ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ

DIRECCIÓN 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:

MODELO DE GESTIÓN DE CONTINUIDAD EN LA INFRAESTRUCTURA TECNOLÓGICA DE LA UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ, BASADA EN LA NORMA ISO 22301

AUTORAS:

MARÍA TERESA CANO MONTESDEOCA

YANINA ALEXANDRA VITERI ALCÍVAR

TUTORA:

ING. AURA DOLORES ZAMBRANO RENDÓN, MGs.

CALCETA, MAYO 2019

DERECHOS DE AUTORÍA

MARÍA TERESA CANO MONTESDEOCA y YANINA ALEXANDRA VITERI ALCÍVAR, declaramos bajo juramento que el trabajo aquí escrito es de nuestra autoría, que no ha sido previamente presentado para ningún grado o calificación profesional, y que hemos consultado las referencias bibliográficas que se incluyen en este documento.

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

_____	_____
María T. Cano Montesdeoca	Yanina A. Viteri Alcívar

CERTIFICACIÓN DE TUTORA

ING. AURA D. ZAMBRANO RENDÓN, **MGs.** certifica haber tutelado el trabajo de titulación: **MODELO DE GESTIÓN DE CONTINUIDAD EN LA INFRAESTRUCTURA TECNOLÓGICA DE LA UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ, BASADA EN LA NORMA ISO 22301**, que ha sido desarrollada por **MARÍA TERESA CANO MONTESDEOCA** y **YANINA ALEXANDRA VITERI ALCÍVAR**, previa la obtención del título de Magister en Tecnología de la Información mención en Redes y Sistemas Distribuidos, de acuerdo al **REGLAMENTO PARA LA ELABORACIÓN DE TRABAJO DE TITULACIÓN DE UNIDAD DE TITULACIÓN** de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López.

_____

Ing. Aura D. Zambrano Rendón, MGs.

APROBACIÓN DEL TRIBUNAL

Los suscritos integrantes del tribunal correspondiente, declaramos que hemos **APROBADO** el trabajo de titulación **MODELO DE GESTIÓN DE CONTINUIDAD EN LA INFRAESTRUCTURA TECNOLÓGICA DE LA UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ, BASADA EN LA NORMA ISO 22301**, que ha sido propuesto y desarrollado por **MARÍA TERESA CANO MONTESDEOCA** y **YANINA ALEXANDRA VITERI ALCÍVAR**, previa la obtención de título de Magister en Tecnología de la Información mención en Redes y Sistemas Distribuidos, de acuerdo al **REGLAMENTO PARA LA ELABORACIÓN DE TRABAJO DE TITULACIÓN** de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López.

_____ _____

Ing. Gustavo G. Molina Garzón, MGs.
MIEMBRO

Ing. Sergio A. Intriago Briones, MGs.
MIEMBRO

_____

Dr. Inf. Marlon R. Navia Mendoza
PRESIDENTE

AGRADECIMIENTO

Nos complace expresar nuestra inmensa gratitud a la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, a todo el talento humano que con eficiencia compartieron sus conocimientos para potencializar el aprendizaje en cada uno de nosotros, a la tutora Ing. Aura Zambrano Rendón quien con profesionalismo y dedicación transmitió la guía necesaria para el desarrollo del trabajo de titulación. Asimismo a la Universidad Laica Eloy Alfaro de Manabí por concedernos la apertura para la recopilación de la información y de manera especial a los Funcionarios de la Unidad Central de Coordinación de Informática, por su gran gentileza y apoyo incondicional en el proceso de la investigación.

LAS AUTORAS

DEDICATORIA

A Dios todo poderoso por el don de la vida y guiarme siempre por el camino correcto.

A mi tía que más que eso es una madre para mí, por ser incondicional, por vivir juntas los buenos y malos momentos y por el apoyo brindado en este largo camino. Gracias por todo tu amor.

A mí querido esposo por apoyarme incondicionalmente en cada una de mis metas planteadas.

A mi hijo por ser la razón de mi existencia y con su amor darle sentido y color a mis días y por ser la fuente inagotable de inspiración y motivación para seguir adelante.

A mi amada madre y hermanas por su absoluto apoyo durante este tiempo de esfuerzo y sacrificio e impulsarme a seguir adelante. Gracias por estar siempre a mi lado.

María T. Cano Montesdeoca

DEDICATORIA

A Dios, motor esencial de mi vida, por concederme la fuerza y sabiduría a través de sus bendiciones.

A mi amado esposo por haberme brindado su apoyo y comprensión en todo momento, en especial en esta jornada académica.

A mis padres que desde la eternidad se convirtieron en Ángeles protectores guiándome y acompañándome día a día por el sendero de la Vida.

A mis sobrinos origen de motivación para llegar a los objetivos planteados.

A mis familiares y amigos quienes con sus sabios consejos motivaron a ser perseverante en esta nueva etapa de mi vida.

Yanina A. Viteri Alcívar

CONTENIDO GENERAL

CONTENIDO DE TABLAS Y GRÁFICOS

RESUMEN

Es importante reconocer el nivel de relevancia que conlleva al desarrollo de esta investigación, cuyo objetivo principal es elaborar un Modelo de Gestión de Continuidad en la Infraestructura Tecnológica de la Universidad Laica Eloy Alfaro de Manabí, basado en la Norma ISO 22301, con el propósito de mejorar la disponibilidad de los servicios al momento de ocurrir alguna eventualidad. Para efecto de la investigación se utilizó la metodología por niveles para dar cumplimiento a cada uno de los objetivos propuestos. Inicialmente se determinó la situación actual de la Unidad Central de Coordinación Informática (UCCI) y se identificaron las principales incidencias las cuales fueron valoradas de muy sensibles a no sensibles. Con la metodología Análisis Modal de Fallos y Efectos (AMFE) se alcanzaron los niveles de probabilidad e impacto de los riesgos así mismo como complemento a la investigación se aplicó la metodología MAGERIT permitiendo identificar los activos de la unidad y las amenazas a las que pueden estar expuestos. Finalmente se elaboró el Modelo de Gestión de Continuidad, fundamentado en las siguientes fases: Alcance del Plan de Continuidad de Negocio (BCP), Evaluación de Riesgos, Análisis de Impactos de Negocios (BIA), Estrategias de Recuperación y Desarrollo del Plan. Se concluye que la UCCI está expuesta al 59% de riesgos críticos causados por amenazas de acuerdo al análisis realizado con un nivel alto de criticidad, por lo que el modelo propuesto permitirá responder significativamente ante posibles incidentes con la finalidad de dar continuidad a las operaciones en beneficios de la comunidad Universitaria.

PALABRAS CLAVES

Infraestructura Tecnológica, Norma ISO 22301, AMFE, MAGERIT, BCP.

ABSTRACT

It is important to recognize the level of relevance that leads to the development of this research, whose main objective is to develop a Continuity Management Model in the Technological Infrastructure of the Eloy Alfaro University of Manabí, based on ISO 22301, for the purpose of improve the availability of services at the time of occurrence any eventuality. For the purpose of the research, the methodology by levels was used to comply with each of the proposed objectives. Initially, the current situation of the Central Computer Coordination Unit (UCCI) was determined and the main incidents were identified, which were assessed from very sensitive to not sensitive. With the Modal Analysis of Faults and Effects (AMFE) methodology, the probability and impact levels of the risks were reached, and as a complement to the research, the MAGERIT methodology was applied to identify the assets of the unit and the threats to which they may be exposed. Finally, the Continuity Management Model was elaborated, based on the following phases: Scope of the Business Continuity Plan (BCP), Risk Assessment, Business Impact Analysis (BIA), Recovery Strategies and Plan Development. It is concluded that the UCCI is exposed to critical risks caused by threats according to the analysis made with 59% of the level of criticality, so that the proposed model will significantly respond to possible incidents in order to continue operations in benefits of the University community.

KEYWORDS

Technological Infrastructure, ISO 22301 Standard, AMFE, MAGERIT, BCP.

CAPÍTULO I. ANTECEDENTES

1.1. DESCRIPCIÓN DEL PROBLEMA

Hoy en día a nivel mundial el Estándar Internacional ISO (2016), establece que la Continuidad de Negocio es el término para referirse a las estrategias y planificación, mediante las cuales las organizaciones se preparan para dar respuesta a eventos catastróficos tales como incendios, inundaciones, ataques cibernéticos, accidentes o errores humanos. Por esta razón es importante adoptar medidas y planes que mitiguen el impacto ante cualquier incidente o riesgo; por lo ante expuesto es necesario aplicar la norma ISO 22301 del Sistema de Gestión de Continuidad de Negocio (SGCN) que permite definir los procedimientos a seguir tal como lo define cada una de sus cláusulas ligadas al modelo PHVA.

Considerando la alta competencia de un mundo globalizado expuesto día a día la Continuidad de Negocio reafirma claramente que se debe hacer en el antes, durante y después de un evento de crisis. Así mismos en los últimos años algunas entidades a lo largo del territorio nacional se han expuesto a un ambiente de negocios muy dinámico con mucha competencia y alto riesgo, esta realidad conlleva a los organismos a planear el control de los posibles impactos de negocio de forma anticipada bajo un análisis integral interdisciplinario.

Con estos antecedentes, es pertinente estimar lo normado dentro del Sistema de Gestión de Continuidad de Negocios, ya que si bien es cierto, toda organización tiene la necesidad de definir los requisitos relativos para la Continuidad del Negocio; la norma determina como tratar y desarrollar los procedimientos para la gestión de un evento disruptivo. Es por esto que la presente investigación se enfocará en la Universidad Laica Eloy Alfaro de Manabí, misma que no tiene establecido puntualmente que se debe de hacer al momento que ocurra un evento que afecte la infraestructura tecnología de la Institución.

1.2. OBJETIVOS

1.2.1. OBJETIVO GENERAL

Proponer un modelo de Gestión de Continuidad en la Infraestructura Tecnológica de la ULEAM aplicando el estándar internacional ISO 22301, para mejorar la disponibilidad de los servicios, activos y recursos de información al momento de ocurrir alguna eventualidad o incidencia.

1.2.2. OBJETIVOS ESPECÍFICOS

- Determinar la situación actual de la infraestructura tecnológica en la ULEAM, en referencia a los requisitos establecidos en la norma.
- Identificar las principales incidencias o riesgos que pueden interrumpir la Continuidad del Negocio, para la aplicación de acciones y mitigación de los mismos, en base a la ficha de riesgos de la metodología AMFE (Análisis Modal de Fallos y Efectos)
- Diseñar el modelo de Gestión Continuidad de Negocios para la infraestructura tecnológica de la institución, que permita avalar la continuidad de las operaciones ante la ocurrencia de eventos imprevistos.

1.3. IDEA A DEFENDER

La elaboración de un modelo de Gestión de Continuidad del Negocio basado en la Norma ISO 22301, permitirá conocer las acciones a seguir en caso de una eventualidad en la infraestructura tecnológica de la ULEAM.

CAPÍTULO II. REVISIÓN BIBLIOGRÁFICA

MODELO DE GESTIÓN DE CONTINUIDAD EN LA INFRAESTRUCTURA TECNOLÓGICA

Un modelo de gestión es un sistema por el cual se llevan a cabo distintas funciones de una organización, según García (2015) y Euskalit (2018) testifican que en un modelo de gestión deben tomarse en cuenta medidas que contemplen aspectos económicos, logística, talento humano y marketing; además que es vital considerar los servicios institucionales, con el fin de involucrar estos conceptos en el marco del modelo de gestión. Es indispensable añadir que los nuevos tiempos requieren empresas más competitivas, que ofrezcan mejores servicios y estén en constante innovación, lo que hace necesario la realización y ajustes de sistemas de gestión adaptados a los nuevos productos y servicios tal como lo afirma la Guía Operativa Modelos de Gestión (2018).

Así mismo Pradel y Climent (2018) declaran que las organizaciones están permanentemente en competitividad con el entorno, razón por la que es necesario aplicar los grandes beneficios que brindan los modelos de gestión y eso obliga a mejorar la disciplina y el enfoque para contribuir a la elevación del nivel de vida social. Adicionalmente Gette, Sánchez, Salgado y Peralta (2018) puntualizan que para enfrentar los desafíos de productividad y competitividad, las organizaciones consideran la implementación de modelos de gestión, que estimulen la mejora sistemática y continua.

Es sustancial resaltar que un modelo de gestión eficiente debe estar asociado a una Infraestructura Tecnológica, que fortalezca los procesos a través de aplicaciones informáticas, y a la vez permita el desarrollo de las actividades con más rapidez y menor posibilidad de errores, además es preciso argumentar que hoy en día la Infraestructura se convierte en la base fundamental de toda organización, debido a que cuentan con la integración de equipos para desarrollar su negocio.

En relación a lo expuesto en el párrafo anterior Morales, Cedeño, Párraga y Molina (2018) coinciden que las infraestructuras tecnológicas tienen como objetivo indispensable satisfacer las necesidades de una organización, de tal forma que los procesos se vuelvan más eficientes; complementando la investigación Cedeño (2017) narra que la utilización de una infraestructura adecuada garantiza el desarrollo regular de funciones tecnológicas de las instituciones.

La infraestructura tecnológica de la gestión universitaria puede estar constituida por elementos sólidos, que permitan llevar a cabo las funciones de gestión acordes a los requerimientos de la organización. Al mismo tiempo esta infraestructura debe poseer altos niveles de seguridad por la delicadeza de la información que se maneja, garantizando un recurso óptimo en la gestión. En síntesis, una infraestructura tecnológica está compuesta por una parte de software y una parte de hardware, que conformados hacen posible la gestión tecnológica. Esta combinación es meritoria para poder acoplar las funciones y servicios de las instituciones, dando lugar a una plataforma informática con características administrativas.

Las principales funciones de la infraestructura tecnológica están enmarcadas en los beneficios que ofrece, mismas que a continuación se detallan: Lograr la integración de servicios de manera eficiente, garantizar la operatividad óptima administrativa, consolidar la agilidad de respuestas y mejorar los costos aportando soluciones eficientes.

De igual forma es necesario sostener que un modelo de gestión con una infraestructura tecnológica acorde a las características de la empresa, debe considerar lo que estable los estándares internacionales. Por lo es preciso discernir la Norma ISO, expuesta por Van Der Berghe (2018), que indica que estas reúnen los requisitos que debe cumplir toda organización para obtener procesos de calidad y eficiencia.

Es evidente entonces que la Norma ISO 22301 (2012) ha evolucionado en base a la norma BS25999-2, siendo la primera norma internacional para la Gestión de la Continuidad de Negocio (GCN), desarrollada a contribuir con las organizaciones tanto Públicas como Privadas, permitiendo implementar las normas de acuerdo a los requerimientos Castro (2013). Consecuentemente Loján, Navarro y Cagua (2017) comentan sobre los nuevos conceptos introducidos en la Norma ISO 22301, y hacen énfasis en el liderazgo de la alta dirección para dar secuencia al aseguramiento de la compatibilidad del SGCN. De igual forma Tellez (2015) diserta que la verdadera visión dentro de la Norma Internacional de Gestión de Continuidad del Negocio se establece en principios y terminología.

La Norma ISO 22301 ofrece una base de conocimientos relacionados con la instauración de la Continuidad de Negocio en las instituciones, cabe recalcar que contiene elementos para continuar trabajando aun en situaciones imprevistas, sin perder la calidad del producto ni la reputación del negocio. Así mismo pretende evitar los contratiempos producidos por posibles desastres, que vienen asociados a la gestión administrativa, igualmente evitan la pérdida de tiempo causada por incidencias y situaciones inesperadas que podrían ocasionar el retraso en la prestación de servicios y calidad del producto, como aquellos eventos inesperados que afectan la continuidad del proceso de negocios.

Cabe mencionar que en las últimas décadas, después de algunos acontecimientos traumáticos sufridos por empresas a nivel mundial, varios autores entre ellos Tellez (2015) expresan que el Sistema de Gestión de Continuidad del Negocio se lo conoce como una estrategia y modo de una organización para recuperar, restituir funciones, planificar y responder ante sucesos o desastres que tengan algún tipo de incidencia en la disponibilidad de recursos a nivel de información.

En concordancia con lo antes mencionado y teniendo en cuenta lo que indican Figueroa y Salamanca (2013) se interpreta como Continuidad de Negocio a la

capacidad estratégica y táctica de las organizaciones, para responder ante desastres o incidentes mayores que interrumpan el negocio, con la intención de reanudar las operaciones en un tiempo aceptable.

Como se puede inferir Quevedo (2012) asevera que el SGCN es un proceso efectuado por el personal, que implementan respuestas efectivas para que la operatividad del negocio continúe de una manera razonable. Así mismo coincidiendo con el criterio de otros autores Olarte (2016) difunde que la Continuidad del Negocio es considerable dentro de los planes, puesto que al no contar con estos preceptos hace que las organizaciones sean vulnerables. Por consiguiente es esencial tener presente lo que enaltece Morales (2014) en cuanto a la implementación de un plan de Continuidad del Negocio, deben existir dos factores inevitable: Compromiso y Conocimiento de las personas encargadas del desarrollo.

Es necesario destacar que toda Institución tanto Pública como Privada, al momento que quiera ser certificada por estos estándares, deben ser avalados por Instituciones especializadas en el tema de Continuidad de Negocio, los mismos que se hallan bajo el enfoque de la Norma ISO 22301 (Sáez, 2018).

Es trascendental reconocer que cuando una Organización implemente el Sistema de Gestión de Continuidad, debe ir en concordancia con la metodología de trabajo ofrecido que es el ciclo de vida PHVA (Planificar, Hacer, Verificar y Actuar) Echeverría (2013), que es una guía básica para la gestión de actividades y procesos, ofreciendo una estructura ejemplar de un sistema aplicable para cualquier organización, tal como lo determina Tellez (2015).

En término general Oviedo (2016) explica que la adopción del ciclo PHVA actúa sobre los procesos y no sobre las personas, de ahí la gran jerarquía que tiene el compromiso gerencial, pues en este nivel es donde se deben buscar las estrategias que permita a las empresas liderar el mercado, ser auto sostenible y rentable. Así mismo es significativo reconocer la trayectoria del modelo PHVA, ya que es un estándar presentado inicialmente por Deming en la

década de 1950, así lo acentúa en la investigación Ocrospoma (2017). A continuación se presenta la relación entre las fases del PHVA y las cláusulas referidas en la Norma ISO 22301 (Tabla 2.1).

Tabla 2. 1. Comparativa entre Modelo PHVA y la Cláusula de la Norma ISO 22301

MODELO PHVA	CLÁUSULA ISO 22301	CONTENIDO
P (Plan) Planificar	Cláusula Nº4: Contexto de la Organización	Introduce los requerimientos obligatorios para construir el contexto del Sistema de Gestión de Continuidad del Negocio (SGCN) en la organización
	Cláusula Nº5: Liderazgo	Resume los requisitos específicos de la función de la alta dirección.
	Cláusula Nº6: Planificación	Describe los requisitos relativos al establecimiento de los objetivos estratégicos y de los principios de guía para el SGCN en su conjunto.
	Cláusula Nº7: Apoyo	Apoya las operaciones del SGCN relativas a la determinación de las competencias y al establecimiento de comunicaciones.
D (Do) Hacer	Cláusula Nº8: Operación	Define los requisitos relativos a la Continuidad del Negocio, determina como tratar y desarrollar los procedimientos para la gestión de un incidente disruptivo.
C (Check) Verificar	Cláusula Nº9: Evaluación del Desempeño	Sintetiza los requisitos necesarios para medir el rendimiento de la gestión de la Continuidad del Negocio.
A (Act) Actuar	Cláusula Nº10: Mejora	Identifica y actúa sobre las no conformidades del SGCN por medio de las acciones correctoras.

Elaborado por: Las autoras.

En contexto general la Norma ISO 22301 sostiene las fases PHVA que permite elaborar el Plan de Continuidad de Negocios (BCP), de acuerdo a lo mencionado por Rojas (2017) un plan emergente permite equilibrar la estabilidad del negocio ante situaciones de contingencia o adversidad, apropiándose de las prevenciones y los procedimientos para la restauración del sistema de continuidad.

Este estudio aborda valiosos criterios de varios autores entre ellos el de Sáez (2018) quien describe al Plan de Continuidad del Negocio como una metodología interdisciplinaria, basada en procedimientos y medidas de seguridad, utilizadas para crear y validar planes logísticos. Esta metodología busca reforzar que los productos o servicios continúen siendo entregados, a los diferentes canales de distribución durante una interrupción no planeada.

Al respecto Bautista (2014) narra que el BCP es responsabilidad de la alta gerencia debido a que se encarga de la protección de los activos y la viabilidad de la organización, en afinidad con sus políticas. De igual modo Jácome (2013) esclarece aciertos sobre el Plan de Continuidad, considerándose como un mecanismo de respuesta que promete orden y control durante una interrupción operacional.

Partiendo de lo mencionado por los autores es posible decir que el BCP es un conjunto de acciones preventivas sujetas a circunstancias que dan consistencia al modelo de gestión previo a situaciones extremas, de tal manera que sea efectivo el servicio y la calidad de los productos, manteniendo la imagen y la eficacia de la empresa. Esta prevención o recuperación se hace en base a los objetivos administrativos de la organización, para no interrumpir las funciones inherentes de la gestión.

Dentro de las situaciones extremas, se encuentran inmersos los desastres naturales, que son parte de los posibles riesgos que puede abordar la organización, y es aquí donde interviene el BCP para evitar el decaimiento de las organizaciones frente a los tipos de eventos perjudiciales. No obstante también existen riesgos informáticos que nada tienen que ver con la naturaleza, sino más bien de carácter humano, estos incluso son afrontados por el BCP.

Cabe indicar que en el BCP se debe realizar el Análisis de Impacto del Negocio (BIA), el cual da respuestas a las políticas institucionales que rigen las actividades y los servicios de la infraestructura de las tecnologías de la información, y a su vez que contribuyen a reducir las fallas informáticas dentro de la organización, como sugieren Díaz, Mariño y Sierra (2016) las organizaciones deben estar en constante control de las amenazas y poseer mecanismos de protección que garanticen la correcta operatividad de las funciones y la Continuidad del Negocio.

Por lo antes expuesto es importante certificar que el BIA incluye procedimientos para minimizar los riesgos, que en ocasiones pueden estar sujetos a afectaciones regulares. Este tipo de protecciones debe formar parte de un plan de gestión de la seguridad, que involucre la Continuidad del Negocio en las tecnologías de la información, para que las organizaciones no desestabilicen sus funciones.

En efecto el BIA propone la continuación del negocio a pesar de los posibles desastres suscitados, por ende deberá cumplirse lo establecido en la Norma ISO/IEC 27002, siendo ineludible que cada organización establezca sus propias directrices y sus normativas internas para hacer cumplir el plan. Es apremiante valorar el tiempo que algunos servicios se encuentran fuera de línea para trabajar en los que estén activos y así no deteriorar todo el sistema.

La información dentro de las organizaciones se constituye en uno de los activos más valiosos de la institución por lo que resulta imprescindible sostener a la seguridad de la misma. Cuando se habla de seguridad de la información atribuye a la Norma ISO 27002. Esta norma considera los siguientes elementos como esenciales: establecer, implantar, mantener y mejorar continuamente, todo lo afín con seguridad informática dentro de la organización. Lo que hace que esta norma tenga una preeminencia en la gestión de seguridad informática, de esa manera reafirman Solarte, Enriquez y Benavidez (2015).

La Norma ISO 27002 es una guía de buenas prácticas que puntualiza los objetivos de control y controles recomendables en cuanto a la seguridad de la información, ésta puede ser de gran utilidad ya que proporciona más información sobre cómo implementar esos controles (Crespo, 2013) (ISO 27001. s.f.) (ISO 27000). Sobre la base de las consideraciones anteriores la Norma ISO/IEC 27002 suministra el modelo y conjunto de mejores prácticas que permiten instaurar roles, responsabilidades y mecanismos, cuya finalidad es lograr un adecuado conjunto de controles administrativos, técnicos y físicos en reciprocidad a las exigencias de la institución (Maquera y Serpa, 2017).

Resulta oportuno detallar que la Norma ISO 27002 está compuesta de 14 dominios que caracterizan las áreas que deben ser atendidas para garantizar la seguridad de la información, en estos dominios se proponen 114 controles para poder afianzar la confiabilidad de la seguridad, los cuales se encuentran divididos en tres que son: controles organizaciones, técnicos y normativos, como se puede apreciar en la (Tabla 2.2).

Tabla 2. 2. Estructura de los controles de la Norma ISO/IEC 27002

CONTROLES	DOMINIIOS
Control Normativo	Cumplimiento
Controles Técnicos	Seguridad Física y del Entorno
	Seguridad de las Comunicaciones
	Adquisición, Desarrollo y Mantenimiento de Sistemas
	Control de Acceso
	Criptografía
	Seguridad de las operaciones
Controles Organizacionales	Gestión de Incidentes de seguridad de la Información
	Aspectos de Seguridad de la Información de la Gestión de Continuidad del Negocio
	Gestión de Activos
	Políticas de Seguridad de Información
	Organización de la Seguridad de la Información
	Seguridad de los recursos Humanos
	Relación con los Proveedores

Elaborado por: Las autoras.

Es importante destacar que las Instituciones al implementar un Plan de Negocios eficiente es necesario que tengan definidos los procesos, mismos que constan de un conjunto de metodologías y técnicas necesarias para apuntalar a la efectividad de las actividades y la eficiencia.

Consecuentemente Carrasco (2012) plantea que la gestión de procesos es una disciplina que favorece a la dirección de la empresa a identificar, representar, diseñar, formalizar, controlar, mejorar y hacer más productivos los procedimientos de la organización para lograr la confianza del cliente. Aseverando lo expresado anteriormente la gestión de proceso es la aplicación de sistemas de calidad y de gestión de operaciones para lograr la eficiencia y

eficacia organizacional, además permite impulsar acciones de mejora para la continuidad de los mismos (Matadamas, Morgan y Diaz, 2015).

Por lo consiguiente la gestión por procesos coordina un plan de actividades que se vincule con los objetivos a alcanzar, que seleccione estratégicamente el personal apropiado para cada uno de los procesos a realizar, dándole sentido a una gestión administrativa y operativa de la organización; esta a su vez permite atestiguar la Continuidad del Negocio y la mejora continua del mismo.

Una vez que se han establecido los elementos esenciales para la gestión por procesos, es preponderante concretar un plan de evaluación y mejora continua, que posea las siguientes particularidades: Establecer metas claras, Definir un período de ejecución conciso, Desarrollar una evaluación continua con documentación de soporte y Contrastar con planes eficientes de la misma categoría.

Para fortalecer una gestión por procesos adecuada que de origen a un sistema de gestión de la Continuidad del Negocio, es imperioso tener una cultura organizacional, para lo cual es urgente delimitar parámetros claros en la organización. Por tanto es posible declarar que la cultura organizacional consta de un conjunto de elementos y percepciones, de actitudes, de valores y creencias, de tradiciones dentro de las organizaciones.

En Relación a lo expresado anteriormente es necesario incluir en la investigación aspectos relevantes sobre la Cultura Organizacional que debe poseer toda organización, debido a que se convierte en el patrón de comportamiento observable de una comunidad u organización, a la vez permite a las instituciones a la adecuada toma de decisiones (Marulanda, López y López 2016). Esta perspectiva enfatiza el interés de contribuir al éxito de la organización por medio de las estrategias colaborativas, de modo que impulsa el uso óptimo del talento humano y la generación de una cultura saludable (Ramírez y Dávila, 2018).

Las organizaciones deben tomar en cuenta la seguridad informática para el manejo de información, valorando la capacidad de detectar y responder eficazmente a situaciones de ataques de *phishing*, pérdida de información, pérdida de datos, dentro y fuera de la red industrial.

En ese mismo sentido las organizaciones deben alimentar la proactividad en las redes informáticas para proteger sus datos y evitar los riesgos que podrían producirse en el manejo de las redes. La gestión de riesgos de seguridad informática accede a la organización de la información y la evaluación constante de los riesgos de seguridad. Así pues, es posible afirmar que las amenazas son parte del riesgo y que dan lugar a una situación inesperada, que puede acarrear en la pérdida de la imagen corporativa o del desempeño de la productividad.

De acuerdo a lo versado por Tola (2015) riesgo es la probabilidad de sufrir un ataque y soportar daños por afectaciones procedentes de la unión de una amenaza o vulnerabilidad. Por ello Solarte *et al.,* (2015) afirman que las amenazas son posibles ataques que puede sufrir una organización provocados por un agente interno o externo aprovechando las vulnerabilidades, mismas que se pueden considerar como la capacidad de reacción ante la presencia de un factor que pueda posibilitar una amenaza o un ataque.

La evaluación de amenazas debe hacerse con frecuencia, según los intereses de la organización. En tal sentido la frecuencia de presentación de los eventos puede ser a corto, mediano y largo plazo, cuya intensidad puede ser alta, media y baja. Para tal efecto es importante indicar que existen diferentes metodologías que permiten efectuar un estudio del nivel de confiabilidad y seguridad dentro de un sistema de información, entre ellas la MAGERIT (Metodología de Análisis y Gestión de Riesgo) y la AMFE (Análisis Modal de Fallos y Efectos).

De acuerdo a lo tipificado en el tomo 1 de la MAGERIT, ésta metodología fue elaborada por el Consejo Superior de Administración Electrónica (CSAE), respondiendo a la percepción de la Administración Pública, cuyo objetivo final es apreciar las vulnerabilidades a las cuáles están comprometidos, teniendo en cuenta las diferentes dimensiones de la seguridad tales como: Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad.

MAGERIT atribuye a todo ente que trabaja con información digital y sistemas informáticos, ya que les permitirá conocer cuánto valor está en juego y por ende les ayudará a resguardar los servicios e información que se prestan. Así mismo percibe el riesgo al que están sometidos los elementos de labores, es loable establecer los elementos para el análisis de riesgo (Tabla 2.3).

Tabla 2. 3. Elementos de la MAGERIT

ELEMENTOS	**DESCRIPCIÓN**
ACTIVOS	Elementos del Sistema de Información, soportan la misión de la organización
AMENAZAS	Situaciones que les pueden pasar a los activos, causando un perjuicio a la organización
SALVAGUARDAS	(o contra medidas), son medidas de protección desplegadas para aquellas amenazas no causen tanto daños
IMPACTO	Lo que podría pasar
RIESGO	Lo que probablemente pase

Elaborado por: Las autoras.

Por lo consiguiente, las organizaciones frente a posible eventualidades deben considerar herramientas valiosas tal como lo destaca Merchán (2015) quien discierne que el Análisis Modal de Fallos y Efectos (AMFE), es una herramienta que orienta a la calidad de un producto o proceso mediante un análisis metódico, además consiste en identificar los modos de fallo antes de que estos ocurran, con el propósito de prevenir y eliminar los mismos, o en su defecto minimizar el riesgo ligado a estos.

En definitiva González, Myer y Panchón (2017) sustenta que AMFE puede constituirse en novedoso instrumento que permita evaluar los riesgos del contexto empresarial. Además esta metodología de divide en cuatro etapas que son: Establecimiento de reglas fundamentales, ejecución del AMFE, resumen, reporte del análisis, y actualización del AMFE.

Finalmente en un Modelo de Continuidad del Negocio, puede dar acciones correctivas ante estos riesgos, debido a que brinda los pasos y lineamientos a seguir para que la Institución establezca, implemente y mantenga la Continuidad del Negocio, y con ello llevar controles preventivos y de recuperación en caso de contingencias mayores o críticas, además de pautas estratégicas y de apoyo para la adecuada gestión administrativa y de operaciones (Valverde, 2018).

CAPÍTULO III DESARROLLO METODOLÓGICO

Para efecto de la investigación se determinó realizar el estudio en la Unidad Central de Coordinación Informática de la Universidad Laica Eloy Alfaro de Manabí, con el propósito de elaborar un Modelo de Gestión de Continuidad en la Infraestructura Tecnológica basado en la NORMA ISO 22301, que permita dar continuidad a sus operaciones en beneficio de la colectividad. Esta investigación se desarrolló mediante la metodología por niveles, para ello se empleó el método descriptivo, permitiendo identificar características y aspectos que son relevantes en las áreas de Infraestructura y Redes, Desarrollo, Mantenimiento y Soporte a Usuarios y Operaciones; mismo que se obtuvo a través de la aplicación de la entrevista y *checklist* instrumentos que fueron utilizados para la recolección de datos, así mismo se recurrió al método exploratorio, permitiendo aportar todo lo referente a características, observaciones, comportamientos y elementos que fueron de gran importancia para la elaboración del Plan de Continuidad.

Es importante mencionar que el primer objetivo, partió desde el estudio de la norma ISO 22301, de esta manera se conoció cómo se aplica y lo esencial de cada requisito normativo, además con el propósito de conocer la situación actual de la Infraestructura Tecnológica de la ULEAM se emplearon los instrumentos de investigación antes expuestos, cabe indicar que ésta investigación es de carácter bibliográfica y de campo, consecuentemente en el segundo objetivo, se utilizó la metodología AMFE (Análisis Modal Fallos y Efectos) para la identificación, evaluación y análisis de los riesgos encontrados con respecto a vulnerabilidades y amenazas, de forma que, se proporcionan medidas como acciones de mitigación y criterios de aceptación de acuerdo a los niveles de riesgos establecidos. Finalmente en el tercer objetivo se aplicó la metodología del BCP para proponer un Modelo de Gestión de Continuidad de Negocios en la Infraestructura Tecnológica de la ULEAM, mismo que está compuesto en cinco fases que son: Alcance de proyecto, Evaluación de Riesgos, Análisis de Impactos de Negocios, Estrategias de Recuperación y

Desarrollo del Plan. A continuación se detalla la consecución de objetivos propuestos.

OBJETIVO 1: DETERMINACIÓN DE LA SITUACIÓN ACTUAL DE LA INFRAESTRUCTURA TECNOLÓGICA EN LA ULEAM, EN REFERENCIA A LOS REQUISITOS ESTABLECIDOS EN LA NORMA.

Para iniciar la investigación se procedió a realizar el levantamiento de información, razón por la cual se emitió una solicitud a la máxima autoridad de la Institución, misma que concedió el respectivo aval para efectuar el proceso de ejecución (Anexo 1).

Seguidamente se aplicó la entrevista al Ing. Becker Briones Veliz Director de la Unidad Central de Coordinación Informática (UCCI) y a los Jefes de las áreas de Infraestructura y Redes, Desarrollo, Mantenimiento y Soporte a Usuarios, Operaciones, con la finalidad de recolectar los datos que permitieron conocer la situación actual de la Infraestructura Tecnológica de la ULEAM, seguidamente se construyó una matriz para plasmar las respuestas obtenidas en el proceso y para mayor comprensión al momento de analizar la información (Anexo 2).

