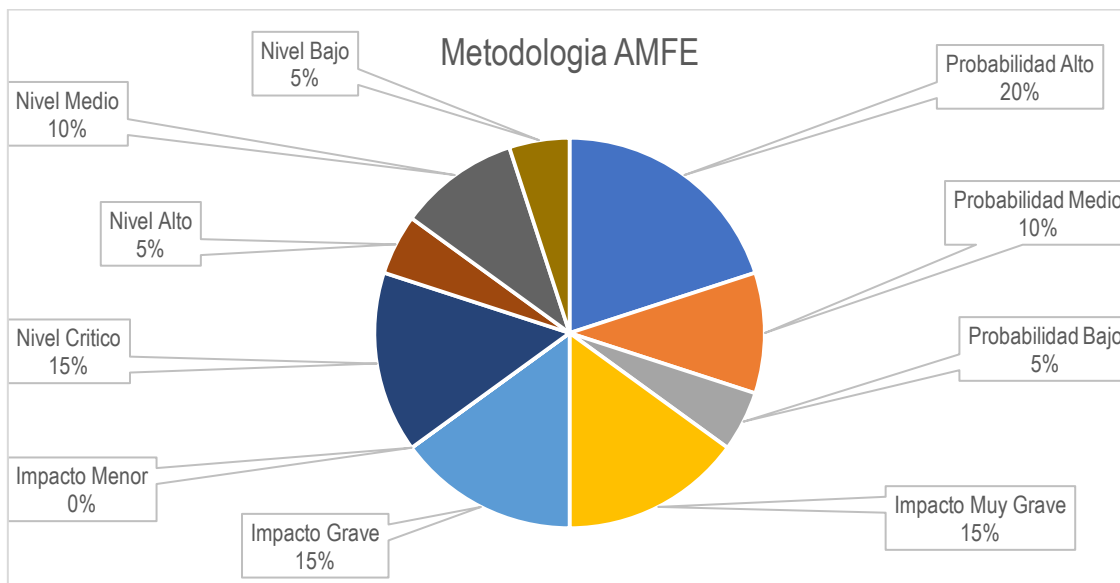


Figura 4. 4. Porcentaje de niveles, impacto y probabilidad generados según las vulnerabilidades de los sistemas de información de la ESPAM MFL de acuerdo a la metodología AMFE.

Elaboración: Propia.

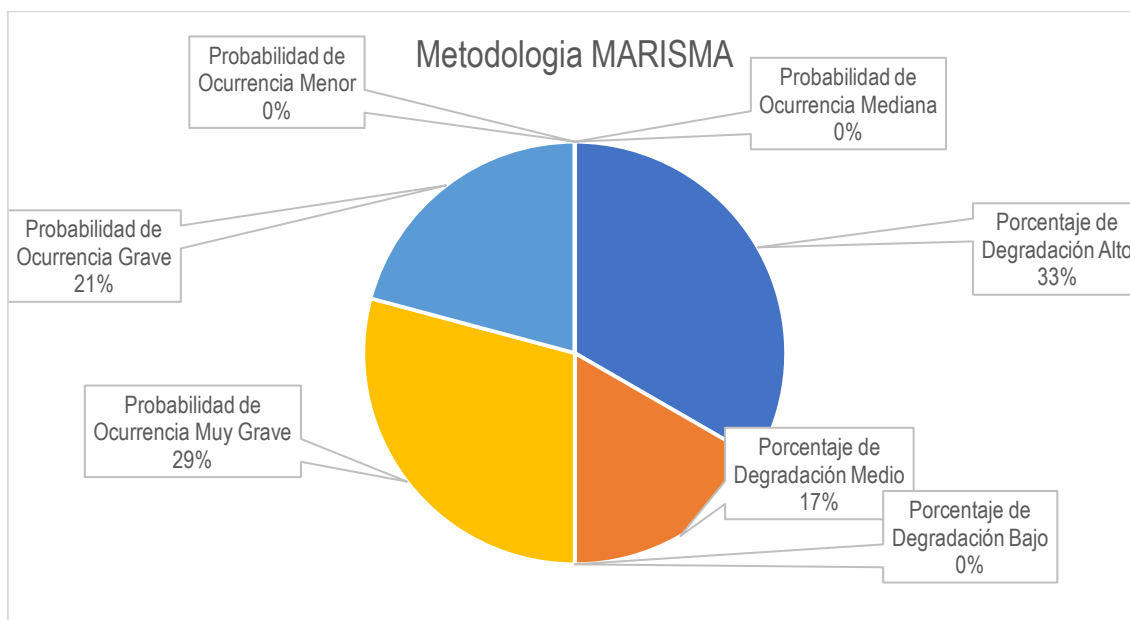


Figura 4. 5. Porcentaje de probabilidades de ocurrencia y degradación generadas según las vulnerabilidades de los sistemas de información de la ESPAM MFL de acuerdo a la metodología MARISMA.

Elaboración: Propia.

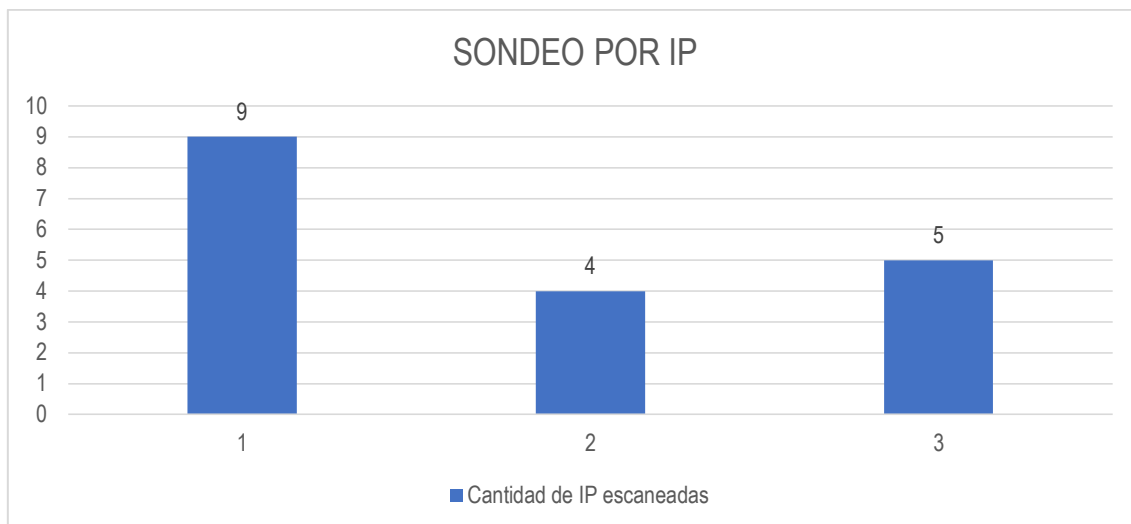


Figura 4. 6. Sondeos por IP, aplicados en eMarisma de acuerdo a las IP de los sistemas de información de la ESPAM MFL.

Elaboración: Propia.

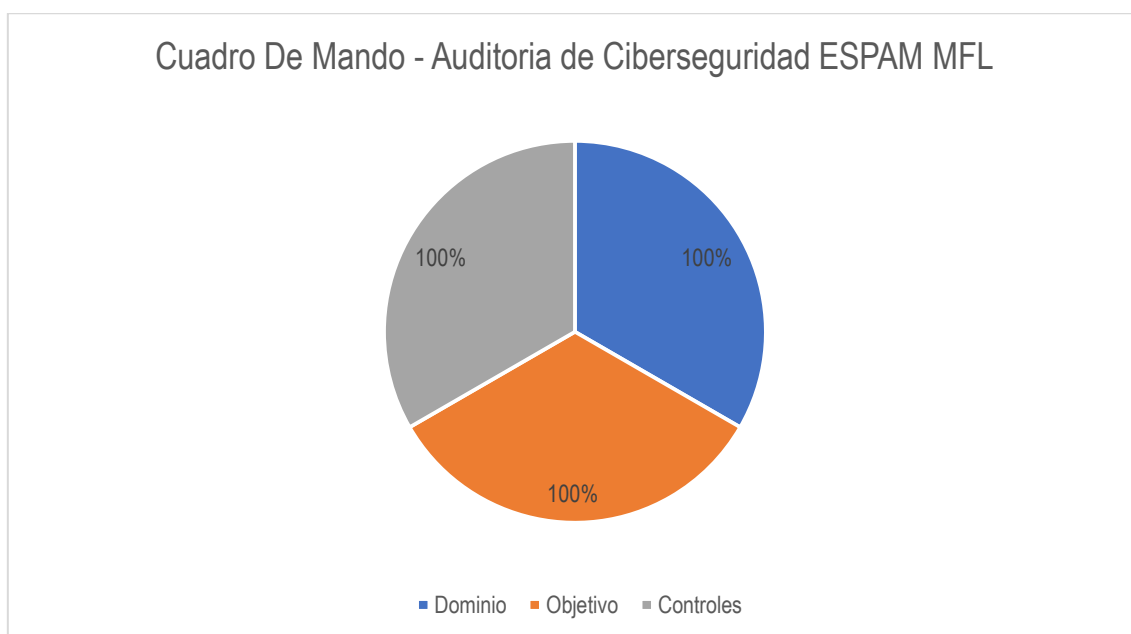


Figura 4. 7. Cuadro de Mando general de acuerdo a la auditoria de los controles, dominios y objetivos de cada patrón ingresado en eMarisma correspondiente a ciberseguridad dentro de la ESPAM MFL.

Elaboración: Propia.

4.1.3.3. MANTENIMIENTO DINÁMICO DEL ANÁLISIS DE RIESGOS

Por medio de las matrices generadas en eMarisma, se efectuó un mantenimiento dinámico de riesgos, para que al momento de recalculer el análisis se pueda mostrar en tiempo real las novedades de riesgos a controlar, de forma

parametrizadas y considerando las sugerencias de la plataforma, dado que así se realizan correcciones con éxito, se mitigan las incidencias en los sistemas distribuidos, además de que se mejora las métricas y parámetros de riesgo en ciberseguridad mediante el análisis de riesgo sistemático basado en modelos asociativos inteligentes en tiempo real aplicados en la ESPAM MFL.

4.1.4. FASE 4: ANÁLISIS DE LOS PARÁMETROS OBTENIDOS CON AMBAS METODOLOGÍAS.

Mediante el análisis de los parámetros obtenidos con ambas metodologías de riesgos se pudo establecer una vinculación de resultados mediante una matriz condensada (Anexo 5), dado que al momento de sincronizar ambos contenidos, se pudo constatar que están ligadas para arrojar un resultado sistemático, cada una tiene su funcionabilidad, a diferencia de AMFE que trabaja con una matriz de riesgos en donde se categoriza prioridades de riesgos en base a un Checklist aplicado según la norma ISO 27032, del cual su operatividad es buena al momento de establecer la mitigación según la probabilidad y el impacto de cada vulnerabilidad, de allí prioriza y permite obtener y conocer el estado de riesgo que se encuentra la Institución según la disponibilidad de los patrones en el ciberespacio.

Cabe recalcar que la metodología MARISMA dentro del análisis se consideró las variables:

- Mantenimiento dinámico.
- Control de los riesgos de vulnerabilidades o amenazadas.
- Distribución de los activos.
- Seguridad y Auditoria.
- Patrones para análisis enfocado a reducir los costes de generación y mantenimiento de procesos de análisis del riesgo.

4.2. DISCUSIÓN

De acuerdo a lo mencionado por Avellán y Zambrano (2019), los riesgos identificados y evaluados con la matriz AMFE (Análisis Modal de Fallos y Efectos), se determinó que el promedio de riesgo crítico en los diferentes dominios de seguridad (información, aplicaciones y redes) de la UNESUM es del 29,02%, ESPAM MFL el 23,21%, UTM el 20,46% y la ULEAM el 9,09%. Teniendo en cuenta que en aquel tiempo las vulnerabilidades presentadas en ciberseguridad de la ESPAM MFL, fue la segunda con más riesgos críticos presentadas en los 3 dominios, Datos, Aplicación y Redes, pero que mediante el análisis de riesgos se pudo considerar como prioritario, a partir de esto se propuso medidas estratégicas de mitigación para solucionar problemas presentados en el ciberespacio.

Dado que seguridad absoluta no existe, por lo que las decisiones estratégicas deberán ir enfocadas a priorizar aquellos riesgos que por su probabilidad de ocurrencia y nivel de impacto podrían hacer más daño al negocio, centrando la mayor parte de los recursos disponibles en su mitigación, aplicando un enfoque de análisis de coste vs beneficio para prevenir los ataques que se fueran a suscitar (UHY FAY & CO, 2020) (Julio, & Rios, 2019).

Tomando como referencia las investigaciones realizadas da a conocer que las cifras del último estudio anual IT Security Risks evidencian que el 25 % de las grandes empresas y el 28 % de las PyMES han admitido que carecen de los recursos internos y de la experiencia necesarios en la gestión y la seguridad informática, lo que determina que sus negocios se vuelvan vulnerables a ataques informáticos (Destinonegocio, 2015).

En donde la ciberseguridad organizacional juega un papel importante como instrumento para la prevención, detección de operaciones fraudulentas y sospechosas, garantizando que las operaciones en la toma de decisiones del capital intelectual vallan de la mano de herramientas que le permitan llevar un análisis sistemático de gestión de riesgos, bajo un enfoque integral, logrando una administración adecuada en la prevención y detección de algún problema cibernético (Fernández & Herrera, 2020).

En los actuales momentos los riesgos de ciberseguridad, no son únicamente una cuestión del departamento de TI, sino que deben formar parte de la estrategia general del negocio por su indudable impacto en la sostenibilidad de las organizaciones; desde esta perspectiva, el análisis de los riesgos de ciberseguridad deben establecerse hasta los comités de dirección, y formar parte de la matriz global de riesgos de las compañías, resulta esencial evaluar de forma pormenorizada los riesgos por área: sistemas, funciones, personal, legal, activos, entre otros, recursos considerados para su mitigación y realizar un seguimiento continuo de los mismos (UHY FAY & CO, 2020) (Gallardo, 2018).

Por tanto el uso de metodologías de gestión de riesgos forma acciones para precautelar la información, es por ello que MARISMA conocido como sistema para el análisis de riesgos y la tasación de activos de información en la nube, es una metodología utilizada por decenas de investigadores en todo el mundo, para avanzar en el campo del análisis y la gestión de riesgos y la ciberseguridad, manteniendo un proceso de análisis y gestión del riesgo denominado eMarisma 3.0-AGR, este proceso se obtiene mediante la aplicación del método de investigación en acción y se enmarca dentro de una metodología (Marisma 3.0) que acomete todos los aspectos relacionados con la gestión del riesgo, y bajo la premisa de cualquier sistema de análisis de riesgos en instituciones que lo requieren (MARISMA, 2018).

En base a las investigaciones realizadas por los diversos autores antes indicados, se considera que es importante el uso de metodologías de riesgos de ciberseguridad, dado que en esta investigación, se pudo determinar que al momento de fusionar ambas metodologías, es decir AMFE y MARISMA, se llevó a cabo un análisis de los procesos de detección de vulnerabilidades de los sistemas de información de la ESPAM MFL, puesto que tanto la metodología AMFE como MARISMA, permite hallar eventualidades que se suscitan en la nube, pero que muchas veces se desconoce si no se realiza la actividad respectiva.

Considerando que en dicho análisis, es relevante la valoración de los patrones, controles, eventos, entre otros indicadores que inciden en la detección óptima de

dichas vulnerabilidades, que si bien, al momento de ingresar los datos a la herramienta eMarisma de la metodología MARISMA, se generan sistematizadamente el recálculo, plan de tratamiento y la gestión de riesgos, presentándolos en auditorias, reportes, consultas; conforme sean los resultados esperados; brindando de esta manera, las estrategias de mejora de la calidad dentro de la toma de decisiones, mitigando así los riesgos y garantizando el cumplimiento de acciones y criterios de aceptación en lo que respecta a la seguridad de la información de los sistemas distribuidos de la institución.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

- Por medio de la identificación de las variables se dio inicio a la creación de los patrones que conforman las áreas de los sistemas distribuidos pertenecientes a la ESPAM MFL, por lo que se vio en la necesidad de estructurarlos de acuerdo a la información obtenida de la metodología AMFE, para luego ser trasladada a la herramienta perteneciente a Marisma.
- Los controles en la metodología MARISMA lograron identificar las pautas (Dominios, Objetivos, Rangos, Controles y Checklist) que permiten proteger los activos de las vulnerabilidades o amenazas, de manera que se produjo un impacto significativo en la mitigación de acuerdo a los patrones obtenidos previamente, para la detección y control de los riesgos.
- Mediante la implementación de un plan de gestión de riesgos, se indican las estrategias, auditoría y mantenimiento que aportaron en la detección de las vulnerabilidades y la mitigación conforme se hallaron los riesgos, según la prioridad establecidas por categorías de impacto y la probabilidad de ocurrencia, brindando diferentes niveles de gestión para el cumplimiento de cada uno de ellos.
- Al analizar los resultados obtenidos con ambas metodologías podemos definir que la principal problemática es que AMFE genera una visión estática del estado actual de la institución, mientras que MARISMA mediante su herramienta eMARISMA, se puede gestionar y actualizar de forma automática el estado de la compañía en todo momento según los acontecimientos que vayan surgiendo.