Además es necesario mencionar que para darle mayor relevancia a la investigación se realizó un compendio bibliográfico de la Norma ISO 22301, con la finalidad de conocer la importancia, el funcionamiento y lo principal de cada requerimiento para emplearse en la ejecución de un Modelo de Gestión de Continuidad de Negocio. También se efectuó un análisis sobre los controles de TI establecidos en la Norma ISO 27002.

Posteriormente dando continuidad a la investigación se aplicó un *checklist* en la UCCI, el cual fue elaborado tomando como referencia los controles establecidos en la norma ISO 27002 y en la Evaluación de Riesgos (EDR), el cual permitió identificar las incidencias de la infraestructura tecnológica, al

mismo tiempo sirvió para verificar la validez de la información que se obtuvo en las entrevistas.

Con los resultados del *checklist* se consideró necesario emplear la escala de Likert por el nivel de importancia que atribuye a la investigación permitiendo determinar los criterios de identificación y ponderación valorizados de la siguiente manera: 1 para Muy Sensible, 2 para Sensible, 3 para Poco sensible y 4 No Sensible, dejando como más relevantes las críticas en intervalos del 1 al 3 (Anexo 3).

Adicionalmente la UCCI brindó información complementaria que permitió argumentar y sustentar algunos procesos que se llevan a cabo en las diferentes áreas de la unidad (Anexo 4).

OBJETIVO 2: IDENTIFICACIÓN DE LAS PRINCIPALES INCIDENCIAS O RIESGOS QUE PUEDEN INTERRUMPIR LA CONTINUIDAD DEL NEGOCIO, PARA LA APLICACIÓN DE ACCIONES Y MITIGACIÓN DE LOS MISMOS, EN BASE A LA FICHA DE RIESGOS DE LA METODOLOGÍA AMFE (ANÁLISIS MODAL DE FALLOS Y EFECTOS)

Con el propósito de obtener resultados que abalicen datos concretos para identificar las principales incidencias o riesgos que puedan interrumpir la Continuidad del Negocio, se aplicó la metodología AMFE, así mismo para complementar dicha información se empleó particularidades de la metodología MAGERIT. A continuación se detalla el procedimiento realizado con cada una de ellas.

Para iniciar con la aplicación de la metodología MAGERIT, primeramente se determinó los activos tecnológicos con los que dispone la Unidad Central de Coordinación Informática de la ULEAM, misma que está claramente

correspondida con la generalidad del uso de las tecnologías de la información (TI).

Consecuentemente considerando que las amenazas son hechos que pueden suceder en cualquier momento, es decir causar daños y por ende comprometer el funcionamiento adecuado de los activos, se procedió a determinar las amenazas a las que podían estar expuestos los mismos.

Cabe indicar que en la metodología MAGERIT se han desarrollado los dos primeros pasos dejando clarificado que los que a continuación se detallan: Determinar las salvaguardas, el impacto y el riesgo no son aplicados porque dichos resultados son validados con la metodología AMFE.

Es preciso fortificar la investigación, con la aplicación de la metodología AMFE, cuya finalidad permitió conocer los riesgos o incidentes relevantes a la situación actual de la infraestructura tecnológica de la Institución. Siendo así que con ésta metodología primero se enumeraron todos los posibles modos de fallo, posteriormente se estableció el índice de prioridad, a continuación se priorizaron los modos de fallos para buscar soluciones.

Además es importante mencionar que la finalidad de la metodología AMFE es proporcionar acciones de mitigación y criterios de aceptación como propuesta de mejora en la ocurrencia de las incidencias y eventualidades que se podrían presentar en la Continuidad del Negocio (Anexo 5).

OBJETIVO 3: DISEÑO DEL MODELO DE GESTIÓN CONTINUIDAD DE NEGOCIOS PARA LA INFRAESTRUCTURA TECNOLÓGICA DE LA INSTITUCIÓN, QUE PERMITA AVALAR LA CONTINUIDAD DE LAS OPERACIONES ANTE LA OCURRENCIA DE EVENTOS IMPREVISTOS.

Finalmente para concluir con la investigación se elaboró el Plan de Continuidad de Negocios basado en el ciclo de vida denominado PHVA tal como lo establece la norma ISO 22301. Por lo cual una vez recopilada la información relevante como aporte a la creación del Plan, se dio continuación a las pautas proporcionadas por la metodología para su desarrollo.

FASE 1: ALCANCE DEL BCP

Para el cumplimiento de esta fase inicialmente se determinó la situación actual de la infraestructura tecnológica de la ULEAM, a través de la entrevista y checklist que se aplicaron para la investigación en las diversas áreas de la UCCI. Además con la finalidad de lograr la adaptación adecuada del Plan de Continuidad de Negocio, se generó una revisión bibliográfica de la norma Internacional ISO 22301 de la cual se seleccionó aspectos relevantes sobre el compromiso que debe existir de la alta Dirección.

Consecuentemente para designar el coordinador de Continuidad del Negocio se exploró información sobre liderazgo y cultura organizacional, con el objetivo de realizar de forma adecuada la elección del talento humano idóneo para desempeñar la función del mismo.
Así mismo para dar legalización al plan se cumplió con la exigencia de la norma ISO 22301, como es la construcción de las políticas de Continuidad de Negocio, en donde permitió establecer características fundamentales que debe poseer la institución, para aquello se desarrolló un estudio de diversos contenidos de fuentes bibliográficas confiables.

De igual forma con el propósito de tener una visión en la organización se realizó un estudio detallado determinando las responsabilidades y funciones organismo competente que será responsable del Plan de Continuidad de Negocios.

FASE 2: EVALUACIÓN DE RIESGOS

Seguidamente se evaluó los riesgos mediante la ficha eventualidades de la metodología AMFE, de la cual, se obtuvo la valoración de las incidencias y amenazas, de acuerdo a la prioridad de la ocurrencia y la magnitud del impacto; dicha matriz permitió lograr determinar los desastres y tomar decisiones en acciones preventiva, correctivas o de contingencias. Consecuentemente para complementar dichos resultados se empleó la metodología MAGERIT, considerando los criterios con respecto a los activos y recursos de información correspondiente a las diferentes áreas de la infraestructura tecnología de la UCCI.

FASE 3: ANÁLISIS DE IMPACTO DE NEGOCIOS (BIA)

Para realizar el compendio del BIA se analizó lo establecido en las normas ISO 22301 y 27002, con el propósito de determinar las incidencias de mayor relevancia que se puedan presentar en cada proceso de las diversas áreas de Infraestructura Tecnológica de la UCCI y su impacto en la entidad, para lo cual se analizó sus principales atribuciones con todos sus procesos definidos.

Además se consideró como medidas preventivas lo referido en la norma ISO 22301 para prevenir y evitar los riesgos que afectan la disponibilidad de las operaciones.

FASE 4: ESTRATEGIAS DE RECUPERACIÓN

Toda vez que se realizó el análisis de los resultados obtenidos de la metodología AMFE y se determinó los riesgos de mayor incidencia, procediendo a la evaluación de los criterios de estrategias de recuperación, tales como: técnica de recuperación, en caso de pérdidas de activos o recursos de información aplicar pasos o mecanismo; recuperación para usuario, efectuar respaldos o rehabilitación de información correspondiente al usuario; alternativas recuperación

y recuperación del negocio, en el caso de una eventualidad o incidentes permita rescatar la información de los recursos disponibles.

Cabe indicar que en las estrategias se consideró los factores tecnológicos, ambientales, humanos y los servicios de la infraestructura tecnológica de la ULEAM, de manera que se garantice el estado y la capacidad del negocio en los procesos que esta ofrece.

FASE 5: DESARROLLO DEL PLAN

Finalmente en ésta fase se desarrolló el plan, que abarcó los requisitos estipulados en el campo de aplicación del SGCN según la ISO 22301; así mismo quedó determinado cuales son las instrucciones a seguir secuencialmente para su aplicación. Para concluir con la investigación se socializará a las autoridades y responsables de la Unidad Central de Coordinación Informática, dejando constancia que dicha propuesta permitirá tomar medidas de control en caso de surgir eventualidades o incidencias en las diferentes áreas de TI.

CAPÍTULO IV RESULTADOS Y DISCUSIÓN

4.1. RESULTADOS

La pertinencia que tiene la investigación se refleja a través de los resultados obtenidos de la metodología por sucesión de objetivos específicos expresada en el capítulo anterior. En este capítulo se indica cómo se llevó a cabo cada uno de ellos.

OBJETIVO 1: DETERMINACIÓN DE LA SITUACIÓN ACTUAL DE LA INFRAESTRUCTURA TECNOLÓGICA EN LA ULEAM, EN REFERENCIA A LOS REQUISITOS ESTABLECIDOS EN LA NORMA.

A partir de las entrevistas aplicadas en las diversas áreas de la Unidad Central de Coordinación Informática de la ULEAM, se efectuó el análisis correspondiente de acuerdo a la información adquirida, la cual sirvió para determinar la situación actual de la infraestructura tecnológica de la Institución:

ANÁLISIS DE LA ENTREVISTA DEL ÁREA GENERAL DE LA UCCI– ULEAM: Una de las principales carencias en la unidad en base al Anexo 2A, es que no tienen un plan de continuidad para casos de eventualidades o incidentes, solo se efectúan controles de riesgos pero no se documentan los procesos de identificación, análisis, evaluación y mitigación de los mismos, por lo tanto, no hay un relevamiento formal de los posibles riesgos. La configuración segura de equipos no se la realiza uniformemente a toda la institución porque no hay implementados dominios que le permita a la unidad distribuir políticas y reglas para este proceso. La poseen la gestión de inventarios con lo que respecta a la unidad, como custodios, pero del resto de los equipos de la institución es manejado por el área de Bienes, tampoco existe un acta de entrega-recepción de los custodios actuales ni información actualizada del estado y ubicación de los equipos.

Tienen implementado políticas de seguridad de información que les permita mantener la confidencialidad, integridad, autenticación y disponibilidad de la información. Cuenta con equipos auxiliares para continuar brindando los servicios en caso de que alguno interrumpa sus funciones, además tienen prioridad para reanudar los servicios. A partir del terremoto del 2016 la Universidad ha sufrido eventualidades de desastre y de incidentes en Ciberseguridad. El tiempo estimado que tienen para restaurar un servicio en caso de desastre natural es de 5 días y los incidentes de Ciberseguridad están en un promedio de 4 horas en contenerlos y recuperar los servicios.

Actualmente la institución tiene 23000 estudiantes y 13000 docentes, por lo que si el servicio sufre una eventualidad, el mayor impacto que tendría sería en el proceso de enseñanza aprendizaje debido a la utilización del sistema de gestión académica y plataforma virtual. Las redes LAN, WAN tienen 25000 usuarios aproximadamente.

Hoy en día la unidad, aunque no tiene un plan de contingencia formalmente establecido y documentado, trabaja con un protocolo de respuestas de incidentes específicos y quien declara la alerta es el director de TI, además cuenta con 14 técnicos en varias áreas de la unidad y 5 administrativos. La alta universidad no puede expresar un compromiso activo con la unidad porque se ve impedida por los agentes externos que le provee recursos y con la comunidad, es decir esto afecta el cumplimiento de los programas o proyectos TI.

ANALISIS DE LA ENTREVISTA DEL ÁREA DE DESARROLLO Y PROGRMACIÓN DE LA UCCI–ULEAM: Los procesos principales que se llevan a cabo en el área de Desarrollo son la Gestión de proyectos y la organización de la metodología de desarrollo (Anexo 2B). Esta área se maneja de acuerdo a lineamientos establecidos en la unidad como Lenguaje de programación PHP y JAVA SCRIPT, diseño HTML y CC y de consulta SQL, para lo que se refiere a una aplicación (programa) nueva, de este modo se

puede determinar si este se desarrolla de forma integrada, semi-integrada o aislada.

El equipo de desarrollo cuenta con 3 personas, lo que se identifica como una insuficiencia de personal en el área puesto que el mínimo de personas que debe tener un equipo de desarrollo es de 5 personas. Utilizan metodologías formales y ágiles como: XP, HAS, CMI; como marco de trabajo el estándar MBC en el lado del servidor, MVVM en el lado del cliente de manera técnica y en los servicios web, el estándar REST para las comunicaciones entre sistemas.

En el almacenamiento de datos se utilizan los gestores POSTGRE SQL y SQL Server, para modelado de datos manejan el lenguaje DAX y en el análisis y transformación de datos el lenguaje M. Actualmente tienen 9 sistemas desarrollados entre formales y semiformales. El control de funcionalidad de estos sistemas, manipulan una herramienta tecnológica que les permite llevar la metodología y el inventario de softwares desarrollados (formales), y en los softwares informales un gestor de ciclo de vida de aplicaciones (SCLA); además cuenta con un repositorio de código fuente.

El tipo de licencia que tienen para el desarrollo de las aplicaciones es abierto ya que sus estaciones de trabajo tienen Windows Estudiantil que está cubierto por licencia gratuita. El mantenimiento que dan soporte a las aplicaciones es mediante fallos de error en base al tiempo que el cliente envíe un error para ser arreglado. No tienen una gestión de cambios y de incidencias formal, solamente es interna cuando ocurre la misma; y, no cuenta con manual de usuarios actualizados ni documentación técnica.

ANÁLISIS DE LA ENTREVISTA DEL ÁREA DE MANTENIMIENTO Y SOPORTE A USUARIOS DE LA UCCI – ULEAM: La principal función de esta área es realizar la reparación a equipos tecnológicos de la institución; darles mantenimiento preventivo y correctivo de los mismos y componentes electrónicos (Anexo 2C). Cuentan con un pequeño stop de insumos y

herramientas, pero igualmente se ha hecho solicitud formal en el proceso de adquisición para más insumos que puedan solventar las necesidades en caso de incidencias por equipos que han cumplido su vida útil. El proceso de solicitud de mantenimiento se lo realiza directamente con el director de la UCCI mediante un oficio formal o a través de llamada telefónica en caso de emergencia, considerando también las prioridades de nivel jerárquico.

La planificación operativa anual (POA) se la efectúa semestralmente tomando en cuenta lo que ocurre en el día a día. Con relación a políticas y reglamentos están aprobadas por el OCS y no todas las aplicaciones tienen desarrollado manuales de usuarios. Los equipos tecnológicos cuentan con 3 años de garantía, según el catálogo electrónico del SERCOP, además se realizan pruebas o testing a los softwares y aplicaciones para verificar el funcionamiento y uso institucional, desde la instalación del sistema operativo hasta los paquetes de ofimática, verificando también el hardware, si este soporta el elemento a instalar. Actualmente cuenta con 1000 licencias de antivirus en Kaspersky, los cuales son instalados en equipos que lo soportan, caso contrario se instala un antivirus gratuito.

El personal del área está capacitado en varios campos y actualizan sus conocimientos con la auto preparación. Existen niveles de accesibilidad hacia los respaldos, estos son autorizados por el coordinador de operaciones a través de credenciales para permitir el acceso y así poder ver los cambios que han surgido y exportar un reporte llevando un proceso protocolario.

ANÁLISIS DE LA ENTREVISTA DEL ÁREA DE OPERACIONES DE LA UCCI–ULEAM: Esta área tiene como función llevar a cabo todos los procesos de monitoreo, tanto en los sistemas como en los equipos de comunicaciones y servidores (Anexo 2D). Actualmente cuenta con políticas para la seguridad de la información tales como: políticas de contraseña, correo institucional y acceso a internet; a pesar de que la gestión de continuidad de servicios no está ejecutada, pero está en proceso de desarrollo, manejan la estrategia de

monitorear los procesos de manera remota para dar solución de manera ágil y así evitar que el usuario final note la caída del sistema.

Otra de las carencias que tiene la unidad son los procedimientos operacionales en TIC, ya que no están definidos en su totalidad. Los equipos críticos son monitorizados frecuentemente al igual que los sistemas de información son comprobados en funcionalidad de acuerdo a los estándares aplicados. Los cambios que se efectúan en los sistemas o aplicaciones son autorizados por el director de área, los registros de auditoría cuando tienen cambios se revisan y coordinan frecuentemente.

Con relación a los registros de actividades y auditorías, algunas aplicaciones tienen incluidas un blog de auditoría, al igual que servidores y servicios web, estos arrojan un reporte trimestral, el control de acceso a la UCCI se la realiza mediante control de dactilares y cámaras.

Directamente no se utiliza una herramienta para monitorear el desempeño, capacidad, disponibilidad y falla de los recursos de información, pero si existen como recursos tecnológicos algunas aplicaciones; la asignación de los recursos para apoyar las operaciones a nivel institucional es lo que más falla, ya que el presupuesto no abastece para asignar todos los recursos necesarios, por ende, se trabaja con lo que cuenta cada área.

ANÁLISIS DE LA ENTREVISTA DEL ÁREA DE INFRAESTRUCTURA Y REDES DE LA UCCI–ULEAM: El área de Infraestructura y Redes encargada de llevar todo lo referente a las tecnologías de información y comunicación (TIC) (Anexo 2E). Tienen una estructura bien definida en las redes LAN, WAN y WIFI, ya que permite conectar 671 equipos en la institución. El control de monitoreo se lo realiza en un período de 12 horas distribuidos en la semana, y hay un técnico de área para atender alguna falla en los equipos de comunicación cuando se presenta alguna emergencia; las herramientas que se utilizan para el monitoreo de red son Nexus, loot de servidores, loot de equipos de comunicación y otros permiten controlar el hacking ético.

Se realizan reportes generales del monitoreo de control, exista o no anomalías en la red. En caso de que se presente alguna anomalía se toman medidas como bloqueo de MAC, IP y otros escaneos más específicos, según la gravedad de la anomalía. El testeo de la red lo hacen los mismos equipos de comunicación, aunque también cada equipo por medio de ping, verifica si otro equipo está logueado, procediendo a emitir un reporte. Esta área tiene una estructura que sigue estándares de conexión, cableado estructurado, llevan a tiempo su control de inventarios de los recursos físicos y lógicos con un modelo de calidad de servicios en toda la red institucional. Además, su capacidad de almacenamiento es bastante amplia de 1TB hasta 8TB, con una velocidad en la red muy eficiente.

Seguido de esto se aplicó el *checklist* del cual se determinó las amenazas, la identificación y valoración según los parámetros de la escala de Likert correspondiente a Muy Sensible equivalente a 1, Sensible con 2, poco sensible con 3 y por ultimo No sensible con 4, comparando así cada índice según su rango o nivel de acuerdo a la información proporcionada por la UCCI.

Posteriormente se presentan las vulnerabilidades halladas, donde se empleó el nivel o clasificación de cada vulnerabilidad y se pudo observar que no sensible cuenta con un total de 148 equivalente al 70% como más alto, seguido de muy sensible con 14%, sensible con 29 equivalente a 14% y poco sensible con 4 equivalente a 2% (Tabla 4.1).

Tabla 4. 1. Total de vulnerabilidades por secciones de la norma.

NIVEL (CLASIFICACIÓN)	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
Muy sensible	29	14%
Sensible	29	14%
Poco sensible	4	2%
No sensible	148	70%
Total	210	100%

Elaborado por: Las autoras.

Así mismo se describe el total de vulnerabilidades de manera detalla por cada una de las secciones que determina las normas y los criterios establecidos (Tabla 4.2).

Tabla 4. 2. *Identificación de vulnerabilidades según la secciones de la normas.*

SECCIÓN	IDENTIFICACIÓN	CANTIDAD
Directrices de gestión de la seguridad de la Información.	Muy sensible	6
	Sensible	0
	Poco sensible	0
	No sensible	0
Roles y responsabilidades en seguridad de la información.	Muy sensible	0
	Sensible	1
	Poco sensible	0
	No sensible	6
Segregación de tareas.	Muy sensible	0
	Sensible	1
	Poco sensible	0
	No sensible	3
Propiedad de los activos.	Muy sensible	1
	Sensible	2
	Poco sensible	0
	No sensible	8
Uso aceptable de los activos y Devolución de activos.	Muy sensible	1
	Sensible	2
	Poco sensible	0
	No sensible	8
Áreas seguras.	Muy sensible	0
	Sensible	0
	Poco sensible	0
	No sensible	2
Seguridad de los equipos.	Muy sensible	8
	Sensible	5
	Poco sensible	1
	No sensible	21
Documentación de procedimientos de la operación.	Muy sensible	3
	Sensible	5
	Poco sensible	1
	No sensible	32
Gestión de cambios.	Muy sensible	0
	Sensible	1
	Poco sensible	0
	No sensible	1

Gestión de capacidades.	Muy sensible	0
	Sensible	0
	Poco sensible	0
	No sensible	9
Separación de los recursos de desarrollo, prueba y operación.	Muy sensible	1
	Sensible	4
	Poco sensible	0
	No sensible	1
Copias de Seguridad de la Información.	Muy sensible	0
	Sensible	1
	Poco sensible	0
	No sensible	8
Registro de eventos.	Muy sensible	3
	Sensible	1
	Poco sensible	0
	No sensible	11
Protección de la información de registro.	Muy sensible	0
	Sensible	1
	Poco sensible	0
	No sensible	3
Gestión de las vulnerabilidades técnicas.	Muy sensible	0
	Sensible	0
	Poco sensible	0
	No sensible	4
Restricción en la instalación de software.	Muy sensible	2
	Sensible	2
	Poco sensible	0
	No sensible	6
Controles de Red.	Muy sensible	0
	Sensible	1
	Poco sensible	0
	No sensible	6
Seguridad de los servicios de red.	Muy sensible	0
	Sensible	0
	Poco sensible	0
	No sensible	5
Segregación en redes.	Muy sensible	0
	Sensible	1
	Poco sensible	0
	No sensible	5
Planificación de la continuidad de la seguridad de la información.	Muy sensible	0
	Sensible	1
	Poco sensible	0
	No sensible	5

Implementar la continuidad de la seguridad de la información.	Muy sensible	1
	Sensible	0
	Poco sensible	0
	No sensible	1
Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	Muy sensible	3
	Sensible	0
	Poco sensible	2
	No sensible	3
TOTAL		**210**

Elaborado por: Las autoras.

Seguido de esto se efectuó la clasificación de vulnerabilidades por áreas, expresada a continuación:

Inicialmente se muestra el total de vulnerabilidades en el área general de UCCI, teniendo como más alto el criterio de muy sensible con 17 equivalente al 48%, seguido de sensible con 16 equivalente al 46% y poco sensible con 2 equivalente al 6% (Tabla 4.3).

Tabla 4. 3. Total de vulnerabilidades en la UCCI.

TOTAL DE VULNERABILIDADES EN LA UCCI		
CLASIFICACIÓN	**FRECUENCIA ABSOLUTA**	**FRECUENCIA RELATIVA**
MUY SENSIBLE	17	48%
SENSIBLE	16	46%
POCO SENSIBLE	2	6%
TOTAL	35	100%

Elaborado por: Las autoras.

Posteriormente se describen el total de vulnerabilidades en el área de desarrollo y programación, teniendo como más alto el criterio de sensible con 7 equivalente al 100% y 0 para la los criterios de muy sensible y poco sensible equivalente al 0% (Tabla 4.4).

Tabla 4. 4. Total de vulnerabilidades en Área Desarrollo.

TOTAL DE VULNERABILIDADES ÁREA DE DESARROLLO		
CLASIFICACIÓN	**FRECUENCIA ABSOLUTA**	**FRECUENCIA RELATIVA**
MUY SENSIBLE	0	0%
SENSIBLE	7	100%
POCO SENSIBLE	0	0%
TOTAL	7	100%

Elaborado por: Las autoras.

Seguidamente se describe el total de vulnerabilidades en el área de Mantenimiento y soporte a usuarios, teniendo como más alto el criterio de sensible y 0 para la los criterios de muy sensible y poco sensible (Tabla 4.5).

Tabla 4. 5. Total de vulnerabilidades en Área Mantenimiento.

TOTAL DE VULNERABILIDADES ÁREA DE MANTENIMIENTO		
CLASIFICACIÓN	**FRECUENCIA ABSOLUTA**	**FRECUENCIA RELATIVA**
MUY SENSIBLE	0	0%
SENSIBLE	1	100%
POCO SENSIBLE	0	0%
TOTAL	1	100%

Elaborado por: Las autoras.

Así mismo se detalla el total de vulnerabilidades en el área de operación, teniendo como igualdad los criterios de muy sensible y sensible correspondiente a 4 equivalente al 50% cada uno y con la cantidad de 0 la de poco sensible equivalente al 0% (Tabla 4.6).

Tabla 4. 6. Total de vulnerabilidades en Área Operación.

TOTAL DE VULNERABILIDADES ÁREA DE OPERACIÓN		
CLASIFICACIÓN	**FRECUENCIA ABSOLUTA**	**FRECUENCIA RELATIVA**
MUY SENSIBLE	4	50%
SENSIBLE	4	50%
POCO SENSIBLE	0	0%
TOTAL	8	100%

Elaborado por: Las autoras.

Por último se describe el total de vulnerabilidades en el área de redes, teniendo como más alto el criterio de muy sensible con 5 equivalente al 62%, seguido de sensible con 2 equivalente al 25% y poco sensible con 1 equivalente al 13% (Tabla 4.7).

Tabla 4. 7. Total de vulnerabilidades en Área Redes.

TOTAL DE VULENERABILIDADES ÁREA DE INFRAESTRUCTURA Y REDES		
CLASIFICACIÓN	**FRECUENCIA ABSOLUTA**	**FRECUENCIA RELATIVA**
MUY SENSIBLE	5	62%
SENSIBLE	2	25%
POCO SENSIBLE	1	13%
TOTAL	8	100%

Elaborado por: Las autoras.

Una vez obtenida esta información se pudo concluir que han existido vulnerabilidades de tipo severas (muy sensibles y sensibles) y leves (poco sensibles) que si bien se detectaron por áreas según la situación actual de la infraestructura.

OBJETIVO 2: IDENTIFICACIÓN DE LAS PRINCIPALES INCIDENCIAS O RIESGOS QUE PUEDEN INTERRUMPIR LA CONTINUIDAD DEL NEGOCIO, PARA LA APLICACIÓN DE ACCIONES Y MITIGACIÓN DE LOS MISMOS, EN BASE A LA FICHA DE RIESGOS DE LA METODOLOGÍA AMFE (ANÁLISIS MODAL DE FALLOS Y EFECTOS)

Con la aplicación de la metodología AMFE en complemento con la MAGERIT, se logró identificar los principales riegos en base las vulnerabilidades con respecto a incidencias y eventualidad que pueden afectar a los activos y recursos de información de las diferentes áreas de la UCCI, haciendo énfasis a los procesos críticos y como se pueden mitigar en la infraestructura tecnológica de la UCCI.

En donde se efectuó la clasificación de los activos que posee la UCCI, considerada de la siguiente manera (Tabla 4.8):

Tabla 4. 8. Clasificación del inventario de activos de la UCCI.

ÍTEM	DETALLE	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
1	EQUIPO ELECTRONICO/SERVIDOR	2	1%
2	EQUIPO ELECTRONICO/MONITOR	14	4%
3	BIENES SUJETOS A CONTROL/TECLADO	34	10%
4	BIENES SUJETOS A CONTROL/MOUSE	34	10%
5	BIENES SUJETOS A CONTROL/PATCH PANEL	2	1%
6	SISTEMAS PARA PROCESAMIENTO DE DATOS/ACCES POINT	9	3%
7	SISTEMAS PARA PROCESAMIENTO DE DATOS/SISTEMA DE APLICACIÓN	1	0%
8	EQUIPO ELECTRONICO/UPS/10 KVA	2	1%
9	EQUIPO ELECTRONICO/COMPUTADORA PORTATIL NOTEBOOK	5	1%
10	EQUIPO ELECTRONICO/CPU	13	4%
11	EQUIPO ELECTRONICO/DISCOS INFORMATICOS/DISCO DURO INTERNO	6	2%

12	EQUIPO ELECTRONICO/RACK	70	20%
13	EQUIPO ELECTRONICO/SWITCH	100	29%
14	EQUIPO ELECTRONICO/RUTEADOR	12	3%
15	EQUIPO ELECTRONICO/MODULO TRANSCEIVER	20	6%
16	EQUIPO ELECTRONICO/TARJETA DE RED	5	1%
17	SISTEMAS PARA PROCESAMIENTO DE DATOS/SOFTWARE	1	0%
18	SISTEMAS PARA PROCESAMIENTO DE DATOS/LICENCIAS	1	0%
19	BIENES SUJETOS A CONTROL/DISCO DURO	5	1%
20	EQUIPO ELECTRONICO/FUENTE DE PODER	3	1%
21	EQUIPO ELECTRONICO/DISCOS INFORMATICOS/DISCO DURO EXTERNO	1	0%
22	BIENES SUJETOS A CONTROL/MEMORIA RAM	2	1%
23	EQUIPO ELECTRONICO/MEMORIA RAM	5	1%
24	EQUIPO ELECTRONICO/MICROPROCESADOR	1	0%
25	SISTEMAS PARA PROCESAMIENTO DE DATOS/FIREWALL	1	0%
TOTAL		349	100%

Elaborado por: Las autoras.

Posteriormente se efectuó también la clasificación de las amenazas a las cuales puede estar propensa las áreas activas de la UCCI según la metodología MAGERIT: [N] Desastres Naturales, [I] De Origen Industrial, [E] Errores y Fallos y no Intencionados y [A] Ataques Intencionados en referencia a los activos y recursos de la información, en la cual se observa mayor relevancia en el área general de la UCCI, siendo la amenaza más critica la de Errores y Fallos y no Intencionados. (Gráfico 4.1 y Tabla 4.9)

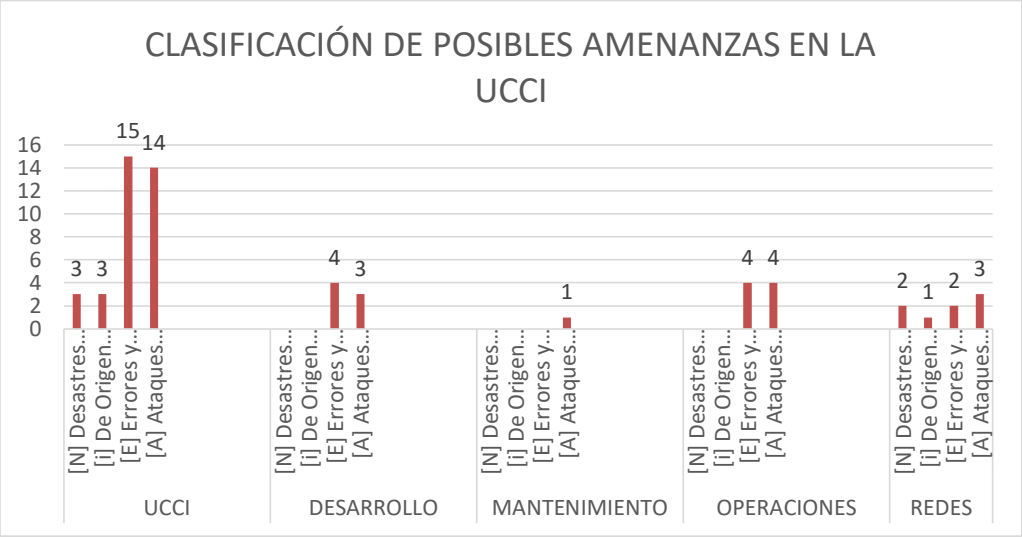


Gráfico 4. 1. Clasificación de las posibles amenazas en la UCCI.
Elaborado por: Las autoras.

Tabla 4. 9. Total de vulnerabilidades en área redes.

ÁREA	AMENAZA	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
UCCI	[N] Desastres Naturales	3	5%
	[I] De Origen Industrial	3	5%
	[E] Errores y Fallos y no Intencionados	15	25%
	[A] Ataques Intencionados	14	24%
DESARROLLO	[N] Desastres Naturales	0	0%
	[I] De Origen Industrial	0	0%
	[E] Errores y Fallos y no Intencionados	4	7%
	[A] Ataques Intencionados	3	5%
MANTENIMIENTO Y SOPORTE A USUARIOS	[N] Desastres Naturales	0	0%
	[I] De Origen Industrial	0	0%
	[E] Errores y Fallos y no Intencionados	0	0%
	[A] Ataques Intencionados	1	2%
OPERACIONES	[N] Desastres Naturales	0	0%
	[I] De Origen Industrial	0	0%
	[E] Errores y Fallos y no Intencionados	4	7%
	[A] Ataques Intencionados	4	7%
INFRAESTRUCTURA Y REDES	[N] Desastres Naturales	2	3%
	[I] De Origen Industrial	1	2%
	[E] Errores y Fallos y no Intencionados	2	3%
	[A] Ataques Intencionados	3	5%
		59	100%

Elaborado por: Las autoras.

Luego de haber obtenido los resultados con la aplicación de la AMFE se realizó la interpretación de los mismos de acuerdo a las áreas existentes.

Del total de vulnerabilidades según los niveles establecidos en el documento AMFE específicamente para la UCCI, se puedo observar que el nivel más alto de vulnerabilidad es medio con 42%, seguido de crítico y alto con 29% y con un total de 0 el nivel bajo (Tabla 4.10).

Tabla 4. 10. Total de vulnerabilidades según niveles AMFE UCCI.

TOTAL DE VULNERABILIDADES SEGÚN NIVELES AMFE UCCI		
NIVEL	**FRECUENCIA ABSOLUTA**	**FRECUENCIA RELATIVA**
CRITICO	10	29%
ALTO	10	29%
MEDIO	14	42%
BAJO	0	0%
TOTAL	34	100%

Elaborado por: Las autoras.

Así mismo el total de vulnerabilidades según los niveles establecidos en el documento AMFE específicamente para el área de Desarrollo se puede

constatar que las vulnerabilidades en el nivel alto corresponden al 57%, seguido de medio con 29%, crítico con 14% y con un total de 0 el nivel bajo. (Tabla 4.11).

Tabla 4. 11. Total de vulnerabilidades según niveles AMFE Área de Desarrollo

TOTAL DE VULNERABILIDADES SEGÚN NIVELES AMFE DESARROLLO		
NIVEL	**FRECUENCIA ABSOLUTA**	**FRECUENCIA RELATIVA**
CRITICO	1	14%
ALTO	4	57%
MEDIO	2	29%
BAJO	0	0%
TOTAL	7	100%

Elaborado por: Las autoras.

También el total de vulnerabilidades según los niveles establecidos en el documento AMFE específicamente para el área de Mantenimiento y Soporte a Usuarios se puede observar que las vulnerabilidades nivel alto corresponden al 100% y 0% para los otros niveles (Tabla 4.12).

Tabla 4. 12. Total de vulnerabilidades según niveles AMFE Mantenimiento y Soporte a Usuarios.

TOTAL DE VULNERABILIDADES SEGÚN NIVELES AMFE MANTENIMIENTO		
NIVEL	**FRECUENCIA ABSOLUTA**	**FRECUENCIA RELATIVA**
CRITICO	0	0%
ALTO	1	100%
MEDIO	0	0%
BAJO	0	0%
TOTAL	1	

Elaborado por: Las autoras.

Por otra parte se detalla el total de vulnerabilidades según los niveles establecidos en el documento AMFE específicamente para el área de Operaciones en donde se puede observar que hay una igualdad en los niveles de vulnerabilidades crítico, alto y medio con un total de 33% por cada nivel y 0% para bajo. (Tabla 4.13).

Tabla 4. 13. Total de vulnerabilidades según niveles AMFE Operaciones.

TOTAL DE VULNERABILIDADES SEGÚN NIVELES AMFE OPERACIONES		
NIVEL	**FRECUENCIA ABSOLUTA**	**FRECUENCIA RELATIVA**
CRITICO	2	33%
ALTO	2	33%
MEDIO	2	33%
BAJO	0	0%
TOTAL	6	100%

Elaborado por: Las autoras.

Finalmente se detalla el total de vulnerabilidades según los niveles establecidos en el documento AMFE específicamente para el área de Infraestructura y Redes, en donde se puedo observar que el nivel alto es el mayor correspondiente al 62%, seguido de crítico con 38% y 0% para medio y bajo respectivamente (Tabla 4.14).

Tabla 4. 14. Total de vulnerabilidades según niveles AMFE Infraestructura y Redes

TOTAL DE VULNERABILIDADES SEGÚN NIVELES AMFE INFRAESTRUCTURA Y REDES		
NIVEL	**FRECUENCIA ABSOLUTA**	**FRECUENCIA RELATIVA**
CRITICO	3	38%
ALTO	5	62%
MEDIO	0	0%
BAJO	0	0%
TOTAL	8	100%

Elaborado por: Las autoras.

Dado este análisis, se procedió a la evaluación de los niveles de la AMFE según su grado de criticidad e influencia de las vulnerabilidades halladas:

RIESGO SEGÚN EL NIVEL CRÍTICO

De la Unidad y las Áreas el riesgo de mayor influencia en aspecto crítico fue el de la UCCI, con un nivel crítico de 10 vulnerabilidades equivalente al 63% de carácter severa (Tabla 4.15).

Tabla 4. 15. Nivel de riesgo critico

NIVEL DE RIESGO CRITICO		
UNIDAD Y SUS ÁREAS	**FRECUENCIA ABSOLUTA**	**FRECUENCIA RELATIVA**
UCCI	10	63%
DESARROLLO	1	6%
MANTENIMIENTO Y SOPORTE A USUARIOS	0	0%
OPERACIONES	2	13%
INFRAESTRUCTURA Y REDES	3	19%
TOTAL	16	100%

Elaborado por: Las autoras.

RIESGO NIVEL ALTO

Así mismo, el riesgo de mayor influencia en aspecto alto fue el de la UCCI, con un nivel de 10 vulnerabilidades equivalente al 45% de carácter severa (Tabla 4.16).

Tabla 4. 16. Nivel de riesgo alto

NIVEL DE RIESGO ALTO		
UNIDAD Y SUS ÁREAS	**FRECUENCIA ABSOLUTA**	**FRECUENCIA RELATIVA**
UCCI	10	45%
DESARROLLO	4	18%
MANTENIMIENTO Y SOPORTE A USUARIOS	1	5%
OPERACIONES	2	9%
INFRAESTRUCTURA Y REDES	5	23%
TOTAL	22	100%

Elaborado por: Las autoras.

RIESGO NIVEL MEDIO

El riesgo de mayor influencia en aspecto medio fue el de la UCCI, con un nivel de 14 vulnerabilidades equivalente al 78% de carácter medianamente severa y leve. (Tabla 4.17).

Tabla 4. 17. Nivel de riesgo medio

NIVEL DE RIESGO MEDIO		
UNIDAD Y SUS ÁREAS	**FRECUENCIA ABSOLUTA**	**FRECUENCIA RELATIVA**
UCCI	14	78%
DESARROLLO	2	11%
MANTENIMIENTO Y SOPORTE A USUARIOS	0	0%
OPERACIONES	2	11%
INFRAESTRUCTURA Y REDES	0	0%
TOTAL	18	100%

Elaborado por: Las autoras.

RIESGO NIVEL BAJO

Cabe indicar, que en el nivel bajo de riesgo no se encontró ninguna, puesto que la mayoría se centraron en el nivel alto, por ser la de mayor influencia con respecto a vulnerabilidades encontradas.

Continuando con el análisis de la investigación, es importante hacer énfasis en los criterios por área, dando por resultado lo siguiente: Que el área que tuvo mayor impacto en cuanto a criticidad fue la del área General de la UCCI con un 59% equivalente a 35 criterios, Redes con el 14% equivalente a 8, seguidamente de operaciones correspondiente a 14% equivalente a 8, desarrollo con 11% equivalente a 7 y por ultimo mantenimiento 2% equivalente a 1, mismos que fueron influencias críticas en algunos de los procesos de la infraestructura tecnológica (Tabla 4.18 y Gráfico 4.2).

Tabla 4. 18. Análisis de criterios de la Unidad y sus Áreas.

UNIDAD Y SUS ÁREAS	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
UCCI	35	59%
DESARROLLO	7	11%
MANTENIMIENTO Y SOPORTE A USUARIOS	1	2%
OPERACIONES	8	14%
INFRAESTRUCTURA Y REDES	8	14%
TOTAL	59	100%

Elaborado por: Las autoras.

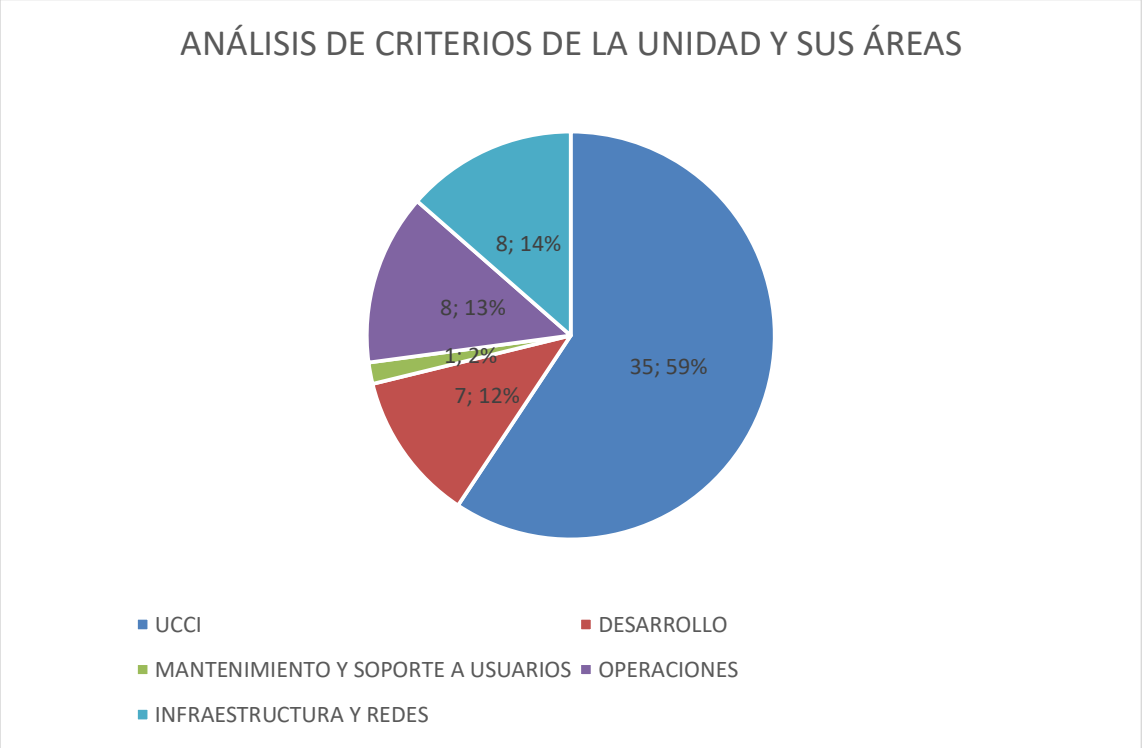


Gráfico 4.2. Análisis de criterios de la Unidad y sus Áreas.
Elaborado por: Las autoras.

OBJETIVO 3: DISEÑAR EL MODELO DE GESTIÓN CONTINUIDAD DE NEGOCIOS PARA LA INFRAESTRUCTURA TECNOLÓGICA DE LA INSTITUCIÓN, QUE PERMITA AVALAR LA CONTINUIDAD DE LAS OPERACIONES ANTE LA OCURRENCIA DE EVENTOS IMPREVISTOS.

Finalmente para en la investigación se elaboró el Modelo de Gestión de Continuidad de Negocios para la Infraestructura Tecnológica de la ULEAM, mismo que al ser aplicado mejorará las acciones a tomar en caso de eventualidades e incidentes que afecte a los procesos que se manejen en las diferentes áreas de la UCCI, y de esta manera se estará previsto con mecanismos y criterios de carácter estratégicos y de apoyo para la protección de los activos y de recursos de la información de la institución.

Cabe indicar que este plan está compuesto por la introducción, alcance, cronología y situación actual de la UCCI, reseña cronológica de la UCCI, análisis de la situación actual, objetivos general y objetivos específicos, marco legal, estructura, propuesta metodológica, métodos y procesos, medidas y controles de Continuidad de Negocio, glosario de términos, marcador no definido, evaluación de riesgos, criterios de la metodóloga MAGERIT, criterios de la metodología AMFE, análisis de impacto del negocio (BIA), características del análisis de impacto, medida preventivas y correctivas, estrategias de recuperación, planificación y políticas para la Continuidad de Negocios de ti, programa de capacitación de responsabilidades y funciones, conclusiones y recomendaciones, bibliografía y anexos, de acuerdo a los requerimientos y composición de la Institución (Anexo 6)**.**

4.2. DISCUSIÓN

El diseño de un Sistema de Gestión de Continuidad del Negocio (SGCN) en base a la norma ISO 22301 permite efectuar la corroboración del cumplimiento de los aspectos que comprende los escenarios actuales y de posible eventualidades, en donde se encuentran inmersos los recursos es de vital importancia dentro de una Institución y que deben ser controlados por una adecuada consecución de procesos y procedimientos que garanticen la disponibilidad continua del personal y de las instalaciones necesarias (Castro,2013). En concordancia a esto, Salazar (2012) afirma que, este tipo de sistema aplicado mediante un plan, determina las actividades de seguridad esperadas, mecanismos de control y prevé los riesgos que se pueden producir en incidentes generados de una eventualidad, ejecutando así mismo, procedimientos de supervisión y revisión dentro de la organización en futuras situaciones.

Es importante indicar que en la actualidad toda organización debe hacer frente a un sin número de amenazas inesperadas que pueden situar en peligro su infraestructura tecnológica; considerando lo anterior la empresa de alimentos TSK de Singapur decidió aplicar un Sistema de Gestión de Continuidad de Negocio, basado en la norma ISO 22301 para identificar las amenazas y proteger sus operaciones, el cual lo puso en marcha cuando existió una contaminación en la empresa, riesgo que pudo ser controlado en muy corto tiempo, lo cual demostró su capacidad de respuesta a situaciones inesperadas (ISO, 2018). Así mismo Cargua (2017) afirma que con la implementación del Modelo de Gestión de Continuidad de Negocio la empresa METALCONSTRUCCIONES CIA.LTDA. logró ser más competitiva y capaz de responder ante cualquier circunstancia no prevista, convirtiéndose en una empresa más invulnerable ante una amenaza que induzca a la interrupción de sus actividades. Finalmente es necesario hacer relevancia al informe AXA PIC. 2007 donde consta que el 80% de las empresas que sufre un incidente crítico cierran al cabo de 18 meses.

Es importante referirse a los resultados expuestos anteriormente por diversos autores en donde se refleja la relevancia de la implementación de un Modelo de Continuidad Negocio, criterios que coinciden con los resultados de la investigación realizada en la infraestructura tecnológica de la ULEAM, por lo que las autoras concluyen que efectivamente existe un alto nivel de criticidad causado por las amenazas y vulnerabilidades razón por la cual fue necesario proponer el Modelo de Continuidad Negocios para ser aplicado en caso de producirse algún tipo de eventualidad que interrumpas sus operaciones y saber cómo actuar antes, durante y después del evento suscitado.

CAPÍTULO V CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

- La Infraestructura Tecnológica de la ULEAM posee medidas de seguridad, pero no se encuentran guiadas ni documentadas, por lo tanto no son efectivamente utilizadas al momento de ocurrir un incidente.(pág. 22-23)

- La metodología AMFE y como complemento la metodología MAGERIT aportan gran ayuda al momento del análisis y gestión de riesgo, además como resultado de esta investigación se concluye que la Unidad Central de Coordinación Informática está expuesta a riesgos críticos causados por amenazas.(pág. 36-37)

- Se elaboró un Modelo de Gestión de Continuidad para la Infraestructura Tecnológica de la ULEAM tomando en consideración el ciclo de vida PHVA, sustentado en la Norma ISO 22301, mismo que proporciona una visión global en cuanto a los riesgos que se han identificados en la Institución, además permite hacer énfasis en la continuidad de las actividades.(Anexo 6)

5.2. RECOMENDACIONES

- Tomar medidas de control en la situación actual que se encuentran la Infraestructura Tecnológica de la ULEAM, misma que permitirá reducir y minimizar riesgos.

- Emplear en la UCCI la metodología AMFE y MAGERIT para el análisis, gestión y monitoreo de la Infraestructura Tecnológica de la ULEAM, con la finalidad de determinar las diversas amenazas, especialmente las que muestra un alto valor de riesgo.

- Aplicar el Modelo de Gestión de Continuidad en la Unidad Central de Coordinación Informática de la ULEAM, cuando se presente un incidente para identificar y analizar las amenazas y evaluar los riesgos, con el fin de proponer estrategias de recuperación que permitan mitigarlos.

BIBLIOGRAFÍA

Asociación Española de Normalización y Certificación [AENOR], (2015ª). Norma Sistema de Gestión de Continuidad del Negocio Directrices. Norma Española UNE-ENiso

AXA Plc. (2007). Empresas que sufren un incidente crítico. Recuperado de: https://www.valoradata.com/vd-continuity/

Bautista, M. (2014). Marco de Referencia para la Formulación de un Plan de Continuidad de Negocio para TI, un caso de estudio. Revista Técnica Energía, 200-207. Recuperado de: http://dspace.udla.edu.ec/handle/33000/3081

Cargua, B. (2017). Implementación de un Sistema de Gestión de Continuidad de Negocio basado en la Norma ISO 22301 para la Empresa Metalconstrucciones Cía. Ltda. Recuperado de: http://repositorio.ute.edu.ec/xmlui/bitstream/handle/123456789/14526/69366_1.pdf?sequence=1&isAllowed=y

Castro, L. (2013). Diseño de un Sistema de Gestión de Continuidad de Negocios (SGCN) para la RENIEC bajo la óptica de la Norma ISO/IEC 22301. Ingeniero Informático Recuperado de: http://tesis.pucp.edu.pe/repositorio/handle/123456789/5110

Cedeño, Y. (2017). Evaluación de la Infraestructura Tecnológica basado en e. stándares de control interno caso: Empresa Nationaltire Experts S.A. Tesis de Ingeniería en Sistemas y Computación. Pontifica Universidad Católica del Ecaudro Sede Esmeraldas. Recuperado de: https://repositorio.pucese.edu.ec/bitstream/123456789/1142/1/CEDE%C3%91O%20RODR%C3%8DGUEZ%20YNGE%20VANESSA.pdf

Echeverría, A. (2013). Herramienta para el diagnóstico de la gestión en gobiernos locales cubanos Ingeniería Industrial. Instituto Superior Politécnico José Antonio Echeverría. vol. XXXIV, núm. 3, pp. 239-251. La Habana, Cuba

Crespo, M. (2013). El análisis de riesgos dentro de una Auditoría Informática: Pasos y Posibles Metodologías. Proyecto de fin de Carrera. Universidad Carlos III de Madrid. Recuperado de:https://e-archivo.uc3m.es/bitstream/handle/10016/16802/PFC_Carmen_Crespo_Rin.pdf?sequence=1&isAllowed=y

Euskalit (2018). Recuperado de: https://www.euskalit.net/archivos/201803/modelogestionavanzada_2018.pdf?1

Díaz, P., Mariño, O., Sierra, F. (2016). Elaboración del análisis de impacto al negocio (BIA) como parte fundamental del plan de continuidad de negocio

de la cadena radial. Extraído de http://polux.unipiloto.edu.co:8080/00002972.pdf.

Figueroa, H. I. y Salamanca, M. E. (2013). Guías para la implementación y auditoria de planes de continuidad de negocio desde la perspectiva de la norma ISO 22301, BS 22599, NTC 5722 y las prácticas profesionales del DRII y de ISACA. Recuperado de: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2621/00000803.pdf?sequence=1

García, D., (2015) Hacia un nuevo modelo de gestión local Municipio y Sociedad Civil en Argentina Recuperado de: http://municipios.unq.edu.ar/modules/mislibros/archivos/gdfgd.pdf

Gette, M., Sánchez, A., Salgado, C. H, Peralta, M. (2018). Gestión de la Calidad en empresas de Software y Servicios Informáticos (SSI) de la República Artentima: Un modelo para su implementación eficiente. XIX Simposio Argentino de Ingeniería de Software (ASSE). Recuperado de: http://sedici.unlp.edu.ar/handle/10915/70880

González, J. C., Myer, R. A., & Panchón-Muñoz, W. (2017). La evaluación de los riesgos antrópicos en la seguridad corporative: del Análisis Modal de Fallos y Efectos (AMFE) a un modelo de evaluación integral del riesgo. Revista Científica General José María Córdova, 15(9), 269-289. Recuperado de: http://dx.doi.org/10.21830/19006586.81

Guía Operativa Modelos de Gestión (2018). Recuperado de: https//www.gorecoquimbo.cl/guía-operativa-moelos-de-gestion-p-v-p-.2018/gorecoquimbo/2018-08-06/094408.html

ISO Organización Internacional para la Estandarización (2018). ISO 22301 para salvar su empresa. Recuperado de: https://www.intedya.com/internacional/intedyanoticias.php?id=123#submenuhome

ISO (International Standard Organization). (2016). ISO 22301: Sistema de Gestión de Continuidad de Negocio. Recuperado de: https://www.isotools.cl/iso/22301/ sistema-gestion–continuidad-negocio

ISO (Organización Internacional para la Estandarización). (2005). ISO ISO/IEC 27002:2005: Tecnologías de la información – Técnicas de Seguridad - Código de buenas prácticas para la Gestión de la Seguridad de la Información. Recuperado de: http://www.iso.org/iso/catalogue_detail?csnumber=50297.

ISO (Organización Internacional para la Estandarización). (2005). ISO ISO/IEC 27001:2005: Tecnologías de la información - Técnicas de Seguridad - Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos Recuperado de:

http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103

Jácome, W. (2013). Administración de Continuidad del Negocio en el Departamento de TI. Recuperado de: http://repositorio.puce.edu.ec/bitstream/handle/22000/12656/Tesis_JacomeWilsonMGTI.pdf?sequence=1

Loján Granda, E., Navarro Espinoza, J., & Cagua Vásquez, C. (2017). Modelo de evaluación de gestión de continuidad del negocio basado en la norma ISO 22301:2012. Revista ESPACIO, 38 (54), 3 Recuperado de: http://www.revistaespacios.com/a17v38n54/a17v38n54p03.pdf

Maquera, H. G., Serpa, P. N. (2017). Gestión de activos basados en ISO/IEC 27002 para garantizar seguridad de la información. Revista Ciencia & Desarrollo, 16, 21 (2), 100-112. Recuperado de: http://revistas.unjbg.edu.pe/index.php/CYD/article/view/510/456

Matadamas, L. S., Morgan, J., Diaz, E. S. (2015). Gestión por procesos como factor de competitividad de PYMES del sector industrial en el estado de Querétaro. Red Internacional de Investigadores en Competitividad, 9, (1), 816-832. Recuperado de: https://www.riico.net/index.php/riico/article/view/45/163

Morales, J. J., Cedeño, L. C., Párraga Álava, J. A., & Molina, B. A. (2018). Propuesta Metodológica para Proyectos de Infraestructura Tecnológica en Trabajos de Titulación. Revista Información Tecnológica, 29(4), 249-258. Recuperado de: http://search.ebscohost.com/login.aspx?direct=true&db=fua&AN=131273589&lang=es&site=ehost-live

Morales Moreno, H. P. (2014). Continuidad del Negocio. Tesis de Licenciatura. Universidad Piloto de Colombia. Recuperado de: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2795/00001618.pdf?sequence=1

Marulanda, C., López, M., López, F. (2016). La cultura organizacional y las competencias para la gestión del conocimiento en las pequeñas y medianas empresas PYMES de Colombia. Información Tecnológica, 27, (6), 3-10. Recuperado de: https://scielo.conicyt.cl/pdf/infotec/v27n6/art02.pdf

Merchán Ulloa, A. C. (2015). Análisis modal de fallos y efectos (AMFE), en el proceso de producción de tableros eléctricos de la Empresa Ec-Box. Recuperado de: http://dspace.uazuay.edu.ec/handle/datos/4278

Ocrospoma, I. (2017). Aplicación del ciclo de Deming para mejorar la productividad en el área de producción de la empresa tecnipack S.A.C,

ATE- 2017. Lima: Universidad Cesar Vallejo. Recuperado de: http://repositorio.ucv.edu.pe/handle/UCV/1711

Olarte Rojas Darío, A. (2016). Propuesta metodológica para la evaluación de la madurez del sistema de gestión de continuidad del negocio en el sector financiero bancario colombiano bajo el enfoque de la norma ISO 22301:2012. Signos, 8(1), 31-44. Recuperado de: http://revistas.usta.edu.co/index.php/signos/article/view/3786

Oviedo Morales, E.D. (2016). Gestión de la continuidad de negocio como factor de confianza empresarial desde la perspectiva de la seguridad informática. Recuperado de: http://polux.unipiloto.edu.co:8080/00002721.pdf

Pradel, M. y Climent,J. (2018) Tranformaciones del modelo de gestión del espacio público de Barcelona. Recuperado de: http://diposit.ub.edu/dspace/bitstream/2445/127303/1/681802.pdf

Quevedo Jesús (2012). Revisión de gestión de continuidad del negocio. Revista de Investigación de Sistemas e Informática 9(1), 91-110. Recuperado de: http://revistasinvestigacion.unmsm.edu.pe/index.php/sistem/article/download/5620/4877

Ramírez, E. y Dávila, E. (2018). Validación de la escala para la caracterización de la cultura organización en MIPYMES. Universidad del Norte, 35. Recuperada de: http://rcientificas.uninorte.edu.co/index.php/psicologia/article/viewFile/11750/214421443449

Rojas Bustamente, J. D. (2017). Propuesta de un Plan de Continuidad de Negocio para una Institución Financiera del Sector Privado Bancario del Ecuador. Trabajo de Titulación de Magister en Gerencia de Sistemas y Tecnología de Información. Universidad de la Américas. Recuperado de: http://dspace.udla.edu.ec/bitstream/33000/7531/1/UDLA-EC-TMGSTI-2017-08.pdf

Sáez Vargas, V.A. (2018). Modelo Integral para la implementación de un Plan de Continuidad. Recuperado de: http://cybertesis.uach.cl/tesis/uach/2013/bpmfcis127m/doc/bpmfcis127m.pdf

Salazar López, G. E. (2012). Plan de Continuidad de Negocios en el Área de TI (Bachelor's thesis, Quito: Universidad de las Américas, 2014.). Recuperado de: http//www. http://dspace.udla.edu.ec/bitstream/33000/2751/1/UDLA-EC-TIS-2012-05%28S%29.pdf

Solarte, F. N., Enriquez, E. R., y Benavides, M. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. Revista Tecnológica ESPOL, 28 (5), 492-507. Recuperado desde: http//www.rte.espol.edu.ec/index.php/tecnologica/article/view/456

Tola, A. M. (2015). Análisis de riegos aplicando la metodología OWASP. Recuperado de DOCPLAYER https://docplayer.es/39436742-Analisisde-riesgos-aplicando-la-metodologia-owasp.html

Tellez Mondragón, C. A. (2015). Diseñar un plan de continuidad del negocio en el proceso de administración de recursos de ti de la oficina de informática y telemática de la alcaldía de Santiago de CALI. Recuperado de http://hdl.handle.net/10614/8037

Van Der Berghe (2018). Aplicación de las normas ISO 9001 a la enseñanza y la educación. Recuperado de: https://es.scribd.com/document/329171158/Dialnet-AplicacionDeLasNormasISO9000ALaEnsenanzaYLaFormaci-131241.pdf

Valverde, H. (2018). PROPUESTA DE UN PLAN DE CONTINUIDAD DE NEGOCIO PARA LA EMPRESA GANADERA PALMIRA S.A CARTAGO, COSTA RICA 2018 .

ANEXOS

ANEXO 1.
OFICIOS DE SOLICITUD PARA LEVANTAMIENTO DE INFORMACIÓN DIRIGÍDO AL RECTOR DE LA ULEAM

Uleam
VIRTUAL
ELOY ALFARO DE MANABÍ

2016-2021

Memorando n.°: ULEAM-R-2018-5729-M

Manta, 10 de septiembre de 2018

PARA: Mg. Dolores Muñoz
DECANA FACULTAD CIENCIAS INFORMÁTICAS

Ing. Bécquer Briones Vélia
Director de la Unidad Central de Coordinación Informática

ASUNTO: **Comunicado**

En atención a comunicación de 27 de agosto, suscrita por la Lic. Yanina Alexandra Viteri Alcivar y María Teresa Cano Montesdeoca, estudiantes de la Maestría en Tecnología de la Información mención Redes y Sistemas Distribuidos de la ESPAM, quienes solicitan se les brinde información referente a su trabajo de investigación "Modelo de Gestión de Continuidad en la Infraestructura Tecnológica de la ULEAM, Basada en la Norma ISO 22301"

Por lo antes expuesto les pido se brinde las facilidades a mencionadas profesionales, con el fin de aportar a su investigación.

Atentamente,

RECTOR

Arq. Miguel Camino Solórzano, MAD
RECTOR UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ

jp

RECIBIDO

Teléfono: 05 2625095 / 2623740 Ext 102
Av. Circunvalación Vía San Mateo

ANEXO 2.
ENTREVISTA EFECTUADA AL DIRECTOR Y LOS JEFES DE LAS ÁREAS DE LA UCCI DE LA ULEAM

ANEXO 2A. ANÁLISIS DE LA ENTREVISTA DEL ÁREA GENERAL DE LA UCCI – ULEAM.

OBJETIVO DE LA ENTREVISTA	Conocer la situación actual de la infraestructura tecnológica en la ULEAM

ÁREA:	UCCI
ENTREVISTADO:	Mgs. Bécquer Briones V.
CARGO:	Coordinador de la UCCI
ENTREVISTADOR:	Ing. María Teresa Cano Montesdeoca y Lic. Yanina Alexandra Viteri Alcívar
1. ¿La Institución cuenta con un Plan de Continuidad de Negocios en caso de una eventualidad o desastre, aprobado por Organismos competentes y de conocimientos de los funcionarios?	La Institución actualmente no cuenta con un Plan de Continuidad para casos de eventualidades.
2. ¿Se ha efectuado un análisis de los posibles riesgos en la Infraestructura Tecnológica de la ULEAM?	Sí, pero no se ha documentado los procesos de Identificación, análisis, evaluación y mitigación por lo que no existe un relevamiento formal de los posibles riesgos.
3. ¿Los equipos informáticos se encuentran configurados de manera segura y poseen uniformidad en toda la organización?	Los equipos que pertenecer a la UCCI si, el resto de equipos no porque no hay implementados dominios Institucional que me permita distribuir políticas y reglas además la mayoría de los equipos están entrando en obsolescencia y no soportan estas implementaciones.
4. ¿Existen inventarios de los equipos de cómputo y dispositivos de comunicación que conforman la red de datos?	La gestión de inventario corresponde al área de bienes; en cuanto a equipos de comunicación UCCI si posee un inventario, pero de computadoras, impresoras u otros periféricos no hay y tampoco existe en la Institución información actualizada de su estado, ubicación y custodio es decir no se cuenta con actas de entrega resección de los custodios actuales.
5. ¿Qué políticas y normativas tienen la UCCI para mantener la confidencialidad, integridad, autenticación y disponibilidad de la información que se genera y cómo se cumplen?	Tenemos una política de seguridad de información, usuario y contraseña, uso de correo electrónico, uso de internet, acuerdo de confidencialidad para la infraestructura tecnológica de la Universidad, acuerdo del buen uso de aplicaciones y servicios de tecnología de la información y el reglamento de seguridad de la información se encuentra listo para segundo debate en el Consejo Universitario.
6. ¿Existen equipos auxiliares que permiten continuar con los servicios en caso de que el	Si, existen equipos auxiliares que permiten continuar brindando los servicios.

equipo principal donde está la base interrumpa sus funciones?	
7. ¿La Unidad tiene determinado cuales son los servicios que deben ser reanudados con prioridad en el periodo de recuperación frente a una eventualidad o desastre?	Como Unidad si tenemos determinado cuales son los servicios que deben ser reanudados con prioridad.
8. ¿La Organización ha sufrido una eventualidad o desastre?	Si, el terremoto de 2016 y varios incidentes de Cyber Seguridad.
9. ¿Cuál fue el tiempo estimado en que se restauraron todos los servicios?	En el caso del desastre natural 5 días y los incidentes de Cyber Seguridad un promedio de 4 horas en contenerlos y recuperar servicios.
10.¿Qué impacto tendría la Institución al no dar continuidad con los servicios que brinda la misma por causa de una eventualidad o desastre?	El proceso enseñanza aprendizaje es el que se vería más afectado por cuanto tenemos 23.000 estudiantes que usan la plataforma, ya sea a través del correo electrónico institucional o aula virtual; además 1300 docentes que verían afectada su gestión con el aula virtual, sistema de gestión académica y el correo institucional; también actividades neurálgicas que tienen que ver con la Gestión Financiera y de Talento Humano, porque estás áreas consumen recursos del Estado.
11.¿Cuántos usuarios se tiene en la red WAN y LAN y que elementos de seguridad tienen?	Las redes WAN y LAN tienen 25.000 usuarios aproximadamente.
12.¿Posee algún plan de contingencia que permitan el normal desempeño de las actividades aun cuando se presenten algún inconveniente? ¿Cómo se lleva a cabo este plan?	Formalmente establecido no, ni documentado. Si existe un protocolo de respuesta para incidentes específicos como los que se han presentado de Cyber Seguridad y quien declara la alerta es el Coordinador de la Unidad.
13.¿Cuántos funcionarios colaboran en la Unidad Central de Coordinación Informática?	El área cuenta con 14 Técnicos en varias áreas y 5 Administrativos.
14.¿Considera que la alta dirección o administración expresa su compromiso o liderazgo en el cumplimiento de los programas o proyectos de ti?	La alta dirección se ve impedida de participar activamente porque la Universidad requiere de una intensa gestión al exterior con los entes que proveen recursos y con la comunidad; muchas de estas actividades han sido delegadas por confianza en el Coordinador articulados con otros Directores.

ANEXO 2B. ANÁLISIS DE LA ENTREVISTA DEL ÁREA DE DESARROLLO Y PROGRAMACIÓN DE LA UCCI – ULEAM.

OBJETIVO DE LA ENTREVISTA	Conocer la situación actual de la infraestructura tecnológica en la ULEAM

ÁREA:	DESARROLLO
ENTREVISTADO:	Ing. Freddy Alarcón
CARGO:	Coordinador Área de Desarrollo
ENTREVISTADOR:	Ing. María Teresa Cano Montesdeoca y Lic. Yanina Alexandra Viteri Alcívar
1. ¿Qué función cumple el área de desarrollo?	La principal función del Área de Desarrollo es la Gestión de Proyectos y la organización de la metodología de desarrollo.
2. ¿Cuándo se desarrolla un sistema se observa cuál es su funcionalidad y operatividad?	Si, técnicamente debe cumplir con los lineamientos que tiene el Departamento como por ejemplo Lenguaje de Programación, herramientas, marcos de trabajo. Como programa depende si es una aplicación nueva se lleva de manera integrada, semi integrada o aislada. El requirente necesita tener claro lo que desea de alguna u otra manera el requirente debe cumplir con los parámetros sugeridos.
3. ¿Qué normas o estándares se emplean para el desarrollo de aplicaciones o sistemas?	Si se habla de normas o estándares son muchas, pero se puede hacer referencia a las Metodologías formales de categoría ágiles porque no se enfocan en una metodología especifica como XP, HAS, CMI, sino que en categorías más amplia porque dan un margen con el cual se puede jugar internamente. Por ejemplo, un equipo de desarrollo tiene que tener 5 personas por proyectos para hacerlo ágil pero el área solo se cuenta con 3 personas, en consecuencia, se trabaja con los recursos disponible. Internamente utilizan el estándar MBC que es un marco de trabajo a nivel de código en temas del Servidor, Marco de trabajo a nivel de Cliente MVVM utilizados de manera técnica; Servicios Web o estándar Rest para comunicaciones entre sistemas. Este año se planea implementar metodologías de entrega.