5.2. RECOMENDACIONES

- Se debe realizar una adecuada identificación de variables, que garanticen la efectividad de los datos al momento de generar los resultados en la herramienta de eMarisma, con el propósito de ir llevando de manera secuencial cada proceso sistematizado y así evitar cometer errores que podrían afectar a corto, mediano y largo plazo la obtención de los reportes de auditorías.
- Al momento de establecer los controles de Marisma, es necesario definir los mecanismos a utilizar dentro de la herramienta, debido a que esta secuencia incide potencialmente en el manejo de los procesos de control de riesgos, que permiten proteger los activos de las amenazas.
- Al realizar un plan de gestión de riesgo con la herramienta eMarisma, permitirá obtener resultados eficientes y con el menor esfuerzo y coste posible, considerando a futuro las acciones pertinentes y toma de decisiones dentro de la Institución, así mismo los riesgos que pueden presentarse en diversas áreas, el cual facilitará la mitigación en las eventualidades presentadas y las que se van generando.
- Se debe utilizar metodologías de análisis de riesgos que permitan una visión actualizada y continua de las vulnerabilidades, en donde se reporten auditorías de gestión de riesgos, para prevenir eventualidades, que puedan adaptarse a todas áreas institucionales, teniendo éxito a la hora de implementarse, de fácil manejo y con las características deseadas.

BIBLIOGRAFÍA

- Anchundia, C. (2017). Ciberseguridad en los sistemas de información de las universidades. *Dominio de Las Ciencias*, 3(3), 200–217. <https://doi.org/10.23857/dom.cien.pocaip.2017.3.mono1.ago.200-217>
- Alonso, G. M. P., & Tejada, R. R. (2017). La cooperación público-privada en el fomento de la cultura de ciberseguridad. *Cuadernos de estrategia*, (185), 217-246.
- Astier Peña, M. P., Maderuelo Fernández, J. Á., Jiménez Julvez, M. T., Maderuelo Fernández, J. Á., Martín Rodríguez, M. D., & Palacio Lapuente, J. (2010). Análisis proactivo del riesgo: el análisis modal de fallos y efectos (AMFE). *Revista clínica electrónica en atención primaria*, (18), 0001-8.
- Betancourt, C. E. A. (2017). Ciberseguridad en los sistemas de información de las universidades. *Dominio de las Ciencias*, 3(3), 200-217.
- Cárdenas, L., Martínez, H., & Becerra, L. (2016). Gestión de seguridad de la información: revisión bibliográfica/ Information security management: A bibliographic review. *El Profesional de La Información*, 25(6), 931–948. <https://doi.org/10.3145/epi.2016.nov.10>
- CO, U. F. (2020). El análisis de los riesgos de ciberseguridad dentro de la estrategia general del negocio. Disponible en: <https://www.elblogdetusasesores-consultores.com/ciberseguridad-y-accesibilidad-de-la-informacion/analisis-los-riesgos-ciberseguridad/>
- Consejo de Aseguramiento de la Calidad de la Educación Superior (CACES). (2018). Política de Evaluación Institucional de Universidades y Escuelas Politécnicas en el Marco del Sistema de Aseguramiento de la Calidad de la Educación Superior. Disponible en: [https://www.ueb.edu.ec/images/pdf/planeamiento/evalauacion%20intern a/\(documento%20\)%20política%20de%20evaluación%20institucional%20de%20universidades%20y%20escuelas%20politécnicas%20en%20el %20marco%20del%20sistema%20de%20aseguramiento%20de%20la%20%20calidad%20de%20la%20educación%20superior\(1\).pdf](https://www.ueb.edu.ec/images/pdf/planeamiento/evalauacion%20intern a/(documento%20)%20política%20de%20evaluación%20institucional%20de%20universidades%20y%20escuelas%20politécnicas%20en%20el %20marco%20del%20sistema%20de%20aseguramiento%20de%20la%20%20calidad%20de%20la%20educación%20superior(1).pdf)
- Destinonegocio. (2015). 4 beneficios de contratar el servicio de gestión de la seguridad de la información para pequeñas y medianas empresas. Disponible en: <https://destinonegocio.com/pe/gestion-pe/4-beneficios-de-contratar-el-servicio-de-gestion-de-la-seguridad-de-la-informacion/>
- El Fray, I. (2012). A Comparative Study of Risk Assessment Methods, MEHARI

& CRAMM with a New Formal Model of Risk Assessment (FoMRA) in Information Systems. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 7564 LNCS, 428–442. <https://doi.org/10.1007/978-3-642-33260-9-37>

- Espinosa, D., Martínez, J., & Amador, S. (2014). Gestión del riesgo en la seguridad de la información con base en la Norma ISO/IEC 27005 de 2011, proponiendo una adaptación de la Metodología OCTAVE-S. Caso de estudio: proceso de inscripciones y admisiones en la división de admisión registro y control AC. *Ingenierías USBmed*, 5(2), 33. <https://doi.org/10.21500/20275846.309>
- Fernández, E. E. C., & Herrera, R. D. J. G. (2020). Prevención de riesgos por ciberseguridad desde la auditoría forense: conjugando el talento humano organizacional. *NOVUM*, 1(10), 61-80.
- Francischetti, C., Bertassi, A., Camargo, L., Padoveze, C., & Calil, J. (2014). El Análisis de riesgos como herramienta para la toma de decisiones relativas a inversiones. *Invenio: Revista de Investigación Académica*, 33, 73–85.
- Gallardo, S. (2018). Ciberseguridad industrial, seguridad de la información y negocio: ¿encuentro o divorcio?. *Sistemas*, (147), 43-64.
- Gómez-Suarez, Á. J. (2019). Diseño de un programa de ciberseguridad de una empresa basado en el Marco de Trabajo NIST.
- González, E. C. (2017). Importancia del Aprendizaje de Ciberseguridad ante los Riesgos de las Tecnologías de Información. *Tecnología Vital*, 1(1).
- González, J., Myer, R., & Pachón, W. (2017). La evaluación de los riesgos antrópicos en la seguridad corporativa: del Análisis Modal de Fallos y Efectos (AMFE) a un modelo de evaluación integral del riesgo. *Revista Científica General José María Córdova*, 15(19), 269. <https://doi.org/10.21830/19006586.81>
- Govindarajan, R., Molero, J., Tuset, V., Arellano, A., Ballester, R., Cardenal, J., Caro, M., Fernández, J., Jové, J., Luguera, E., Melero, A., Del Mar Puertas, M., Sal, R., Sánchez, J. L., Vidal, À., & Feliu, E. (2007). El análisis modal de fallos y efectos (AMFE) ayuda a aumentar la seguridad en radioterapia. *Revista de Calidad Asistencial*, 22(6), 299–309. [https://doi.org/10.1016/S1134-282X\(07\)71238-1](https://doi.org/10.1016/S1134-282X(07)71238-1)
- Hamidian-Fernández, B. F., & Ospino-Sumoza, G. R. (2015). ¿Por qué los sistemas de información son esenciales? *Anuario*, 38(2011), 161–183.

<http://servicio.bc.uc.edu.ve/derecho/revista/idc38/art07.pdf>

- Julio, M. L. G., & Rios, C. U. (2019). Evaluación del contexto organizacional en la gestión del riesgo de tecnología de información con un enfoque basado en COBIT. *Revista de Investigación en Tecnologías de la Información*, 7(14), 38-51.
- Kitchenham, B., & Charters, S. (2007). Performing systematic literature reviews in software engineering. *Proceedings - International Conference on Software Engineering, 2007*, 1051–1052. <https://doi.org/10.1145/1134285.1134500>
- Kluge, D., & Sambasivam, S. (2008). Formal Information Security Standards in German Medium Enterprises. *Phoenix Usa, 9000(Isms)*. <http://proc.conisar.org/2008/1533/CONISAR.2008.Kluge.pdf>
- Ley del Sistema Nacional de Registro de Datos Públicos, 53 *Journal of Chemical Information and Modeling* 1689 (2018). <https://doi.org/10.1017/CBO9781107415324.004>Linares Lizarazo, Y. (2018). ¿Cómo estamos en ciberseguridad nacional e internacional, su gestión de riesgos y tendencias?.
- Liu, H., Deng, X., & Jiang, W. (2017). Risk evaluation in failure mode and effects analysis using fuzzy measure and fuzzy integral. *Symmetry*, 9(8). <https://doi.org/10.3390/sym9080162>
- Lugani, C. F., & Peña, R. L. (2018). Desarrollo de un esquema de Gestión de Riesgos Informáticos en la Universidad Nacional de Río Negro. In XII Simposio de Informática en el Estado (SIE 2018)-JAIIO 47 (CABA, 2018).
- MARISMA Shield S.L.(2018). Marisma 3.0 Methodology for the Analysis of Risks of Information Security, based on Meta-Pattern and Adaptability.
- Martínez Landrove, N. (2019). Ciberseguridad y riesgo operacional en las organizaciones.
- Mateus, O. C. (2015). Metodología AMFE como herramienta de gestión de riesgo en un hospital universitario. *Cuadernos Latinoamericanos de Administración*, 11(21), 37-49.
- Mena, N. (2012). REDES SOCIALES Y GESTION DE LA INFORMACION: UN ENFOQUE DESDE LA TEEORIA DE GRAFOS. *CIENCIAS DE LA INFORMACION Y TECNOLOGIA*, 43, 10.
- Mere, H., & Humberto, M. (2019). Gestión de riesgos de seguridad de la información para empresas del sector telecomunicaciones.

- Molina García, J. A. (2019). La importancia de la gestión de riesgos y seguridad en el internet de las cosas (IOT).
- Montalvo, R. (2017). *Generación de políticas para la gestión de riesgos de seguridad en el desarrollo de software*. [ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO]. <http://dspace.esPOCH.edu.ec/handle/123456789/7224>
- Murillo, S. (2009). Beneficios Del Comercio Electrónico. *Perspectivas*, 24, 151–164.
- Naharro, F. J., Montañés, C. S., & Barrios, M. S. (2018). La transferencia de los riesgos cibernéticos en empresas internacionales con alto nivel de capitalización bursátil. *Revista de Pensamiento Estratégico y Seguridad CISDE*, 3(1), 67-90.
- Paredes-Atenciano, J. A., Roldán-Aviña, J. P., González-García, M., Blanco-Sánchez, M. C., Pinto-Melero, M. A., Pérez-Ramírez, C., Calvo Rubio-Burgos, M., Osuna-Navarro, F. J., & Jurado-Carmona, A. M. (2015). Análisis modal de fallos y efectos en las prescripciones farmacológicas informatizadas. *Revista de Calidad Asistencial*, 30(4), 182–194. <https://doi.org/10.1016/j.cali.2014.12.011>
- Parra, A., Santos, E., Crespo, S., & Fernández, E. (2013). *Desarrollando una metodología para gestionar los riesgos de seguridad asociativos y jerárquicos y tasar de forma objetiva los Sistemas de Información*. October.
- Roussos, A. (2011). *Preparación De Una Revisión Bibliográfica Para Su Publicación Cuando Un Solo Artículo Nos Habla De Muchos Trabajos*. 2005, 1–7.
- Santos, A., Sánchez, L., Fernández, E., & Piattini, M. (2012). A systematic review of methodologies and models for the analysis and management of associative and hierarchical risk in SMEs. *Proceedings of the 9th International Workshop on Security in Information Systems, WOSIS 2012, in Conjunction with ICEIS 2012*, 117–124. <https://doi.org/10.5220/0004102601170124>
- Santos, A., Sánchez, L., Fernández, E., & Piattini, M. (2015). Desarrollando una metodología de análisis de riesgos para que el sector asegurador pueda tasar los riesgos en las PYMES. *ResearchGate*, SEPTEMBER 2014, 2–5.
- Schneider, A. (2018). Ciberseguridad | Gestión de riesgo de ciberseguridad y utilidad neta. *AADECA Revista*, 8. Disponible en: https://www.editores-srl.com.ar/revistas/aa/8/schneider_ciberseguridad

- Shukla, N., & Kumar, S. (2012). A comparative study on information security risk analysis practices. *International Journal of Computer Applications, Special Is*(November), 975–8887.
- Tarazona, C. (2006). *AMENAZAS INFORMÁTICAS Y SEGURIDAD DE LA INFORMACIÓN*. 137–146.
- Tejena, M. (2018). Análisis de riesgos en seguridad de la información. *Polo Del Conocimiento*, 3(4), 230. <https://doi.org/10.23857/pc.v3i4.809>
- Tibaquira Cortes, Y. A. (2015). Metodología de gestión de incidentes de seguridad de la información y gestión de riesgos para la plataforma SIEM de una entidad financiera basada en la Norma ISO/IEC 27035 e ISO/IEC 27005.
- Tubío, P., López, C., & Rivas, J. (2019). Improving information security risk analysis by including threat-occurrence predictive models. *Computers & Security*, 88, 101609. <https://doi.org/10.1016/j.cose.2019.101609>
- Velázquez, B. M., Contrí, G. B., Saura, I. G., & Blasco, M. F. (2008). Análisis del comportamiento de queja del consumidor: una investigación exploratoria en el contexto de los restaurantes. *Investigaciones europeas de dirección y economía de la empresa*, 14(2), 13-33.
- Zambrano, N., & Zambrano, M. (2019). Ciberseguridad Y Su Aplicación En Las Instituciones De Educación Superior Públicas De Manabí [ESPAM MFL]. In *Espam*.
<http://repositorio.esпам.edu.ec/bitstream/42000/1032/1/TTMTI3.pdf>

ANEXOS

ANEXO 1
SOLICITUD DE INFORMACIÓN

Anexo 1.1. Solicitud del levantamiento de información.

REPÚBLICA DEL ECUADOR



ESPAMMFL

ESCUELA SUPERIOR POLITÉCNICA
ACROPOCUMBI - EC - PASTAZA - MIRIAM FÉLIX LÓPEZ



Oficio N.º: **ESPAM-MFL-CAPP-MTI-2020-002-O**
Calcuta, 21 de febrero de 2020

PARA: Ec. Miryam Félix López, Ph. D
RECTORA DE LA ESPAM MFL.

ASUNTO: Solicitud de Información para Trabajo de Titulación, Maestría en TI, cohorte II.

Reciba un cordial saludo de la Coordinación Académica de Programas de Posgrado de la ESPAM MFL, deseándole éxitos en sus labores diarias.

Como es de su conocimiento nuestra institución se encuentra ejecutando la Maestría en Tecnologías de la Información, Mención Redes y Sistemas Distribuidos, misma que consta de un proceso de titulación, en donde se realiza un trabajo de investigación previo a la obtención del título de Magister.

Es así que, con este antecedente, me es grato comunicarle que, la Ing. CEDEÑO SANTANA KARINA LISBETH y la Ing. LOOR VALENCIA GINA ELIZABETH, se encuentran ejecutando el trabajo de investigación titulado: **"ANÁLISIS DE CIBERSEGURIDAD EN LA ESPAM MFL, UTILIZANDO LAS METODOLOGÍAS AMFE Y MARISMA"**, por lo que, solicitamos a usted de la manera más comedida autorice a quien corresponda se brinde la apertura necesaria para hacer uso de la información respecto al análisis de Ciberseguridad que se realizó previamente por la Mg. Nerina Avellán y Fernanda Bravo; y así las mencionados Maestranes puedan realizar un trabajo de calidad que contribuya con su formación de cuarto nivel.

Esperando que lo solicitado sea atendido de la mejor manera anticipamos nuestro agradecimiento.

Atentamente,

Mg. Jessica Morales Carrillo
COORDINADORA ACADÉMICA MAESTRÍA EN TI.

Anexo 1.2. Fotos de reuniones para clasificar la información recopilada de la ESPAM MFL.



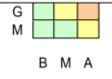

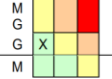
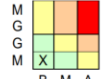
ANEXO 2
MATRIZ AMFE DE CIBERSEGURIDAD EN LA ESPAM MFL

Anexo 2.1. Matriz de riesgos según la metodología AMFE, dominio Seguridad de la Información.