4. ¿Considera usted que los elementos diseñados en los sistemas cumplen con el criterio de extensibilidad?	Técnicas de reutilización a escala mayor y escala menor.
5. ¿El diseño de software es entendible y de fácil lectura?	Si es de acuerdo a los resultados finales no se ha realizado una encuesta de satisfacción a nivel de diseño, sin embargo, se ha recibido críticas buenas, regulares y malas.
6. ¿Cuál es el lenguaje de programación que utilizan para el desarrollo de software?	Actualmente se utiliza el PHP y JAVA SCRIPT para programar; el estándar HTML y CC para diseño y de consulta SQL; además indirectamente utilizan el Lenguaje DAX para modelado de datos y Lenguaje M para análisis de datos y transformación de datos.
7. ¿Qué Base de Datos utilizan para el almacenamiento de datos?	Se utiliza la Base de Datos POSTGRE SQL y SQL Server y en un 5% MySQL para dos proyectos externos.
8. ¿Aproximadamente cuántos sistemas se han desarrollado para la Institución?	Se han desarrollado 9 sistemas entre formales y semiformales
9. ¿Existe un registro del control de funcionalidad de los sistemas implementados?	Si se utiliza una herramienta que ayuda a llevar la metodología y el inventario de los softwares en desarrollo y para los informales un gestor de ciclo de vida de aplicaciones además se tiene un gestor o repositorio de código fuente.
10.¿Qué tipo de mantenimiento se efectúa a los sistemas y cada qué tiempo se lo realiza?	Se realiza mantenimiento por error en base al poco tiempo y recurso disponible. Prueba el cliente lanza un error se arregla.
11.¿Se encuentran bajo licencia las herramientas utilizadas para el desarrollo de aplicaciones Web?	Si se encuentran con licencias abiertas todas las herramientas para el desarrollo de aplicaciones. Las estaciones de trabajo tienen Windows Estudiantil que está cubierto por licencia gratuita.
12.¿Existe un proceso formal para la gestión de las vulnerabilidades técnicas de los sistemas en uso?	Si se utiliza la herramienta gestión de cambios y gestión de incidencias pero es interna no formal
13.¿Los softwares desarrollados tienen manual de usuarios y documentación Técnica de cómo se han desarrollado?	No se cuentan con manuales de usuarios actualizados ni con documentación técnica.

ANEXO 2C. ANÁLISIS DE LA ENTREVISTA DEL ÁREA DE MANTENIMIENTO Y SOPORTE A USUARIOS DE LA UCCI – ULEAM.

OBJETIVO DE LA ENTREVISTA	Conocer la situación actual de la infraestructura tecnológica en la ULEAM

ÁREA:	MANTENIMIENTO Y SOPORTE A USUARIOS
ENTREVISTADO:	Ing. José Baque Chancay
CARGO:	Director de Área
ENTREVISTADOR:	Ing. María Teresa Cano Montesdeoca y Lic. Yanina Alexandra Viteri Alcívar
1. ¿Qué función cumple el área de mantenimiento y soporte a usuarios?	La principal función es brindar soporte a los usuarios, reparación, mantenimiento preventivo y correctivo de los equipos informáticos y componentes electrónicos.
2. ¿El personal del área de mantenimiento y soporte a usuarios cuenta con los recursos necesarios para dar soluciones inmediatas ante posibles incidentes?	Actualmente se ha adquirido herramientas y se cuenta con un pequeño stop de insumos. Para el nuevo año se está haciendo el proceso para la adquisición y reparación de equipos informáticos para poder solventar los incidentes que se presenten en el 2019, teniendo presente que varios equipos ya han cumplido su vida útil.
3. ¿De qué manera y a quien se realiza la solicitud de mantenimiento de los equipo y software en general?	Directamente se realizan por medio de oficio al Director de la UCCI o directamente con llamada telefónica al área en caso de urgencias y considerando las prioridades de acuerdo al nivel jerárquico.
4. ¿Realizan una planificación de mantenimiento correctivo y preventivo a los activos de tecnologías de la información y comunicación de la Institución?	Si se realiza la planificación semestral que va en conjunto con el POA Institucional. Hay que tener en cuenta la circunstancia que ocurre en el día a día.
5. ¿Existen reglamentos, políticas y manuales de usuario de la UCCI?	En término general es muy extenso, pero se cuenta con algunas plataformas informáticas que si tienen manuales de usuarios para el uso de los sistemas de la Institución. En cuanto a la políticas si existen políticas aprobadas por el OCS.
6. ¿Actualmente poseen equipos con garantía?	Si, se han realizado adquisiciones de equipo informáticos desde computadoras hasta impresoras por medio de catálogo electrónico del SERCOP en el cual consta 3 años de garantía.
7. ¿Se realiza una evaluación periódica al funcionamiento del software?	A nivel de Windows si, realiza los testing de los programas a aplicar para el funcionamiento y uso institucional, desde la instalación del Windows hasta los programas de paquetes de ofimática; también se verifica si el hardware soporta el elemento de software a instalar.
8. ¿Todas las computadoras de la Unidad tienen instalado antivirus y cuentan con licencia?	Si, se adquirió inicialmente un paquete de 650 licencias y después un agregado de 350 completando un total de 1000 licencias en

	Kaspersky. Los cuales se instalan en equipos que soporten porque consume muchos recursos de memoria y en los que no soportan se les instala un programa gratuito.
9. ¿Se capacita al personal del área constantemente de acuerdo a las funciones desempeñadas?	Si se ha recibido capacitaciones en varios campos como mantenimiento de equipos y a nivel de redes. Además, actualizan sus conocimientos con la AUTOPREPARACION.
10.¿Existen niveles de accesibilidad hacia los respaldos y hardware del departamento de tecnología?	Si existen niveles de accesibilidad, para lo cual se solicita al Coordinador de Operaciones que le habilitan credenciales para poder ingresar a ver los cambios que se han dado y sacar algún reporte; mismo que se debe realizar a través de proceso protocolario.

ANEXO 2D. ANÁLISIS DE LA ENTREVISTA DEL ÁREA DE OPERACIONES DE LA UCCI – ULEAM.

OBJETIVO DE LA ENTREVISTA	Conocer la situación actual de la infraestructura tecnológica en la ULEAM

ÁREA:	OPERACIONES
ENTREVISTADO:	Ing. Yuber Zamora
CARGO:	Director de Área
ENTREVISTADOR:	Ing. María Teresa Cano Montesdeoca y Lic. Yanina Alexandra Viteri Alcívar
1. ¿Qué función cumple el Área de Operaciones?	La función que cumple el área es el monitoreo de todos los sistemas, por otra parte, es el monitoreo de los equipos de comunicación y servidores.
2. ¿La institución ha desarrollado un proceso de gestión para continuidad de los servicios?	La Institución no ha desarrollado un proceso de gestión para continuidad de los servicios, recién ahora se están implementando los cambios, a través de las proyecciones que se está dando desde la unidad.
3. ¿Existe alguna reglamentación vigente en la Institución para establecer las políticas de seguridad de la información?	A nivel institucional muy a parte del departamento de TI es el departamento OyM se encarga de institucionalizar los procesos de la Universidad, al hablar políticas de TI existen políticas sobre todo para el uso de contraseña, correo institucional y acceso internet.
4. ¿Cuál es la estrategia que dispone esta unidad para la continuidad de los servicios?	Por lo general están monitoreado permanente mente los procesos, es decir se tiene acceso desde la casa con BPM, llegan notificaciones de los incidentes y se trata de solucionar de la manera más rápida evitando que el usuario se entere que el servicio esta caído.
5. ¿Los procedimientos operacionales de las TIC están definidos y documentados?	Los procedimientos operacionales de TIC no están definidos en su totalidad.
6. ¿Los Equipos críticos de TIC son monitorizados frecuentemente?	Si son monitoreados frecuentemente los equipos.
7. ¿Regularmente se comprueban los sistemas de información para constatar su adecuación de acuerdo a los estándares de seguridad implementados?	Si, constantemente se comprueban los sistemas de información para verificar su funcionalidad de acuerdo a los estándares aplicados.
8. ¿Quién es el responsable de autorizar los cambios en los cronogramas de las operaciones?	El responsable de autorizar los cambios es el Director de área.
9. ¿Se revisan y coordinan las autorizaciones de los cambios en los registros de auditoría?	Frecuentemente si se revisan y coordinan los cambios, existe coordinación entre las áreas.

10.¿Se realizan reportes de registros de actividades y otros registros de auditoría?	Si, ciertas aplicaciones tienen su propio blog de auditoria, así mismo los servidores, servicios Web. Se realiza informe trimestral.
11.¿Se monitorea el acceso autorizado y no autorizado al data center y a la información sensible de la Institución?	Definitivamente el centro de datos tiene accesos dactilares y cámaras.
12.¿Se utiliza alguna herramienta tecnológica para que monitoree el desempeño, capacidad, disponible y falla de los recursos de la información?	No directamente, como recurso tecnológico si existen algunas aplicaciones.
13.¿Se asignan recursos para apoyar las operaciones de los sistemas de información?	A nivel institucional es en lo que más falla la Universidad, no se asignan los recursos necesarios.

ANEXO 2E. Análisis de la entrevista del área de Infraestructura y redes de la UCCI – ULEAM.

OBJETIVO DE LA ENTREVISTA	Conocer la situación actual de la infraestructura tecnológica en la ULEAM
ÁREA:	INFRAESTRUCTURA Y REDES
ENTREVISTADO:	Ing. Cesar Jorge Manrique
CARGO:	Coordinador de Área
ENTREVISTADOR:	Ing. María Teresa Cano Montesdeoca y Lic. Yanina Alexandra Viteri Alcívar
1. ¿Qué función cumple el área de Infraestructura y Redes?	Está área es la encargada de todo lo que tiene que ver con tecnología de la información y comunicación.
2. ¿Cómo están diseñadas las Redes LAN, WAN y redes Inalámbricas?	De una red WAN que se compone de un enlace backup y un principal el cual es la conexión que otorga el proveedor y entra por WAN, se pasa hacia un router principal institucional el que comparte la conexión con los cuatro router que comprenden la infraestructura principal de la red los cuales son para red LAN, Wifi, DMZ y Extensiones. Existen 671 equipos conectados.
3. ¿Se realiza monitoreo a los servicios de la red y cuentan con personal exclusivo para realizar dicha actividad?	Si, se realiza un monitoreo de 12 horas de lunes a viernes y alertas vía mensajes electrónicos que les llega a los técnicos del área que son atendidas en el momento o al día siguiente dependiendo de la gravedad
4. ¿Cuáles son las herramientas que manejan para el monitoreo de los recurso de la red y con qué frecuencia se lo efectúa?	Las herramientas que se utilizan son nexus, loot de servidores, loot de equipos de comunicación y otros aplicativos de control utilizando hacking ético.
5. ¿Se elaboran reportes de monitoreo y en caso de anomalías que acciones se realizan?	Se elaboran reportes de monitoreo generales existan o no anomalías y cuando existen se ve cuál es el tipo de falla o de inconveniente que hay si es algún virus se comunica al departamento técnico el cual se encarga de la revisión del equipo; si son ataque desde fuera o desde dentro de la Institución se hacen bloqueos de mac, ip, escaneos más específicos y se ven cuáles son los incidentes que han causado y se da solución.
6. ¿Los enlaces de la Red se testean continuamente?	Siempre están siendo testeados por los mismos equipos de comunicación, el monitoreo por medio de ping que lo hace cada equipo cada cierto tiempo hacia los otros equipos, este es el que reporta si un equipo este logueado.
7. ¿Qué tipo de cableado utilizan en las redes y qué estándar aplican para el etiquetado?	Se utiliza cableado estructurado categoría 6A blindado y el estándar 186 A.

8. ¿Considera que la velocidad de la red es eficiente?	Si es eficiente la velocidad.
9. ¿Cuántos proveedores de Internet tienen contratados y cuál es el ancho de banda?	Hay contratado 1 proveedor de Internet con 450 de Internet Comercial y 500 de Internet Avanzado.
10.¿Ha sufrido algún incidente de seguridad en la Red?	Si ha sufrido incidente de seguridad como por ejemplo la negación de servicios o ataque DOS y se demoró un día en solucionarlo.
11.¿Qué programas poseen para la identificación y corrección de software malicioso?	Herramientas de seguridad como por ejemplo Nexus, Wireshark entre otros.
12.¿Qué tecnología o técnicas utilizan para dar seguridad a la Red?	Se utiliza el Fireware
13.¿Qué sistemas operáticos utiliza en sus servidores de aplicaciones?	Se utiliza Software Libre: Centos y Red Hat (licenciado), además Windows Server 2016.
14.¿Con qué tipo de servidor cuenta la Unidad Académica y cuán es su capacidad de almacenamiento?	Cuentan con varios Servidores (12 aproximadamente) con distintas capacidades de almacenamiento de 1 hasta 8 TB y de 8 a 64 GB, con tarjeta de Ethernet de 10 GB.
15. ¿A qué recursos y con qué frecuencia se realizan acciones de respaldo y restauración?	A los sistemas de gestión (Gestión Académico, correo electrónico) y a las aplicaciones de la Institución.
16. ¿Qué mecanismo utilizan para la autorización de acceso físico al centro de datos?	Para el Data Center con niveles de control para acceso como biométrico y cámaras de seguridad.
17. ¿Cuentan con inventarios de los recursos lógicos y físicos?	Si
18. ¿Cómo es el control de las IP y qué criterios se tienen en cuenta para asignar la dirección IP a un dispositivo?	Se realiza el control por rango dependiendo de la cantidad de quipo que este en cada área.
19. ¿La cantidad de dispositivos Access points es la adecuada en función del número de usuarios que se conectan, como lo establece el Estándar 802.11?	No, se encuentra en encuentra en proceso de instalación de nuevos equipos para una mejor cobertura tipo MESH.
20. ¿Está implementado un modelo de QoS (Quality of Service) en la red?	Si se encuentra implementado el modelo QoS en toda la Red.

ANEXO 3.
CHECKLIST APLICADO A LA UCCI DE LA ULEAM

ÁREA: UCCI - UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ								
COMPONENTE	**SECCIÓN**	**HITOS**	**S**	**N**	**N/A**	**OBSERVACIÓN**	**PONDERACIÓN**	**IDENTIFICACIÓN**
POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN	**Directrices de gestión de la seguridad de la información**	¿Tienen políticas de seguridad de la información aprobadas por la dirección de la ULEAM?		X			1	Muy Sensible
		¿Estas políticas de seguridad son publicadas y comunicadas a los empleados de TI y partes externas relevantes?					1	Muy Sensible
		Dentro de las políticas de seguridad de la información, ¿está incluida la seguridad física de TI y las copia de respaldo de la información?					1	Muy Sensible
		¿Se revisan las políticas de seguridad de la información con el fin de mejorar la misma y así responder a los cambios del entorno de la universidad y de la UCCI?					1	Muy Sensible
		La Dirección toma en cuenta los resultados de las revisiones de las políticas de seguridad?					1	Muy Sensible
		¿Tienen un sistema de gestión de Continuidad del Negocio?		X			1	Muy Sensible
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	**Roles y responsabilidades en seguridad de la información**	¿Tienen un Manual de funciones y responsabilidades?	X				4	No Sensible
		En este manual ¿se definen las responsabilidades para las actividades de gestión de riesgos de seguridad de la información?	X				4	No Sensible

		¿Existe una guía detallada de ubicaciones e instalaciones de tratamiento de información específicas?	X				4	No Sensible
		¿Existen responsabilidades locales para la protección de activos TI?	X				4	No Sensible
		¿Existen responsabilidades locales para llevar a cabo los procesos de seguridad de la información?	X				4	No Sensible
		¿Hay asignada un área responsable para cada activo o proceso de seguridad de la información?		X			2	Sensible
	Segregación de tareas	¿Se ha hecho segregación de tareas en la UCCI?	X				4	No Sensible
		¿Se realizan controles o monitorización de las actividades que tienen a cargo los empleados en la unidad?	X				4	No Sensible
		¿Se ha realizado auditoría interna a las áreas de la UCCI?		X			2	Sensible
		¿La Dirección realiza un control de las actividades que ejerce la UCCI?	X				4	No Sensible
GESTIÓN DE ACTIVOS	**Propiedad de los activos**	¿Cuentan con un inventario de activos en la unidad?	X				4	No Sensible
		¿En qué formatos llevan el inventario de activos?					4	No Sensible
		a) físicos						
		b) digital	X					
		La UCCI es responsable de los activos	X				4	No Sensible

		tecnológicos de la unidad?						
		¿La UCCI asigna un custodio para los activos tecnológicos dentro de la unidad?	X				4	No Sensible
		¿Cómo hace la asignación de propiedad de los activos tecnológicos la unidad?					4	No Sensible
		a) Por áreas de la institución						
		b) Individualmente en cada área	X					
		c) Mediante oficio						
		d) Informalmente						
		¿La UCCI clasifica los activos y los protege debidamente para asegurar su cuidado?		X			1	Muy Sensible
		¿La unidad revisa periódicamente las restricciones de acceso a los activos más importantes tomando en cuenta las políticas aplicables de control de acceso?	X				4	No Sensible
		¿Llevan los inventarios de los activos de soporte de hardware:	X				4	No Sensible
		a) Equipos Móviles (smartphone, tablets, celular, computadoras portátiles, etc.)	X					
		b) Equipos fijos (servidores, computadoras de escritorio, portátiles, etc.)	X					
		c) Periféricos de entrada (teclado, ratón, escáners, cámara	X					

		digital, cámara web, etc)						
		d) Periféricos de salida (monitor, audífonos, impresoras, proyector, etc.)	X					
		e) Periféricos y dispositivos de almacenamiento (disco duro portátil, disco flexible, grabador de discos, CD, DVD, Blu-Ray, Memoria USB, etc.)	X					
		f) Periféricos de Comunicaciones (Tarjetas USB y tarjeta PCMCIA para redes inalámbricas: WiFi, Bluetooth, GPRS, HSDPA; tarjeta USB para redes inalámbricas/inalámbricas de datos y telefonía, etc.)						
		g) Tableros (de transferencia (baypass) de la unidad de energía (UPS); transferencia de salidas de energía, de transferencia automática de energía, etc.)						
		h) Sistemas de control de acceso, de aire acondicionado, automático de extinción de incendios, etc)						
		¿Llevan los inventarios de los activos de soporte de software?		X			2	Sensible
		a) Sistemas Operativos						
		b) Software de servicio, mantenimiento, administración de : servidores, sistema de redes de datos,						

		sistemas de almacenamiento, telefonía, sistemas de UPS, etc.						
		c) Paquetes de software o software base (suite de ofimática, navegador de internet, mensajería instantánea, etc)						
		¿Llevan los inventarios de los activos de soporte de redes?	X				4	No Sensible
		a) Cable de Comunicaciones (Interfaces: RJ-45, RJ-11, etc; Interfaz: RS232, USB, etc.; Panel de conexión, toma de red o puntos, etc.)	X					
		b) Switches	X					
		c) Router, Firewall, Controlador de red inalámbrica, etc.	X					
		d) Sistema de detección/prevención de intrusos (IDS/IPS), firewall de aplicaciones web, etc.	X					
		¿Existen activos o grupos de activos que no tienen custodios asignados?	X				2	Sensible
	Uso aceptable de los activos y Devolución de activos	¿Se identifican, documentan e implementan reglas de uso aceptable de la información y de los activos asociados de los recursos para el tratamiento de la información?	X				4	No Sensible
		¿Se devuelve un activo cuando el custodio finaliza sus actividades laborales en la institución?	X				4	No Sensible

		¿Se realiza de manera formal esta devolución?	X				4	No Sensible
SEGURIDAD FÍSICA Y DEL ENTORNO	**Áreas Seguras**	¿Se utilizan perímetros de seguridad para proteger las áreas que contienen información sensible así como los recursos de tratamiento de la información?	X				4	No Sensible
		¿Los perímetros de seguridad están claramente definidos en la unidad?	X				4	No Sensible
		¿La situación y fortaleza de cada perímetro está de acuerdo a los requisitos de seguridad de los activos dentro del perímetro y de los resultados de evaluación de riesgo?	X				4	No Sensible
		¿Los perímetros de la instalación donde se trata la información es físicamente sólido (sin huecos en el perímetro o áreas donde se pueden producir rupturas fácilmente)?	X				4	No Sensible
		¿El tejado, muros externos y el piso son de construcción sólida en la unidad?	X				4	No Sensible
		¿Las puertas externas de la unidad están adecuadamente protegidas contra los accesos no autorizados a través de mecanismos de control como barras, cerraduras, alarmas, etc.?	X				4	No Sensible
		¿Se bloquean las puertas y ventanas de las oficinas que están sin uso dentro de la unidad?	X				4	No Sensible

		¿Se ha considerado protección externa para las ventanas, en especial para las que se encuentran a nivel del suelo?	X				4	No Sensible
		¿Existe algún sistema de detección de intruso en la unidad de acuerdo a las normas nacionales e internacionales?	X			SENSORES DE MOVIMIENTO	4	No Sensible
		¿Se registra la fecha y la hora de entrada y salida de los visitantes o personas externas a la unidad?		X			1	Muy Sensible
		¿Se proporcionan las instrucciones de los requisitos de seguridad del área y los procedimientos de emergencia a los visitantes?		X			2	Sensible
		¿El acceso a las áreas dónde se procesa o se almacena información sensible es controlado y restringido únicamente a personal autorizado?	X				4	No Sensible
		¿Se utilizan controles de autenticación para autorizar y validar todos los accesos como tarjetas de control de acceso con número de identificación personal secreto (PIN)?	X				4	No Sensible
		¿Se mantiene y monitoriza de manera segura un libro físico de registro o una pista de auditoría electrónica de todos los accesos?	X				4	No Sensible
		¿Todos los empleados, contratistas y terceros y a todos los visitantes que llegan a la unidad, llevan una identificación visible?		X			2	Sensible

		¿Se notifica al personal de seguridad que se encuentran visitantes sin autorización o alguna persona sin llevar visible la identificación?		X			2	Sensible
		¿El personal proveniente de terceros que prestan servicios de apoyo tiene acceso restringido a las áreas seguras o a los recursos de tratamiento de la información sensible únicamente en caso de ser requerido?	X				4	No Sensible
		¿Este acceso es autorizado y controlado?	X				4	No Sensible
		¿Los derechos de acceso a las áreas seguras son revisados y actualizados regularmente?	X				4	No Sensible
		¿Se diseña y aplica seguridad física a las oficinas, despachos y recursos de la unidad?		X			1	Muy Sensible
		Dentro o fuera de la unidad ¿Se indica de manera discreta la función que tiene y que identifique la existencia de actividades de tratamiento de información?	X				4	No Sensible
		¿Las instalaciones de la unidad están configuradas para prevenir que las actividades o la información de tipo confidencial sean visibles o audibles desde el exterior?		X			1	Muy Sensible

		¿Los directorios o guías telefónicas internas que identifican el establecimiento de los recursos de tratamiento de la información son de fácil acceso a la lectura por personas no autorizadas?		X			4	No Sensible
		¿La unidad cuenta con un diseño aplicable de protección física contra desastres naturales, ataques provocados por el hombre o accidentes?		X			1	Muy Sensible
		¿La unidad tiene asesoramiento especializado sobre cómo evitar daños causados por fuego, inundación, terremoto, explosión, revueltas sociales y otras formas de desastres naturales o provocados por el hombre?	X				4	No Sensible
		¿La unidad tiene un plan de contingencia y de emergencia contra amenazas externas y ambientales?				SEGURIDAD INFORMATICA SI, FISICA NO	1	Muy Sensible
		¿Se han diseñado e implementados procedimientos para trabajar en las áreas seguras?		X			1	Muy Sensible
		¿El personal de la unidad conoce la existencia de un área segura, o de sus actividades, únicamente en el caso de que sea necesario para su trabajo?	X				4	No Sensible

		¿Se evita el trabajo no supervisado en áreas seguras tanto por motivos de seguridad como para evitar oportunidades de actividades maliciosas?	X				4	No Sensible
		¿Las áreas seguras vacías están físicamente cerradas y son comprobadas periódicamente que lo están?		X			2	Sensible
		¿Se permite el ingreso de equipos de fotografía, video, audio u otros equipos de grabación sin autorización?	X				2	Sensible
		El material que entra a la unidad ¿Es inspeccionado para evitar amenazas potenciales como explosivos, productos químicos y otros materiales de riesgo?		X			1	Muy Sensible
		¿El material (equipos tecnológicos) que entra a la unidad es registrado de acuerdo a los procedimientos de gestión de activos?		X			1	Muy Sensible
		¿Se inspecciona el material entrante a la unidad para verificar que no haya sido manipulado durante su traslado?	X				4	No Sensible
		¿Si el material ha sido manipulado se informa de inmediato al personal responsable?	X				4	No Sensible

	Seguridad de los equipos	¿Los equipos están protegidos de forma que reduzcan los riesgos de las amenazas y los riesgos ambientales así como las oportunidades de que se produzcan accesos no autorizados?	X				4	No Sensible
		¿Los equipos dentro de la unidad están situados de tal manera que se minimicen los accesos innecesarios a las áreas de trabajo?	X				4	No Sensible
		¿Los equipos de tratamiento de la información que manejan datos sensibles se encuentran instalados donde se reduzca el riesgo de que la información sea vista durante su uso por personas no autorizadas?	X				4	No Sensible
		¿Se adoptan controles para minimizar el riesgo de posibles amenazas físicas y ambientales?	X				4	No Sensible
		¿Se establecen directrices para comer, beber y fumar en las proximidades de las instalaciones de tratamiento de la información?		x			2	Sensible
		¿Se controlan las condiciones ambientales (temperatura y humedad) que puedan afectar negativamente al funcionamiento de los equipos de tratamiento de la información?	X				4	No Sensible
		¿Se ha aplicado sistemas de protección contra rayos en la unidad?		x			1	Muy Sensible

		¿Se han colocado filtros de protección contra rayos en todas las entradas de corriente eléctrica y en todas las líneas de comunicación?		X			1	Muy Sensible
		¿Se utilizan métodos de protección especial para los equipos?		X			2	Sensible
		¿Se protegen equipos que procesan información sensible para minimizar el riesgo de fugas de información debidas a una emanación electromagnética?	X				4	No Sensible
		¿Los equipos están protegidos contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro?	X				4	No Sensible
		Los suministros de apoyo como electricidad, telecomunicaciones, agua, gas aguas residuales, calefacción/ventilación y aire acondicionado:					4	No Sensible
		a) Están conforme a las especificaciones del fabricante de los equipos y a los requisitos legales locales.	X					
		b) Son evaluados regularmente con respecto a la capacidad de satisfacer el desarrollo de la unidad y a la interacción con otros servicios de apoyo.	X					
		c) Disponen de múltiples fuentes con canales de alimentación	X					

		independientes.						
		d) Se inspeccionan regularmente mediante pruebas apropiadas para asegurar su correcto funcionamiento.	X					
		e) Disponen de alarmas para detectar fallos en su funcionamiento.	X					
		¿Los interruptores y válvulas de emergencia para cortar el suministro de energía, agua, gas u otro servicio están ubicados fuera de las salidas de emergencia o de las salas de equipos?		X			1	Muy Sensible
		¿La unidad tiene redundancia adicional para la conectividad de las redes por medio de múltiples rutas aportadas por sus proveedores de servicios?	X				4	No Sensible
		¿El cableado eléctrico y de telecomunicaciones que transmite datos o que sirve de soporte a los servicios de la información está protegido frente a interceptaciones, interferencias o daños?	X				4	No Sensible
		¿Las líneas de energía y telecomunicaciones en las zonas de tratamiento de la información están soterradas o tienen medidas alternativas de protección?	X				4	No Sensible

		¿Están separado los cables de energía de los de comunicaciones para evitar interferencias?	X				4	No Sensible
		Se ha considerado medidas adicionales para sistemas sensibles o críticos como:	X				3	Poco Sensible
		a) Instalación de conductos blindados y cajas o salas cerradas en los puntos de inspección y terminación.	X					
		b) Uso de apantallamiento electromagnético para proteger los cables.	X					
		c) Implantación de barreras técnicas e inspecciones físicas para detectar la conexión al cableado de dispositivo no autorizado.		X				
		d) Accesos controlados a los paneles de parcheo y a las salas de cableado.	X					
		¿Los equipos reciben un mantenimiento correcto que asegure su disponibilidad y su integridad continua?	X				4	No Sensible
		¿Se llevan registros de todos los fallos, reales o sospechados, así como de todo el mantenimiento preventivo y correctivo dentro y fuera de la unidad?	X				4	No Sensible
		¿Se cumple con todos los requisitos de mantenimiento que exigen las pólizas de seguros?	X				4	No Sensible

		Antes de poner el equipo de nuevo en funcionamiento después de su mantenimiento, ¿Es inspeccionado para asegurar que el equipo no ha sido manipulado y que funciona correctamente?				LOS MANTENIMIENTOS SE REALIZAN EN LA INSTITUCIÓN	4	No Sensible
		¿Los equipos, la información o el software sale de la unidad con autorización previa?	X				4	No Sensible
		¿Los empleados y usuarios de terceras partes que tienen permiso para sacar los activos de la unidad, son claramente identificados?	X			FIRMAN ACUERDOS DE CONFIDENCIALIDAD	4	No Sensible
		¿Se establece un límite de tiempo que el equipo puede estar fuera de la unidad y se verifica a su retorno que se ha cumplido con dicha limitación?	X				4	No Sensible
		¿Se registra la salida de los equipos fuera de la unidad así como su retorno?	X				4	No Sensible
		¿Cuándo sale un equipo, la identidad, las funciones y la afiliación de cualquier persona que maneje o usa los activos de la unidad son documentados y esta documentación regresa junto con el equipo, información o software?	X				4	No Sensible
		La unidad realiza inspecciones al azar a los usuarios internos y externos para detectar salida de activos no autorizados o entrada de dispositivos		X			2	Sensible

		de grabación no autorizados, armas, entre otros?						
		¿Estas inspecciones al azar se llevan a cabo de acuerdo a la legislación y normativa aplicable?			x			
		¿Los usuarios externos tienen conocimiento de que se llevan inspecciones al azar?			x			
		¿Tienen controles de acceso a los ordenadores de la unidad?	X				4	No Sensible
		¿Se comprueban que los equipos contienen medios de almacenamiento o no antes de su retirada o reutilización?	X				4	No Sensible
		¿Se destruyen físicamente los soportes que contienen información sensible o con derechos de autor que hagan imposible la recuperación de la información original?				SE ALMACENAN NO SE DESTRUYE	4	No Sensible
		¿Las técnicas que utilizan para la eliminación segura o reutilización es?					4	No Sensible
		a) Destruir, borrar o sobrescribir sin opción a recuperación.	X					
		b) Borrar o formateado normal						
		¿Los dispositivos de almacenamiento dañados que contienen datos sensibles se evalúan para determinar su destrucción física en lugar de	X				4	No Sensible

		repararse o eliminarse?						
		¿Se hace un cifrado completo a los discos que ya han tenido un borrado seguro para reducir el riesgo de divulgación de la información confidencial cuando el equipo es retirado?	X				4	No Sensible
		En caso de ser redistribuido el/los discos:		X			4	No Sensible
		a) El proceso de cifrado es suficientemente fuerte y cubre el disco completamente (espacio libre, archivos temporales de intercambio de memoria, etc.)						
		b) Las contraseñas de cifrado son suficientemente largas para resistir ataques de fuerza bruta.						
		c) Las contraseñas de cifrado se mantienen confidenciales (nunca se almacenan en el mismo disco duro)						
		¿Las herramientas de sobrescritura segura se revisan para asegurar que son aplicables a la tecnología de los dispositivos de almacenamiento?			x			
		Los usuarios de equipos son asesorados en:		X		SE REALIZA POR INTUICION	4	No Sensible

		a) Terminar las sesiones activas cuando se acaben las actividades en el día.						
		b) Asegurar las sesiones mediante un mecanismo de bloque adecuado como protector de pantalla con contraseña.						
		c) Salir de las aplicaciones o servicios de red cuando ya no se necesiten.						
		d) Asegurar los ordenadores personales o los terminales frente a accesos no autorizados a través de un bloqueo con clave cuando no estén en uso.						
		¿Tienen políticas de puesto de trabajo despejado de papeles y pantalla limpia para los recursos de tratamiento de la información?		X			2	Sensible
		¿La información de negocio sensible o crítica (documentos, almacenamiento electrónico) es guardada en caja fuerte, armario u otro tipo de mueble de seguridad, cuando no se necesita, especialmente cuando la oficina está vacía?		X			2	Sensible

		¿Los ordenadores y terminales se quedan apagados o protegidos mediante un mecanismo de bloqueo de pantalla y teclado mediante contraseña, dispositivo hardware de autenticación de usuario cuando estén desatendidos y protegidos mediante claves de bloqueo cuando no estén en uso?	X				4	No Sensible
		¿Se ha considerado el uso de impresoras con función de código PIN?	X				4	No Sensible
		¿Los soportes que contienen información sensible o clasificada se retiran de forma inmediata de las impresoras?	X				4	No Sensible
SEGURIDAD DE LAS OPERACIONES	**Documentación de procedimientos de la operación**	Los procedimientos operativos especifican las instrucciones para la ejecución detallada de cada tarea como:		X			2	Sensible
		a) Instalación y configuración de sistemas						
		b) El tratamiento o manipulación de la información tanto automatizada como manual						
		c) Copias de respaldo						
		d) Los requisitos de planificación, incluyendo las interdependencias con otros sistemas, con tiempos más tempranos de comienzo y tiempos más tardíos de						

		finalización posibles para cada tarea.						
		e) Instrucciones para manejar errores u otras condiciones excepcionales que puedan ocurrir durante la ejecución del trabajo.						
		f) Los contactos de soporte y escalado, incluye soporte externo en el caso de dificultades operacionales o técnicas inesperadas.						
		g) El reinicio del sistema y los procedimientos de recuperación a utilizar en caso de fallo del sistema						
		h) Los procedimientos de monitorización						
		¿Los procedimientos operacionales y los procedimientos documentados para las actividades del sistema son tratados de manera formal y autorizados por el Director de TI y la máxima autoridad?	X				4	No Sensible
	Gestión de cambios	¿Se identifican y registran los cambios significativos (procesos de negocio, instalaciones de tratamiento de la información y los sistemas) en la unidad?	X				4	No Sensible
		¿Se planifica y se realizan pruebas de los cambios en la unidad?	X				4	No Sensible

		¿Se evalúan los impactos potenciales, incluyendo los impactos en la seguridad de la información de dichos cambios?	X				4	No Sensible
		¿Se realiza el control de procedimientos formales de la aprobación de los cambios propuestos?	X				4	No Sensible
		¿Se verifica que los requisitos de seguridad de la información se cumpla?	X				4	No Sensible
		¿Se comunica los detalles de los cambios a todas las personas correspondientes?	X				4	No Sensible
		¿Se controlan los procedimientos y responsabilidades para abortar y recuperar los cambios infructuosos y los eventos imprevistos?	X				4	No Sensible
		¿Se controla el proceso de cambio de emergencia que habilite la implantación rápida y controlada de los cambios necesarios para resolver un incidente?	X				4	No Sensible
		¿Los procedimientos y las responsabilidades formales de gestión aseguran de manera satisfactoria el control de todos los cambios?	X				4	No Sensible
		¿Se lleva un registro de auditoría que contenga toda la información necesaria cuando se efectúan los cambios?	X				4	No Sensible