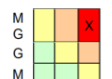
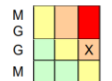
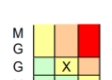
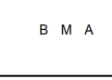
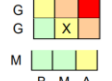
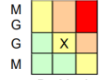

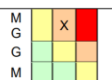
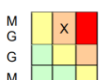
ID. Riesgo	Vulnerabilidades	Probabilidad	Impacto	Nivel	Matriz de Riesgos	Responsable	Mitigación acción ID	Acciones de mitigación	Criterio de aceptación
R.1.1.	No se monitorea el acceso a los sistemas de información web.	Alto	Grave	Alto		Coordinador TI	A.1.1.1	Utilizar herramientas tecnológicas para el monitoreo del acceso a los sistemas de información.	Reportes de acceso a los sistemas mediante autenticación de usuario.
		3	2						
R.1.2.	No se mantiene preparación continua en Ciberseguridad en la institución.	Alto	Muy Grave	Critico		Coordinador TI	A.1.2.1	Capacitar al personal de TI en ciberseguridad de manera continua.	Capacitación a Congresos, seminarios, Talleres de seguridad informática.
		3	3						
R.1.3.	No se estandarizan los datos en base a normas de calidad.	Alto	Muy Grave	Critico		Coordinador TI	A.1.3.1	Estandarizar la gestión de calidad de los procesos de la información mediante normas de calidad.	Mejorar la calidad de los procesos de seguridad de la información en el ciberespacio
		3	3						
R.1.4.	No emplean normas de calidad como ISO, INEN, Control interno, entre otras para la estandarización de sus procesos.	Alto	Muy Grave	Critico		Coordinador TI	A.1.4.1	Implementar Normas de calidad como ISO 9000 y normas de control interno 410-09 para mejorar la calidad de los servicios y brindar seguridad en sus procesos.	Mejorar la gestión de calidad de los procesos y seguridad de la información
		3	3						
R.1.5.	No aplican regulaciones de normas en escenarios de seguridad.	Alto	Muy Grave	Critico		Coordinador TI	A.1.5.1	Aplicar Normas de Control Interno 410-09 de TI de la Contraloría	Complementar con norma ISO/IEC 27001 Sistema de
		3	3					General del Estado ecuatoriano para escenarios de seguridad.	Gestión de Seguridad de la información
R.1.6.	No se alerta a los usuarios cuando existe algún tipo de ataque o implementación de controles de seguridad.	Alto	Grave	Alto		Coordinador TI	A.1.6.1	Informar a los usuarios de los controles de seguridad en los sistemas y de los ataques que se han presentado en los mismos a nivel institucional.	Reporte e informe de ataques y controles de seguridad a los usuarios.
		3	2						
R.1.7.	No emplean normas en escenarios de ciberseguridad.	Alto	Muy Grave	Critico		Coordinador TI	A.1.7.1	Seguir el plan propuesto de Ciberseguridad	Mejorar el escenario de ciberseguridad
		3	3						
R.1.8.	Los manuales de usuario para el manejo de los sistemas de información están en proceso de elaboración.	Medio	Grave	Medio		Coordinador TI	A.1.8.1	Implementar manuales de usuarios para el uso efectivo de los sistemas o aplicaciones web.	Aplicar controles internos periódicos de cumplimiento.
		2	2						
R.1.9	No se llevan a cabo los datos de informes como estrategia para la continuidad del negocio.	Medio	Grave	Medio		Coordinador TI	A.1.9.1	Elaborar estrategias para mejorar los servicios TI.	PETI (Plan estratégico de Tecnologías de Información)
		2	2						
R.1.10.		Medio	Grave	Medio		Coordinador TI	A.1.10.1		
	Han sufrido ataques de robo de identidad o robo de información de los usuarios en Aplicaciones web.	2	2					Elaborar medidas de prevención contra ataques de robo de información de los usuarios en aplicaciones web.	Mejorar la seguridad de las aplicaciones.
R.1.11.	Los tipos de ataques que se han presentado en la unidad son: DDoS, Dos.	Alto	Muy Grave	Critico		Coordinador TI	A.1.11.1	Utilizar herramientas tecnológicas para el monitoreo del acceso a los sistemas de información.	Mejorar controles contra ataques cibernéticos.
		3	3						
R.1.12.	No se usan técnicas de visualización de datos para presentar información de eventos.	Medio	Grave	Medio		Coordinador TI	A.1.12.1	Elaborar técnicas de visualización de datos para verificar la pérdida de información.	Escalabilidad y disponibilidad de las aplicaciones.
		2	2						

Anexo 2.2. Matriz de riesgos según la metodología AMFE, dominio Seguridad de las Aplicaciones

ID. Riesgo	Vulnerabilidades	Probabilidad	Impacto	Nivel	Matriz de Riesgos	Responsable	Mitigación acción ID	Acciones de mitigación	Criterio de aceptación
R.2.1	No tienen un plan de seguridad para todo el ciclo de vida del desarrollo del software (SDLC), desde su desarrollo, pasando por las pruebas y producción.	Alto	Muy Grave	Crítico		Área de desarrollo de aplicaciones	A.2.1.1	Elaborar un plan de seguridad para todo el ciclo de desarrollo, prueba, y retroalimentación de las aplicaciones	Madurez en los procesos de desarrollo de aplicaciones.
R.2.2		Medio	Alto						
	realizar pruebas de vulnerabilidades.	2	2					sugiere la norma ISO/IEC 27032 de ciberseguridad.	detectar vulnerabilidades.
R.2.7	No se han realizado pruebas de penetración o pentest a las aplicaciones, incluidas la red, la plataforma de alojamiento y la aplicación en sí, para verificar las medidas de seguridad que protegen la aplicación tanto internas como externas.	Medio	Muy Grave	Alto		Área de desarrollo de aplicaciones	A.2.7.1	Implementar esta prueba de pentest para verificar las medidas de seguridad de las aplicaciones, red, plataforma de alojamiento, aplicación o sistemas web.	Proteger las aplicaciones de ataques cibernéticos.
		2	3						
R.2.8	No se establecen responsables y procedimientos formales de aplicación de seguridad en los equipos tecnológicos y software.	Medio	Muy Grave	Alto		Área de desarrollo de aplicaciones y Coordinador TI	A.2.8.1	Establecer responsabilidades y procedimientos formales a custodios de los equipos tecnológicos y software para el buen uso y seguridad de las aplicaciones.	Políticas de seguridad de los equipos tecnológicos y software a cargo de los custodios.
		2	3						
R.2.9	No se aprueban de manera formal los cambios de equipos tecnológicos y software.	Medio	Grave	Medio		Coordinador TI	A.2.9.1	Elaborar actas de entrega-recepción de equipos tecnológicos cuando haya cambios de custodios.	Seguridad en los cambios de equipos tecnológicos y software.
		2	2						
R.2.10	La unidad no posee alertas o fallas de los sistemas de información, sitios web, equipos tecnológicos.	Medio	Muy Grave	Alto		Área de desarrollo de aplicaciones y Coordinador TI	A.2.10.1	Realizar reportes o informes de eventos maliciosos o fallas en los sistemas de información, sitios web, equipos tecnológicos.	Mantener la seguridad de los sistemas en el ciberespacio.
		2	3						
R.2.11	El equipo de desarrollo no aplica seguimientos o revisión en los mensajes recibidos en	Medio	Muy Grave	Alto		Área de desarrollo de	A.2.11.1	Asegurar que los mensajes recibidos en los sitios web no contengan contenido malicioso,	Seguimiento de la seguridad de las aplicaciones.
	El departamento de tecnología no cuenta con una metodología y procesos de desarrollo de aplicaciones maduros.	2	Muy Grave			Área de desarrollo de aplicaciones		Elaborar flujogramas de procesos de desarrollo con metodologías ágiles como SCRUM.	Mejora de los procesos de desarrollo de aplicaciones.
R.2.3	La universidad no cuenta con el personal, capacitación y herramientas especializadas en la seguridad de las aplicaciones para contrarrestar los riesgos que implican las ciberamenazas.	Medio	Grave	Medio		Área de desarrollo de aplicaciones	A.2.3.1	Contratar talento humano especializado o capacitar al personal necesario en seguridad de las aplicaciones.	Contrarrestar los riesgos que implican las ciberamenazas.
		2	2						
R.2.4	El departamento de tecnología no ha establecido un protocolo de autoevaluación de control para monitorear, medir e informar la efectividad de las prácticas de seguridad de aplicaciones e identificar lo que no se hizo bien para mejorar continuamente la práctica.	Medio	Grave	Medio		Área de desarrollo de aplicaciones	A.2.4.1	Elaborar un protocolo de autoevaluación de control para la efectividad de la seguridad de las aplicaciones.	Trabajar con la norma de seguridad de las aplicaciones ISO/IEC 27034
		2	2						
R.2.5	No se utilizan herramientas tecnológicas para realizar pruebas de vulnerabilidades altamente probables, sospechosas y potenciales de criticidad variable.	Medio	Muy Grave	Alto		Área de desarrollo de aplicaciones	A.2.5.1	Utilizar las herramientas tecnológicas que brinda la norma ISO/IEC 27032 de ciberseguridad para efectuar pruebas de vulnerabilidades en las aplicaciones.	Nessus, Acunetix, Shodan
		2	3						
R.2.6	No utilizan herramientas tecnológicas como SAST, DAST, RASP, SCA para	Medio	Grave	Medio		Área de desarrollo de aplicaciones	A.2.6.1	Aplicar al menos una de estas herramientas o en su defecto utilizar las herramientas que	Pruebas regulares con estas herramientas para

	el sitio, para asegurarse que no contengan algún tipo de contenido malicioso o enlaces de sitios web de phishing o descargas maliciosas.	2	3			aplicaciones y Área de Redes		enlaces de sitios web de phishing o descargas maliciosas.	
R.2.12.	No se logra los objetivos desarrollados en base a la sensibilización y formación en proporcionar informes periódicos sobre el estado de la Ciberseguridad, Sesiones de formación enfocada en escenarios simulados de ataque cibernética o talleres sobre áreas requeridas de acciones específicas y tampoco en pruebas regulares con recorridos en escenarios permanentes.	Medio	Grave	Medio		Coordinador TI	A.2.12.1	Considerar como objetivos de sensibilización y formación a informes periódicos sobre el estado de ciberseguridad, enfoques de escenarios simulados de ataques cibernéticos o talleres de acciones específicas y pruebas regulares en escenarios permanentes.	Mejorar la ciberseguridad.
		2	2						
R.2.13.	No se prohíbe el uso de software no autorizado por la institución.	Bajo	Grave	Bajo		Coordinador TI	A.2.13.1	Usar software legal o software libre según lo requiera la aplicación a desarrollar.	Visual, SQL, Windows, Linux
		1	2						
R.2.14.	No se mantienen los sistemas operativos actualizados con las últimas versiones.	Bajo	Menor	Bajo		Coordinador TI	A.2.14.1	Mantener actualizados los sistemas operativos de acuerdo a las características de los equipos.	Mejorar la productividad del desarrollo de aplicaciones.
		1	1						

Anexo 2.3. Matriz de riesgos según la metodología AMFE, dominio Seguridad de las Redes.

ID. Riesgo	Vulnerabilidades	Probabilidad	Impacto	Nivel	Matriz de Riesgos	Responsable	Mitigación acción ID	Acciones de mitigación	Criterio de aceptación
R.3.1.	La unidad no tiene medidas de prevención y respuestas a los ataques cibernéticos.	Alto	Muy Grave	Critico		Coordinador TI	A.3.1.1	Elaborar indicadores de prevención y respuestas para tomar medidas de seguridad frente a ataques cibernéticos.	Controlar los ataques cibernéticos.
		3	3						
R.3.2.	No se realiza informes de eventos sospechosos o encuentros maliciosos en las redes.	Alto	Grave	Alto		Coordinador TI y Área de Redes	A.3.2.1	Elaborar o adquirir una herramienta que permita detectar eventos maliciosos en las redes y emitan reportes de los mismos.	Informes mensuales de eventos sospechosos o maliciosos en las redes.
		3	2						
R.3.3.	Entre las políticas, procedimientos y controles que están en proceso de aprobación en la unidad para seguridad de la red están: Políticas de control de acceso a la red, controles de acceso a los servidores, procedimientos de respaldo de la información cuando existen pérdidas de fallos físicos, control de filtros de tráfico en la red interna y externa.	Medio	Grave	Medio		Coordinador TI, Área de Redes y Área de Datos (Data Center)	A.3.4.1	Agilizar el proceso de aprobación de las políticas, procedimientos y controles de la seguridad de la red.	Política de control de acceso, política de filtros de tráfico en la red interna y externa.
		2	2						
R.3.4.	No tienen protocolos de autenticación de computadoras dentro de la red.	Medio	Grave	Medio		Área de Redes.	A.3.5.1	Utilizar protocolos de autenticación de computadoras dentro de la red para evitar posibles ataques.	Evitar los ataques de Man in the middle.
		2	2						
R.3.5.	No existen controles que restrinjan la dirección MAC de cada equipo.	Medio	Grave	Medio		Área de Redes.	A.3.6.1	Autenticar los equipos para que haya mayor control y seguridad en la comunicación entre equipos.	Mejorar la seguridad en las redes.
		2	2						
R.3.6.	El director /coordinador de la unidad no se asegura que la URL de su contenido web este citado como un enlace seguro en su navegador.	Medio	Grave	Medio		Coordinador TI	A.3.7.1	Asegurar que toda la información que vaya a subirse en una aplicación web, debe estar con un enlace seguro en la URL. Como HTTPS.	Proteger la información en el ciberespacio
		2	2						
R.3.7.	El SSL que utiliza el sitio web, no identifica el contenido original del nuevo contenido dañado, plantado por un atacante.	Medio	Muy Grave	Alto		Área de Redes.	A.3.8.1	Verificar que el tráfico de la información esté cifrado para evitar ataques como DDoS.	SSL certificado.
		2	3						
R.3.8.	Utilizan protocolos de comunicación como HTTP.	Medio	Muy Grave	Alto		Área de Redes y Área de desarrollo de aplicaciones.	A.3.9.1	Utilizar protocolos de comunicación seguro en el ciberespacio como HTTPS.	Mejorar la Seguridad en la transmisión de datos en las redes.
		2	3						

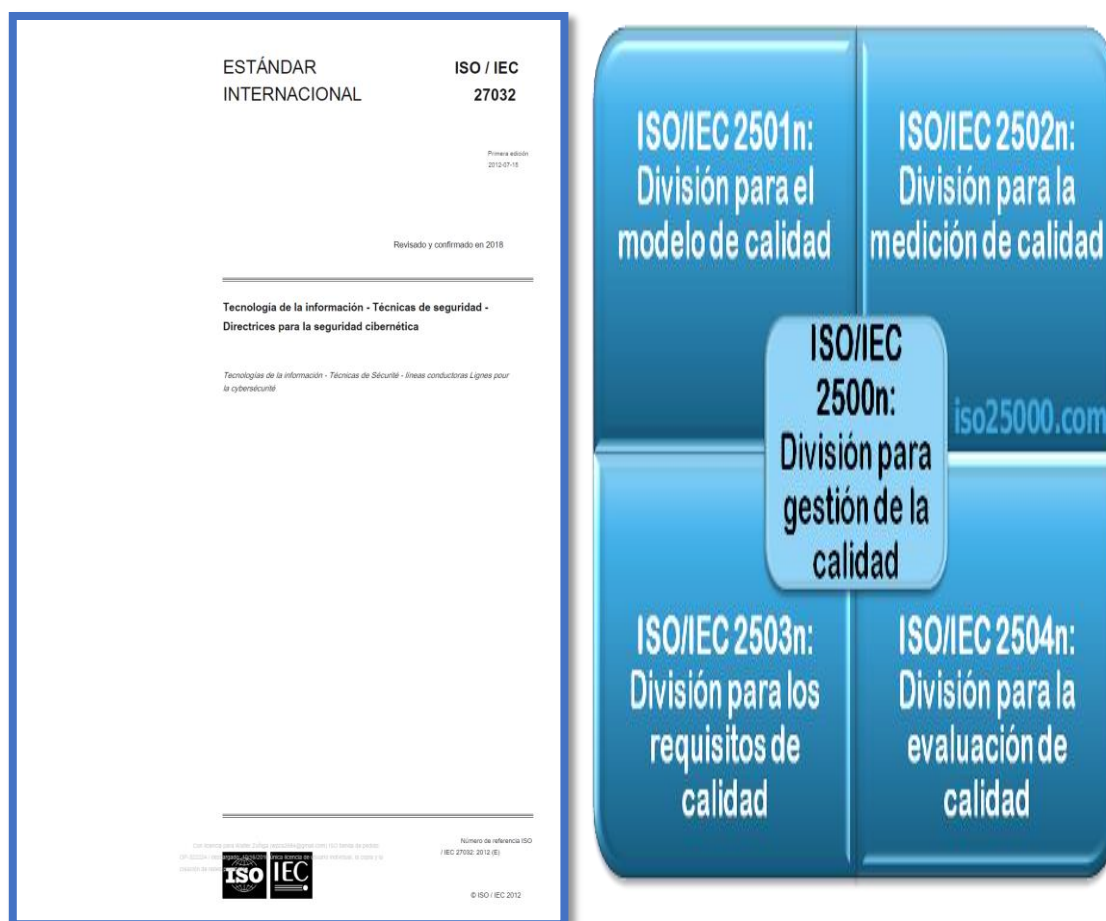
ANEXO 3
PLATAFORMA DE EMARISMA

Anexo 3.1. Plataforma eMARISMA, usuario de proyectos de riesgos.