	Gestión de capacidades	¿Se aplican sistemas de control y de ajuste para asegurar la mejora de la disponibilidad y de la eficiencia de los sistemas?	X				4	No Sensible
		¿Se han implantado controles de detección de fallos para identificar la existencia de problemas a su debido tiempo?		X			2	Sensible
		¿Se identifican las tendencias de uso, en lo particular a las aplicaciones de negocio o a las herramientas del sistema de gestión de la información?		X			2	Sensible
		¿Los directivos o responsables utilizan los resultados de los sistemas de control y tendencias de uso para evitar posibles cuellos de botellas o dependencias de personal clave que represente una amenaza para el sistema de seguridad o para los servicios y de esta manera planificar las acciones adecuadas?		X			2	Sensible
		¿Tiene la unidad un plan de gestión de la demanda de capacidad?		X			2	Sensible
		En caso de tenerlo, este plan incluye:			x			
		a) Borrado de datos obsoletos (espacio de disco duro)						
		b) Desmantelamiento de aplicaciones, sistemas, base de datos o entornos						

		c) Optimización del tratamiento por lotes y la planificación						
		d) Optimización de la lógica de la aplicación o las consultas de base de datos						
		e) Denegación o restricción del ancho de banda para servicios consumidores de muchos recursos, si estos no son críticos para la unidad y la institución.						
		¿Tiene un plan documentado de gestión de la capacidad para los sistemas de misión crítica?		X			1	Muy Sensible
		¿La unidad controla la capacidad de los recursos humanos, así como oficinas e instalaciones?	X				4	No Sensible
	Separación de los recursos de desarrollo, prueba y operación	¿Se definen y documentan las reglas de transferencia de software desde el estado de desarrollo hasta el estado de operación?	X				4	No Sensible
		¿El software de desarrollo y explotación se ejecuta en diferentes sistemas o procesadores de ordenador y en diferentes dominios o directorios?		X			2	Sensible
		¿Los cambios en las aplicaciones y sistemas en operación son probados en un entorno de pruebas o ensayo de modo previo a ser aplicados en sistemas de operación?	X				4	No Sensible

		¿Los compiladores, editores y otras herramientas de desarrollo o utilidades del sistema son accesibles desde los sistemas de operación cuando es necesario?	X				4	No Sensible
		¿Los usuarios utilizan diferentes perfiles para los sistemas de operación y de prueba, con menú que muestren mensajes de identificación adecuados para reducir el riesgo de error?	X				4	No Sensible
		¿Los datos sensibles en el entorno del sistema de prueba son copiados para proporcionar controles equivalentes en dicho entorno?	X				4	No Sensible
		¿Las actividades de desarrollo y prueba, alguna vez han causado problemas serios como la modificación no deseada de ficheros o del entorno del sistema o fallo del mismo?	X				4	No Sensible
		¿Se ha introducido código no autorizado en el desarrollo y de prueba para cometer fraude o causar problemas operacionales serios?		X			4	No Sensible
		¿La unidad ha separado los recursos de desarrollo, pruebas y operación para reducir los riesgos de acceso no autorizado o los cambios del sistema en producción?	X				4	No Sensible
COPIAS DE SEGURIDAD	**Copias de Seguridad de la Información**	¿Tienen políticas de copias de seguridad?	X				4	No Sensible

		¿Se realizan copias de seguridad de la información, del software y del sistema en la unidad?	X				4	No Sensible
		¿Se verifica periódicamente estas copias de seguridad de acuerdo a sus políticas?	X				4	No Sensible
		¿Se ha establecido una política de respaldo con requisitos para las copias de respaldo de la información, del software y de los sistemas en la unidad?	X				4	No Sensible
		En caso de haber una política de respaldo ¿se ha definido en ella los requisitos de conservación y protección de la información, software y sistemas de la unidad?	X				4	No Sensible
		¿Tienen los recursos adecuados para realizar las copias de respaldo para que toda la información y los softwares esenciales puedan ser recuperados después de un desastre o fallo de los soportes?		X			1	Muy Sensible
		¿Se ha diseñado un plan de respaldo en la unidad?	X				4	No Sensible
		¿Se llevan registros precisos y completos de las copias de respaldo, así como de los procedimientos de recuperación documentados?		X			1	Muy Sensible

		Las copias de respaldo totales o diferenciales y la frecuencia con que se realizan éstas, ¿reflejan los requisitos de la unidad, los requisitos de la seguridad de la información implicada y la criticidad de la información para el funcionamiento continuo de la unidad?	X				4	No Sensible
		¿Las copias de respaldo son almacenadas en un establecimiento alejado, a una distancia suficiente para salvarse de cualquier daño proveniente de un desastre en el establecimiento principal?	X				4	No Sensible
		¿El nivel de protección tanto física como ambiental de la información de respaldo es consistente con las normas aplicadas en la unidad?	X				4	No Sensible
		¿Los soportes de las copias de respaldo se comprueban (funcionamiento de los procedimientos de recuperación y pruebas) periódicamente para asegurarse de su efectividad, que puedan responder en caso de uso de emergencia cuando sea necesario y que puedan cumplirse dentro del tiempo asignado en los procedimientos operacionales para recuperación ?	X				4	No Sensible

		¿Las copias de respaldo están protegidas mediante cifrado, sobre todo en aquellas donde es importante la confidencialidad?		X			1	Muy Sensible
		¿En los procedimientos operacionales supervisan e identifican los fallos de realización de copias de respaldo programadas para garantizar la integridad de las copias de respaldo, de acuerdo con la política de respaldo?	X				4	No Sensible
		¿Las disposiciones de copias de respaldo para los sistemas críticos cubren los sistemas de información, así como las aplicaciones y los datos necesarios para la recuperación del sistema completo en caso de desastre?	X				4	No Sensible
		¿La unidad ha determinado el tiempo de conservación para la información esencial tomando en cuenta cualquier requisito para las copias de archivo que hayan de ser conservadas de manera permanente?		X		NO ESTA NORMADO	2	Sensible
REGISTROS Y SUPERVISIÓN	**Registro de eventos**	¿Se registran, protegen y revisan periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información?	X				4	No Sensible
		Los registros de eventos relevantes que tiene la unidad incluyen:	X				4	No Sensible

		a) Identificadores (ID) de usuario.	X					
		b) Actividades del sistema.	X					
		c) Fechas, tiempos y detalles de eventos claves, ejemplo: conexión (log-on) y desconexión (log-off).	X					
		d) Identidad o localización del dispositivo, si es posible identidad del sistema.	X					
		e) Registro de intentos de acceso a los sistemas exitosos y fallidos.	X					
		f) Registro de intentos de acceso a los recursos y a los datos exitosos y fallidos.	X					
		g) Cambios en la configuración del sistema.	X					
		h) Uso de privilegios.	X					
		i) Uso de utilidades y aplicaciones del sistema.	X					
		j) Ficheros a los que se ha accedido y el tipo de acceso.		X				
		k) Direcciones y protocolos de red.	X					
		l) Alarmas generadas por el sistema de control de acceso.	X			NO ESTAN ACTIVAS A NIVEL DE EQUIPO A NIVEL DE APLICACIONES		

						SI		
		m) Activación y desactivación de los sistemas de protección, como sistemas antivirus y de detección de intrusión	X					
		n) Registro de transacciones ejecutadas por usuarios en las aplicaciones.	X					
		¿Se han tomado medidas adecuadas de protección de la privacidad en los registros de eventos?		X			2	Sensible
		¿Los administradores del sistema tienen permiso para borrar o desactivar los registros de sus propias actividades?		X			4	No Sensible
	Protección de la información de registro	¿Los dispositivos de registro y la información del registro están protegidos contra manipulaciones indebidas y accesos no autorizados?	X				4	No Sensible
		Los controles de protección contra los cambios no autorizados y los problemas operacionales relativos a los dispositivos e información de registro, incluye:	X				4	No Sensible
		a) Alteraciones en los tipos de mensajes que son registrados.	X					

		b) Edición o borrado de los ficheros de registro.		X				
		c) Superación de la capacidad de almacenamiento de los soportes de ficheros de registro, provocando bien un fallo del registro de eventos o bien sobrescribiendo los registros de eventos pasados.		X				
		¿Se archivan los registros de auditoría como parte de la política de conservación de registros o debido a requisitos para recopilar y conservar evidencias?	X				4	No Sensible
		¿El copiado en tiempo real de los registros se lo realiza en un sistema fuera del control del administrador u operador del sistema?	X				4	No Sensible
GESTIÓN DE LA VULNERABILIDAD TÉCNICA	**Gestión de las vulnerabilidades técnicas**	¿La unidad ha establecido las funciones y responsabilidades asociadas a la gestión de las vulnerabilidades técnicas, incluyendo la supervisión de las mismas, la evaluación de los riesgos de la vulnerabilidad, el parcheo, el seguimiento de activos y cualquier responsabilidad de coordinación necesaria?		X		CONFIRMAR CON EL ING. BECQUER	1	Muy Sensible

		¿Se identifican los recursos de información que se utilizan para identificar las vulnerabilidades técnicas pertinentes para mantener la alerta sobre ellas, tanto para el software como para otras tecnologías (inventario de activos)?	X				4	No Sensible
		¿Se ha definido una escala temporal para reaccionar a las notificaciones de vulnerabilidades técnicas que puedan resultar relevantes?		X			2	Sensible
		¿Cuándo se ha identificado la vulnerabilidad técnica, la unidad identifica los riesgos asociados y las medidas que se deben adoptar, como el parcheo de sistemas vulnerables o la aplicación de otros controles?	X				4	No Sensible
		¿Si la vulnerabilidad técnica es urgente, la unidad adopta medidas de controles relativos a la gestión de cambios o siguiendo los procedimientos de respuesta a incidentes de seguridad de la información?	X				4	No Sensible
		¿Existen parches disponibles de fuente legítima para tratar algún sistema vulnerable?		X			2	Sensible

		¿Se evalúa el riesgo asociado con la instalación del parche o se compara los riesgos planteados por la vulnerabilidad con los riesgos de instalación del parche?	X				4	No Sensible
		Si no hay ningún parche ¿qué controles llevan para tratar la vulnerabilidad técnica?					4	No Sensible
		a) Desactivación de servicios o capacidades relacionadas con la vulnerabilidad.						
		b) Adaptación o la inclusión de controles de acceso como cortafuegos en los límites de la red.	X					
		c) Incremento de la supervisión para detectar o evitar ataques reales.	X					
		d) Aumento de la concienciación sobre la vulnerabilidad.	X					
		¿La gestión de vulnerabilidades técnicas está alineado con las actividades de gestión de incidentes para proporcionar procedimientos técnicos a desarrollar cuando ocurra un incidente?	X				4	No Sensible
		¿Se ha definido un procedimiento para considerar la situación donde la vulnerabilidad ha sido identificada pero no es posible adoptar una contramedida?		X			2	Sensible

		¿Si existiera esta situación la unidad evalúa los riesgos relativos a la vulnerabilidad conocida y define acciones de detección y corrección adecuadas?			x			
	Restricción en la instalación de software	¿Se han establecido y aplicado reglas que rijan la instalación de software por parte de los usuarios?	X				4	No Sensible
		¿La unidad ha definido y ha hecho cumplir una estricta política sobre qué tipos de software pueden instalar los usuarios?	X				4	No Sensible
		¿Aplican el principio de menor privilegio para los usuarios?	X				4	No Sensible
		¿El privilegio que se les otorga a los usuarios le ha permitido tener la capacidad para instalar software?			X	DEPENDE EL TIPO DE USUARIO	4	No Sensible
		¿La unidad identifica qué tipos de instalaciones de software están permitidas (actualizaciones y parches de seguridad para el software existente) y qué tipos de instalaciones están prohibidas (software de uso personal, software cuya procedencia se desconoce y que puede ser potencialmente malicioso) ?	X				4	No Sensible
		¿La asignación de privilegios se da en función de los usuarios en cuestión?			X	DEL ROL DE DESEMPEÑO	4	No Sensible

		¿La instalación incontrolada de software en equipos informáticos ha causado fugas de información, pérdidas de integridad u otros incidentes de seguridad de la información o violación de derechos de propiedad intelectual?	X				2	Sensible
SEGURIDAD DE LAS COMUNICACIONES	**Controles de Red**	¿La unidad ha establecido las responsabilidades y procedimientos para la gestión de los equipos de red?	X				4	No Sensible
		¿La responsabilidad operacional de las redes está separada de las operaciones de los sistemas informáticos en un lugar apropiado?	X				4	No Sensible
		¿Las actividades de gestión están coordinadas para optimizar el servicio en la universidad y asegurar que los controles sean aplicados consistentemente en toda la infraestructura de tratamiento de la información?	X				4	No Sensible
		¿Los sistemas de red están autenticados?	X				4	No Sensible
		¿La conexión de los sistemas a la red están restringidos?	X				4	No Sensible
	Seguridad de los servicios de red	¿Se identifican los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red?	X				4	No Sensible

		¿Existe algún acuerdo de servicios de red?		X			4	No Sensible
		¿Se supervisa la capacidad del proveedor del servicio de red para gestionar los servicios acordados de una manera segura y que éste tiene derecho a ser auditado?	X				4	No Sensible
		¿Se aplica tecnología para la seguridad de los servicios de red tales como autenticación, cifrado y controles de conexión de red?	X				4	No Sensible
		¿Tienen parámetros técnicos para conexiones seguras con los servicios de red de acuerdo a las reglas de seguridad y conexión de redes?	X				4	No Sensible
		¿Existen procedimientos para el uso de los servicios de red para restringir el acceso a los mismos o a las aplicaciones, donde sea necesario?		X			2	Sensible
	Segregación en redes	¿Los grupos de servicios de información, los usuarios y los sistemas de información están segregados en redes distintas?	X				4	No Sensible
		¿Para gestionar la seguridad de la red, la dividen en dominios de red separados?	X				4	No Sensible

		¿Estos dominios se eligen en base a un nivel de confianza (ejemplo: dominio de acceso público, dominio de puestos de usuario, dominio de servidores) junto a áreas de la universidad (recursos humanos, finanzas, comercial) o una combinación como un dominio de servidor a múltiples áreas de la universidad?	X				4	No Sensible
		La segregación se hace usando:					4	No Sensible
		a) Diferentes Redes físicas	X					
		b) Diferentes redes lógicas (ejemplo: interconexión con redes privadas virtuales.	X					
		¿La unidad ha definido bien el perímetro de cada dominio?	X				4	No Sensible
		¿La unidad tiene una política de control de red?		X			2	Sensible
ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	**Planificación de la continuidad de la seguridad de la información**	¿La unidad ha determinado sus necesidades de seguridad de la información y de continuidad para la gestión de seguridad de la información en situaciones adversas como una crisis o desastre?	X				4	No Sensible
		¿La unidad tiene un plan de recuperación de desastres?		X			1	Muy Sensible

		¿La unidad realiza un análisis de impacto de negocio para los aspectos de seguridad de la información para determinar los requisitos de seguridad de la información aplicables en situaciones adversas?			X			
	Implementar la continuidad de la seguridad de la información	¿Existe una estructura de gestión adecuada y preparada para mitigar y responder a un evento disruptivo usando el personal con la autoridad, experiencia y competencia necesarias?	X			DE VEZ EN CUANDO	4	No Sensible
		¿En la unidad se ha nombrado al personal de respuesta al incidente y éste cuenta con la responsabilidad, autoridad y competencia necesarias para gestionar el incidente y mantener la seguridad de la información?	X				4	No Sensible
		¿Se ha desarrollado y aprobado planes documentados y procedimientos de respuesta y recuperación que detallan como la Universidad gestionará un evento disruptivo y mantendrá la seguridad de su información en un nivel predeterminado?		X			1	Muy Sensible
		De acuerdo con los requisitos de continuidad de seguridad de la información, la unidad establece, documenta, implanta y mantiene:					3	Poco Sensible

		a) Controles de seguridad de la información en los procesos, procedimientos y sistemas y herramientas de soporte de continuidad del negocio o de recuperación de desastres.	X					
		b) Procesos, procedimientos e implantación de cambios para mantener los controles existentes de seguridad de la información durante una situación adversa.	X					
		c) Controles compensatorios para aquellos controles de seguridad de la información que no puedan mantenerse durante una situación adversa.		X				
		¿La universidad ha involucrado especialistas de seguridad de la información para establecer, implantar y mantener los procesos y procedimientos para la Continuidad del Negocio o recuperación de desastres?		X			4	No Sensible
		¿Los controles de seguridad de la información que han sido implantados continúan operativos durante una situación adversa?		X			1	Muy Sensible
		¿Cuál es el nivel de seguridad de la información que tiene la unidad:					3	Poco Sensible
		a) Muy aceptable						

		b) Aceptable	X					
		c) Poco aceptable						
		d) No aceptable						
	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	¿Se comprueban los controles establecidos e implementados a intervalos regulares para asegurar que son válidos y eficaces durante situaciones adversas?		X			1	Muy Sensible
		La unidad verifica su gestión de continuidad de la seguridad de la información:					4	No Sensible
		a) Ejecutando y probando la funcionalidad de los procesos, procedimientos y controles para la continuidad de la seguridad de la información		X				
		b) Ejecutando y probando el conocimiento y la rutina para operar los procesos , procedimientos y controles para asegurar su rendimiento	X					
		c) Revisando la validez y efectividad de las medidas para la continuidad de la seguridad de la información cuando cambien los sistemas de información, los procesos de seguridad de la información, los procedimientos y controles o los procesos y soluciones de recuperación de desastres.	X					

		¿Se separa la prueba y verificación general de la seguridad de la información con el de la prueba de los cambios?		X			2	Sensible

ANEXO 4.
OFICIOS DE ENTREGA DE INFORMACIÓN POR PARTE DE LA UCCI DE LA ULEAM.

Uleam
UNIVERSIDAD LAICA
ELOY ALFARO DE MANABÍ

Unidad Central de Coordinación Informática

Oficio Nº 063-2019-UCCI-IBBV
Manta, 08 de febrero de 2019

Ingeniera
Teresa Cano Montesdeoca
Licenciada
Yanina Viteri Alcivar
MAESTRANTES
Ciudad. –

De mi consideración:

En atención a Oficio SN del 1 de febrero de 2019, se adjunta al presente la información solicitada, brindándoles la ayuda necesaria para que puedan continuar con su proceso de investigación.

Se hace entrega en medio óptico digital, lo siguiente:

1. PETI
2. PLAN DE CONTINGENCIA
3. INVENTARIO DE ACTIVOS DE LA UCCI
4. REGISTRO DE INCIDENTES Y FALLOS
5. POLITICAS DE SEGURIDAD INFORMACION

La información que no se pudo brindar, corresponde a documentos en los que, aún se encuentra trabajando la Unidad Central de Coordinación Informática, o no son competencia de este departamento.

Particular que informo para los fines pertinentes.

Atentamente,

Bécquer Briones Veliz, Mg.
Director

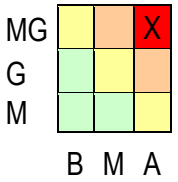
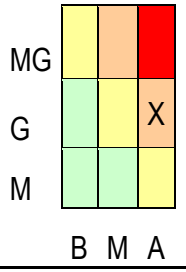
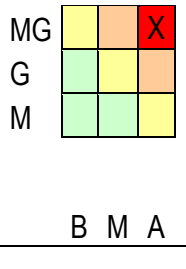
UNIDAD CENTRAL DE INTERNET

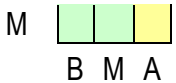
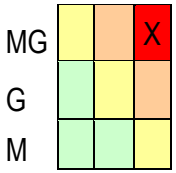
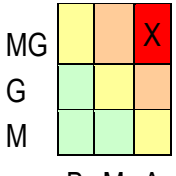
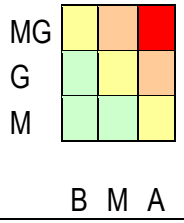
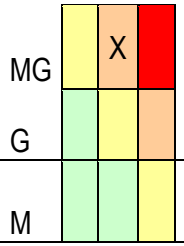
C.c: Archivo UCCI

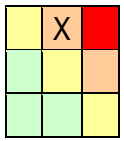
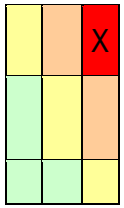
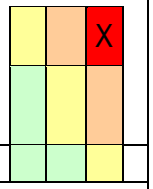
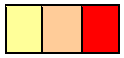
Elaborado por:	Revisado por:	Aprobado por:
Carlos Z.	Soraida O.	Bécquer B.

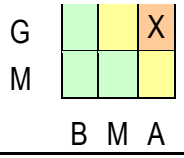
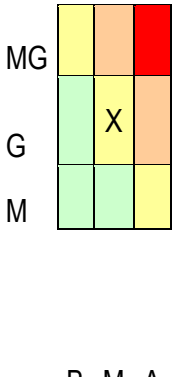
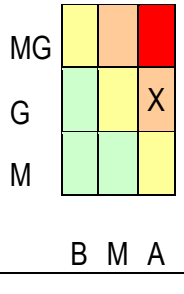
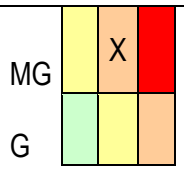
ANEXO 5.
MATRIZ ANÁLISIS MODAL DE FALLOS Y EVENTOS (AMFE) POR ÁREAS DE LA UCCI.

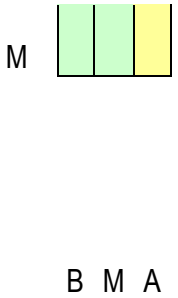
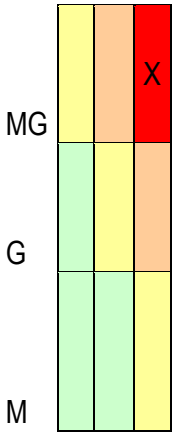
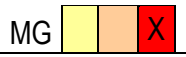
ANEXO 5A.- MATRIZ DE RIESGOS AMFE DE LA ÁREA GENERAL UCCI

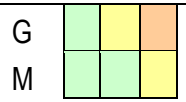
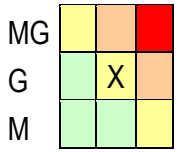
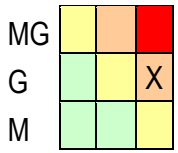
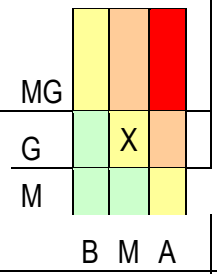
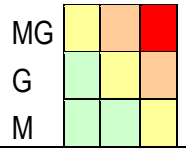
ID. Riesgo	Vulnerabilidades UCCI	Probabilidad	Impacto	Nivel	Matriz de Riesgos	Responsables	ID de Mitigación	Acciones de mitigación	Criterio de aceptación
R.1.1.	No posee políticas de seguridad de la información aprobadas por la dirección.	Alto 3	Muy Grave 3	Crítico		Director/Coordinador TI	A.1.1.1	Aprobar las políticas de seguridad de la información por parte de la máxima autoridad	Seguridad en el entorno TI.
R.1.2.	Las políticas de seguridad no son publicadas ni comunicadas a los empleados de TI y partes externas relevantes.	Alto 3	Grave 2	Alto		Director/Coordinador de TI - Áreas asignadas	A.1.2.1	Socializar las políticas de seguridad a todos los empleados de TI y partes externas relevantes para la entidad.	Cumplimiento de las políticas de seguridad.
R.1.3.	En las políticas de seguridad de la información, no incluye la seguridad física de TI y ni las copia de respaldo de la información.	Alto 3	Muy Grave 3	Crítico		Director/Coordinador TI	A.1.3.1	Elaborar las políticas de seguridad física de TI y las políticas de copia de respaldo de la información.	Mantener las áreas seguras y en conjunto con la información.
R.1.4.	No se revisan las políticas de seguridad de la	Alto	Muy Grave	Crítico		Director/Coordinador TI	A.1.4.1	Revisión periódica del cumplimiento de las políticas de seguridad de	Al menos cada 6 meses hacer la revisión.

	información en la UCCI.	3	3					la información.	
R. 1.5.	La Dirección no toma en cuenta los resultados de las revisiones de las políticas de seguridad.	Alto 3	Muy Grave 3	Crítico		Director/Coordinador TI	A.1.5.1	Revisar los resultados semestrales de las revisiones de las políticas de seguridad de la información.	Mejorar la seguridad de la información.
R.1.6.	No cuenta con un sistema de gestión de Continuidad del Negocio.	Alto 3	Muy Grave 3	Crítico		Director/Coordinador TI	A.1.6.1	Elaborar un plan de gestión de continuidad del negocio	Directrices de la norma ISO/IEC 22301
R.1.7	En la UCCI no clasifica los activos ni los protege debidamente para asegurar su cuidado.	Alto 3	Muy Grave 3	Crítico		Director/Coordinador TI	A.1.7.1	Clasificar los activos custodios dentro de la unidad para asegurar su cuidado.	Protección de activos.
R.1.8.	No se registra la fecha y la hora de entrada y salida de los visitantes o personas externas a la unidad.	Medio 2	Muy Grave 3	Alto		Director/Coordinador de TI - Áreas asignadas	A.1.8.1	Registrar todas las entradas y salidas con fechas de las visitas externas a la unidad.	Control de acceso a la unidad.

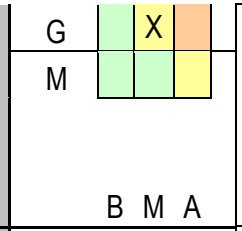
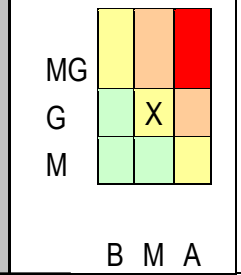
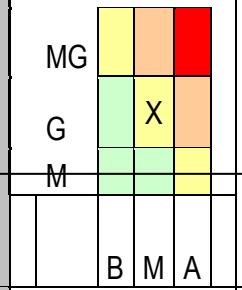
					B M A				
R.1.9.	No se diseña ni se aplica seguridad física a las oficinas, despachos y recursos de la unidad.	Medio 2	Muy Grave 3	Alto	MG G M B M A 	Director/Coordinador de TI - Áreas asignadas	A.1.9.1	Asegurar que todas las áreas de TI apliquen seguridad física en sus oficinas y recursos de la unidad.	Seguridad de las áreas de trabajo.
R.1.10.	La unidad no cuenta con un diseño aplicable de protección física contra desastres naturales, ataques provocados por el hombre o accidentes.	Alto 3	Muy Grave 3	Crítico	MG G M B M A 	Director/Coordinador TI	A.1.10.1	Elaborar un diseño aplicable de protección física contra desastres naturales, o ataques provocados por el hombre o accidentes.	Preparación futura para desastres naturales o accidentes
R.1.11.	La unidad no tiene un plan de contingencia y de emergencia contra amenazas externas y ambientales.	Alto 3	Muy Grave 3	Crítico	MG G M B M A 	Director/Coordinador TI	A.1.11.1	Elaborar un plan de contingencia y de emergencia contra amenazas externas y ambientales.	Mitigar riesgos contra desastres naturales o amenazas externas y ambientales.
R.1.12.	No se ha diseñado ni	Alto	Grave	Alto	MG 	Director/Coordinador de TI - Áreas	A.1.12.1	Diseñar e implementar los procedimientos para	Verificar que las áreas seguras tengan todo el

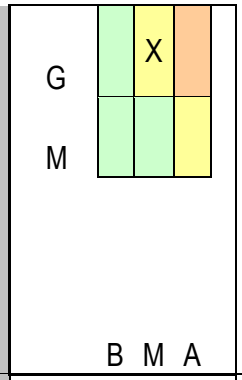
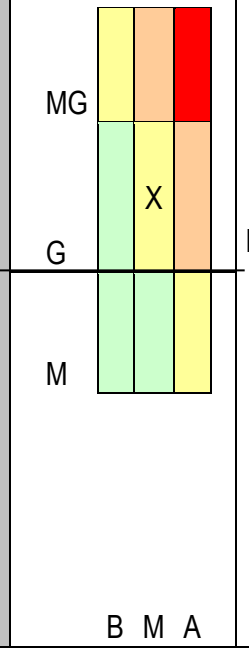
	implementado procedimientos para trabajar en áreas seguras.	3	2			asignadas		trabajar en áreas seguras	recurso para trabajar.
R.1.13.	El material que entra a la unidad, no es inspeccionado para evitar amenazas potenciales como explosivos, productos químicos y otros materiales de riesgo.	Medio 2	Grave 2	Medio		Director/Coordinador TI	A.1.13.1	Revisar todo el material que entra en la unidad.	Inspeccionar para evitar amenazas potenciales como explosivos, químicos u otro material de riesgo.
R.1.14.	El material (equipos tecnológicos) que entra a la unidad no es registrado de acuerdo a los procedimientos de gestión de activos.	Alto 3	Grave 2	Alto		Director/Coordinador de TI - Áreas asignadas	A.1.14.1	Registrar los equipos tecnológicos que ingresan a la unidad.	Procedimientos de gestión de activos.
R.1.15.	Los interruptores y válvulas de emergencia para cortar el suministro de	Medio	Muy Grave	Alto		Director/Coordinador de TI - Áreas asignadas	A.1.15.1	Ubicar fuera de las salidas de emergencia o de sala de equipos los interruptores y válvulas de emergencia para	Mantener la seguridad del área de trabajo.

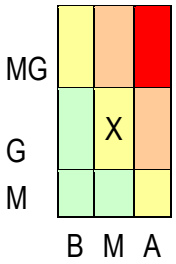
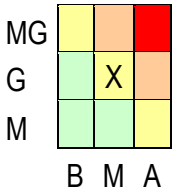
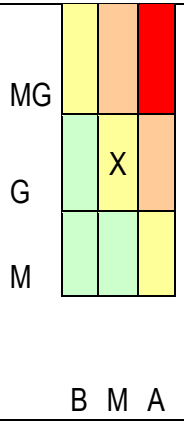
	energía, agua, gas u otro servicio no están ubicados fuera de las salidas de emergencia o de las salas de equipos.	2	3					cortar el suministro de energía, agua, gas u otros.	
R.1.16.	La unidad no ha establecido las funciones y responsabilidades asociadas a la gestión de las vulnerabilidades técnicas, incluyendo la supervisión de las mismas, la evaluación de los riesgos de la vulnerabilidad, el parcheo, el seguimiento de activos y cualquier responsabilidad de coordinación necesaria.	Alto 3	Muy Grave 3	Crítico		Director/Coordinador TI	A.1.16.1	Elaborar un manual de funciones y responsabilidades asociadas a la gestión de vulnerabilidades técnicas: supervisión, evaluación de riesgos, seguimiento de activos.	Supervisión y aprobación del manual de funciones y responsabilidades.
R.1.17.	La unidad no tiene un plan de	Alto	Muy Grave	Crítico		Director/Coordinador TI	A.1.17.1	Elaborar un plan de recuperación de	Servicios disponibles ante un desastre.

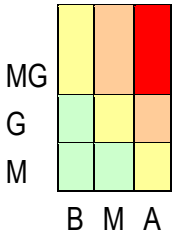
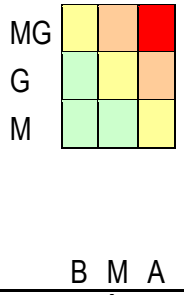
	recuperación de desastres.							desastres.	
		3	3						
R.1.18.	No se ha realizado auditoría interna a las áreas de la UCCI.	Medio	Grave	Medio		Director/Coordinador TI	A.1.18.1	Realizar auditorías internas en las diferentes áreas de la UCCI.	Una vez al año hacer las auditorías.
		2	2						
R.1.19.	Los activos o grupos de activos no tienen custodios asignados.	Alto	Grave	Alto		Director/Coordinador de TI - Áreas asignadas	A.1.19.1	Asignar custodios a los activos dentro de la unidad.	Gestión de activos
		3	2						
R.1.20.	No se proporcionan las instrucciones de los requisitos de seguridad del área ni los procedimientos de emergencia a los visitantes.	Medio	Grave	Medio		Director/Coordinador TI	A.1.20.1	Informar a los visitantes las instrucciones de seguridad del área y los procedimientos de emergencia antes de ingresar.	Mantener la protección del área y los visitantes.
		2	2						
R.1.21.	Todos los empleados, contratistas y terceros y los visitantes que	Alto	Grave	Alto		Director/Coordinador de TI - Áreas asignadas	A.1.21.1	Poseer una identificación visible para todas las personas que ingresan a la unidad	Control de acceso a la unidad.
		3	2						

	llegan a la unidad, no llevan una identificación visible.				B M A				
R.1.22.	No se notifica al personal de seguridad que se encuentran visitantes sin autorización o alguna persona sin llevar visible la identificación.	Medio 2	Grave 2	Medio	MG G M B M A	Director/Coordinador TI	A.1.22.1	Notificar a seguridad que vendrán visitantes mediante una lista de las personas que van a ingresar a la unidad con identificación visible.	Mantener la seguridad de la unidad.
R.1.23.	Las áreas seguras vacías no están físicamente cerradas ni son comprobadas periódicamente.	Medio 2	Grave 2	Medio	MG G M B M A	Director/Coordinador TI	A.1.23.1	Revisar las áreas seguras que están vacías para verificar que estén cerradas.	Mantener la seguridad en las áreas.
R.1.24.	Se permite el ingreso de equipos de fotografía, video, audio u otros equipos de grabación sin autorización.	Medio 2	Grave 2	Medio	MG G M B M A	Director/Coordinador TI	A.1.24.1	Se debe permitir el ingreso de equipos de fotografía, video, audio u otros equipos con autorización previa del director de la unidad.	Medidas de seguridad del área TI.
R.1.25.	No se establecen directrices para	Medio	Grave	Medio	MG	Director/Coordinador TI	A.1.25.1	Establecer reglamentos para comer, beber y	Directrices de la norma ISO/IEC 27002

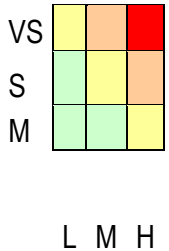
	comer, beber y fumar en las proximidades de las instalaciones de tratamiento de la información.	2	2					fumar en las proximidades de las instalaciones donde se trata la información.	
R.1.26.	La unidad no realiza inspecciones al azar a los usuarios internos y externos para detectar entrada y salida de activos no autorizados.	Medio 2	Grave 2	Medio		Director/Coordinador TI	A.1.26.1	Realizar inspecciones al azar a los visitantes y empleados de TI para detectar la salida de activos no autorizados.	Inspecciones una vez al azar cada semana
R.1.27.	No tienen políticas de puesto de trabajo despejado de papeles y pantalla limpia para los recursos de tratamiento de la información.	Medio 2	Grave 2	Medio		Director/Coordinador TI	A.1.27.1	Elaborar políticas de los puestos de trabajo, que permita mantener limpia el área del tratamiento de la información.	Espacios de trabajo limpios.
R.1.28.	La información de negocio sensible o crítica (documentos, almacenamiento electrónico) no es	Medio	Grave	Medio		Director/Coordinador TI	A.1.28.1	Guardar la información sensible o crítica, no solo en digital sino física en un mueble de seguridad, ya sea una caja fuerte cuando la oficina esté	Disponibilidad de la información en cualquier medio.