Producto software ISO 25000 Acreditación PERSONAL AENOR conform

Anexo 3.2. Plataforma eMARISMA, usuario para patrones y análisis de riesgos.

Anexo 3.3. Normas ISO 27032, 25001



Anexo 3.4. Tipos de activos en eMarisma.

Código	Nombre	Fecha Creación	Acciones
ASI01	Activo Físicos	23/4/2020 6:58:29	 
ASI02	Activos Información	23/4/2020 6:59:10	 
ASI03	Activos de servicios	23/4/2020 7:0:8	 
ASI04	Activos Personales	23/4/2020 7:1:10	 

ANEXO 4
PLAN DE GESTIÓN DE RIESGOS

ESCUELA SUPERIOR POLITÉCNICA
AGROPECUARIA DE MANABÍ
MANUEL FÉLIX LÓPEZ



PLAN DE GESTIÓN DE RIESGOS DE
CIBERSEGURIDAD DE LA ESPAM MFL,
BASADO EN LAS METODOLOGÍAS AMFE Y
MARISMA

AGOSTO 2020

CONTENIDO

1. INTRODUCCIÓN.....	50
2. OBJETIVOS	52
1.1. OBJETIVO GENERAL.....	52
1.2. OBJETIVOS ESPECÍFICOS.....	52
3. ALCANCE	52
4. GESTIÓN DE RIESGOS EN CIBERSEGURIDAD DE LA ESPAM MFL ...	53
4.1.1. PROCESOS DE LA METODOLOGÍA DE RIESGOS AMFE PARA CIBERSEGURIDAD.....	55
4.1.2. PROCESOS DE IMPLEMENTACIÓN DE MARISMA PARA LA GESTIÓN DE RIESGOS EN CIBERSEGURIDAD.....	59
4.1.2.1. PROCESO 1: GENERACIÓN DE PATRONES PARA EL ANÁLISIS DE RIESGOS (GPRA).	59
4.1.2.2. PROCESO 2: GENERACIÓN DEL ANÁLISIS Y GESTIÓN DEL RIESGO (GARM).	61
4.1.2.3. PROCESO 3: MANTENIMIENTO DINÁMICO DEL ANÁLISIS DE RIESGOS (DRM).	64
5. ACCIONES DE MEJORA PARA EVITAR RIESGOS APLICANDO MARISMA.....	66
6. CONCLUSIONES.....	66
BIBLIOGRAFÍAS.....	67

1. INTRODUCCIÓN

Desarrollando una metodología en la actualidad, generar gran importancia en las empresas de todos los campos, de análisis de riesgos para que el sector asegurador pueda tasar los riesgos dentro de una sociedad gobernada por la información, las empresas y en particular de la capacidad de información que manejan; dado que al hablar de activos, las aseguradoras se enfrentan a la problemática de que no existen metodologías de Análisis de Riesgos adecuadas que permitan tasar y garantizar la información de forma objetiva (Saltos-Olmo, 2014).

La calidad del producto, junto con la calidad del proceso, es uno de los aspectos más importantes actualmente en el desarrollo de Software, relacionada con la calidad del producto, recientemente ha aparecido la familia de normas ISO/IEC 25000, que proporciona una guía para el uso de la nueva serie de estándares internacionales llamada Requisitos y Evaluación de Calidad de Productos de Software (*SQuaRE – System and Software Quality Requirements and Evaluation*) (Rcamara, 2020).

ISO/IEC 25000 constituye una serie de normas basadas en ISO/IEC 9126 y en ISO/IEC 14598 cuyo objetivo principal es guiar el desarrollo de los productos de software mediante la especificación de requisitos y evaluación de características de calidad (Rcamara, 2020).

Por otro lado, Sicaman ha recibido la certificación de AENOR de conformidad con ISO/IEC 25000 – Adecuación Funcional, para Marisma, en la evaluación de la adecuación funcional realizada por el laboratorio acreditado AQCLab, dicho producto ha alcanzado el máximo nivel de calidad (Rcamara, 2020).

Esta certificación se ha realizado gracias a la colaboración entre AENOR, el laboratorio AQCLab y SICAMAN-NT, siguiendo el proceso de evaluación y certificación de la calidad del producto software. Así, AQCLab ha realizado la evaluación del producto software MARISMA y ha apoyado a SICAMAN-NT en la mejora de la calidad del mismo para lograr la certificación ISO/IEC 25000 (Rcamara, 2020).

MARISMA como un producto certificado en calidad, permite analizar los riesgos de compañías de forma dinámica y basado en patrones reutilizables y adaptables (Rcamara, 2020).

Dado que es herramienta que optimiza el análisis y gestión de riesgos de negocio, en donde los usuarios agilitan el análisis de riesgo de su compañía reduciendo los tiempos de forma notoria, así como gestionar de forma dinámica la evolución de los riesgos oportunamente (ISO, 2019).

Entre las funcionalidades proporcionadas por MARISMA, se incluyen la generación de checklist para valorar el estado de dominios, objetivos, y controles, la generación de planes detallado de tratamiento para solucionar los controles y la generación automática de análisis de riesgo, en base a las valoraciones de activos y posibles amenazas, para llevar a cabo matrices de control y evaluación de los riesgos (ISO, 2019).

Además, incorpora dentro de la misma herramienta, un sistema de gestión de eventos a diferencias de metodologías tradicionales, mediante mecanismos para localizar los eventos o incidencias que afectan al riesgo, re-alimentan el sistema para determinar un plan de tratamiento y actualizar el riesgo del proceso en cada momento de forma dinámica al momento de ser implementada.

2. OBJETIVOS

I.1. OBJETIVO GENERAL

Implementar el plan de gestión del riesgo, en base a los resultados de las metodologías AMFE y MARISMA en ciberseguridad de la ESPAM MFL.

I.2. OBJETIVOS ESPECÍFICOS

- Determinar los patrones de riesgos en ciberseguridad en la Unidad de Tecnología de la ESPAM MFL.
- Efectuar el análisis y gestión de riesgos en eMARISMA, según los datos de la metodología AMFE.
- Generar acciones de mejora según el mantenimiento dinámico proporcionado por la herramienta.

3. ALCANCE

Para llevar a cabo el siguiente plan de gestión de riesgos, se consideraron los siguientes lineamientos:

- Definición de patrones para el análisis de riesgos de ciberseguridad en la Unidad de tecnología.
- Generación de análisis y gestión del riesgo según el levantamiento de información de la metodología AMFE y MARISMA en ciberseguridad.
- Creación de acciones de mejora, conforme los resultados del mantenimiento dinámico de los sistemas de información de la Institución.

4. GESTIÓN DE RIESGOS EN CIBERSEGURIDAD EN LA ESPAM MFL

En la Escuela Superior Politécnica Agropecuaria de Manabí ESPAM MFL, se encuentra la Unidad de Tecnología que se encarga del desarrollo de software y hardware, servicios de red, soporte técnico y mantenimiento a los equipos de cómputo, de tal manera, dicho departamento tiene el deber de elaborar e implementar políticas que aseguren el buen uso de los recursos informáticos, por parte de los usuarios de la institución, quienes lo utilizan para el progreso de sus actividades laborales (ESPAM MFL, 2019).

En los actuales momentos la Unidad se encuentra aplicando nuevas reformas en aspectos Legales y Normativos, como son las normas de control interno para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos, como consta en la norma 410 Tecnologías de la Información, en la que menciona, que toda entidad pública debe contar con una unidad de Tecnología de Información (Figura 1) y estas elaborar manuales de políticas, como lo indica el apartado 410-04 manual de políticas y procesos (ESPAM MFL, 2019).

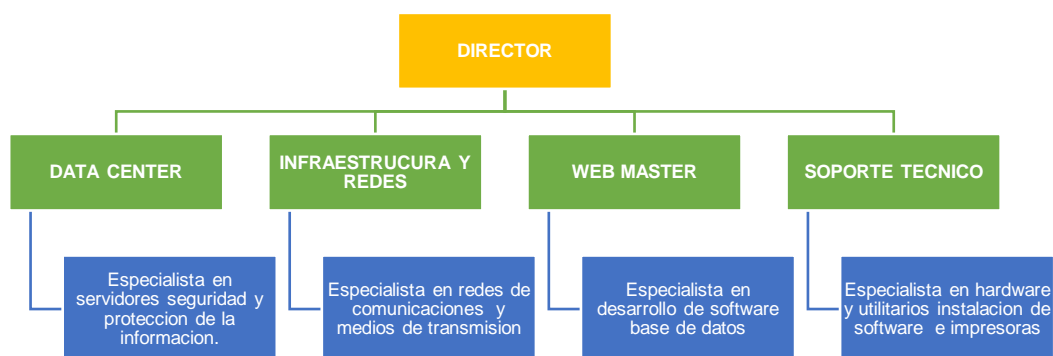


Figura 1. Organigrama Estructural de la Unidad de Tecnología de la ESPAM MFL.

Fuente: (ESPAM MFL, 2019)

Por otro lado, con lo que respecta a la Ciberseguridad, se basa en las actividades necesarias para la protección de infraestructuras críticas, y, al mismo tiempo, una protección adecuada de los servicios de infraestructura crítica contribuye a las necesidades básicas: seguridad, fiabilidad y disponibilidad de la infraestructura crítica, para llevar a cabo las medidas y control en los sistemas de información de la unidad de tecnologías, de acuerdo al cumplimiento de

normas internacionales de calidad y metodologías de riesgos, en donde se especifica las acciones a tomar para llevar a cabo una adecuada aplicación en cuanto a la prevención y mitigación de los riesgos de vulnerabilidades y posibles amenazas o ataques presentes y futuros dentro del área de auditoría informática aplicada a mantenimientos dinámicos de proceso de gestión de riesgos (Figura 2).

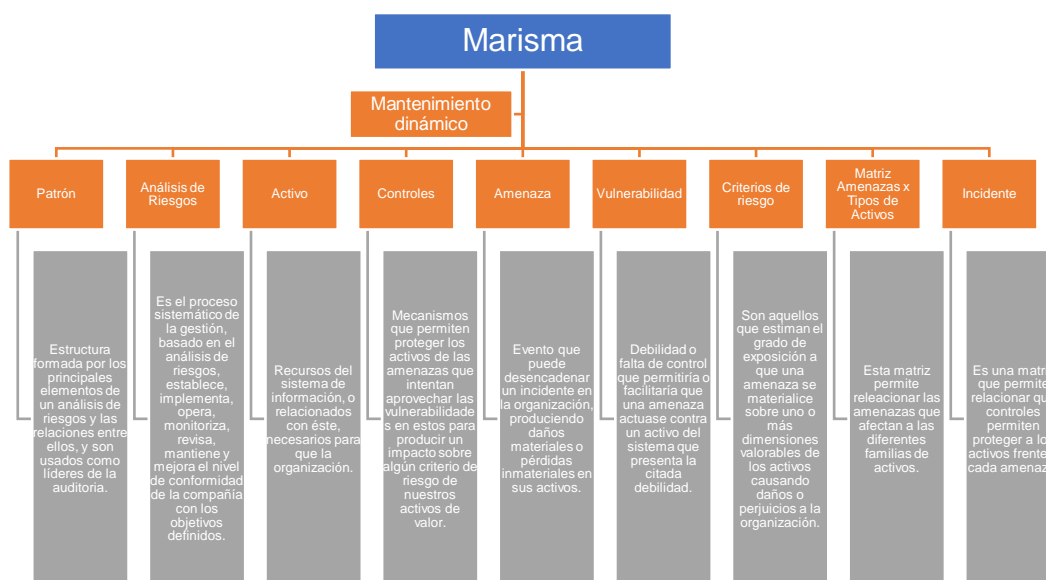


Figura 2. Estructura de Marisma.
Fuente: (Marisma, 2018)

Cabe indicar que para análisis de riesgos en eMarisma, se debe ingresar información mediante dos roles de usuario, uno que comprende a la creación de proyectos de gestión de riesgos (figura 3), y otro que se trabaja para la gestión de patrones y componentes previos para el análisis (figura 4).

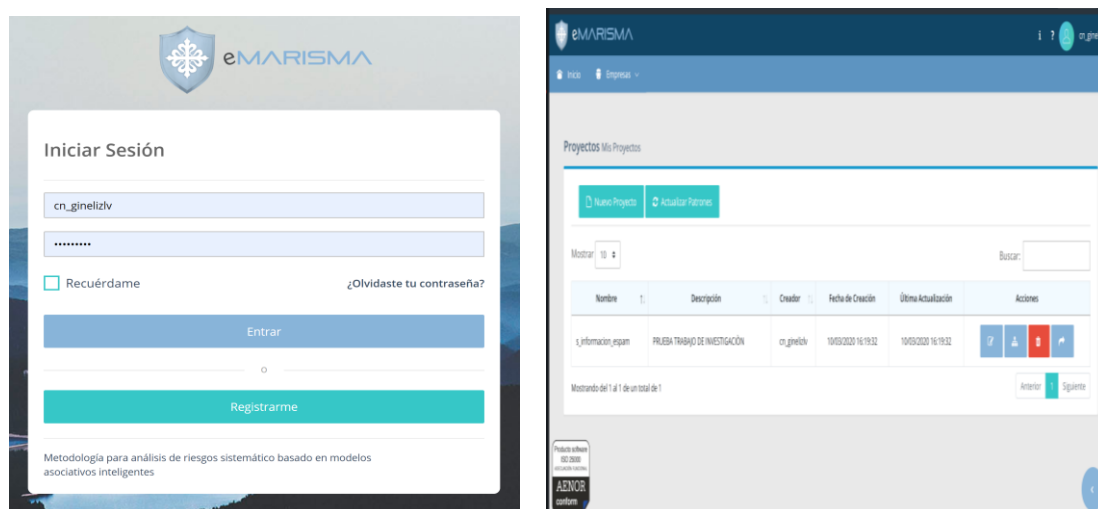


Figura 3. Usuario para creación de proyectos de gestión de riesgos.
Fuente: (Marisma, 2018)

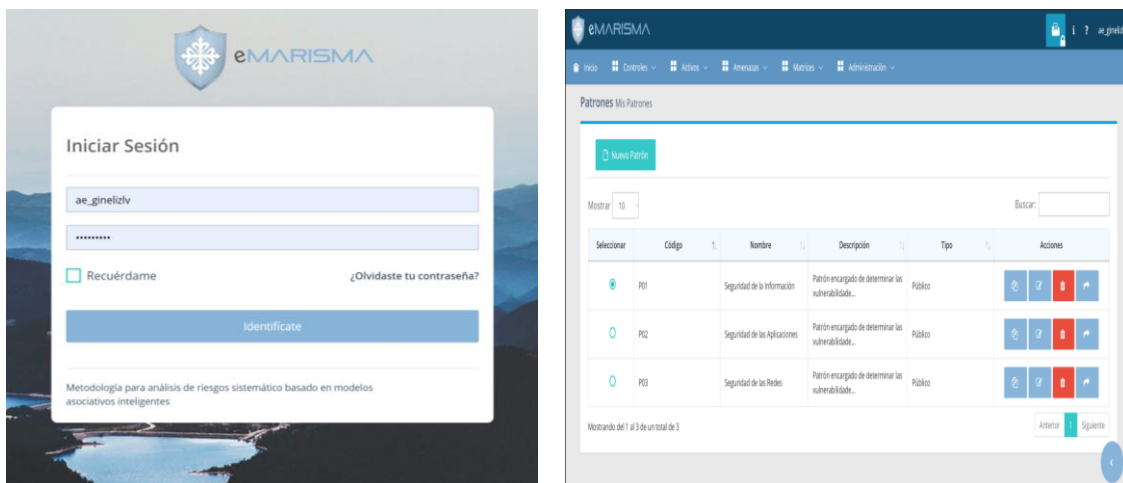


Figura 4. Usuario para gestión de patrones y componentes previos al análisis.
Fuente: (Marisma, 2018)

4.1.1. PROCESOS DE LA METODOLOGÍA DE RIESGOS AMFE PARA CIBERSEGURIDAD

Esta metodología tiene como procesos de análisis de riesgos de ciberseguridad las fases de Identificación, Análisis del impacto y de la probabilidad de ocurrir a partir de vulnerabilidades o amenazas, en las que lleva a cabo componentes como probabilidad, impacto, nivel, acciones de mitigación y criterios de aceptación (Figura 5); que una vez determinados se procede a elevar un plan de contingencia o acción para la respectiva aplicación de estrategias correctivas/preventiva, conforme la monitorización de los parámetros de prioridad (gravedad y seguridad) en sistemas de información alojados en infraestructuras tecnológicas.

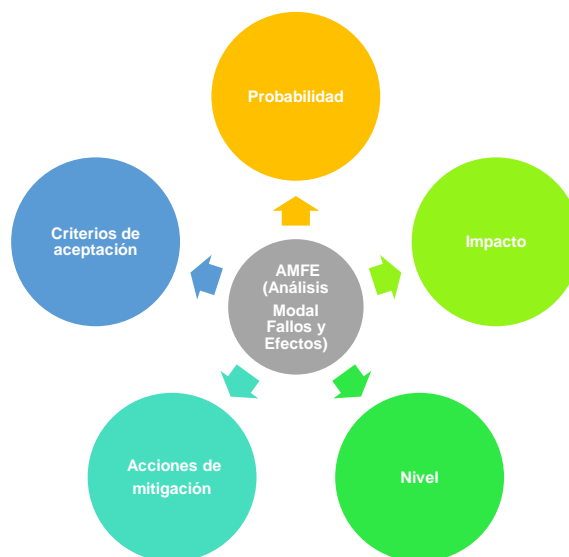


Figura 5. Componentes de AMFE (Análisis Modal Fallos y Efectos).
Fuente: Propia.

En lo que respecta a la ESPAM MFL, esta metodología partió del listado de vulnerabilidades de la propuesta “Plan de Acción de Ciberseguridad 2019”, que fueron llevadas a las matrices AMFE, en donde indicaban la prioridad del riesgo según el tipo de dominio definición en seguridad de la información, seguridad de aplicación y seguridad de redes de los sistemas distribuidos de la Institución, a los que pueden ser propensos a sufrir ataques en ciberseguridad de no tomar en cuenta los riesgos encontrados y la mayor incidencia según el caso.

- Dominio Seguridad de la Información.

ID. Riesgo	Vulnerabilidades	Probabilidad	Impacto	Nivel	Matriz de Riesgos	Responsable	Mitigación acción ID	Acciones de mitigación	Criterio de aceptación
R.1.1.	No se monitorea el acceso a los sistemas de información web.	Alto	Grave	Alto		Coordinador TI	A.1.1.1	Utilizar herramientas tecnológicas para el monitoreo del acceso a los sistemas de información.	Reportes de acceso a los sistemas mediante autenticación de usuario.
		3	2						
R.1.2.	No se mantiene preparación continua en Ciberseguridad en la institución.	Alto	Muy Grave	Critico		Coordinador TI	A.1.2.1	Capacitar al personal de TI en ciberseguridad de manera continua.	Capacitación a Congresos, seminarios, Talleres de seguridad informática.
		3	3						
R.1.3.	No se estandarizan los datos en base a normas de calidad.	Alto	Muy Grave	Critico		Coordinador TI	A.1.3.1	Estandarizar la gestión de calidad de los procesos de la información mediante normas de calidad.	Mejorar la calidad de los procesos de seguridad de la información en el ciberespacio
		3	3						
R.1.4.	No emplean normas de calidad como ISO, INEN, Control interno, entre otras para la estandarización de sus procesos.	Alto	Muy Grave	Critico		Coordinador TI	A.1.4.1	Implementar Normas de calidad como ISO 9000 y normas de control interno 410-09 para mejorar la calidad de los servicios y brindar seguridad en sus procesos.	Mejorar la gestión de calidad de los procesos y seguridad de la información
		3	3						
R.1.5.	No aplican regulaciones de normas en escenarios de seguridad.	Alto	Muy Grave	Critico		Coordinador TI	A.1.5.1	Aplicar Normas de Control Interno 410-09 de TI de la Contraloría	Complementar con norma ISO/IEC 27001 Sistema de

		3	3					General del Estado ecuatoriano para escenarios de seguridad.	Gestión de Seguridad de la información
R.1.6.	No se alerta a los usuarios cuando existe algún tipo de ataque o implementación de controles de seguridad.	Alto	Grave	Alto		Coordinador TI	A.1.6.1	Informar a los usuarios de los controles de seguridad en los sistemas y de los ataques que se han presentado en los mismos a nivel institucional.	Reporte e informe de ataques y controles de seguridad a los usuarios.
		3	2						
R.1.7.	No emplean normas en escenarios de ciberseguridad.	Alto	Muy Grave	Critico		Coordinador TI	A.1.7.1	Seguir el plan propuesto de Ciberseguridad	Mejorar el escenario de ciberseguridad
		3	3						
R.1.8.	Los manuales de usuario para el manejo de los sistemas de información están en proceso de elaboración.	Medio	Grave	Medio		Coordinador TI	A.1.8.1	Implementar manuales de usuarios para el uso efectivo de los sistemas o aplicaciones web.	Aplicar controles internos periódicos de cumplimiento.
		2	2						
R.1.9	No se llevan a cabo los datos de informes como estrategia para la continuidad del negocio.	Medio	Grave	Medio		Coordinador TI	A.1.9.1	Elaborar estrategias para mejorar los servicios TI.	PETI (Plan Tecnológico de Información)
		2	2						
R.1.10.		Medio	Grave	Medio		Coordinador TI	A.1.10.1		

	Han sufrido ataques de robo de identidad o robo de información de los usuarios en Aplicaciones web.							Elaborar medidas de prevención contra ataques de robo de información de los usuarios en aplicaciones web.	Mejorar la seguridad de las aplicaciones.
		2	2						
R.1.11.	Los tipos de ataques que se han presentado en la unidad son: DDoS, Dos.	Alto	Muy Grave	Critico		Coordinador TI	A.1.11.1	Utilizar herramientas tecnológicas para el monitoreo del acceso a los sistemas de información.	Mejorar controles contra ataques cibernéticos.
		3	3						
R.1.12.	No se usan técnicas de visualización de datos para presentar información de eventos.	Medio	Grave	Medio		Coordinador TI	A.1.12.1	Elaborar técnicas de visualización de datos para verificar la pérdida de información.	Escalabilidad y disponibilidad de las aplicaciones.
		2	2						

- Dominio Seguridad de las Aplicaciones

ID. Riesgo	Vulnerabilidades	Probabilidad	Impacto	Nivel	Matriz de Riesgos	Responsable	Mitigación acción ID	Acciones de mitigación	Criterio de aceptación
R.2.1	No tienen un plan de seguridad para todo el ciclo de vida del desarrollo del software (SDLC), desde su desarrollo, pasando por las pruebas y producción.	Alto	Muy Grave	Crítico		Área de desarrollo de aplicaciones	A.2.1.1	Elaborar un plan de seguridad para todo el ciclo de desarrollo, prueba, y retroalimentación de las aplicaciones	Madurez en los procesos de desarrollo de aplicaciones.
R.2.2		Medio	Alto				A.2.2.1		
	realizar pruebas de vulnerabilidades.	2	2					sugiere la norma ISO/IEC 27032 de ciberseguridad.	detectar vulnerabilidades.
R.2.7	No se han realizado pruebas de penetración o pentest a las aplicaciones, incluidas la red, la plataforma de alojamiento y la aplicación en sí, para verificar las medidas de seguridad que protegen la aplicación tanto internas como externas.	Medio	Muy Grave	Alto		Área de desarrollo de aplicaciones	A.2.7.1	Implementar esta prueba de pentest para verificar las medidas de seguridad de las aplicaciones, red, plataforma de alojamiento, aplicación o sistemas web.	Proteger las aplicaciones de ataques cibernéticos.
		2	3						
R.2.8	No se establecen responsables y procedimientos formales de aplicación de seguridad en los equipos tecnológicos y software.	Medio	Muy Grave	Alto		Área de desarrollo de aplicaciones y Coordinador TI	A.2.8.1	Establecer responsabilidades y procedimientos formales a custodios de los equipos tecnológicos y software para el buen uso y seguridad de las aplicaciones.	Políticas de seguridad de los equipos tecnológicos y software a cargo de los custodios.
		2	3						
R.2.9	No se aprueban de manera formal los cambios de equipos tecnológicos y software.	Medio	Grave	Medio		Coordinador TI	A.2.9.1	Elaborar actas de entrega-recepción de equipos tecnológicos cuando haya cambios de custodios.	Seguridad en los cambios de equipos tecnológicos y software.
		2	2						
R.2.10	La unidad no posee alertas o fallas de los sistemas de información, sitios web, equipos tecnológicos.	Medio	Muy Grave	Alto		Área de desarrollo de aplicaciones y Coordinador TI	A.2.10.1	Realizar reportes o informes de eventos maliciosos o fallas en los sistemas de información, sitios web, equipos tecnológicos.	Mantener la seguridad de los sistemas en el ciberespacio.
		2	3						
R.2.11	El equipo de desarrollo no aplica seguimientos o revisión en los mensajes recibidos en	Medio	Muy Grave	Alto		Área de desarrollo de	A.2.11.1	Asegurar que los mensajes recibidos en los sitios web no contengan contenido malicioso,	Seguimiento de la seguridad de las aplicaciones.
	El departamento de tecnología no cuenta con una metodología y procesos de desarrollo de aplicaciones maduros.	2	Muy Grave			Área de desarrollo de aplicaciones		Elaborar flujogramas de procesos de desarrollo con metodologías ágiles como SCRUM.	Mejora de los procesos de desarrollo de aplicaciones.
R.2.3	La universidad no cuenta con el personal, capacitación y herramientas especializadas en la seguridad de las aplicaciones para contrarrestar los riesgos que implican las ciberamenazas.	Medio	Grave	Medio		Área de desarrollo de aplicaciones	A.2.3.1	Contratar talento humano especializado o capacitar al personal necesario en seguridad de las aplicaciones.	Contrarrestar los riesgos que implican las ciberamenazas.
		2	2						
R.2.4	El departamento de tecnología no ha establecido un protocolo de autoevaluación de control para monitorear, medir e informar la efectividad de las prácticas de seguridad de aplicaciones e identificar lo que no se hizo bien para mejorar continuamente la práctica.	Medio	Grave	Medio		Área de desarrollo de aplicaciones	A.2.4.1	Elaborar un protocolo de autoevaluación de control para la efectividad de la seguridad de las aplicaciones.	Trabajar con la norma de seguridad de las aplicaciones ISO/IEC 27034
		2	2						
R.2.5	No se utilizan herramientas tecnológicas para realizar pruebas de vulnerabilidades altamente probables, sospechosas y potenciales de criticidad variable.	Medio	Muy Grave	Alto		Área de desarrollo de aplicaciones	A.2.5.1	Utilizar las herramientas tecnológicas que brinda la norma ISO/IEC 27032 de ciberseguridad para efectuar pruebas de vulnerabilidades en las aplicaciones.	Nessus, Acunetix, Shodan
		2	3						
R.2.6	No utilizan herramientas tecnológicas como SAST, DAST, RASP, SCA para	Medio	Grave	Medio		Área de desarrollo de aplicaciones	A.2.6.1	Aplicar al menos una de estas herramientas o en su defecto utilizar las herramientas que	Pruebas regulares con estas herramientas para

	el sitio, para asegurarse que no contengan algún tipo de contenido malicioso o enlaces de sitios web de phishing o descargas maliciosas.	2	3			aplicaciones y Área de Redes		enlaces de sitios web de phishing o descargas maliciosas.	
R.2.12.	No se logra los objetivos desarrollados en base a la sensibilización y formación en proporcionar informes periódicos sobre el estado de la Ciberseguridad, Sesiones de formación enfocada en escenarios simulados de ataque cibernético o talleres sobre áreas requeridas de acciones específicas y tampoco en pruebas regulares con recorridos en escenarios permanentes.	Medio	Grave	Medio		Coordinador TI	A.2.12.1	Considerar como objetivos de sensibilización y formación a informes periódicos sobre el estado de ciberseguridad, enfoques de escenarios simulados de ataques cibernéticos o talleres de acciones específicas y pruebas regulares en escenarios permanentes.	Mejorar la ciberseguridad.
		2	2						
R.2.13.	No se prohíbe el uso de software no autorizado por la institución.	Bajo	Grave	Bajo		Coordinador TI	A.2.13.1	Usar software legal o software libre según lo requiera la aplicación a desarrollar.	Visual, SQL, Windows, Linux
		1	2						
R.2.14.	No se mantienen los sistemas operativos actualizados con las últimas versiones.	Bajo	Menor	Bajo		Coordinador TI	A.2.14.1	Mantener actualizados los sistemas operativos de acuerdo a las características de los equipos.	Mejorar la productividad del desarrollo de aplicaciones.
		1	1						

• Dominio Seguridad de las Redes.

ID. Riesgo	Vulnerabilidades	Probabilidad	Impacto	Nivel	Matriz de Riesgos	Responsable	Mitigación acción ID	Acciones de mitigación	Criterio de aceptación
R.3.1.	La unidad no tiene medidas de prevención y respuestas a los ataques cibernéticos.	Alto	Muy Grave	Crítico		Coordinador TI	A.3.1.1	Elaborar indicadores de prevención y respuestas para tomar medidas de seguridad frente a ataques cibernéticos.	Controlar los ataques cibernéticos.
		3	3						
R.3.2.	No se realiza informes de eventos sospechosos o encuentros maliciosos en las redes.	Alto	Grave	Alto		Coordinador TI y Área de Redes	A.3.2.1	Elaborar o adquirir una herramienta que permita detectar eventos maliciosos en las redes y emitan reportes de los mismos.	Informes mensuales de eventos sospechosos o maliciosos en las redes.
		3	2						
R.3.3.	Entre las políticas, procedimientos y controles que están en proceso de aprobación en la unidad para seguridad de la red están: Políticas de control de acceso a la red, controles de acceso a los servidores, procedimientos de respaldo de la información cuando existen pérdidas de fallos físicos, control de filtros de tráfico en la red interna y externa.	Medio	Grave	Medio		Coordinador TI, Área de Redes y Área de Datos (Data Center)	A.3.4.1	Agilizar el proceso de aprobación de las políticas, procedimientos y controles de la seguridad de la red.	Política de control de acceso, política de filtros de tráfico en la red interna y externa.
		2	2						
R.3.4.	No tienen protocolos de autenticación de computadoras dentro de la red.	Medio	Grave	Medio		Área de Redes.	A.3.5.1	Utilizar protocolos de autenticación de computadoras dentro de la red para evitar posibles ataques.	Evitar los ataques de Man in the middle.
		2	2						
R.3.5.	No existen controles que restrinjan la dirección MAC de cada equipo.	Medio	Grave	Medio		Área de Redes.	A.3.6.1	Autenticar los equipos para que haya mayor control y seguridad en la comunicación entre equipos.	Mejorar la seguridad en las redes.
		2	2						
R.3.6.	El director /coordinador de la unidad no se asegura que la URL de su contenido web este citado como un enlace seguro en su navegador.	Medio	Grave	Medio		Coordinador TI	A.3.7.1	Asegurar que toda la información que vaya a subirse en una aplicación web, debe estar con un enlace seguro en la URL. Como HTTPS.	Proteger la información en el ciberespacio
		2	2						
R.3.7.	El SSL que utiliza el sitio web, no identifica el contenido original del nuevo contenido dañado, plantado por un atacante.	Medio	Muy Grave	Alto		Área de Redes.	A.3.8.1	Verificar que el tráfico de la información esté cifrado para evitar ataques como DDoS.	SSL certificado.
		2	3						
R.3.8.	Utilizan protocolos de comunicación como HTTP.	Medio	Muy Grave	Alto		Área de Redes y Área de desarrollo de aplicaciones.	A.3.9.1	Utilizar protocolos de comunicación seguro en el ciberespacio como HTTPS.	Mejorar la Seguridad en la transmisión de datos en las redes.
		2	3						

4.1.2. PROCESOS DE IMPLEMENTACIÓN DE MARISMA PARA LA GESTIÓN DE RIESGOS EN CIBERSEGURIDAD

La metodología MARISMA, es dinámica y operativa, permite analizar riesgos en tiempo real, mediante un sistema de calidad en donde se lleva a cabo procesos de manera sistemática y controla la información por medio de auditorías aplicadas a ciberseguridad; la misma que consta de tres procesos para la respectiva ejecución.

4.1.2.1. PROCESO 1: GENERACIÓN DE PATRONES PARA EL ANÁLISIS DE RIESGOS (GPRA).

En este proceso se establece una estructura de relaciones entre los diferentes elementos involucrados en el análisis del riesgo y los controles necesarios para gestionar los riesgos. Estas relaciones se establecen mediante el conocimiento adquirido en las diferentes implantaciones, que es almacenado en una estructura denominada patrón para ser reutilizado con posterioridad en el análisis de riesgos (Marisma, 2018).