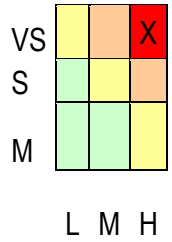
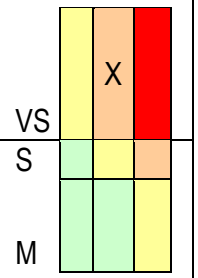
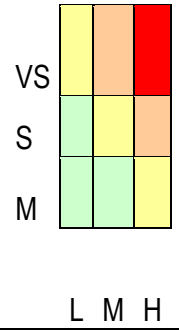
	guardada en caja fuerte, armario u otro tipo de mueble de seguridad, cuando no se necesita, especialmente cuando la oficina está vacía.							vacía.	
		2	2						
R.1.29.	Los directivos o responsables no utilizan los resultados de los sistemas de control y tendencias de uso para evitar posibles cuellos de botellas o dependencias de personal clave que represente una amenaza para el sistema de seguridad o para los servicios y de esta manera planificar las acciones adecuadas.	Medio	Grave	Medio		Director/Coordinador TI	A.1.29.1	Realizar planes de acción con los resultados que arrojan los sistemas de control y que representan una amenaza para la seguridad de la información, de la unidad o de los servicios.	Acciones adecuadas para mejorar la seguridad.
		2	2						

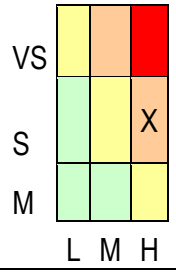
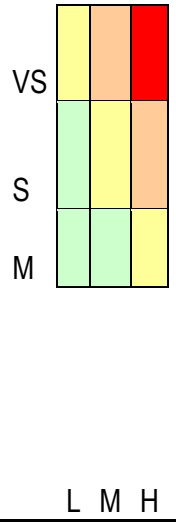
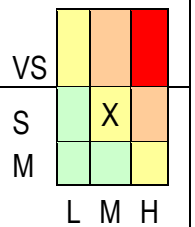
R.1.30.	La unidad no tiene un plan de gestión de la demanda de capacidad.	Medio 2	Grave 2	Medio		Director/Coordinador TI	A.1.30.1	Elaborar un plan de gestión de la demanda de capacidad de los empleados, de los sistemas o servicios de la unidad.	Personal, sistema o servicios, preparados para soportar alta demanda.
R.1.31.	No tiene un plan documentado de gestión de la capacidad para los sistemas de misión crítica.	Medio 2	Grave 2	Medio		Director/Coordinador TI	A.1.31.1	De acuerdo con el ID de mitigación A.1.30.1	Llevar registros de la capacidad de los sistemas de misión crítica.
R.1.32.	La unidad no ha determinado el tiempo de conservación de la información esencial tomando en cuenta cualquier requisito para las copias de archivo que hayan de ser conservadas de manera permanente.	Medio 2	Grave 2	Medio		Director/Coordinador TI	A.1.32.1	Determinar el tiempo de conservación de la información esencial de acuerdo a los requisitos de archivo que se conservan de manera permanente.	El tiempo se estima de acuerdo a la importancia que tiene la información.

R.1.33.	No se ha definido una escala temporal para reaccionar a las notificaciones de vulnerabilidades técnicas que puedan resultar relevantes.	Medio 2	Muy Grave 3	Alto		Director/Coordinador de TI - Áreas asignadas	A.1.33.1	Elaborar una escala de tiempo para trabajar con las vulnerabilidades técnicas que se presentan y son relevantes en la unidad.	Acciones inmediatas para disminuir riesgos.
R.1.34.	La unidad no establece, documenta, implanta ni mantiene los requisitos de continuidad de seguridad de la información.	Medio 2	Muy Grave 3	Alto		Director/Coordinador de TI - Áreas asignadas	A.1.34.1	Documentar, implantar requisitos para la continuidad de la seguridad de la información.	Mantener segura la información en el tiempo.

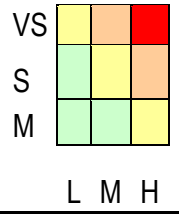
ANEXO 5B.- MATRIZ DE RIESGOS AMFE DE LA ÁREA DESARROLLO Y PROGRAMACIÓN

ID. Riesgo	Vulnerabilidades	Probabilidad	Impacto	Nivel	Matriz de Riesgos	Responsables	ID de Mitigación	Acciones de mitigación	Criterio de aceptación
R.2.1	No se llevan inventarios de los activos de soporte de software.	Alto 3	Grave 2	Alto		Director/Coordinador de TI - Áreas asignadas	A.2.1.1	Realizar los inventarios de los activos de soporte de software, equipos tecnológicos dentro de la unidad.	Gestión de activos.

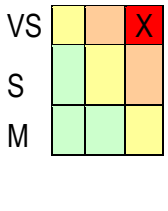
R.2.2.	No se han implantado controles de detección de fallos para identificar la existencia de problemas a su debido tiempo.	Alto 3	Muy Grave 3	Crítico		Director/Coordinador TI	A.2.2.1	Implementar controles de detección de fallos con herramientas tecnológicas	Desarrollo con metodologías ágiles.
R.2.3.	No se identifican las tendencias de uso, en lo particular de las aplicaciones de negocio o las herramientas del sistema de gestión de la información.	Medio 2	Muy Grave 3	Alto		Director/Coordinador de TI - Áreas asignadas	A.2.3.1	Elaborar políticas y manuales de uso de aplicaciones de negocio o herramientas de gestión de la información.	Uso adecuado de los recursos TI.
R.2.4	El software de desarrollo y explotación no se ejecuta en diferentes sistemas o procesadores de ordenador ni en diferentes dominios o directorios.	Alto 3	Menor 1	Medio		Director/Coordinador TI	A.2.4.1	Elaborar procesos de prueba de ejecución del software en desarrollo en diferentes plataformas para ver su funcionalidad y escalabilidad.	Software escalable.
R.2.5.	No existen parches	Alto	Grave	Alto		Director/Coordin	A.2.5.1	Comprar parches	Parches Microsoft, Unix

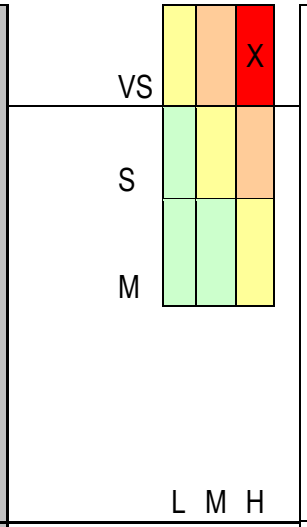
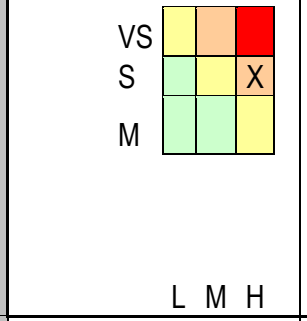
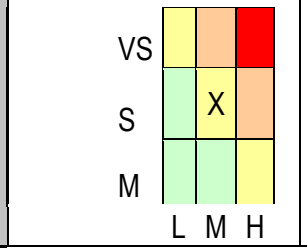
	disponibles de fuente legítima para tratar algún sistema vulnerable.	3	2			ador de TI - Áreas asignadas		de sistemas de fuente legítima para evitar problemas con las aplicaciones en desarrollo.	
R.2.6.	La instalación incontrolada de software en equipos informáticos ha causado fugas de información, pérdidas de integridad u otros incidentes de seguridad de la información o violación de derechos de propiedad intelectual.	Medio 2	Muy Grave 3	Alto		Director/Coordinador de TI - Áreas asignadas	A.2.6.1	Controlar el permiso de los usuarios para instalar software maliciosos que causen incidentes de seguridad de la información.	Control de permisos
R.2.7.	No se separa la prueba y verificación general de la seguridad de la información con el de la prueba de los cambios.	Medio 2	Grave 2	Medio		Director/Coordinador TI	A.2.7.1	Realizar pruebas por separado de los cambios que se realicen en el software de desarrollo.	Retroalimentación general de los cambios efectuados individualmente.

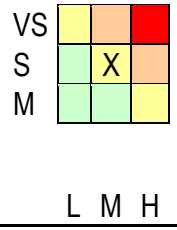
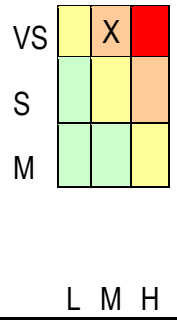
ANEXO 5C.- MATRIZ DE RIESGOS AMFE DE LA ÁREA DE MANTENIMIENTO Y SOPORTE A USUARIOS

ID. Riesgo	Vulnerabilidades	Probabilidad	Impacto	Nivel	Matriz de Riesgos	Responsables	ID de Mitigación	Acciones de mitigación	Criterio de aceptación
R. 3.1.	No se utilizan métodos de protección especial para los equipos.	Alto 3	Grave 2	Alto		Director/Coordinador de TI - Áreas asignadas	A.3.1.1	Proteger los equipos con métodos de seguridad que trabajan con información sensible.	Políticas de seguridad de los equipos tecnológicos.

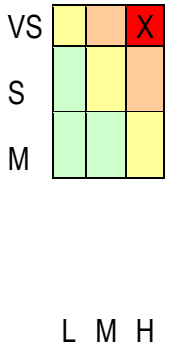
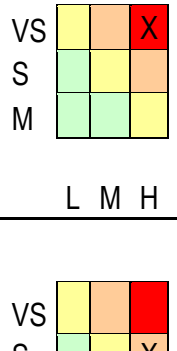
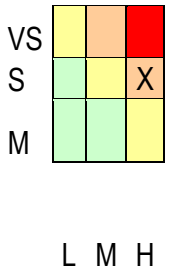
ANEXO 5D.- MATRIZ DE RIESGOS AMFE DE LA ÁREA DE OPERACIONES.

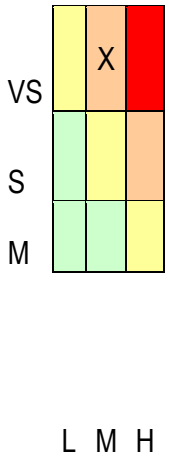
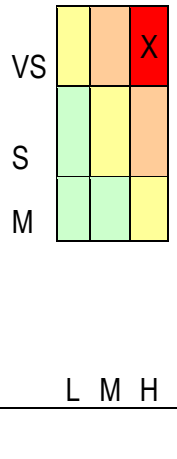
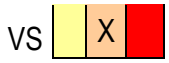
ID. Riesgo	Vulnerabilidades	Probabilidad	Impacto	Nivel	Matriz de Riesgos	Responsables	ID de Mitigación	Acciones de mitigación	Criterio de aceptación
R. 4.1.	Las copias de respaldo no están protegidas mediante cifrado, sobre todo en aquellas donde es importante la confidencialidad.	Alto 3	Muy Grave 3	Critico		Director/Coordinador TI	A.4.1.1	Proteger las copias de respaldo con cifrado para mantener la confidencialidad de la información.	Encriptación de información.
R.4.2.	No se ha desarrollado ni	Alto	Muy Grave	Crítico		Director/Coordinador TI	A.4.2.1	Elaborar las políticas,	Plan de respuesta y recuperación frente a

	aprobado planes documentados y procedimientos de respuesta y recuperación que detallan como la Universidad gestionará un evento disruptivo y mantendrá la seguridad de su información en un nivel predeterminado.							procedimientos, planes y controles de respuesta y recuperación contra incidentes o desastres naturales para mantener la seguridad de la información.	desastres naturales o incidentes informáticos.
		3	3						
R.4.3.	Los controles de seguridad de la información que han sido implantados no continúan operativos durante una situación adversa.	Alto	Grave	Alto		Director/Coordinador de TI - Áreas asignadas	A.4.3.1	Implementar un control de seguridad que funcione antes, durante y después de un evento disruptivo.	Disponibilidad y Confidencialidad de la información con controles de seguridad.
		3	2						
R.4.4.	No se comprueban los controles establecidos ni los implementados a intervalos	Medio	Grave	Medio		Director/Coordinador TI	A.4.4.1	De los controles de seguridad implementados, realizar pruebas de su aplicabilidad para medir su eficacia frente a una	Indicadores de desempeño de controles de seguridad.
		2	2						

	regulares para asegurar que son válidos y eficaces durante situaciones adversas.							situación adversa.	
R.4.5.	No se han tomado medidas adecuadas de protección de la privacidad en los registros de eventos.	Medio 2	Grave 2	Medio		Director/Coordinador TI	A.4.5.1	Realizar un plan de medidas referente a los registros de eventos presentados en la unidad.	Medidas de protección para la privacidad de la información.
R.4.6.	No se ha definido un procedimiento para considerar la situación donde la vulnerabilidad ha sido identificada pero no es posible adoptar una contramedida.	Medio 2	Muy Grave 3	Alto		Director/Coordinador de TI - Áreas asignadas	A.4.6.1	Realizar un plan de acción para vulnerabilidades identificadas pero que no es posible adoptar una contramedida en el momento.	Proteger la información.

ANEXO 5E.- MATRIZ DE RIESGOS AMFE DE LA ÁREA DE INFRAESTRUCTURA Y REDES

ID. Riesgo	Vulnerabilidades	Probabilidad	Impacto	Nivel	Matriz de Riesgos	Responsables	ID de Mitigación	Acciones de mitigación	Criterio de aceptación
R. 5.1.	Las instalaciones de la unidad no están configuradas para prevenir que las actividades o la información de tipo confidencial sean visibles o audibles desde el exterior.	Alto 3	Muy Grave 3	Crítico		Director/Coordinador TI	A.5.1.1	Aumentar la seguridad de las instalaciones a nivel físico para mantener la confidencialidad y que esta no sea visible ni audible para el exterior.	Vidrios polarizados para las separaciones de áreas.
R.5.2.	No se ha aplicado sistemas de protección contra rayos en la unidad.	Alto 3	Muy Grave 3	Crítico		Director/Coordinador TI	A.5.2.1	Adoptar medidas de protección para temporadas invernales o cambios climáticos en la unidad.	Asegurar el área de TI contra tempestades invernales.
R.5.3.	No se han colocado filtros de protección contra rayos en todas las entradas de corriente eléctrica y en todas las líneas de	Alto 3	Grave 2	Alto		Director/Coordinador de TI - Áreas asignadas	A.5.3.1	Colocar filtros de protección contra rayos en las entradas de corriente eléctrica y en todas las líneas de comunicación.	Instalación eléctrica con filtros de protección contra rayos.

	comunicación.								
R.5.4	No tienen los recursos adecuados para realizar las copias de respaldo para que toda la información y los softwares esenciales puedan ser recuperados después de un desastre o fallo de los soportes.	Medio 2	Muy Grave 3	Alto		Director/Coordinador de TI - Áreas asignadas	A.5.4.1	La unidad debe contar con todos los recursos necesarios para realizar las copias de respaldo de la información para que estas puedan ser recuperadas después de un evento disruptivo o desastre natural.	Recursos TI para el tratamiento de la información después de un desastre natural.
R.5.5.	No se llevan registros precisos y completos de las copias de respaldo, así como de los procedimientos de recuperación documentados.	Alto 3	Muy Grave 3	Crítico		Director/Coordinador TI	A.5.5.1	Llevar los registros y procedimientos documentados, completos y precisos de las copias de respaldo para su recuperación después de un evento o desastre natural o incidente informático.	Documentación completa de todos los registros de las copias de respaldo de la información.
R.5.6.	No existen procedimientos para el uso de los	Medio	Muy Grave	Alto		Director/Coordinador de TI - Áreas asignadas	A.5.6.1	Elaborar procedimientos para el uso de	Control de acceso a los 'servicios de la red.

	servicios de red para restringir el acceso a los mismos o a las aplicaciones.				S M L M H			servicios de red que permita solo el acceso autorizado a ellos.	
		2	3						
R.5.7.	La unidad no tiene una política de control de red.	Medio	Muy Grave	Alto	VS S M L M H	Director/Coordinador de TI - Áreas asignadas	A.5.7.1	Elaborar políticas de control de red para la institución.	Proteger la información que se transmite en la red.
		2	3						
R.5.8.	No se ha considerado medidas adicionales para sistemas sensibles o críticos.	Medio	Muy Grave	Alto	VS S M L M H	Director/Coordinador de TI - Áreas asignadas	A.5.8.1	Elaborar medidas de seguridad para los sistemas sensibles o críticos que tratan la información.	Adoptar medidas que mejoren la seguridad de la red y de las aplicaciones.
		2	3						

ANEXO 6.
MODELO DE GESTIÓN CONTINUIDAD DE NEGOCIOS PARA LA INFRAESTRUCTURA TECNOLÓGICA DE LA UCCI

MODELO DE GESTIÓN DE CONTINUIDAD PARA LA INFRAESTRUCTURA TECNOLÓGICA DE LA UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ

MAYO, 2019

CONTENIDO

1. INTRODUCCIÓN

Hoy en día los modelos de Gestión de Continuidad de Negocios responden a un gran número de requerimiento en los servicios que aportan al funcionamiento de las Infraestructuras Tecnológicas de una Institución, de tal manera que garantizan el mínimo de fallas o dificultades que se presentan en las organizaciones.

Dadas las condiciones que anteceden, resulta oportuno considerar la elaboración de un modelo de Gestión de Continuidad en la Infraestructura Tecnológica de la Universidad Laica Eloy Alfaro de Manabí, mismo que permite mejorar la disponibilidad de los servicios y recursos de información al momento de ocurrir un acontecimiento informático o natural aplicando el estándar internacional ISO 22301.

Por lo consiguiente se desarrolló el Plan de Continuidad utilizando la metodología Análisis Modal de Fallos y Efecto (AMFE), con la que se evaluó el problema y a través de la cual se calculó el número de prioridad de riesgos, así mismo se empleó la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas (Magerit), misma que se convirtió en base fundamental para el análisis y gestión de los riesgos.

Es importante destacar que para la continuidad de actividades la Unidad Central de Coordinación Informática (UCCI) de la ULEAM, permanentemente debe estar aliado al plan que certifique la prolongación de los servicios, el cual determina los pasos para dar solución a los inconvenientes que puedan ser generados por algún evento natural o humano que de forma intencional o accidental suceda.

En consecuencia el Pan de Continuidad de Negocio debe ser de total empoderamiento por la Alta Dirección, ya que al emplearse exitosamente en la Institución permitirá priorizar la recuperación y reanudación del buen funcionamiento de las operaciones.

2. ALCANCE

Este plan está encaminado a los procesos críticos de la UCCI y orientados a cada una de las áreas, a continuación se plasman las etapas a las que se debe proyectar dicho plan:

- **Análisis y Evaluación:** Se valoran los riesgos y vulnerabilidades de los procesos críticos de las diversas áreas de la Unidad Central de Coordinación Informática de la ULEAM.
- **Planificación y Políticas:** Son puntos claves, cuya finalidad es enriquecer procedimientos que conlleve al buen funcionamiento en la Infraestructura Tecnológica.
- **Estrategias y recuperación:** Permite controlar de manera preventiva y correctiva una serie de procesos previamente planeados en caso de ocurrir alguna eventualidad o incidencias, es decir efectuar debidamente acciones para minimizar en lo posible causas de pérdidas y promover la recuperación de los activos y recursos de información de la Institución.

3. CRONOLOGÍA Y SITUACIÓN ACTUAL DE LA UNIDAD CENTRAL DE COORDINACIÓN DE INFORMÁTICA (UCCI)

3.1. RESEÑA CRONOLÓGICA DE LA UCCI

Es importante puntualizar aspectos relevantes sobre la reseña cronológica de la Unidad Central de Coordinación Informática (UCCI), es decir en referencia a lo versado en el Plan Estratégico de Tecnología de la Información (PETI) y el Plan de Continencia, la UCCI inicialmente fue un laboratorio de computación hasta diciembre del 2000, siendo designado el Ing. Jacinto Reyes como Director del Laboratorio, seguidamente al laboratorio se lo denominó como una Unidad del Sistema Central de Computación (ULEAM, 2018).

Posteriormente en diciembre del 2002 la Unidad se independiza, quedando un Centro de Cómputo para los estudiantes y las Oficinas Administrativas en el edificio del CEPIRCI. Cabe indicar que durante esta administración se logró aumentar el ancho de banda del Internet y la gratuidad del mismo para los Estudiantes y para el Área Administrativa. Así mismo transcurridos dos años aproximadamente se asigna un nuevo Jefe de Unidad, el cual no escatimó esfuerzo para incrementar el alcance del Internet en toda la Universidad, para tal efecto interviene el anillo de Red de Fibra Óptica; proporcionando la interconectividad entre Departamentos Administrativos y Unidades Académicas (ULEAM, 2018).

Consecuentemente la Unidad Central de Coordinación Informática (UCCI) fue creada con la finalidad de brindar soporte informático al Servicio de Internet y Proyectos Tecnológico, misma que funcionó en el Edificio del CEPIRCI hasta el año 2016, además es necesario mencionar que en esta dependencia se encontraba la Central de Servidores. Adicionalmente es indispensable resaltar las funciones primordiales que tiene la UCCI, tales como asegurar el servicio permanente y de calidad del Internet, de igual forma el monitoreo de la Red y el mantenimiento preventivo y correctivo de equipos de computación y por ende el

empoderamiento de la administración de la Página Web Institucional (ULEAM, 2018).

Finalmente el Ing. Bécquer Briones Veliz, Mg., asume la Dirección de la Unidad desde el 4 de enero de 2016 hasta la actualidad; fecha desde la cual se han realizado varios cambios que van desde el incremento del personal con la creación de nuevas áreas de trabajo; seguidamente el incremento del nivel de madurez de los procesos, siendo evaluado bajo el modelo CMMI; mismo que permite mejorar y estandarizar productos de Software e información para uso de todas las unidades académicas y administrativas y a su vez otros procesos que han permitido brindar un mejor servicio (ULEAM, 2018).

3.2. ANÁLISIS DE LA SITUACIÓN ACTUAL

Es imprescindible destacar que la Unidad Central de Coordinación Informática tiene como objetivo primordial ejecutar cursos de acción para estructurar de una mejor forma la Unidad, aplicando normativas, estándares, marcos de referencias y buenas prácticas existentes en el área (ULEAM, 2018). Posteriormente se presenta la estructura de la Unidad Central de Coordinación de Informática (UCCI), misma que está conformada por 5 área que son: Área de Infraestructura y Redes; Desarrollo; Mantenimiento y Soporte a Usuarios; Operaciones y Gestión de Riesgos de TI, (Figura 1).

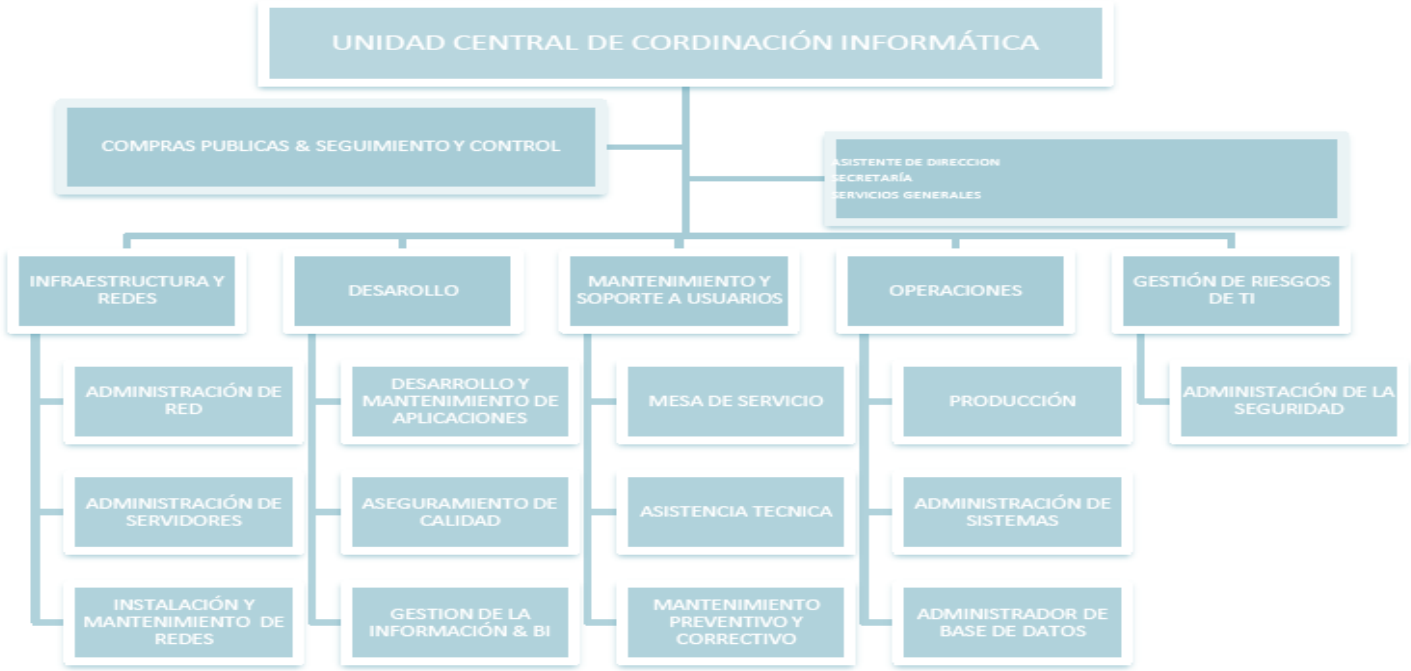


Figura 1. Organigrama de la UCCI
Fuente: (ULEAM, 2018).

De acuerdo a lo tipificado en la figura anterior es valioso destacar que cada área tiene asignado un responsable con sus atribuciones y por ende las responsabilidades que deben cumplir. Cabe indicar que en la actualidad no se encuentra habilitada el Área de Gestión de Riesgos de TI, pero sin embargo las funciones de mayor relevancia es desempeñada por el Director de la Unidad. En referencia a la investigación realizada los equipos de la UCCI se encuentran configurados de manera segura; así mismo poseen política de seguridad de información, usuario y contraseña, de igual forma gozan de correo electrónico, uso de internet y acuerdo de confidencialidad para el personal que labora en la misma (ULEAM, 2018).

También se conoció que el diseño de la red consta de una Red WAN, misma que se compone de un enlace backup y un principal; el cual es la conexión que otorga el proveedor, así mismo que entra por la WAN y posteriormente se comunica a través de un router principal institucional; a su vez comparte la conexión con los cuatros routers para la red LAN, Wifi, DMZ y Extensiones. Además para el monitoreo se utilizan NEXUS, Loot de servidores, Loot de equipos de comunicación entre otros.

Siguiendo la investigación se constató que para el desarrollo de un sistema se debe cumplir con los lineamientos establecidos por el área; por lo que es importante mencionar que depende del programa es la aplicación de tal manera que puede ser integrada, semintegrada o aislada. Cabe indicar que además utilizan internamente el estándar MBC, mismo que es un marco de trabajo a nivel de código en temas del Servidor, Marco de trabajo a nivel de Cliente MVVM aplicados de manera técnica; Servicios Web o estándar Rest para comunicaciones entre sistemas. Consecuentemente se maneja la Base de Datos POSTGRE SQL y SQL Server y en un 5% se incrementa MySQL para los proyectos externos. Finalmente es relevante indicar que en la Unidad se han desarrollado 9 sistemas entre formales y semiformales. De igual modo se han determinado los servicios que se deben reanudar con prioridad en caso de eventualidad o desastre, y también los equipos auxiliares que permiten dar continuidad tanto a los activos y los servicios de la Institución.

4. OBJETIVOS

4.1. OBJETIVO GENERAL

Diseñar un modelo de Gestión de la Continuidad en la Infraestructura Tecnológica de la ULEAM, en base a la aplicación de la Norma ISO 22301, para proveer soluciones de continuidad en los procesos críticos de todas las áreas de la UCCI, de manera que les permitan actuar preventiva y correctivamente en caso de incidentes y eventualidades.

4.2. OBJETIVOS ESPECÍFICOS

- Analizar y evaluar los riesgos y vulnerabilidades para determinar cualquier impacto potencial.

- Diseñar políticas y la planificación del plan para llevar a cabo la continuidad de la Infraestructura tecnológica de la Institución.

- Plantear estrategias de recuperación que avalen la calidad en seguridad y continuidad de los procesos críticos de las áreas de la UCCI en caso de eventualidades o incidencias.

5. MARCO LEGAL

Es importante resaltar las bases legales que sustentan la esencia del estudio de la investigación, por tal razón primeramente se analizó la Norma ISO (ORGANIZACIÓN INTERNACIONAL PARA LA ESTANDARIZACIÓN), ya que desde el ámbito mundial esta norma prevalece la satisfacción del usuario y la calidad de los servicios que brinda una organización.

Posteriormente se consideró oportuno disertar la Norma ISO 27002 (Estándar de Seguridad de la Información), cabe indicar que ésta norma permitió corroborar la importancia en la protección de los activos y por ende la información de la Institución, de igual forma determinó tipos de controles para prevenir riesgo o detectar algún incidente.

Continuando con el propósito de la investigación como es la elaboración del Plan de Continuidad para la Infraestructura Tecnológica de la ULEAM se aplicó la base legal que contempla la Norma ISO 22301(Sistema de Gestión de Continuidad de Negocio), cuyo objetivo es dar respuesta a los imprevistos que pueden ocurrir en cualquier momento.

Así mismo se utilizó información relevante del PETI (Plan Estratégico de Tecnologías de Información y Comunicación) y del Plan de Contingencia, dichos elementos accedieron a confirmar la situación actual de la Institución, al mismo tiempo se obtuvo un análisis proactivo, para tal efecto se destinó la metodología AMFE (Análisis de Modo y Efectos de Fallo), cumpliendo con el propósito de identificar y prevenir los posibles fallos.

Finalmente en referencia a lo expuesto en la AMFE se complementó con la metodología MAGERIT, cuyo enfoque dio lugar al análisis de los activos y evaluación de los riesgos y amenazas presentadas en la infraestructura tecnológica de la UCCI, siendo así que permite mejorar la toma de decisiones y usabilidad de estrategias de carácter preventivo y correctivo en cada una de sus áreas.

6. ESTRUCTURA

Es oportuno resaltar los aspectos de gran relevancia que conforman la Norma ISO 22301, cabe indicar que este compendió se convirtió en la base primordial para el sustento del desarrollo del Modelo de Gestión de Continuidad de la Infraestructura Tecnológica (Figura 2).

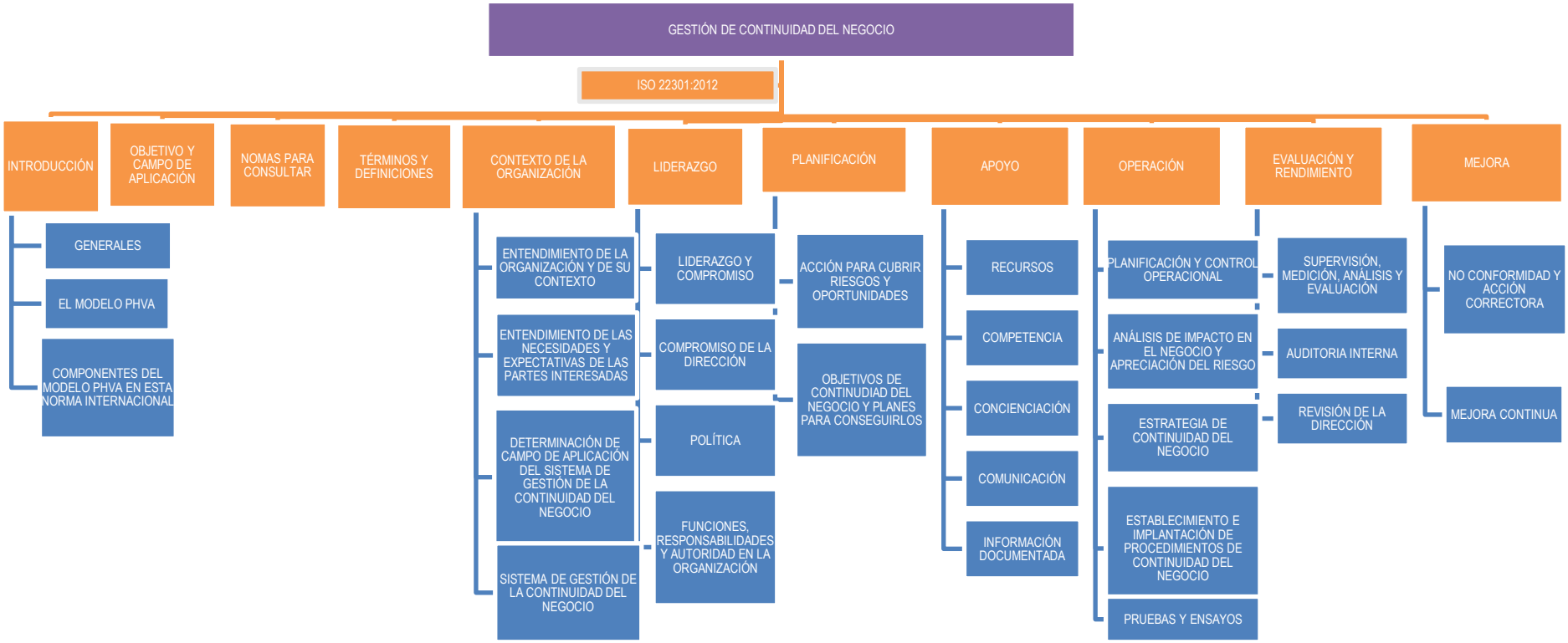


Figura 2. Estructura de Modelo de Continuidad en base a la norma ISO 22310
Elaborado por: Las autoras.

Seguidamente se lleva a cabo el enfoque de los procesos que se alinean a las funciones críticas de la UCCI, de acuerdo a los análisis de ejecución para el cumplimiento del Modelo de Continuidad (Figura 3).

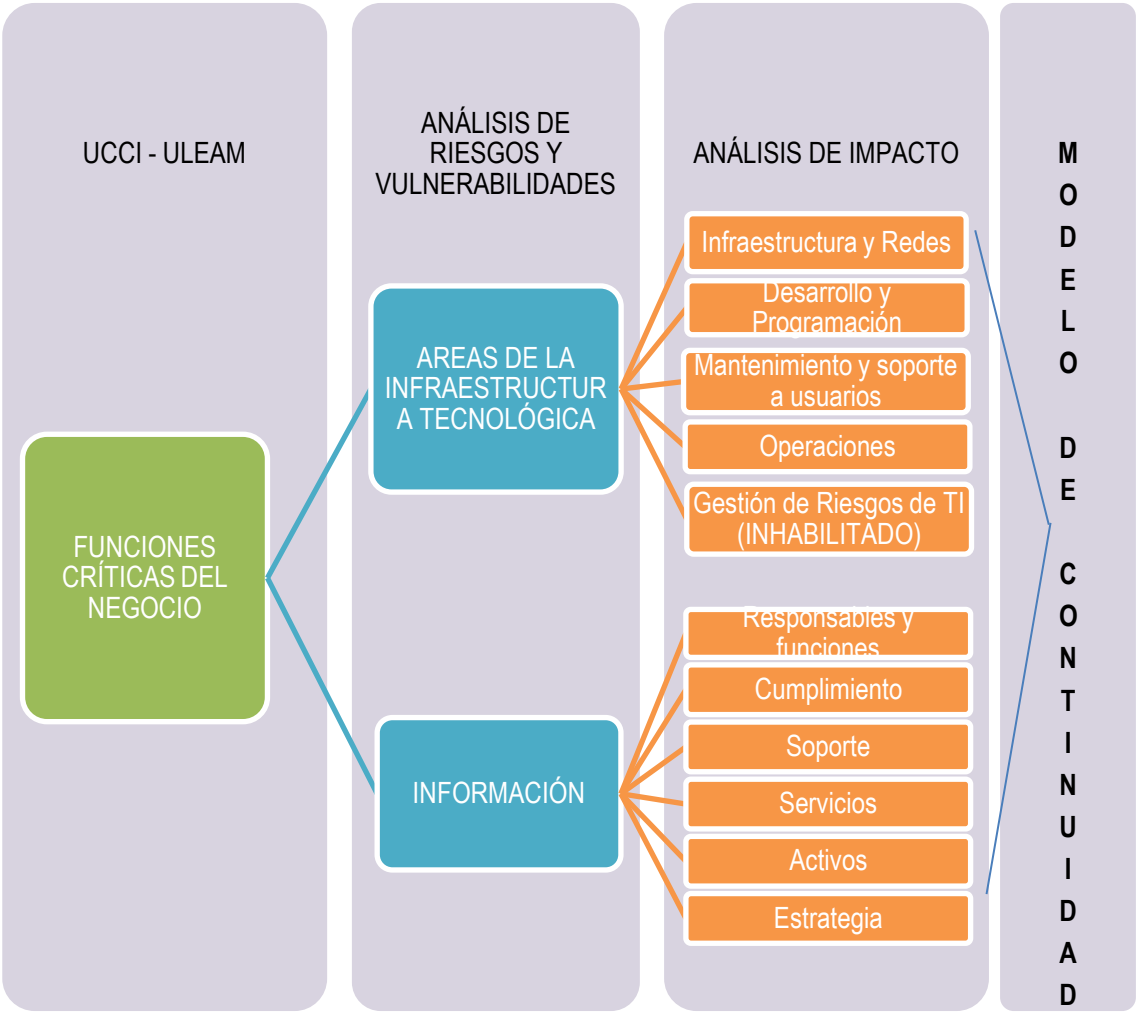


Figura 3. Enfoque del Modelo de Continuidad en base a las funciones criticas del Negocio
Elaborado por: Las autoras.

Es importante recalcar que los dos esquemas antes expuestos trabajan conjuntamente, es decir en relación a cómo llevar la puesta en marcha del modelo, y por ende haciendo hincapié sobre todo en los activos y recursos de información pertenecientes a la UCCI, de forma que se considere en lo posible alcanzar el rendimiento óptimo del negocio y la estabilidad.

7. MÉTODOS Y PROCESOS

Seguidamente se establecen métodos y procesos con los que se llevará a cabo la continuidad de las actividades en las áreas de la UCCI (Tabla 1).

Tabla 1. Métodos y procesos de Continuidad de Negocios.

MÉTODOS	PROCESOS
Seguridad de la información en el proceso de Gestión de la Continuidad del Negocio	• Considerar los requerimientos de seguridad de la información obligatorios para la continuidad del proceso. • Ejecutar y proteger un proceso para la Continuidad del Negocio.
Evaluación del riesgo	• Identificar los sucesos que originan dificultades en los métodos en relación con la probabilidad de impacto. • Análisis y evaluación de riesgos
Análisis de Impacto	• Establecer los procesos críticos • Comprender las actividades de los procesos. • Correlación entre áreas y usuarios • Concordancia de los procesos
Estrategias de recuperación	• Desarrollar alternativas de estrategias • Clarificar los requerimientos mínimos para la recuperación • Establecer capacidad del sitio de recuperación
Desarrollo del Plan de Continuidad	• Desarrollar el Plan de Continuidad para conservar o restituir las operaciones • Asegurar la disponibilidad de la información en el nivel requerido y en tiempo establecido requeridas después de la interrupción o falta en los procesos de negocios críticos
Marco referencial para la planeación de la Continuidad del Negocio	• Conservar el marco referencial del Plan de Continuidad de Negocio y la certificación del plan que cumpla con los requerimientos de la seguridad de la información. • Prevalecer la calidad de los activos e información de la infraestructura tecnológica de la UCCI.

Elaborado por: Las autoras.

8. MEDIDAS Y CONTROLES DE CONTINUIDAD DE NEGOCIO

Desde una perspectiva histórica la Norma ISO 22301, ha sido un compendio de los esfuerzos acciónales en el ámbito empresarial internacional, por obtener un estándar que ayude a gestionar la Continuidad de un Negocio y/o actividades de una organización.

A continuación se establecen las respectivas medidas y controles, para la continuidad de las actividades:

- Establecer una base común de conocimiento para entender la Continuidad del Negocio.

- Desarrollar e implantar una política de Continuidad del Negocio en una organización.

- Acreditar la conformidad y compromiso de una organización con las mejores prácticas internacionales en Continuidad del Negocio.

En conclusión es importante reafirmar que la aplicación correcta de las medidas y controles, deben ser generados en todas las actividades de la Institución, mismos que permitirá la continuidad y reputación en circunstancias adversas.

8.1. PLANES QUE INVOLUCRAN LA CONTINUIDAD DE NEGOCIOS

Es importante dar a conocer que en el Modelo de Continuidad de Negocio se ven involucrados criterios relevantes de planes complementarios, mismos que brindan apoyo en los procesos y actividades según su planificación (Figura 5).

Figura 5. Planes que intervienen en el modelo de Continuidad de Negocios.
Elaborado por: Las autoras.

9. GLOSARIO DE TÉRMINOS

Posteriormente se desglosan términos de gran relevancia, mismos que se encuentran inmersos en la investigación realizada, (Tabla 2).

Tabla 2. Glosario de términos.

TÉRMINO DE REFERENCIA	DEFINICIÓN	CITA BIBLIOGRÁFICA
BCP	Plan de Continuidad de Negocio, es el conjunto de procedimientos y estrategias definidos para asegurar la reanudación oportuna y ordena de los procesos del negocio.	(Morales, 2014)
ULEAM	Unidad Laica Eloy Alfaro de Manabí Extensión Chone	Las autoras
UCCI	Unidad Central de Coordinación Informática	Las autoras
INFRAESTRUCTURA TÉCNOLOGICA	Es el conjunto de hardware y software sobre el que se asientan los diferentes servicios que la Universidad necesita tener en funcionamiento para poder llevar a cabo toda su actividad, tanto docente como de investigación o de gestión interna	(UOC, s.f.).
NORMA ISO 22301	Se especifica los requisitos para la planificación, establecimiento, implementación, operación, revisión y mantenimiento continuo de SGCN, sirve para proteger, reducir la ocurrencia, prepararse, responder y recuperarse de incidentes que interrumpan los procesos, cuando éstos ocurren.	(Isotools, 2017)
NORMA ISO 27002	Es una guía de buenas prácticas que puntualiza los objetivos de control y controles recomendables en cuanto a la seguridad de la información, ésta puede ser de gran utilidad ya que proporciona más información sobre cómo implementar esos controles.	(Crespo Rin, 2013) (ISO 27001. s.f.) (ISO 27000)
AMFE	Análisis Modal de Fallos y Efectos, es una herramienta de gran utilidad y valor, que permite identificar las variables significativas de un producto o proceso para poder determinar y priorizar los riesgos	(González, Myer y Pachón, 2017)
MAGERIT	Metodología de Análisis y Gestión de Riesgos de los	(Cordero, 2015)

	Sistemas de Información, sirve para investigar los riesgos que soportan los sistemas de información y para recomendar las medidas apropiadas que debe adoptar la organización.	
GCN	Gestión de la Continuidad de Negocio	Las autoras
PHVA	Planifica, Hacer, Verificar y Actuar, ciclo de mejora continua del Plan de Continuidad del Negocio.	Las autoras
LIKERT	Escala estadística para obtener niveles de impacto o probabilidad.	Las autoras
CHECKLIST	También se le conoce como listados de control, listados de chequeo, u hojas de verificación, siendo formatos generados para realizar actividades repetitivas y controlar el cumplimiento de un listado de requisitos.	(ISOTOOL, 2018).
BIA	Análisis de Impacto del Negocio, es la etapa que permite identificar la urgencia de recuperación de cada área, determinando el impacto en caso de interrupción.	(Nieto, 2013)
SGCN	Sistema de Gestión de Continuidad de Negocio	Las autoras
BPM	Gestión de Procesos de Negocios (Business Process Management)	Las autoras
CYBERSEGURIDAD	Métodos de uso, procesos y tecnologías para prevenir, detectar y recuperarse de daños a la confidencialidad, integridad y disponibilidad de la información en el ciberespacio.	Las autoras
DATA CENTER	Centro de Procesamiento de Datos	Las autoras
VULNERABILIDAD	Cualquier fallo de diseño que permita que una amenaza pueda afectar a un recurso. Las vulnerabilidades existen no se fabrican.	(Romero *et al.,* 2018)
RIESGO	Es todo lo que podría suceder y afectar el logro de los objetivos organizacionales.	Las autoras
AMENAZA	Sucesos que pueden dañar los procedimientos o recursos.	(Romero *et al.,* 2018)
IMPACTO	Impacto causa la ocurrencia de un incidente o siniestro.	Las autoras
INCIDENCIAS	Problemas ocasionados por factores diferentes y en momentos inesperados.	Las autoras
EDR	Evaluación de Riesgo	Las autoras
PETI	Plan Estratégico de Tecnología de Información	Las autoras

CONTINGENCIA	Es una precaución o alternativa en caso de una eventualidad o incidencia.	Las autoras
EVENTOS	Un suceso o serie de sucesos que pueden ser internos o externos a la empresa, originados por la misma causa, que ocurren durante el mismo periodo de tiempo.	(Ramírez, 2017)
DESASTRE	Evento adverso que se manifiesta en un territorio determinado y cuya magnitud altera en gran medida la vida cotidiana de las personas, sus bienes, actividades y servicios.	Las autoras
ESTRATEGIAS	Indicadores o acciones de mejoras que se llevan a cabo en una planificación.	Las autoras
RECUPERACIÓN	Es cuando un activo o recurso de información ha sufrido por alguna pérdida o fallo.	Las autoras

Elaborado por: Autores diversos.

10. PROPUESTA METODOLÓGICA

Es imprescindible destacar que la propuesta metodológica se realizó en base al ciclo de vida de Continuidad de Negocios PHVA y la norma ISO 22301, aquí se consideraron aspectos relevantes, mismos que fueron clasificados en tres fases, haciendo énfasis en cada una de ella la relación al alcance del Plan. (Figura 4).

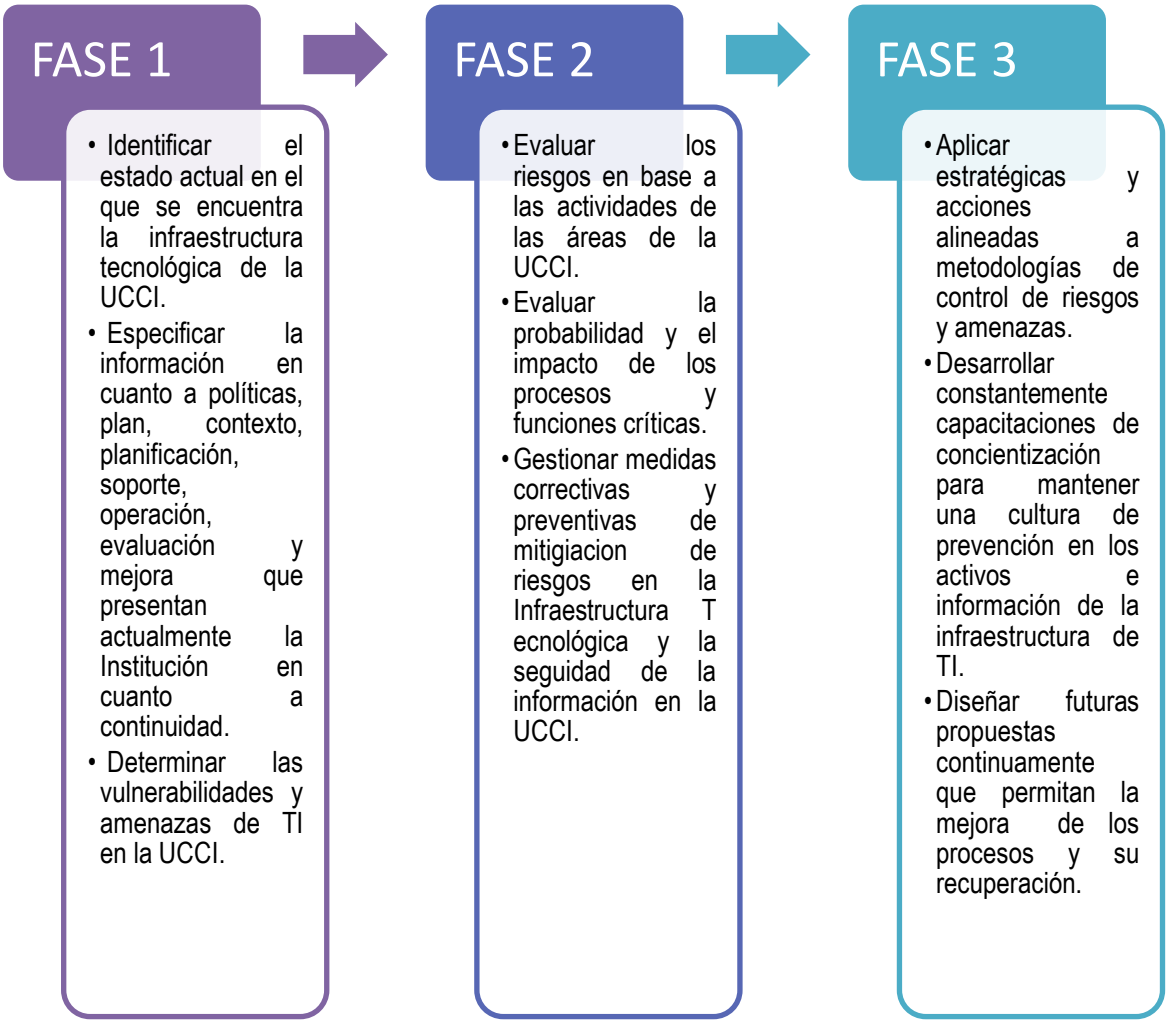


Figura 4. Propuesta Metodológico de Continuidad.
Elaborado por: Las autoras.

Cabe recalcar que esta propuesta establece fases secuenciales a cumplir en la UCCI en caso de ocurrencia de alguna eventualidad o incidente, que para el efecto sean alineados al control efectivo de la Continuidad de Negocio.

11. EVALUACIÓN DE RIESGOS

Es preciso resaltar informaciones relevantes plasmadas en el plan de Contingencia de la UCCI, en donde se menciona que los riesgos de un evento catastrófico tales como: Incendios, terremotos, tormentas, entre otros; mismos que proliferan a nuevas amenazas externas como ataques cibernéticos y virus, permitiendo generar vulnerabilidades a los servicios de tecnologías de información implementadas en la Institución. En consecuencia de estos eventos se crearían enormes pérdidas físicas, económicas, de imagen e incluso humanas si no son mitigadas eficientemente (UCCI, 2013).

Cabe indicar que la Unidad Central de Coordinación Informática de la ULEAM ofrece un amplio catálogo de servicios tecnológicos de soporte e infraestructura orientados a las principales actividades del organismo como la docencia, investigación, gestión y administración, a la vez es importante mencionar que al ejecutar los servicio que brinda el catalogo permitirá asegurar no solo la continuidad de estas operaciones, sino también la información que se genera en cada uno de estos ámbitos. Es importante considerar que siendo la información su activo de mayor valor, la unidad debe recuperar y restaurar sus funciones críticas que han sido parcial o totalmente interrumpidas después de una contingencia o desastre, es decir reduciendo las pérdidas y preservando su buen nombre con la aplicación del proceso de Gestión de la Continuidad (UCCI, 2013).

Dadas las condiciones que anteceden al momento de efectuar la evaluación, se debe considerar diversos aspectos, entre ellos la aplicación de la escala de Likert, estableciendo los criterios (Muy sensible, sensible, poco sensible, no sensible) para las vulnerabilidades encontradas.

Con referencia a lo anterior resulta oportuno presentar el total de vulnerabilidades encontradas en la investigación realizada; cabe indicar que se consideraron las 4 áreas y la unidad en general.

En la Unidad Central de Coordinación Informática del total de vulnerabilidades el criterio de muy sensible obtuvo el mayor porcentaje con su equivalencia a 49%, seguido de sensible con 46% y poco sensible con 6% (Tabla 3).

Tabla 3. Total de vulnerabilidades UCCI.

TOTAL DE VULNERABILIDADES UCCI		
CLASIFICACIÓN	**FRECUENCIA ABSOLUTA**	**FRECUENCIA RELATIVA**
MUY SENSIBLE	17	49%
SENSIBLE	16	46%
POCO SENSIBLE	2	6%
TOTAL	35	100%

Elaborado por: Las autoras.

Seguidamente se detalla el total de vulnerabilidades en el área de desarrollo, teniendo como más alto el criterio de sensible con un equivalente al 100% y 0% para la los criterios de muy sensible y poco sensible (Tabla 4).

Tabla 4. Total de vulnerabilidades en área desarrollo.

TOTAL DE VULNERABILIDADES ÁREA DE DESARROLLO		
CLASIFICACIÓN	**FRECUENCIA ABSOLUTA**	**FRECUENCIA RELATIVA**
MUY SENSIBLE	0	0%
SENSIBLE	7	100%
POCO SENSIBLE	0	0%
TOTAL	7	100%

Elaborado por: Las autoras.

Posteriormente se muestra el total de vulnerabilidades en el área de mantenimiento, teniendo como más alto el criterio de sensible equivalente al 100% y 0% para los criterios de muy sensible y poco sensible (Tabla 5).

Tabla 5. Total de vulnerabilidades en área mantenimiento.

TOTAL DE VULNERABILIDADES ÁREA DE MANTENIMIENTO		
CLASIFICACIÓN	**FRECUENCIA ABSOLUTA**	**FRECUENCIA RELATIVA**
MUY SENSIBLE	0	0%
SENSIBLE	1	100%
POCO SENSIBLE	0	0%
TOTAL	1	100%

Elaborado por: Las autoras.

A si mismo se describen el total de vulnerabilidades en el área de operación, teniendo como igualdad los criterios de muy sensible y el sensible con el 50% y con la cantidad de 0% la de poco sensible (Tabla 6).

Tabla 6. *Total de vulnerabilidades en área operación*.

TOTAL DE VULENERABILIDADES ÁREA DE OPERACIÓN		
CLASIFICACIÓN	**FRECUENCIA ABSOLUTA**	**FRECUENCIA RELATIVA**
MUY SENSIBLE	4	50%
SENSIBLE	4	50%
POCO SENSIBLE	0	0%
TOTAL	8	100%

Elaborado por: Las autoras.

Por ultimo está el total de vulnerabilidades en el área de redes, teniendo como más alto el criterio de muy sensible equivalente al 63%, seguido de sensible con 25% y poco sensible con 13% (Tabla 7).

Tabla 7. Total de vulnerabilidades en área redes.

TOTAL DE VULENERABILIDADES AREA DE REDES		
CLASIFICACIÓN	**FRECUENCIA ABSOLUTA**	**FRECUENCIA RELATIVA**
MUY SENSIBLE	5	63%
SENSIBLE	2	25%
POCO SENSIBLE	1	13%
TOTAL	8	100%

Elaborado por: Las autoras.

11.1. CRITERIOS DE LA METODOLOGÍA MAGERIT

Teniendo en cuenta que las amenazas son sucesos que pueden acontecer en cualquier momento y causar daños irreversibles a los activos de la institución, es importante identificarlos a tiempo y en lo posible evitar que sucedan.

A continuación se presenta la clasificación de amenazas, misma que se determinó en base a la metodología MAGERIT, quedando establecida de la siguiente manera: desastres naturales (Tabla 8), de origen industrial (Tabla 9), errores y fallos no intencionados (Tabla 10), ataques intencionados (Tabla 11).

Tabla 8. Clasificación según Desastres Naturales.

CLASIFICACIÓN	**DENOMINACIÓN**	**DESCRIPCIÓN**
[N] Desastres Naturales	[N.1]Fuego	01. – Incendio
	[N.2]Daño por agua	02 – Perjuicios ocasionados por el agua.
	[N.*] Desastres naturales	03. – Contaminación 04. – Siniestro mayor

		06. – Fenómeno climático. 07. – Fenómeno sísmico 08. – Fenómeno de origen volcánico. 09. – Fenómeno meteorológico. 10. – Inundación

Fuente: Las autoras.

Tabla 9. Clasificación de fallos según Origen Industrial.

CLASIFICACIÓN	DENOMINACIÓN	DESCRIPCIÓN
[i] De Origen Industrial	[I.1]Fuego	01. – Incendio
	[I.2]Daño por agua	02 – Perjuicios ocasionados por el agua.
	[I.*] Desastres Industriales	04. – Siniestro mayor
	[I.3]Contaminación Mecánica	03. – Contaminación
	[I.4] Contaminación Electromagnética	14. – Emisiones electromagnéticas 15. – Radiaciones térmicas 16. – Impulso electromagnético
	[I.5] Avería de Origen Físico o Lógico	28. – Avería del hardware 29. – Falla del funcionamiento del Hardware.
	[I.6] Corte del Suministro Eléctrico	12. – Pérdida de suministro de energía.
	[I.7] Condiciones Inadecuadas de Temperatura o humedad.	11. – Fallas en la climatización
	[I.8] Fallo de Servicios de Comunicaciones	13.- Pérdida de los medios de telecomunicación.
	[I.9] Interrupción de otros Servicios y Suministros Esenciales.	00. – No disponible
	[I.10] Degradación de los soportes de almacenamiento de la Información	28. – Avería del hardware 29. – Falla de funcionamiento del hardware
	[I.11] Emanaciones Electromagnéticas	17. - Interceptación de señales parasitas comprometedoras.

Elaborado por: Las autoras.

Tabla 10. Clasificación de Errores y Fallos y no Intencionados.

CLASIFICACIÓN	DENOMINACIÓN	DESCRIPCIÓN
[E] Errores y Fallos y no Intencionados	[E.1] Errores de los Usuarios.	38. - Error de uso.
	[E.2] Errores del Administrador.	38. - Error de uso.
	[E.3] Errores de Monitorización.	00. – No disponible

	[E.4] Errores de Configuración	00. – No disponible
	[E.7]Deficiencias en la Organización	00. – No disponible
	[E.8] Difusión de Software Dañino.	00. – No disponible
	[E.9] Errores de [re-] Encaminamiento.	00. – No disponible
	[E.10] Errores de Secuencia	00. – No disponible
	[E.14] Escapes de Información	00. – No disponible
	[E.15] Alteración Accidental de la Información.	00. – No disponible
	[E.18] Destrucción de la Información	00. – No disponible
	[E.19] Fugas de Información	00. – No disponible
	[E.20] Vulnerabilidades de los Programas (Software)	00. – No disponible
	[E.21] Errores de Mantenimiento / Actualización de Programas (Software)	31. - Falla de funcionamiento del software. 32. - Perjuicio a la mantenibilidad del sistema de información
	[E.23] Errores de Mantenimiento / Actualización de Equipos (Hardware)	32. -Perjuicio a la mantenibilidad del sistema de información
	[E.24] Caída del Sistema por agotamiento de recursos.	30. – Saturación del sistema informático.
	[E.25] Pérdida de Equipos	22. – Recuperación de soportes reciclados o desechados.
	[E.28] Indisponibilidad del Personal	42. – Daño a la disponibilidad del personal

Elaborado por: Las autoras.

Tabla 11. Clasificación de Ataques Intencionados.

CLASIFICACIÓN	DENOMINACIÓN	DESCRIPCIÓN
[A] Ataques Intencionados	[A.3] Manipulación de los Registros de Actividad (LOG)	00. – No disponible.
	[A.4] Manipulación de la Configuración	00. – No disponible.
	[A.5] Suplantación de la Identidad del Usuario.	40. – Usurpación de derecho.
	[A.6] Abuso de Privilegios de Accesos.	39. - Abuso de derecho
	[A.7] Uso no previsto	00. – No disponible

[A.8] Difusión de Software Dañino.	00. – No disponible
[A.9] [RE-] Encaminamiento de Mensajes.	00. – No disponible
[A.10] Alteración de Secuencia	36. – Alteración de datos.
[A.11] Acceso no Autorizado.	33. – Uso ilícito de hardware.
[A.12] Análisis de Tráfico.	00. – No disponible
[A.13] Repudio	41. – Negación de acciones.
[A.14] Interceptación de Información (Escucha)	19. – Escucha pasiva.
[A. 15] Modificación deliberada de la Información	00. – No disponible
[A.18] Destrucción de Información	00. – No disponible
[A.19] Divulgación de Información.	23. – Divulgación. 27. – Geolocalización 34. – Copia ilegal de software.
[A.22] Manipulación de Programas.	26. – Alteración de Programas.
[A.23] Manipulación de los Equipos	25. – Sabotaje del hardware.
[A.24] Denegación de Servicios.	30. – Saturación del Sistema Informático.
[A.25] Robo	20. Robo de soportes o documentos. 21. – Robo de Hardware.
[A.26] Ataque destructivo	05. – Destrucción de hardware o de soporte.
[A.27] Ocupación Enemiga	00. – No disponible
[A.28] Indisponibilidad del Personal.	42. – Daño a la disponibilidad del personal.
[A.29] Extorsión.	00. – No disponible
[A.30] Ingeniería Social (Picaresca)	00. – No disponible

Elaborado por: Las autoras.

Por consiguiente se muestran las causas más representativas que motivan cada uno de los escenarios más usuales y tolerados por la UCCI: (Tabla 12).

Tabla 12. Causas representadas en escenarios frecuentes en la UCCI.

CAUSAS	ESCENARIOS
• Fallas Corte de Cable UTP • Fallas Tarjeta de Red • Fallas IP asignado • Fallas Punto de Swicht • Fallas Punto Pacht Panel • Fallas Punto de Red •	A. NO HAY COMUNICACIÓN ENTRE CLIENTE – SERVIDOR EN UNO O VARIOS TERMINALES DE LA ULEAM

• Fallas de Componentes de Hardware. • Servidor. • Virus. • Sobrepasar el límite de almacenamiento del Disco • Computador de Escritorio funciona como Servidor.	B. FALLA DE UN SERVIDOR
• Accidente • Renuncia Intempestiva	C. AUSENCIA PARCIAL O PERMANENTE DEL PERSONAL DE UCCI
• Corte General del Fluido eléctrico	D. INTERRUPCIÓN DEL FLUIDO ELÉCTRICO DURANTE LA EJECUCIÓN DE LOS PROCESOS.
• Falla de equipos de comunicación: • SWITCH, Antenas, Fibra Óptica. • Fallas en el software de Acceso a Internet. • Perdida de comunicación con proveedores de Internet	E. PERDIDA DE SERVICIOS DE INTERNET
• Incendio • Sabotaje • Corto Circuito • Terremoto • Tsunami	F. INDISPONIBILIDAD DE LA UNIDAD DE SISTEMAS (DESTRUCCIÓN DEL CUARTO DE SERVIDORES)

Fuente: (ULEAM, 2013).

De acuerdo a la información registrada en la UCCI se analizó el número de incidencias por cada categoría (Servicios, infraestructura, software, hardware y otros), evidenciando que la categoría software posee el mayor número de incidencias equivalente al 58%; seguido de la categoría otros con 21%; servicios con 18%, infraestructura con 2% y hardware con 1%. (Tabla 13).

Tabla 13. Total incidencias solicitadas en la infraestructura tecnológica de la ULEAM.

INCIDENCIAS SOLICITADAS EN LA INFRAESTRUCTURA TECNOLÓGICA DE LA ULEAM			
CATEGORÍA	**INCIDENCIAS**	**FRECUENCIA ABSOLUTA**	**FRECUENCIA RELATIVA**
SERVICIOS	Acceso a información	560	11%
	Acceso a correo institucional	250	5%
	Habilitación de formularios	123	2%
HARDWARE	Reinicio de servicios	50	1%
SOFTWARE	Aula virtual	1053	20%
	Matricula	560	11%
	Asignaturas	200	4%
	Usuarios y contraseñas	357	7%
	Notas	254	5%
	Horarios	134	3%
	Correo institucional	24	0%
	Autoevaluación	112	2%

	Encuesta	158	3%
	Cupos Inglés	150	3%
INFRAESTRUCTURA	Acceso denegado servicios	57	1%
	Problemas a cargar sitios	34	1%
OTROS	OTROS	1113	21%
TOTAL		5189	100%

Elaborado por: Las autoras.

Considerando que cada área influye en cierta medida con aspectos de amenazas según sea la incidencia, se identificó a qué tipo de riesgo o amenaza corresponde y la cantidad de ocurrencia producida en el último año (Tabla 14).

Tabla 14. Total de vulnerabilidades por área.

ÁREA	AMENAZA	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
UCCI	[N] Desastres Naturales	3	5%
	[i] De Origen Industrial	3	5%
	[E] Errores y Fallos y no Intencionados	15	25%
	[A] Ataques Intencionados	14	24%
DESARROLLO	[N] Desastres Naturales	0	0%
	[i] De Origen Industrial	0	0%
	[E] Errores y Fallos y no Intencionados	4	7%
	[A] Ataques Intencionados	3	5%
MANTENIMIENTO	[N] Desastres Naturales	0	0%
	[i] De Origen Industrial	0	0%
	[E] Errores y Fallos y no Intencionados	0	0%
	[A] Ataques Intencionados	1	2%
OPERACIONES	[N] Desastres Naturales	0	0%
	[i] De Origen Industrial	0	0%
	[E] Errores y Fallos y no Intencionados	4	7%
	[A] Ataques Intencionados	4	7%
REDES	[N] Desastres Naturales	2	3%
	[i] De Origen Industrial	1	2%
	[E] Errores y Fallos y no Intencionados	2	3%
	[A] Ataques Intencionados	3	5%
		59	100%

Elaborado por: Las autoras.

Así mismo las vulnerabilidades se clasificaron de acuerdo al tipo de análisis y gestión de riesgos implantado en las tecnologías de la información, donde se logró observar que el área de mayor incidencia es la general de la UCCI y el riesgo que más influencia tiene es seguridad con respectos a las demás (Tabla 15 y gráfico 1)

Tabla 15. Riesgos por áreas según la metodología MAGERIT

ÁREA	RIESGOS EN SEGURIDAD	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
UCCI	Técnicos	3	5%
	Humanos	3	5%
	Gestión	4	7%
	Administración	4	7%
	Accesibilidad	2	3%
	Disponibilidad	5	8%
	Seguridad	13	22%
	Otros	1	2%
DESARROLLO	Técnicos	0	0%
	Humanos	0	0%
	Gestión	2	3%
	Administración	1	2%
	Accesibilidad	1	2%
	Disponibilidad	0	0%
	Seguridad	3	5%
	Otros	0	0%
MANTENIMIENTO	Técnicos	0	0%
	Humanos	0	0%
	Gestión	0	0%
	Administración	0	0%
	Accesibilidad	0	0%
	Disponibilidad	0	0%
	Seguridad	1	2%
	Otros	0	0%
OPERACIONES	Técnicos	0	0%
	Humanos	0	0%
	Gestión	1	2%
	Administración	1	2%
	Accesibilidad	1	2%
	Disponibilidad	1	2%
	Seguridad	4	7%
	Otros	0	0%
REDES	Técnicos	2	3%
	Humanos	1	2%
	Gestión	1	2%
	Administración	0	0%
	Accesibilidad	0	0%
	Disponibilidad	1	2%
	Seguridad	2	3%
	Otros	1	2%
TOTAL		59	100%

Elaborado por: Las autoras.

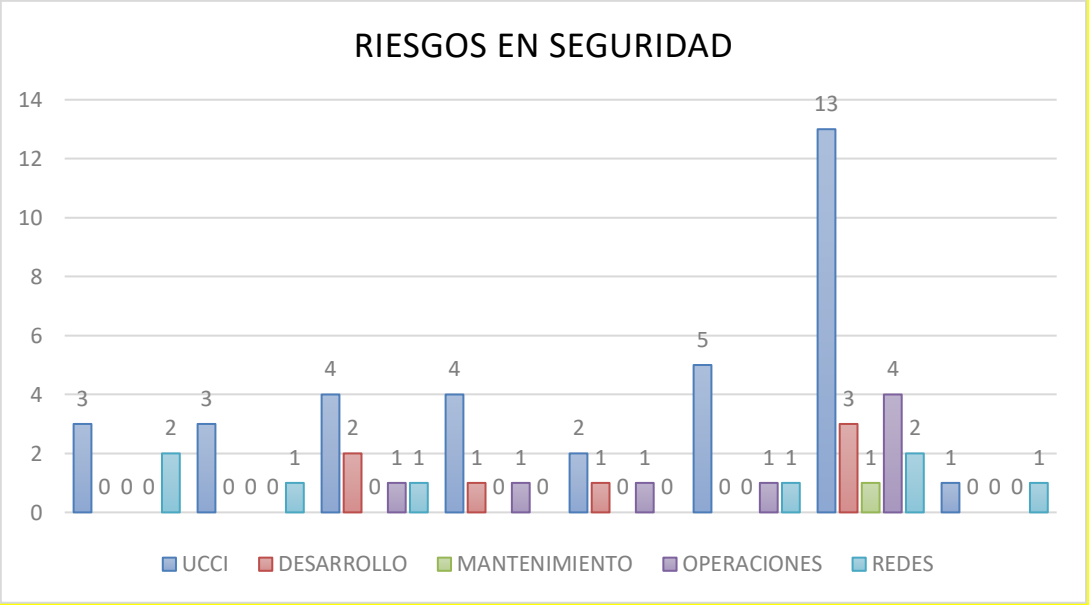


Gráfico 1. Riesgos por áreas.
Elaborado por: Las autoras.