Siendo el principal objetivo de la generación de patrones, es partir de una base para alimentar de información a la herramienta y posteriormente efectuar el análisis de riesgos incluido en la metodología desarrollada, siendo lo menos costosa posible, utilizando una serie de técnicas y matrices predefinidas, obteniendo un resultado con la suficiente calidad y operatividad (Figura 6).

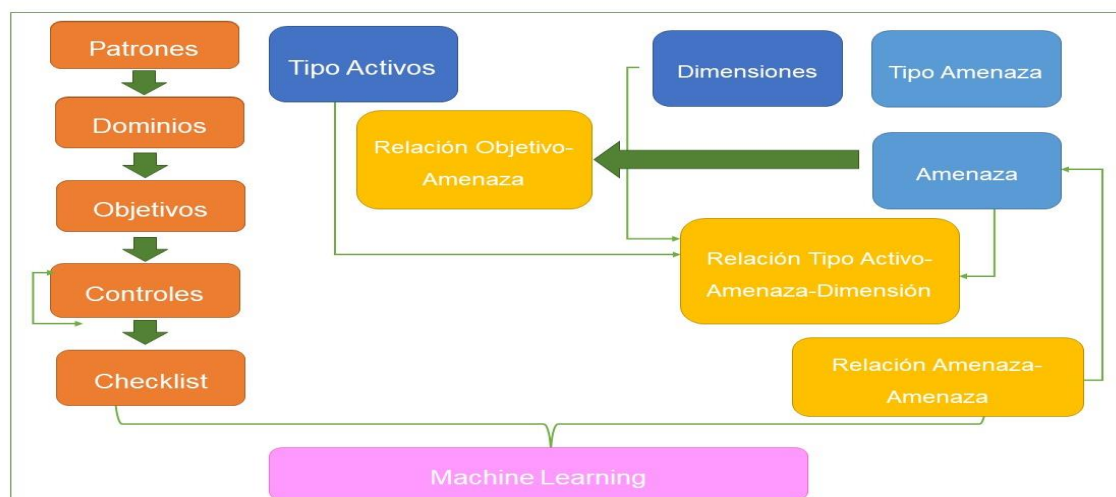


Figura 6. Esquematización de los elementos involucrados en el análisis de riesgo.

Fuente: Propia.

Posteriormente teniendo los patrones definidos (Seguridad de la Información, Seguridad de las Aplicaciones y Seguridad de las Redes) se procede a validar la información, es decir se vincula los activos (Figura 7) y se evalúa los servicios del Checklist según los datos obtenidos de las vulnerabilidades de los sistemas de información de la Unidad (Figura 8), y con ello se tendrá el control del rendimiento de los servicios de Checklist, que en este caso es del 100% de operatividad (Figura 9).

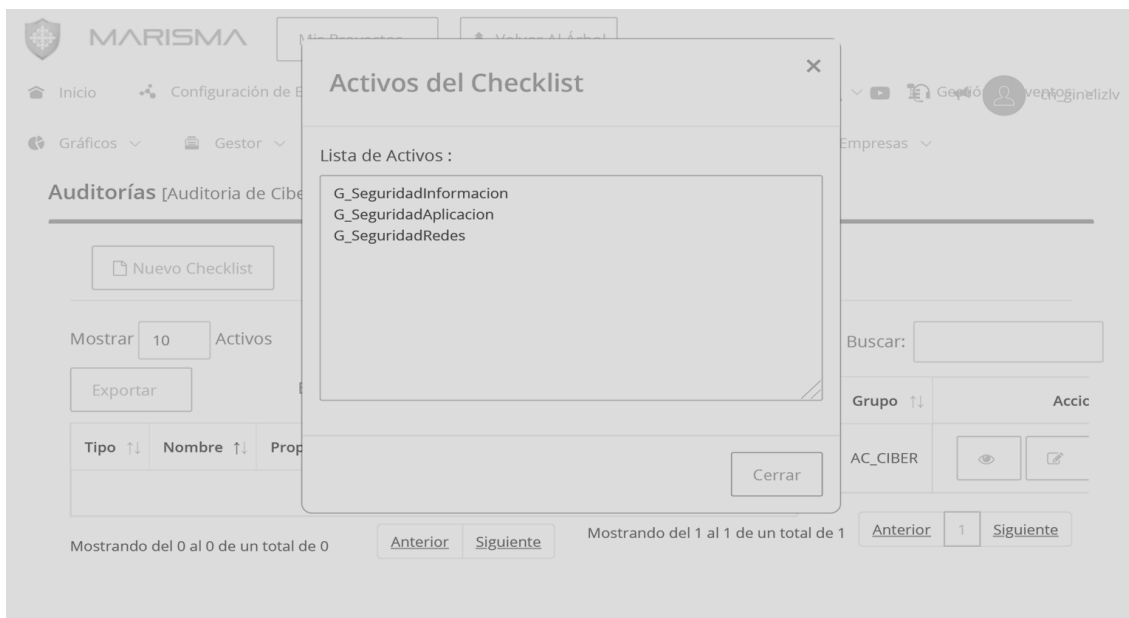


Figura 7. Vinculación de los activos del Checklist.

Fuente: Propia.

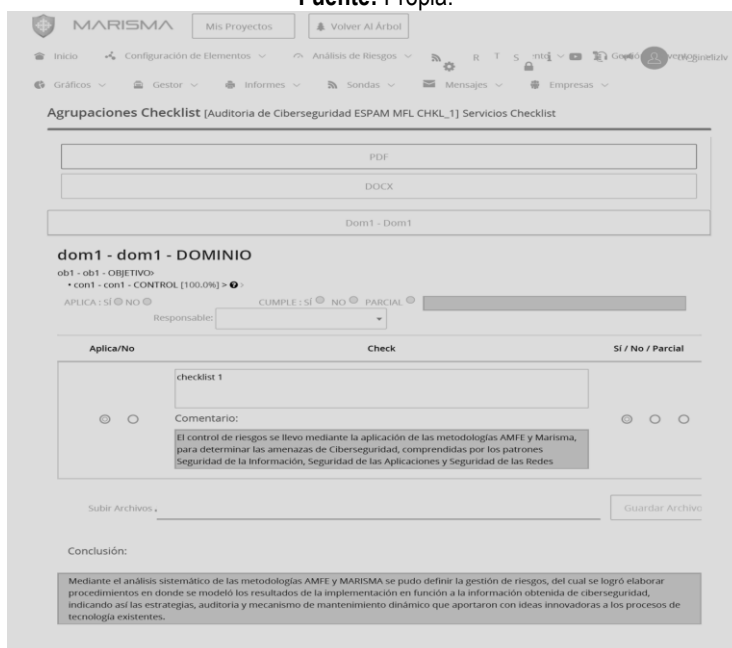


Figura 8. Servicios de Checklists.

Fuente: Propia.

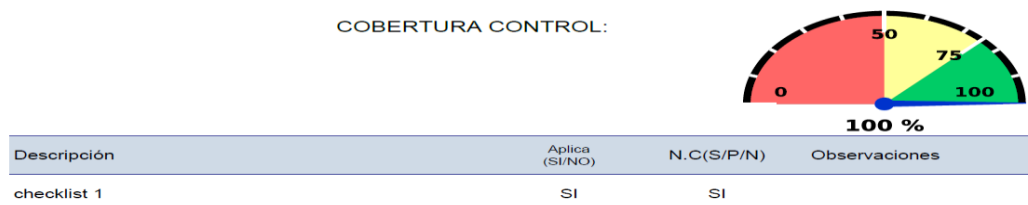


Figura 9. Cobertura control Checklist.
Fuente: Propia.

4.1.2.2. PROCESO 2: GENERACIÓN DEL ANÁLISIS Y GESTIÓN DEL RIESGO (GARM).

Generación del Análisis y Gestión del Riesgo (GARM): Mediante la selección del patrón más adecuado y la identificación de un pequeño conjunto de los principales activos se obtiene un detallado mapa de la situación actual (análisis del riesgo) y un plan de recomendaciones de cómo mejorarlo (gestión del riesgo) (Marisma, 2018).

Es importante tener claro, los elementos de cada estructura para emplearlos al momento de un análisis de riesgos de ciberseguridad, que en este caso corresponden a la figura 10 y 11.

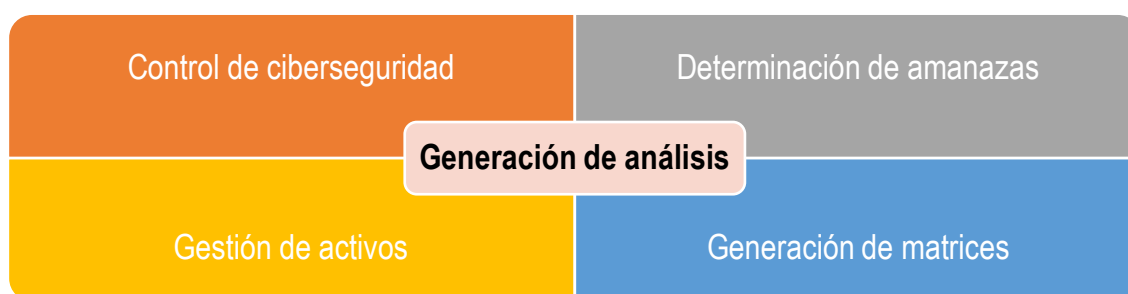


Figura 10. Elementos de la generación de análisis.
Fuente: Propia.



Figura 11. Gestión integral del riesgo.
Fuente: Propia.

Este proceso es llevado a cabo para conocer los resultados del análisis de riesgos, dichos componentes y una vez efectuado generar valores en tiempo real, a partir de los riesgos presentados y según esto las amenazas brindan el estado en el que se encuentran las auditorías de ciberseguridad aplicado en los sistemas de información de la ESPAM MFL (Figura 12, 13, 13, 14, 15,16 y17).

Código	Fecha Apertura	Resp.	Descripción	Causa	Solución	Conclusión	Acciones
00004326	17/05/2020	Coordinación de Tecnología	Control de Riesgos en dominios de Ciberseguridad	Falla en los procesos y procedimientos dentro de a...	--	--	[Iconos de acciones]
00004327	17/05/2020	Coordinación de Tecnología	Cumplimiento a normativas internacionales de Ciber...	Ausencia de estandarización dentro de los procesos...	--	--	[Iconos de acciones]
00004328	17/05/2020	Coordinación de Tecnología	Posible riesgos ante falta de aplicación de proces...	Limitación de Métodos y Técnicas cibernéticas para...	--	--	[Iconos de acciones]

Figura 12. Auditorías de gestión de eventos (Incidentes).

Fuente: Propia.

Análisis de Riesgos_Auditoria de Ciberseguridad ESPAM MFL_eMarisma

Descripción Activo	Activo	Cod. Amenaza	Amenaza	Valor	Fr	V	d1	IT	IMP	Riesgo	Riesgo R.	VRR
--	G_SeguridadAplicacion	am1	am1	4	75	0	100	100	400	300	0	0
--	G_SeguridadRedes	am1	am1	4	75	0	100	100	400	300	0	0
--	G_SeguridadInformacion	am1	am1	5	75	0	100	100	500	375	0	0

Figura 13. Auditoria de análisis de riesgos.

Fuente: Propia.

Activos x Amenazas_Auditoria de Ciberseguridad ESPAM MFL_eMarisma

Cod. Amenaza	Amenaza	Tipo	Activo	Descripción	d1
am1	am1	ta1	G_SeguridadAplicacion	--	100
am1	am1	ta1	G_SeguridadRedes	--	100
am1	am1	ta1	G_SeguridadInformacion	--	100

Figura 14. Auditorías de Activos x Amenazas.

Fuente: Propia.

Activos_Auditoria de Ciberseguridad ESPAM MFL_eMarisma

Cod. Tipo	Tipo	Cod. Amenaza	Amenaza	Probabilidad Ocurrencia	Porcentaje Degradación
tam1	tam1	am1	am1	Bajo (45.0%)Medio (75.0%)Alto (100.0%)	Bajo (45.0%)Medio (75.0%)Alto (100.0%)

Figura 15. Auditoria Activos.
Fuente: Propia.

Mostrar PDF DOCX Buscar:

Código	Control	Aplica	Objetivos	Método de Implantación	Responsable	Documentación
dom1	dom1					
ob1	ob1	objetivo 1				
con1	con1	<input checked="" type="checkbox"/>	control 1	Análisis de riesgos	Coordinación de	

Mostrando del 1 al 1 de un total de 1

[Anterior](#) [1](#) [Siguiete](#)

Figura 16. Auditorias SOA.
Fuente: Propia.

INFORME ANÁLISIS NMAP

Activo: G_SeguridadAplicacion
IP: 190.15.136.154
Fecha: 18/05/20 6:40
Proyecto: s_informacion_espam
Fecha: 18/05/20 3:46
Patrón: P1 - Prueba 1
Responsable: Coordinación de Tecnología

CÓDIGO DOMINIO: [A.11]
NOMBRE DOMINIO: Seguridad física y del entorno
CÓDIGO OBJETIVO: [A.11.1]
NOMBRE OBJETIVO: Areas seguras
DESCRIPCIÓN: Prevenir el acceso físico no autorizado, los daños e interferencia a la información de la organización y a los recursos de tratamiento de la información.

eMARISMA LISO ACADÉMICO
www.emarisma.com - eMarisma IT Risk Management - ©2018 - 2020 eMarisma Shield S.L. All

Figura 17. Informes de NMAP (Sondeos por IP).
Fuente: Propia.

4.1.2.3. PROCESO 3: MANTENIMIENTO DINÁMICO DEL ANÁLISIS DE RIESGOS (DRM).

Mantenimiento Dinámico del Análisis de Riesgos (DRM): Mediante la utilización de las matrices generadas, las cuáles interconectan las diferentes áreas de TI, el sistema irá recalculando el análisis de riesgos según se produzcan eventos, fallen las métricas definidas o los auditores detecten “no conformidades” en los controles (Marisma, 2018).

La información generada en el proceso GPRA será utilizada por los otros dos procesos. De igual forma, la información generada en el proceso GARM será necesaria para el proceso DRM, esto no implica que siempre se deban ejecutar los tres procesos para obtener un resultado, sino que debe existir un patrón generado previamente por el proceso GPRA para que se pueda ejecutar el GARM a partir del cumplimiento de ciclos de auditorías de gestión de riesgo de ciberseguridad (Figura 18).



Figura 18. Ciclo de las auditorías en gestión de riesgo de eMarisma.

Fuente: Propia.

Cabe recalcar que una vez que se lleve a cabalidad la gestión de riesgo, permitan a los responsable la adecuada toma de decisiones con respecto a los riesgos presentados, porque suelen ser mayores, límites y aceptables según sea el caso, por lo tanto la adecuada aplicación de controles, permite que dichas vulnerabilidades, se detecten a tiempo antes que sean amenazas de índole alta, y que puedan afectar en gran medida a los sistemas de información de la Institución, es por ello que el mantenimiento dinámico permite la constante actualización del estado de riesgo presentado en el ciberespacio una vez que los sistemas estén en operatividad (figura 18), y de esta manera se encuentren controlados por el recalcado de datos, para evitar incidencias graves a futuro y así garantizar la calidad del mantenimiento dinámico en las auditorias de riesgos aplicadas en ciberseguridad (figura 19).

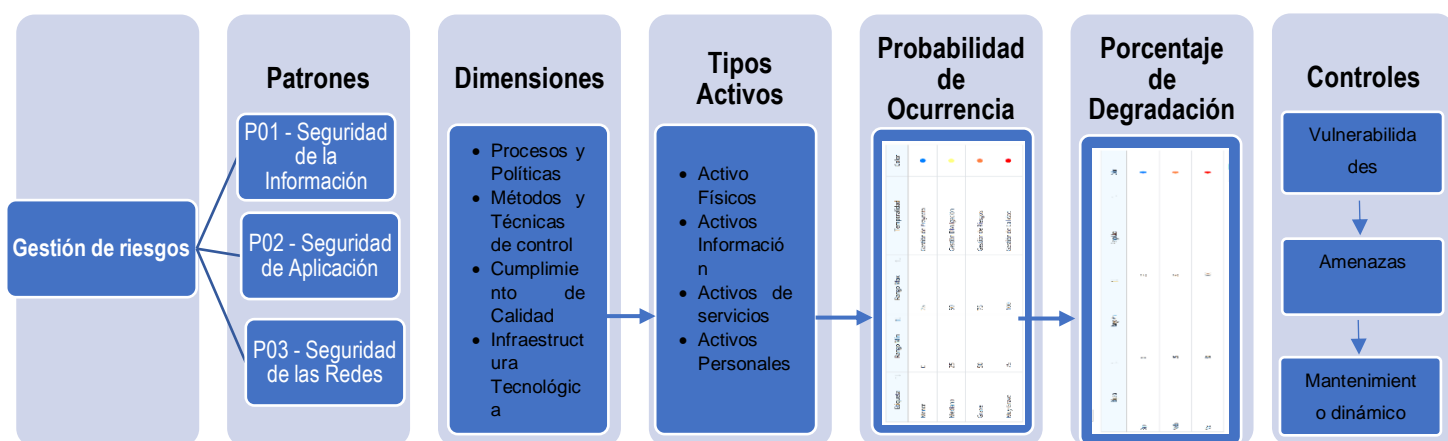


Figura 8. Gestión de riesgos.

Fuente: Propia.

La interfaz de usuario muestra un formulario de configuración para el recálculo de datos. Se encuentran tres interruptores activados: 'Activos x Amenaza', 'Análisis de Riesgos' y 'Plan de Tratamiento'. Se puede seleccionar 'Recalcular' y 'Siguiente'. A continuación se muestra una tabla con los resultados del recálculo.

Cod. Amenaza	Amenaza	Tipo	Activo	Descripción	P. de Ocurrencia	d1	Editar
am1	am1	ta1	G_SeguridadInformacion	--	Medio (75%)	100	[Editar]
am1	am1	ta1	G_SeguridadAplicacion	--	Medio (75%)	100	[Editar]
am1	am1	ta1	G_SeguridadRedes	--	Medio (75%)	100	[Editar]

Figura 9. Recalculación de datos en eMarisma.

Fuente: Propia.

5. ACCIONES DE MEJORA PARA EVITAR RIESGOS APLICANDO MARISMA

A continuación, se da a conocer las acciones de mejoras para evitar riesgos en ciberseguridad en los sistemas de información de la ESPAM MFL:

- Actualizar la información de vulnerabilidades y amenazas en el sistema eMarisma para conocer en tiempo real si las medidas anteriores fueron adoptadas o necesitan ser reestructuradas.
- Aplicar el recalcado de datos para controlar las auditorías existentes y las nuevas, además de la actualización de los activos x amenaza, gestión de riesgos y plan de tratamiento aplicados a ciberseguridad.
- Realizar sondeos de IP constante de manera que se actualicen los informes emitidos por eMarisma y se pueda tomar acciones de mejoras en los sistemas de información, y así controlar los riesgos mediante un adecuado mantenimiento dinámico en los sistemas de información de la Unidad de Tecnología.

6. CONCLUSIONES

- Por medio del plan de gestión de riesgos se pudo determinar los patrones comprendidos en seguridad de la información, seguridad de las aplicaciones y seguridad de redes como base a los riesgos y los componentes para ser utilizadas, así mismo los criterios base de la gestión de riesgos.
- Mediante el análisis de riesgo se pudo evaluar los riesgos presentados en la metodología AMFE y luego implementarlos con MARISMA para la respectiva valoración con respecto a los sistemas de información de la Unidad de Tecnología de la ESPAM MFL.
- Una vez indicadas las acciones de mejora para evitar los riesgos en ciberseguridad, se las direccionó a los procesos existentes de control y con ello la actualización de mantenimientos dinámicos de gestión de riesgos para mejorar y garantizar el cumplimiento de auditorías de gestión de riesgos y con ello mitigar los riesgos existentes y futuros a partir de vulnerabilidades en ciberseguridad.

BIBLIOGRAFÍAS

Rcamara. (2020). Marisma | Consigue la certificación ISO/IEC 25000 de AENOR. Disponible en: <https://www.sicaman.com/category/marisma/>

ISO. (2019). MARISMA 2.0, nuevo producto certificado en ISO/IEC 25000 para Adecuación Funcional. Disponible en: <https://iso25000.com/index.php/9-espanol/noticias/159-marisma-2-0-nuevo-producto-certificado-en-iso-iec-25000-para-adequacion-funcional>

MARISMA. (2018). Methodology for the Analysis of Risks of Information Security, based on Meta-Pattern and Adaptability. España: Versión: 3.0.

Saltos-Olmo. (2014). Desarrollando una metodología de análisis de riesgos para que el sector asegurador pueda tasar los riesgos en las PYMES. Disponible en: https://www.researchgate.net/publication/271850509_Desarrollando_una_metodologia_de_analisis_de_riesgos_para_que_el_sector_asegurador_pueda_tasar_los_riesgos_en_las_PYMES

ANEXO 5
MATRIZ DE ANÁLISIS DE LAS METODOLOGÍAS AMFE Y MARISMA

Anexo 5.1. Tablas de Predeterminados por Amenaza de Marisma

• Seguridad de información

Cod. Tipo	Tipo	Cod. Amenaza ↑↓	Amenaza ↑↓	Probabilidad de Ocurrencia ⚙	Porcentaje de Degradación ⚙
Vulnerabilidad_GR	Gestión de Riesgos	ASI_01	No se monitorea el acceso a los sistemas de informacion web.	Grave (75.0%) ▾	Alto (100.0%) ▾
Vulnerabilidad_GR	Gestión de Riesgos	ASI_02	No se mantiene preparación continua en Ciberseguridad en la institución.	Muy Grave (100.0%) ▾	Alto (100.0%) ▾
Vulnerabilidad_GC	Gestión de Calidad	ASI_03	No se estandarizan los datos en base a normas de calidad.	Muy Grave (100.0%) ▾	Alto (100.0%) ▾
Vulnerabilidad_GC	Gestión de Calidad	ASI_04	No emplean normas de calidad como ISO, INEN, Control interno, entre otras para la estandarización de sus procesos.	Muy Grave (100.0%) ▾	Alto (100.0%) ▾
Vulnerabilidad_GP	Gestión de Proyecto	ASI_05	No aplican regulaciones de normas en escenarios de seguridad.	Muy Grave (100.0%) ▾	Alto (100.0%) ▾
Vulnerabilidad_GD	Gestión Divulgación	ASI_06	No se alerta a los usuarios cuando existe algún tipo de ataque o implementación de controles de seguridad.	Muy Grave (100.0%) ▾	Alto (100.0%) ▾
Vulnerabilidad_GR	Gestión de Riesgos	ASI_07	No emplean normas en escenarios de ciberseguridad.	Muy Grave (100.0%) ▾	Alto (100.0%) ▾
Vulnerabilidad_GP	Gestión de Proyecto	ASI_08	Los manuales de usuario para el manejo de los sistemas de información están en proceso de elaboración.	Grave (75.0%) ▾	Medio (50.0%) ▾
Vulnerabilidad_GP	Gestión de Proyecto	ASI_09	No se llevan a cabo los datos de informes como estrategia para la continuidad del negocio.	Grave (75.0%) ▾	Medio (50.0%) ▾
Vulnerabilidad_GR	Gestión de Riesgos	ASI_10	Han sufrido ataques de robo de identidad o robo de información de los usuarios en Aplicaciones web.	Grave (75.0%) ▾	Medio (50.0%) ▾
Vulnerabilidad_GP	Gestión de Proyecto	ASI_11	Los tipos de ataques que se han presentado en la unidad son: DDoS, Dos.	Muy Grave (100.0%) ▾	Alto (100.0%) ▾
Vulnerabilidad_GR	Gestión de Riesgos	ASI_12	No se usan técnicas de visualización de datos para presentar información de eventos.	Grave (75.0%) ▾	Medio (50.0%) ▾

• Seguridad de aplicaciones

Cod. Tipo	Tipo	Cod. Amenaza	Amenaza	Probabilidad de Ocurrencia	Porcentaje de Degradación
Vulnerabilidad_GP	Gestión de Proyecto	ASA_01	No tienen un plan de seguridad para todo el ciclo de vida del desarrollo del software (SDLC), desde su desarrollo, pasando por las pruebas y producción.	Muy Grave (100.0%)	Alto (100.0%)
Vulnerabilidad_GP	Gestión de Proyecto	ASA_02	El departamento de tecnología no cuenta con una metodología y procesos de desarrollo de aplicaciones maduros.	Muy Grave (100.0%)	Medio (50.0%)
Vulnerabilidad_GP	Gestión de Proyecto	ASA_03	La universidad no cuenta con el personal, capacitación y herramientas especializadas en la seguridad de las aplicaciones para contrarrestar los riesgos que implican las ciberamenazas.	Grave (75.0%)	Medio (50.0%)
Vulnerabilidad_GR	Gestión de Riesgos	ASA_04	El departamento de tecnología no ha establecido un protocolo de autoevaluación de control para monitorear.	Grave (75.0%)	Medio (50.0%)
Vulnerabilidad_GR	Gestión de Riesgos	ASA_05	No se utilizan herramientas tecnológicas para realizar pruebas de vulnerabilidades altamente probables, sospechosas y potenciales de criticidad variable.	Muy Grave (100.0%)	Medio (50.0%)
Vulnerabilidad_GR	Gestión de Riesgos	ASA_06	No utilizan herramientas tecnológicas como SAST, DAST, RASP, SCA para realizar pruebas de vulnerabilidades.	Grave (75.0%)	Medio (50.0%)
Vulnerabilidad_GR	Gestión de Riesgos	ASA_07	No se han realizado pruebas de penetración o pentest a las aplicaciones, incluidas la red, la plataforma de alojamiento y la aplicación en sí, para verificar las medidas de seguridad que protegen la aplicación tanto internas como externas.	Muy Grave (100.0%)	Medio (50.0%)
Vulnerabilidad_GP	Gestión de Proyecto	ASA_08	No se establecen responsables y procedimientos formales de aplicación de seguridad en los equipos tecnológicos y software.	Muy Grave (100.0%)	Medio (50.0%)
Vulnerabilidad_GP	Gestión de Proyecto	ASA_09	No se aprueban de manera formal los cambios de equipos tecnológicos y software.	Menor (25.0%)	Bajo (25.0%)
Vulnerabilidad_GR	Gestión de Riesgos	ASA_10	La unidad no posee alertas o fallas de los sistemas de información, sitios web, equipos tecnológicos.	Grave (75.0%)	Medio (50.0%)
Vulnerabilidad_GR	Gestión de Riesgos	ASA_11	El equipo de desarrollo no aplica seguimientos o revisión en los mensajes recibidos en el sitio, para asegurarse que no contengan algún tipo de contenido malicioso o enlaces de sitios web de phishing o descargas maliciosas.	Muy Grave (100.0%)	Medio (50.0%)
Vulnerabilidad_GP	Gestión de Proyecto	ASA_12	No se logra los objetivos desarrollados en base a la sensibilización y formación en proporcionar informes periódicos sobre el estado de la Ciberseguridad, Sesiones de formación enfocados en escenarios simulados de ataque cibernéticos.	Grave (75.0%)	Medio (50.0%)
Vulnerabilidad_GR	Gestión de Riesgos	ASA_13	No se prohíbe el uso de software no autorizado por la institución.	Grave (75.0%)	Bajo (25.0%)
Vulnerabilidad_GR	Gestión de Riesgos	ASA_14	No se mantienen los sistemas operativos actualizados con las últimas versiones.	Menor (25.0%)	Bajo (25.0%)

- Seguridad de redes

Cod. Tipo	Tipo	Cod. Amenaza ↑↓	Amenaza ↑↓	Probabilidad de Ocurrencia ⓘ	Porcentaje de Degradación ⓘ
Vulnerabilidad_GR	Gestión de Riesgos	ASR_01	No se realizan informes de eventos sospechosos o encuentros maliciosos en las redes.	Muy Grave (100.0%)	Alto (100.0%)
Vulnerabilidad_GR	Gestión de Riesgos	ASR_02	Actualmente está en proceso la aplicación de seguridad en la red.	Grave (75.0%)	Medio (50.0%)
Vulnerabilidad_GR	Gestión de Riesgos	ASR_03	No tienen protocolos de autenticación de computadoras dentro de la red.	Grave (75.0%)	Medio (50.0%)
Vulnerabilidad_GR	Gestión de Riesgos	ASR_04	Han sufrido ataques en la seguridad de la red de Interrupción e Intercepción.	Grave (75.0%)	Medio (50.0%)
Vulnerabilidad_GR	Gestión de Riesgos	ASR_05	No se toman medidas de autenticación de comunicación para evitar el ataque de Man in the Middle.	Muy Grave (100.0%)	Medio (50.0%)
Vulnerabilidad_GC	Gestión de Calidad	ASR_06	Los servidores en Internet se han vistos comprometidos con el método de desbordamiento de búfer provocando que el servidor funcione fuera de su entorno normal (control), facilitando la inserción / ejecución de código malicioso.	Muy Grave (100.0%)	Medio (50.0%)
Vulnerabilidad_GR	Gestión de Riesgos	ASR_07	Entre las políticas, procedimientos y controles que no tiene la unidad para la seguridad de la red está la Política de control de acceso a la red, y en proceso el control de filtros de tráfico en la red interna y externa.	Muy Grave (100.0%)	Bajo (25.0%)

Anexo 5.2. Tablas de Patrones Activo-Amenaza-Dimensión

• Seguridad de información

ASI01	ASI02	ASI03	ASI04	
ASI_01	DISI02 DISI_04	DISI02 DISI_04	DSI_04	DSI_03 DISI02
ASI_02	DSI_04 DISI02	DSI_03 DISI_04	DISI02 DISI_04	DSI_03 DISI_04
ASI_03	DISI02 DISI_04	DISI01 DISI02	DSI_04 DISI_03	DISI01 DISI_03
ASI_04	DISI01 DISI_03	DISI01 DISI_03	DSI_03 DISI_04	DSI_03 DISI01
ASI_05	DSI_03 DISI_04	DSI_03	DSI_03 DISI02	DSI_03 DISI_04
ASI_06	DSI_04 DISI02	DISI02 DISI_04	DSI_04 DISI_03	DSI_03 DISI02
ASI_07	DISI02 DISI_03	DSI_04 DISI02	DSI_04 DISI02	DSI_03 DISI02
ASI_08	DSI_03 DISI02	DISI01 DISI_03	DSI_03 DISI_04	DSI_03 DISI02
ASI_09	DISI02 DISI_04	DSI_03 DISI01	DISI02 DISI_03	DISI02 DISI_03
ASI_10	DISI02 DISI_04	DISI02 DISI_04	DSI_04 DISI_03	DISI01 DISI_03
ASI_11	DISI02 DISI01 DISI_04	DSI_04 DISI_03	DSI_03	DISI02 DISI_03
ASI_12	DSI_03 DISI02	DSI_03 DISI02	DSI_04 DISI_03	DISI02 DISI_03

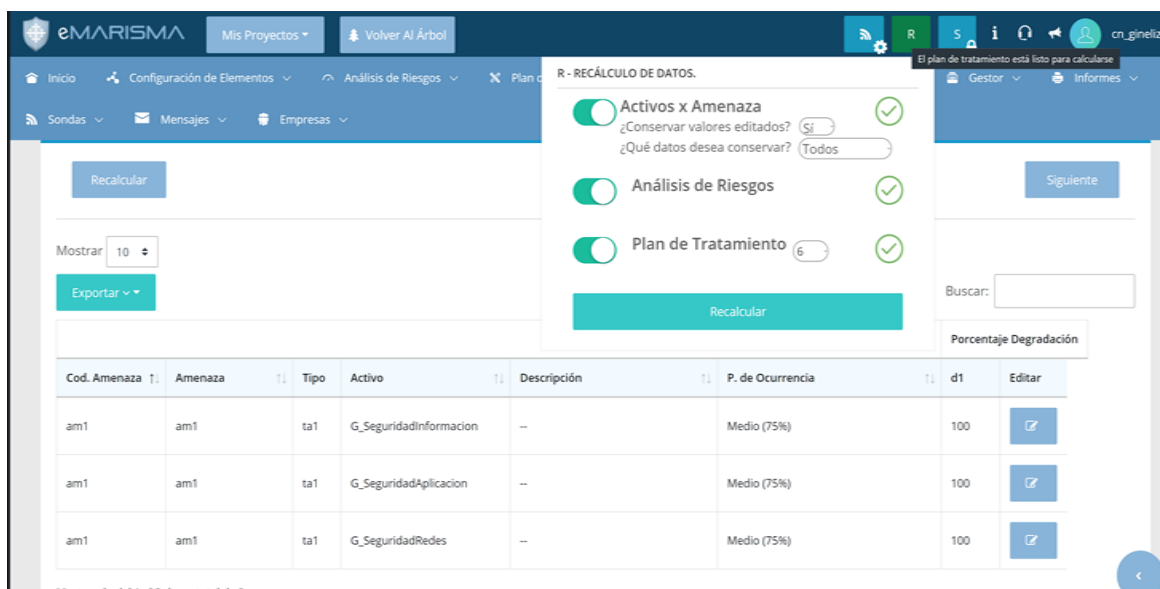
• Seguridad de aplicaciones

ASA02	ASA03	ASA04	ASA_01	
ASA_01	DISA_01 DSA_02	DSA_02 DSA_04	DISA_01 DSA_03	DSA_02
ASA_02	DISA_01	DSA_04 DISA_01	DISA_01 DSA_03	DISA_01 DSA_04
ASA_03	DSA_02	DSA_04 DISA_01	DISA_01 DSA_03	DSA_02 DISA_01
ASA_04	DSA_04 DISA_01	DSA_04 DISA_01	DSA_04 DISA_01	DSA_04 DISA_01
ASA_05	DISA_01	DSA_04 DISA_01	DISA_01 DSA_03	DSA_04 DSA_02
ASA_06	DISA_01 DSA_04	DSA_02 DISA_01	DSA_03 DISA_01	DISA_01 DSA_04
ASA_07	DISA_01 DSA_03	DSA_02 DSA_04	DISA_01 DSA_03	DISA_01 DSA_04
ASA_08	DSA_02 DSA_04	DSA_04 DISA_01	DSA_03 DSA_02	DSA_02 DSA_04
ASA_09	DSA_04 DISA_01	DISA_01 DSA_04	DISA_01 DSA_03	DISA_01 DSA_04
ASA_10	DSA_02 DSA_04	DSA_04	DISA_01 DSA_03	DISA_01 DSA_04
ASA_11	DSA_04 DISA_01	DISA_01 DSA_04	DISA_01 DSA_04	DSA_04 DISA_01
ASA_12	DSA_04 DSA_03	DISA_01 DSA_04	DSA_03 DSA_02	DSA_02 DSA_03
ASA_13	DISA_01 DSA_04	DISA_01 DSA_04	DSA_02 DSA_03	DISA_01 DSA_03
ASA_14	DISA_01	DSA_02 DSA_04	DISA_01 DSA_04	DISA_01 DSA_04

• Seguridad de redes

ASA_04	ASR_01	ASR_02	ASR_03	
ASR_01	DSR_03 DISR_01	DISR_01 DSR_04	DISR_01 DSR_02	DSR_03 DSR_04
ASR_02	DSR_02 DSR_03	DSR_04	DSR_04 DSR_03	DSR_04 DISR_01
ASR_03	DSR_04 DSR_02	DSR_03 DSR_04	DSR_03	DSR_04 DSR_02
ASR_04	DSR_03 DSR_02	DSR_04 DISR_01	DISR_01	DISR_01 DSR_03
ASR_05	DSR_03 DSR_04	DSR_04 DISR_01	DSR_04	DSR_03 DSR_04
ASR_06	DISR_01 DSR_03	DSR_02 DSR_04	DSR_02 DISR_01	DSR_03 DSR_04
ASR_07	DSR_02 DSR_03	DSR_02 DISR_01	DSR_03 DSR_02	DSR_03 DSR_04

Anexo 5.3. Análisis dinámico en la plataforma eMarisma



Anexo 5.4. Resumen de las Auditorías de Ciberseguridad

- Auditorías [Auditoria de Ciberseguridad ESPAM MFL] Análisis de Riesgos

Descripción Activo	Activo	Cod. Amenaza	Amenaza	Valor	Fr	V	d1	IT	IMP	Riesgo	Riesgo R.	VR R
--	G_SeguridadAplicacion	am1	am1	4	75	0	100	100	400	300	0	0
--	G_SeguridadRedes	am1	am1	4	75	0	100	100	400	300	0	0

- Auditorías [Auditoria de Ciberseguridad ESPAM MFL] Activos x Amenazas

Cod. Amenaza	Amenaza	Tipo	Activo	Descripción	P. de Ocurrencia	d1
am1	am1	ta1	G_SeguridadRedes	--	Medio (75%)	100
am1	am1	ta1	G_SeguridadInformacion	--	Medio (75%)	100
am1	am1	ta1	G_SeguridadAplicacion	--	Medio (75%)	100

Descripción Activo	Activo	Cod. Amenaza	Amenaza	Valor	Fr

--	G_SeguridadAplicacion	am1	am1	4	75
--	G_SeguridadRedes	am1	am1	4	75

- Auditorías [Auditoria de Ciberseguridad ESPAM MFL] SOA

Mostrar 10 PDF DOCX Buscar:

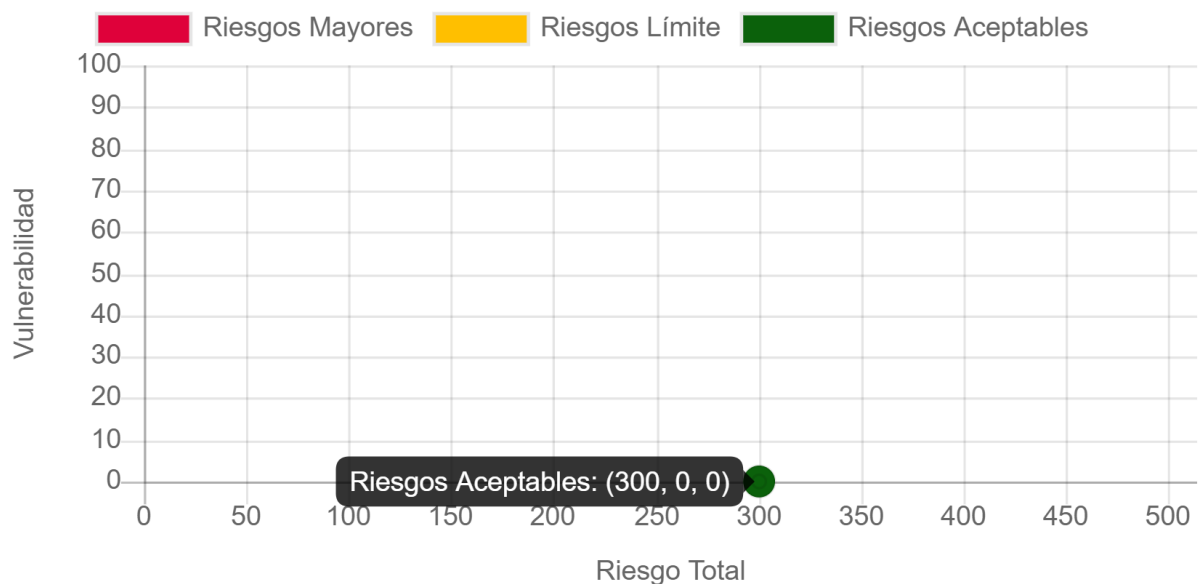
Código	Control	Aplica	Objetivos	Método de Implantación	Responsable	Documentación
dom1	dom1					
ob1	ob1	objetivo 1				
con1	con1	✓	control 1	Análisis de riesgos	Coordinación de Tecnología	

Mostrando del 1 al 1 de un total de 1

Anterior 1 Siguiente

Producto software ISO 25000 ADECUACIÓN FUNCIONAL AENOR conform

- Auditorías [Auditoria de Ciberseguridad ESPAM MFL] Mapa de Riesgos



- Gestión de Eventos [Auditoria de Ciberseguridad ESPAM MFL] Incidentes

Código	Fecha Apertura	Resp.	Descripción	Causa	Solución	Conclusión	Acciones
4326	17/5/2020	Coordinación de Tecnología	Control de Riesgos en	Falla en los procesos y procedimientos dentro de a...	--	--	

			dominios de Ciberseguridad				
4327	17/5/2020	Coordinación de Tecnología	Cumplimiento a normativas internacionales de Ciber...	Ausencia de estandarización dentro de los procesos...	--	--	
4328	17/5/2020	Coordinación de Tecnología	Posible riesgos ante falta de aplicación de proces...	Limitación de Métodos y Técnicas cibernéticas para...	--	--	

- Gestor de Eventos [Auditoria de Ciberseguridad ESPAM MFL] Revisión de Control

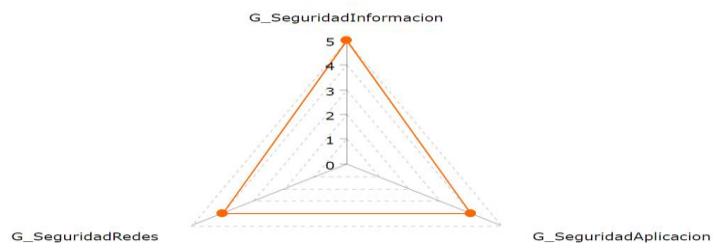
AC_CIBER

Mostrar 10

Buscar:

Código Control	Control	Aplica	Valor	Historial
con1	con1	Si <input type="checkbox"/>	<div style="display: flex; align-items: center;"> <div style="width: 100px; height: 10px; background: linear-gradient(to right, #007bff 0%, #007bff 100%);"></div> <div style="margin-left: 5px;">100</div> </div>	

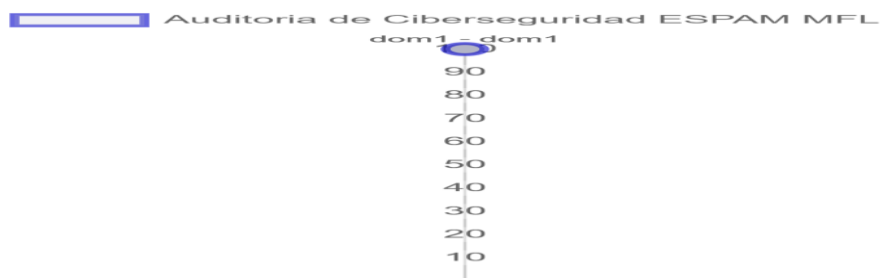
Mostrando del 1 al 1 de un total de 1
Anterior **1** Siguiente



■ Valor Estratégico

- Cuadro de Mando [Auditoria de Ciberseguridad ESPAM MFL] Dominios

Cuadro De Mando - Auditoria de Ciberseguridad ESPAM MFL		TOTAL :	100.0%
dom1	dom1	[Dominio]	100.0%
ob1	ob1	[Objetivo]	100.0%
con1	con1	[Controles]	100.0%



Anexo 5.5. Informes de auditoría en la plataforma eMarisma

Product software
ISO 25000
eMARISMA

Mis Proyectos Volver Al Árbol

Inicio Configuración de Elementos Análisis de Riesgos Plan de Tratamiento Gestión de Eventos Gráficos Gestor Informes

Sondas Mensajes Empresas Plan de Tratamiento

Auditorías [Auditoria de Ciberseguridad ESPAM MFL] SOA

Mostrar 10 PDF DOCK Buscar:

Código	Control	Aplica	Objetivos	Método de Implantación	Responsable	Documentación
dom1	dom1					
ob1	ob1		objetivo 1			
con1	con1	✓	control 1	Análisis de riesgos	Coordinación de Tecnología	

Mostrando del 1 al 1 de un total de 1

Anterior 1 Siguiente

Producto software ISO 25000 eMARISMA AENOR conform

www.e-marisma.com/SCA/index/523#1

INFORME CONTROL DE CAMBIOS



Auditoria: s_informacion_espam
 Fecha Informe: 19/05/20 12:44
 Periodo: 2020-05-19 00:00:00 - 2020-05-19 23:59:59
 Patrón: P1 - Prueba 1
 Responsable: Coordinación de Tecnología

19/05/20 12:44

Anexo 5.6. Matriz condensa de análisis de gestión de riesgo de Ciberseguridad

PATRONES	VULNERABILIDADES	GESTIÓN DE VULNERABILIDADES				DIMENSIONES			
		Gestión de Calidad	Gestión Divulgación	Gestión de Proyecto	Gestión de Riesgos	DSI_01 Procesos y Políticas	DSI_02 Métodos y Técnicas de control	DSI_03 Cumplimiento de Calidad	DSI_04 Infraestructura Tecnológica
G_SeguridadInformacion	12	2	1	4	5	8	24	33	25
G_SeguridadAplicaciones	14	0	0	6	8	40	16	15	34
G_SeguridadRedes	8	0	0	1	7	11	10	15	16



VARIABLE DE AMENAZAS																				
Metodología AMFE										Metodología MARISMA										
Probabilidad			Impacto			Nivel				Porcentaje de Degradación			Probabilidad de Ocurrencia				Rangos			
Alto	Medio	Bajo	Muy Grave	Grave	Menor	Critico	Alto	Medio	Bajo	Alto	Medio	Bajo	Muy Grave	Grave	Mediana	Menor	Critico	Alto	Medio	Bajo

8	4	2	6	6	0	6	2	4	2	8	4	0	7	5	0	0	x	-	-	-
1	11	2	7	6	2	1	6	5	2	1	10	3	6	6	0	2		x	-	-
2	6	2	3	5	0	1	3	4	2	1	5	1	4	3	0	0		-	x	-



TIPOS DE RIESGOS			RIESGOS AMENAZA	RIESGO DE ACTIVOS		
Riesgos Mayores	Riesgos limites	Riesgos Aceptables		Riesgo Mayor	Riesgo Medio	Riesgo Menor
-	-	-	No	0	0	500
-	-	x	Si	0	0	0
-	-	x	Si	0	0	0



REVISIÓN DE CONTROL				MITIGACIÓN DE INCIDENTES			SON DEO POR IP	CUADRO DE MANDO - AUDITORIA DE CIBERSEGURIDAD ESPAM MFL					CONCLUSIONES	RESPONSABLE
Activos x Amenaza	Análisis de Riesgos	Plan de Tratamiento VR = 6.0	Aplicación		Control de Riesgos en dominios de Ciberseguridad	Cumplimiento a normativas internacionales de Ciberseguridad.		Aplicación de Métodos y Técnicas cibernéticas para protección en los sistemas de información.	Cantidad de IP escaneadas	Porcentaje	Dominio	Objetivo		
			SI	NO										
Medio (75%)	0	SUS CONTROLES ESTÁN DENTRO DE LOS LÍMITES	x	-	x	x	x	9	50%	100.0%	100.0%	100.0%	En este patrón, se puede observar que los riesgos que presentan son menores de 500 posibles, no se ve indicio de amenaza dentro de los sistemas de información en los actuales momentos con la aplicación de la metodología MARISMA, aunque en AMFE si indica vulnerabilidades anteriores, en cuanto a las variables de amenazas ambas metodologías en cuanto al análisis del patrón de sistemas de información, dan a conocer que asemejan en resultados, pero MARISMA manifiesta una efectividad más dinámica en los resultados debido a que toma información en tiempo real por medio de IP, que fue equivalente al 50% de direccionamiento a información, además validada los datos ingresados a la plataforma, cabe indicar que dentro de las dimensiones se pudo apreciar que donde más vulnerabilidades podría existir sería Infraestructura tecnología en cuanto a activos tecnológicos, debido a que la actualización y modificación de equipos y sistemas como prevención en la gestión de riesgo es de mucha importancia durante una auditoría del 100% de cumplimiento dentro de la infraestructura tecnología en la ESPAM MFL.	Coordinación de Tecnología

Medio (75%)	300	SUS CONT ROLES ESTÁN DENTR O DE LOS LÍMITE S	x	-	x	x	x	4	22%	100.0%	100.0 %	100.0 %	Por otro lado el patrón de seguridad de aplicaciones indica que en al análisis de riesgos, manifestó un total de 300 comprendidos como activos-amenazadas tipo medio equivalente al 75%, el plan de tratamiento está dentro de los límites de control, presenta riesgos de tipo aceptables, la variable amanezca mantiene entre metodologías similitudes en valores de evaluación, dado que las dimensiones indican que el mayor índice de vulnerabilidad se direcciona a procesos y procedimientos, dado que al momento de desarrollar aplicaciones y darles mantenimientos se debe seguir secuenciales que lleven a cabalidad la elaboración e implementación, por otro lado no presenta riesgos de activos, en mitigación de incidentes mantiene activa las sugerencias, además de establecer un total de 4 sondeos de IP comprendidos en el 25% del total escaneados, así mismo dentro del cuadro de mando establece una auditoria de dominios, objetivos y controles de un 100%.	Coordi nación de Tecnol ogía
Medio (75%)	300	SUS CONT ROLES ESTÁN DENTR O DE LOS LÍMITE S	x	-	x	x	x	5	28%	100.0%	100.0 %	100.0 %	Así mismo en el patrón de seguridad de redes manifiesta que en al análisis de riesgos, manifestó un total de 300 comprendidos como activos-amenazadas tipo medio equivalente al 75%, el plan de tratamiento está dentro de los límites de control, presenta riesgos de tipo aceptables, la variable amanezca mantiene entre metodologías similitudes en valores de evaluación, dado que las dimensiones indican que el mayor índice de vulnerabilidad se direcciona a gestión de riesgos, debido a que se encuentra siempre expuesto la comunicación dentro del ciberespacio y con ello a la interconexión de la información, por otro lado no presenta riesgos de activos, en mitigación de incidentes mantiene activa las sugerencias, además de establecer un total de 5 sondeos de IP comprendidos en el 28% del total escaneados, y también dentro del cuadro de mando establece una auditoria de dominios, objetivos y controles de un 100%.	Coordi nación de Tecnol ogía