Finalmente se muestra el porcentaje de vulnerabilidades según el tipo de riesgo valorado por la escala de Likert, del cual el más alto pertenece a No Sensible con el 70%, seguidamente muy sensible y sensible con el 14% y por último el 2% con el poco sensible (Gráfico 2).

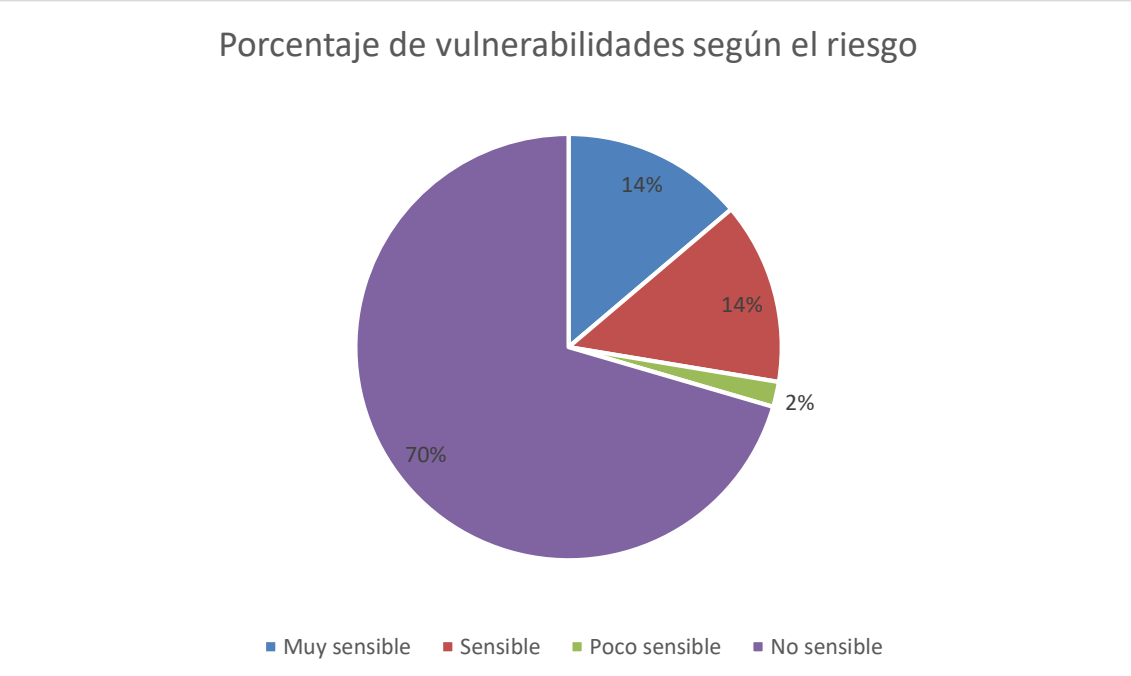


Gráfico 2. Vulnerabilidades según los riesgos.
Elaborado por: Las autoras.

11.2. CRITERIOS DE LA METODOLOGÍA AMFE

Por otra parte con la metodología AMFE, se logró considerar y clasificar las vulnerabilidades expuestas con los datos obtenidos de la aplicación del Checklist, los cuales se encasillaron por áreas, es decir permitiendo conocer las acciones de mitigación y los criterios de aceptación, en base a los cuales se establecen las medidas alternativas preventivas y correctivas, y a la vez que accedan a disminuir en lo posible afectaciones en el negocio con respecto a eventualidad o incidente en los diferentes escenarios.

A continuación se muestra los resultados de las vulnerabilidades obtenidos en la UCCI por medio de la matriz de riesgos AMFE:

- **ÁREA GENERAL UCCI**

ID. Riesgo	Vulnerabilidades UCCI	Probabilidad	Impacto	Nivel	Matriz de Riesgos	Responsables	ID de Mitigación	Acciones de mitigación	Criterio de aceptación
R.1.1.	No posee políticas de seguridad de la información aprobadas por la dirección.	Alto 3	Muy Grave 3	Crítico	MG X G M B M A	Director/Coordinador TI	A.1.1.1	Aprobar las políticas de seguridad de la información por parte de la máxima autoridad	Seguridad en el entorno TI.
R.1.2.	Las políticas de seguridad no son publicadas ni comunicadas a los empleados de TI y partes externas relevantes.	Alto 3	Grave 2	Alto	MG G X M B M A	Director/Coordinador de TI - Áreas asignadas	A.1.2.1	Socializar las políticas de seguridad a todos los empleados de TI y partes externas relevantes para la entidad.	Cumplimiento de las políticas de seguridad.
R.1.3.	En las políticas de seguridad de la información, no incluye la seguridad física de TI y ni las copia de respaldo de la información.	Alto 3	Muy Grave 3	Crítico	MG X G M B M A	Director/Coordinador TI	A.1.3.1	Elaborar las políticas de seguridad física de TI y las políticas de copia de respaldo de la información.	Mantener las áreas seguras y en conjunto con la información.
R.1.4.	No se revisan las políticas de	Alto	Muy Grave	Crítico	MG X	Director/Coordinador TI	A.1.4.1	Revisión periódica del cumplimiento de las	Al menos cada 6 meses hacer la revisión.

	seguridad de la información en la UCCI.	3	3		G M B M A							políticas de seguridad de la información.		
R. 1.5.	La Dirección no toma en cuenta los resultados de las revisiones de las políticas de seguridad.	Alto 3	Muy Grave 3	Crítico	MG G M B M A			X			Director/Coordinador TI	A.1.5.1	Revisar los resultados semestrales de las revisiones de las políticas de seguridad de la información.	Mejorar la seguridad de la información.
R.1.6.	No cuenta con un sistema de gestión de Continuidad del Negocio.	Alto 3	Muy Grave 3	Crítico	MG G M B M A			X			Director/Coordinador TI	A.1.6.1	Elaborar un plan de Gestión de Continuidad del Negocio	Directrices de la norma ISO/IEC 22301
R.1.7	En la UCCI no clasifica los activos ni los protege debidamente para asegurar su cuidado.	Alto 3	Muy Grave 3	Crítico	MG G M B M A						Director/Coordinador TI	A.1.7.1	Clasificar los activos custodios dentro de la unidad para asegurar su cuidado.	Protección de activos.
R.1.8.	No se registra la fecha y la hora de entrada y salida de los visitantes o personas externas a la unidad.	Medio 2	Muy Grave 3	Alto	MG G M		X				Director/Coordinador de TI - Áreas asignadas	A.1.8.1	Registrar todas las entradas y salidas con fechas de las visitas externas a la unidad.	Control de acceso a la unidad.

							B	M	A					
R.1.9.	No se diseña ni se aplica seguridad física a las oficinas, despachos y recursos de la unidad.	Medio	Muy Grave	Alto		MG		X		Director/Coordinador de TI - Áreas asignadas	A.1.9.1	Asegurar que todas las áreas de TI apliquen seguridad física en sus oficinas y recursos de la unidad.	Seguridad de las áreas de trabajo.
		2	3			G							
						M							
							B	M	A				
R.1.10.	La unidad no cuenta con un diseño aplicable de protección física contra desastres naturales, ataques provocados por el hombre o accidentes.	Alto	Muy Grave	Crítico		MG			X	Director/Coordinador TI	A.1.10.1	Elaborar un diseño aplicable de protección física contra desastres naturales, o ataques provocados por el hombre o accidentes.	Preparación futura para desastres naturales o accidentes
		3	3			G							
						M							
							B	M	A				
R.1.11.	La unidad no tiene un plan de contingencia y de emergencia contra amenazas externas y ambientales.	Alto	Muy Grave	Crítico		MG			X	Director/Coordinador TI	A.1.11.1	Elaborar un plan de contingencia y de emergencia contra amenazas externas y ambientales.	Mitigar riesgos contra desastres naturales o amenazas externas y ambientales.
		3	3			G							
						M							
							B	M	A				
R.1.12.	No se ha diseñado ni implementado procedimientos para trabajar en áreas seguras.	Alto	Grave	Alto		MG				Director/Coordinador de TI - Áreas asignadas	A.1.12.1	Diseñar e implementar los procedimientos para trabajar en áreas seguras	Verificar que las áreas seguras tengan todo el recurso para trabajar.
		3	2			G			X				
						M							
							B	M	A				

R.1.13.	El material que entra a la unidad, no es inspeccionado para evitar amenazas potenciales como explosivos, productos químicos y otros materiales de riesgo.	Medio 2	Grave 2	Medio		MG G M		X			Director/Coordinador TI	A.1.13.1	Revisar todo el material que entra en la unidad.	Inspeccionar para evitar amenazas potenciales como explosivos, químicos u otro material de riesgo.
							B	M	A					
R.1.14.	El material (equipos tecnológicos) que entra a la unidad no es registrado de acuerdo a los procedimientos de gestión de activos.	Alto 3	Grave 2	Alto		MG G M			X		Director/Coordinador de TI - Áreas asignadas	A.1.14.1	Registrar los equipos tecnológicos que ingresan a la unidad.	Procedimientos de gestión de activos.
							B	M	A					
R.1.15.	Los interruptores y válvulas de emergencia para cortar el suministro de energía, agua, gas u otro servicio no están ubicados fuera de las salidas de emergencia o de las salas de equipos.	Medio 2	Muy Grave 3	Alto		MG G M		X			Director/Coordinador de TI - Áreas asignadas	A.1.15.1	Ubicar fuera de las salidas de emergencia o de sala de equipos los interruptores y válvulas de emergencia para cortar el suministro de energía, agua, gas u otros.	Mantener la seguridad del área de trabajo.
							B	M	A					
R.1.16.	La unidad no ha establecido las	Alto	Muy Grave	Crítico							Director/Coordinador TI	A.1.16.1	Elaborar un manual de funciones y	Supervisión y aprobación del manual de funciones y

	funciones y responsabilidades asociadas a la gestión de las vulnerabilidades técnicas, incluyendo la supervisión de las mismas, la evaluación de los riesgos de la vulnerabilidad, el parcheo, el seguimiento de activos y cualquier responsabilidad de coordinación necesaria.	3	3			MG G M B	 M	 A	X 			responsabilidades asociadas a la gestión de vulnerabilidades técnicas: supervisión, evaluación de riesgos, seguimiento de activos.	responsabilidades.
R.1.17.	La unidad no tiene un plan de recuperación de desastres.	Alto 3	Muy Grave 3	Crítico		MG G M B	 M	 A	X 	Director/Coordinador TI	A.1.17.1	Elaborar un plan de recuperación de desastres.	Servicios disponibles ante un desastre.
R.1.18.	No se ha realizado auditoría interna a las áreas de la UCCI.	Medio 2	Grave 2	Medio		MG G M B	 M	 A	 	Director/Coordinador TI	A.1.18.1	Realizar auditorías internas en las diferentes áreas de la UCCI.	Una vez al año hacer las auditorías.
R.1.19.	Los activos o grupos de activos no tienen	Alto	Grave	Alto		MG				Director/Coordinador de TI - Áreas	A.1.19.1	Asignar custodios a los activos dentro de la	Gestión de activos

	custodios asignados.	3	2		G M B			X M	A	asignadas		unidad.	
R.1.20.	No se proporcionan las instrucciones de los requisitos de seguridad del área ni los procedimientos de emergencia a los visitantes.	Medio	Grave	Medio	 MG G M B			 X M	 A	Director/Coordinador TI	A.1.20.1	Informar a los visitantes las instrucciones de seguridad del área y los procedimientos de emergencia antes de ingresar.	Mantener la protección del área y los visitantes.
		2	2										
R.1.21.	Todos los empleados, contratistas y terceros y los visitantes que llegan a la unidad, no llevan una identificación visible.	Alto	Grave	Alto	 MG G M B			 M	 A	Director/Coordinador de TI - Áreas asignadas	A.1.21.1	Poseer una identificación visible para todas las personas que ingresan a la unidad	Control de acceso a la unidad.
		3	2										
R.1.22.	No se notifica al personal de seguridad que se encuentran visitantes sin autorización o alguna persona sin llevar visible la identificación.	Medio	Grave	Medio	 MG G M B			 X M	 A	Director/Coordinador TI	A.1.22.1	Notificar a seguridad que vendrán visitantes mediante una lista de las personas que van a ingresar a la unidad con identificación visible.	Mantener la seguridad de la unidad.
		2	2										
R.1.23.	Las áreas seguras vacías no están	Medio	Grave	Medio	 MG			 M	 A	Director/Coordinador TI	A.1.23.1	Revisar las áreas seguras que están vacías para	Mantener la seguridad en las áreas.

	físicamente cerradas ni son comprobadas periódicamente.	2	2			G M	B	X M	A			verificar que estén cerradas.	
R.1.24.	Se permite el ingreso de equipos de fotografía, video, audio u otros equipos de grabación sin autorización.	Medio 2	Grave 2	Medio		MG G M	B	X M	A	Director/Coordinador TI	A.1.24.1	Se debe permitir el ingreso de equipos de fotografía, video, audio u otros equipos con autorización previa del director de la unidad.	Medidas de seguridad del área TI.
R.1.25.	No se establecen directrices para comer, beber y fumar en las proximidades de las instalaciones de tratamiento de la información.	Medio 2	Grave 2	Medio		MG G M	B	X M	A	Director/Coordinador TI	A.1.25.1	Establecer reglamentos para comer, beber y fumar en las proximidades de las instalaciones donde se trata la información.	Directrices de la norma ISO/IEC 27002
R.1.26.	La unidad no realiza inspecciones al azar a los usuarios internos y externos para detectar entrada y salida de activos no autorizados.	Medio 2	Grave 2	Medio		MG G M	B	X M	A	Director/Coordinador TI	A.1.26.1	Realizar inspecciones al azar a los visitantes y empleados de TI para detectar la salida de activos no autorizados.	Inspecciones una vez al azar cada semana
R.1.27.	No tienen políticas de puesto de trabajo despejado de papeles y pantalla limpia para los recursos de	Medio 2	Grave 2	Medio		MG G M		X		Director/Coordinador TI	A.1.27.1	Elaborar políticas de los puestos de trabajo, que permita mantener limpia el área del tratamiento de la información.	Espacios de trabajo limpios.

	tratamiento de la información.						B	M	A					
R.1.28.	La información de negocio sensible o crítica (documentos, almacenamiento electrónico) no es guardada en caja fuerte, armario u otro tipo de mueble de seguridad, cuando no se necesita, especialmente cuando la oficina está vacía.	Medio	Grave	Medio		MG					Director/Coordinador TI	A.1.28.1	Guardar la información sensible o crítica, no solo en digital sino física en un mueble de seguridad, ya sea una caja fuerte cuando la oficina esté vacía.	Disponibilidad de la información en cualquier medio.
						G		X						
		2	2			M								
							B	M	A					
R.1.29.	Los directivos o responsables no utilizan los resultados de los sistemas de control y tendencias de uso para evitar posibles cuellos de botellas o dependencias de personal clave que represente una amenaza para el sistema de seguridad o para los servicios y de esta	Medio	Grave	Medio		MG					Director/Coordinador TI	A.1.29.1	Realizar planes de acción con los resultados que arrojan los sistemas de control y que representan una amenaza para la seguridad de la información, de la unidad o de los servicios.	Acciones adecuadas para mejorar la seguridad.
						G		X						
		2	2			M								

	manera planificar las acciones adecuadas.						B	M	A					
R.1.30.	La unidad no tiene un plan de gestión de la demanda de capacidad.	Medio	Grave	Medio		MG					Director/Coordinador TI	A.1.30.1	Elaborar un plan de gestión de la demanda de capacidad de los empleados, de los sistemas o servicios de la unidad.	Personal, sistema o servicios, preparados para soportar alta demanda.
						G		X						
		2	2			M								
							B	M	A					
R.1.31.	No tiene un plan documentado de gestión de la capacidad para los sistemas de misión crítica.	Medio	Grave	Medio		MG					Director/Coordinador TI	A.1.31.1	De acuerdo con el ID de mitigación A.1.30.1	Llevar registros de la capacidad de los sistemas de misión crítica.
						G		X						
		2	2			M								
							B	M	A					
R.1.32.	La unidad no ha determinado el tiempo de conservación de la información esencial tomando en cuenta cualquier requisito para las copias de archivo que hayan de ser conservadas de manera permanente.	Medio	Grave	Medio		MG					Director/Coordinador TI	A.1.32.1	Determinar el tiempo de conservación de la información esencial de acuerdo a los requisitos de archivo que se conservan de manera permanente.	El tiempo se estima de acuerdo a la importancia que tiene la información.
						G		X						
		2	2			M								
							B	M	A					

R.1.33.	No se ha definido una escala temporal para reaccionar a las notificaciones de vulnerabilidades técnicas que puedan resultar relevantes.	Medio 2	Muy Grave 3	Alto	MG G M B M A						Director/Coordinador de TI - Áreas asignadas	A.1.33.1	Elaborar una escala de tiempo para trabajar con las vulnerabilidades técnicas que se presentan y son relevantes en la unidad.	Acciones inmediatas para disminuir riesgos.
R.1.34.	La unidad no establece, documenta, implanta ni mantiene los requisitos de continuidad de seguridad de la información.	Medio 2	Muy Grave 3	Alto	MG G M B M A						Director/Coordinador de TI - Áreas asignadas	A.1.34.1	Documentar, implantar requisitos para la continuidad de la seguridad de la información.	Mantener segura la información en el tiempo.

- **ÁREA DESARROLLO Y PROGRAMACIÓN**

ID. Riesgo	Vulnerabilidades	Probabilidad	Impacto	Nivel	Matriz de Riesgos						Responsables	ID de Mitigación	Acciones de mitigación	Criterio de aceptación
R.2.1	No se llevan inventarios de los activos de soporte de software.	Alto 3	Grave 2	Alto	VS S M L M H						Director/Coordinador de TI - Áreas asignadas	A.2.1.1	Realizar los inventarios de los activos de soporte de software, equipos tecnológicos dentro de la unidad.	Gestión de activos.

R.2.2.	No se han implantado controles de detección de fallos para identificar la existencia de problemas a su debido tiempo.	Alto 3	Muy Grave 3	Crítico		VS S M			X		Director/Coordinador TI	A.2.2.1	Implementar controles de detección de fallos con herramientas tecnológicas	Desarrollo con metodologías ágiles.
							L	M	H					
R.2.3.	No se identifican las tendencias de uso, en lo particular de las aplicaciones de negocio o las herramientas del sistema de gestión de la información.	Medio 2	Muy Grave 3	Alto		VS S M		X			Director/Coordinador de TI - Áreas asignadas	A.2.3.1	Elaborar políticas y manuales de uso de aplicaciones de negocio o herramientas de gestión de la información.	Uso adecuado de los recursos TI.
							L	M	H					
R.2.4	El software de desarrollo y explotación no se ejecuta en diferentes sistemas o procesadores de ordenador ni en diferentes dominios o directorios.	Alto 3	Menor 1	Medio		VS S M					Director/Coordinador TI	A.2.4.1	Elaborar procesos de prueba de ejecución del software en desarrollo en diferentes plataformas para ver su funcionalidad y escalabilidad.	Software escalable.
							L	M	H					
R.2.5.	No existen parches	Alto	Grave	Alto							Director/Coordinador	A.2.5.1	Comprar parches de	Parches Microsoft,

	disponibles de fuente legítima para tratar algún sistema vulnerable.	3	2			VS S M L	 M	 H	X		de TI - Áreas asignadas		sistemas de fuente legítima para evitar problemas con las aplicaciones en desarrollo.	Unix
R.2.6.	La instalación incontrolada de software en equipos informáticos ha causado fugas de información, pérdidas de integridad u otros incidentes de seguridad de la información o violación de derechos de propiedad intelectual.	Medio 2	Muy Grave 3	Alto		VS S M L	 M	 H			Director/Coordinador de TI - Áreas asignadas	A.2.6.1	Controlar el permiso de los usuarios para instalar software maliciosos que causen incidentes de seguridad de la información.	Control de permisos
R.2.7.	No se separa la prueba y verificación general de la seguridad de la información con el de la prueba de los cambios.	Medio 2	Grave 2	Medio		VS S M L	 X M	 H			Director/Coordinador TI	A.2.7.1	Realizar pruebas por separado de los cambios que se realicen en el software de desarrollo.	Retroalimentación general de los cambios efectuados individualmente.

- **ÁREA DE MANTENIMIENTO Y SOPORTE A USUARIOS**

ID. Riesgo	Vulnerabilidades	Probabilidad	Impacto	Nivel	Matriz de Riesgos	Responsables	ID de Mitigación	Acciones de mitigación	Criterio de aceptación
R. 3.1.	No se utilizan métodos de protección especial para los equipos.	Alto 3	Grave 2	Alto	VS S M L M H	Director/Coordinador de TI - Áreas asignadas	A.3.1.1	Proteger los equipos con métodos de seguridad que trabajan con información sensible.	Políticas de seguridad de los equipos tecnológicos.

- **ÁREA DE OPERACIONES**

ID. Riesgo	Vulnerabilidades	Probabilidad	Impacto	Nivel	Matriz de Riesgos	Responsables	ID de Mitigación	Acciones de mitigación	Criterio de aceptación
R. 4.1.	Las copias de respaldo no están protegidas mediante cifrado, sobre todo en aquellas donde es importante la confidencialidad.	Alto 3	Muy Grave 3	Critico	VS X S M L M H	Director/Coordinador TI	A.4.1.1	Proteger las copias de respaldo con cifrado para mantener la confidencialidad de la información.	Encriptación de información.
R.4.2.	No se ha desarrollado ni aprobado planes documentados y procedimientos de respuesta y recuperación que detallan como la Universidad gestionará un evento disruptivo y mantendrá la seguridad de su información en un	Alto 3	Muy Grave 3	Crítico	VS X S M L M H	Director/Coordinador TI	A.4.2.1	Elaborar las políticas, procedimientos, planes y controles de respuesta y recuperación contra incidentes o desastres naturales para mantener la seguridad de la	Plan de respuesta y recuperación frente a desastres naturales o incidentes informáticos.

	nivel predeterminado.												información.	
R.4.3.	Los controles de seguridad de la información que han sido implantados no continúan operativos durante una situación adversa.	Alto 3	Grave 2	Alto		VS S M			X		Director/Coordinador de TI - Áreas asignadas	A.4.3.1	Implementar un control de seguridad que funcione antes, durante y después de un evento disruptivo.	Disponibilidad y Confidencialidad de la información con controles de seguridad.
							L	M	H					
R.4.4.	No se comprueban los controles establecidos ni los implementados a intervalos regulares para asegurar que son válidos y eficaces durante situaciones adversas.	Medio 2	Grave 2	Medio		VS S M		X			Director/Coordinador TI	A.4.4.1	De los controles de seguridad implementados, realizar pruebas de su aplicabilidad para medir su eficacia frente a una situación adversa.	Indicadores de desempeño de controles de seguridad.
							L	M	H					
R.4.5.	No se han tomado medidas adecuadas de protección de la privacidad en los registros de eventos.	Medio 2	Grave 2	Medio		VS S M		X			Director/Coordinador TI	A.4.5.1	Realizar un plan de medidas referente a los registros de eventos presentados en la unidad.	Medidas de protección para la privacidad de la información.
							L	M	H					
R.4.6.	No se ha definido un procedimiento para considerar la situación donde la vulnerabilidad ha sido identificada pero no es posible adoptar una contramedida.	Medio 2	Muy Grave 3	Alto		VS S M		X			Director/Coordinador de TI - Áreas asignadas	A.4.6.1	Realizar un plan de acción para vulnerabilidades identificadas pero que no es posible adoptar una contramedida en el momento.	Proteger la información.
							L	M	H					

- **ÁREA DE INFRAESTRUCTURA Y REDES**

ID. Riesgo	Vulnerabilidades	Probabilidad	Impacto	Nivel	Matriz de Riesgos	Responsables	ID de Mitigación	Acciones de mitigación	Criterio de aceptación
R. 5.1.	Las instalaciones de la unidad no están configuradas para prevenir que las actividades o la información de tipo confidencial sean visibles o audibles desde el exterior.	Alto 3	Muy Grave 3	Crítico	VS: X S M L M H	Director/Coordinador TI	A.5.1.1	Aumentar la seguridad de las instalaciones a nivel físico para mantener la confidencialidad y que esta no sea visible ni audible para el exterior.	Vidrios polarizados para las separaciones de áreas.
R.5.2.	No se ha aplicado sistemas de protección contra rayos en la unidad.	Alto 3	Muy Grave 3	Crítico	VS: X S M L M H	Director/Coordinador TI	A.5.2.1	Adoptar medidas de protección para temporadas invernales o cambios climáticos en la unidad.	Asegurar el área de TI contra tempestades invernales.
R.5.3.	No se han colocado filtros de protección contra rayos en todas las entradas de corriente eléctrica y en todas las líneas de comunicación.	Alto 3	Grave 2	Alto	VS S: X M L M H	Director/Coordinador de TI - Áreas asignadas	A.5.3.1	Colocar filtros de protección contra rayos en las entradas de corriente eléctrica y en todas las líneas de comunicación.	Instalación eléctrica con filtros de protección contra rayos.
R.5.4	No tienen los recursos adecuados para realizar las copias de respaldo para que toda la información y los	Medio	Muy Grave	Alto	VS: X S	Director/Coordinador de TI - Áreas asignadas	A.5.4.1	La unidad debe contar con todos los recursos necesarios para realizar las copias de respaldo de la	Recursos TI para el tratamiento de la información después de un desastre natural.

	softwares esenciales puedan ser recuperados después de un desastre o fallo de los soportes.	2	3			M							información para que estas puedan ser recuperadas después de un evento disruptivo o desastre natural.	
							L	M	H					
R.5.5.	No se llevan registros precisos y completos de las copias de respaldo, así como de los procedimientos de recuperación documentados.	Alto	Muy Grave	Crítico							Director/Coordinador TI	A.5.5.1	Llevar los registros y procedimientos documentados, completos y precisos de las copias de respaldo para su recuperación después de un evento o desastre natural o incidente informático.	Documentación completa de todos los registros de las copias de respaldo de la información.
						VS			X					
						S								
		3	3			M								
							L	M	H					
R.5.6.	No existen procedimientos para el uso de los servicios de red para restringir el acceso a los mismos o a las aplicaciones.	Medio	Muy Grave	Alto							Director/Coordinador de TI - Áreas asignadas	A.5.6.1	Elaborar procedimientos para el uso de servicios de red que permita solo el acceso autorizado a ellos.	Control de acceso a los 'servicios de la red.
						VS		X						
						S								
		2	3			M								
							L	M	H					
R.5.7.	La unidad no tiene una política de control de red.	Medio	Muy Grave	Alto							Director/Coordinador de TI - Áreas asignadas	A.5.7.1	Elaborar políticas de control de red para la institución.	Proteger la información que se transmite en la red.
						VS		X						
						S								
		2	3			M								
							L	M	H					

R.5.8.	No se ha considerado medidas adicionales para sistemas sensibles o críticos.	Medio	Muy Grave	Alto							Director/Coordinador de TI - Áreas asignadas	A.5.8.1	Elaborar medidas de seguridad para los sistemas sensibles o críticos que tratan la información.	Adoptar medidas que mejoren la seguridad de la red y de las aplicaciones.
						VS		X						
						S								
		2	3			M								
							L	M	H					

Luego de haber obtenido los resultados con la aplicación de la AMFE se realizó la interpretación de los mismos de acuerdo a las áreas existentes.

Del total de vulnerabilidades según los niveles establecidos en el documento AMFE específicamente para la UCCI, se puede observar que el nivel más alto de vulnerabilidad es medio con 42%, seguido de crítico y alto con 29% y con un total de 0 el nivel bajo (Tabla 16).

Tabla 16. Total de vulnerabilidades según niveles AMFE UCCI.

TOTAL DE VULNERABILIDADES SEGÚN NIVELES AMFE UCCI		
NIVEL	**FRECUENCIA ABSOLUTA**	**FRECUENCIA RELATIVA**
CRITICO	10	29%
ALTO	10	29%
MEDIO	14	42%
BAJO	0	0%
TOTAL	34	100%

Elaborado por: Las autoras.

Así mismo el total de vulnerabilidades según los niveles establecidos en el documento AMFE específicamente para el área de Desarrollo y Programación se puede constatar que las vulnerabilidades en el nivel alto corresponden al 57%, seguido de medio con 29%, crítico con 14% y con un total de 0 el nivel bajo. (Tabla 17).

Tabla 17. Total de vulnerabilidades según niveles AMFE desarrollo y programación.

TOTAL DE VULNERABILIDADES SEGÚN NIVELES AMFE DESARROLLO		
NIVEL	**FRECUENCIA ABSOLUTA**	**FRECUENCIA RELATIVA**
CRITICO	1	14%
ALTO	4	57%
MEDIO	2	29%
BAJO	0	0%
TOTAL	7	100%

Elaborado por: Las autoras.

También el total de vulnerabilidades según los niveles establecidos en el documento AMFE específicamente para el área de Mantenimiento y Soporte a Usuarios se puede observar que las vulnerabilidades nivel alto corresponden al 100% y 0% para los otros niveles (Tabla 18).

Tabla 18. Total de vulnerabilidades según niveles AMFE Mantenimiento y soporte a usuarios.

TOTAL DE VULNERABILIDADES SEGÚN NIVELES AMFE MANTENIMIENTO		
NIVEL	**FRECUENCIA ABSOLUTA**	**FRECUENCIA RELATIVA**
CRITICO	0	0%
ALTO	1	100%
MEDIO	0	0%
BAJO	0	0%
TOTAL	1	100%

Elaborado por: Las autoras.

Por otra parte también se detalla el total de vulnerabilidades según los niveles establecidos en el documento AMFE específicamente para el área de Operaciones en donde se puede observar que hay una igualdad en los niveles de vulnerabilidades crítico, alto y medio con un total de 33% por cada nivel y 0% para bajo. (Tabla 19).

Tabla 19. Total de vulnerabilidades según niveles AMFE operaciones.

TOTAL DE VULNERABILIDADES SEGÚN NIVELES AMFE OPERACIONES		
NIVEL	**FRECUENCIA ABSOLUTA**	**FRECUENCIA RELATIVA**
CRITICO	2	33%
ALTO	2	33%
MEDIO	2	33%
BAJO	0	0%
TOTAL	6	100%

Elaborado por: Las autoras.

Finalmente se detalla el total de vulnerabilidades según los niveles establecidos en el documento AMFE específicamente para el área de Infraestructura y Redes, en donde se puedo observar que el nivel alto es el mayor correspondiente al 63%, seguido de crítico con 38% y 0% para medio y bajo respectivamente (Tabla 20).

Tabla 20. Total de vulnerabilidades según niveles AMFE redes.

TOTAL DE VULNERABILIDADES SEGÚN NIVELES AMFE REDES		
NIVEL	**CANTIDAD**	
CRITICO	3	38%
ALTO	5	63%
MEDIO	0	0%
BAJO	0	0%
TOTAL	8	100%

Elaborado por: Las autoras.

12. ANÁLISIS DE IMPACTO DEL NEGOCIO (BIA)

Es importante clarificar que a partir de los riesgos efectuados con anterioridad, se conoció el análisis de impacto del negocio (BIA), cabe indicar que tiene influencia en la continuidad y los servicios que presta la UCCI a lo largo del tiempo, además interviene en los parámetros de carácter prioritarios y de necesidad, de esta manera se concederán las causas de eventualidades o amenazas de incidencias, para la prevención y corrección de los procesos inmersos en la infraestructura tecnológica.

En referencia a lo antes expuesto dichas eventualidades tienden a ser de niveles altos, así mismo se categorizó dichos impactos para la identificación de medidas concretas, tomando en cuenta el peligro que emergen las vulnerabilidades y amenaza en aspectos técnicos, humanos, naturales, gestión, administración, accesibilidad, disponibilidad, seguridad dentro de áreas o escenarios.

12.1. PROCESOS CRÍTICOS PARA LA OPERACIÓN DE UNA ORGANIZACIÓN.

Desde la perspectiva de los procesos y operaciones es fundamental comprender cuáles son los procesos críticos para la continuidad de las operaciones y servicios de la Institución, y cuya falta o ejecución deficiente puede tener un impacto negativo para el organismo y por ende para la ciudadanía.

El impacto de una actividad crítica se encuentra clasificado, dependiendo de la importancia dentro de los procesos TI, tales como:

- **Impacto Alto:** Se considera que una actividad crítica tiene impacto alto sobre las operaciones de la ULEAM, cuando ante una eventualidad en ésta se encuentran imposibilitadas para realizar sus funciones normalmente (ULEAM, 2013).

- **Impacto Medio:** Se considera que una actividad crítica tiene un impacto medio cuando la falla de esta, ocasiona una interrupción en las operaciones de la ULEAM por un tiempo mínimo de tolerancia (ULEAM, 2013).

- **Impacto Bajo:** Se considera que una actividad crítica tiene un impacto bajo, cuando la falla de ésta, no tiene un impacto en la continuidad de las operaciones de la Institución (ULEAM, 2013).

12.2. PRIORIZACIÓN DEL CONJUNTO DE PROCESOS

Para considerar los aspectos de priorización en base a los procesos críticos se tomó como referencia los hitos del Checklist que poseen impacto en niveles vulnerabilidad por áreas, expresadas a continuación (Tabla 21).

Tabla 21. Total de vulnerabilidades según niveles AMFE redes.

PRIORIZACIÓN DE PROCESOS CRÍTICOS MUY SENSIBLES			PRIORIZACIÓN DE PROCESOS CRÍTICOS SENSIBLES			PRIORIZACIÓN DE PROCESOS CRÍTICOS POCO SENSIBLE		
ÁREAS	**HITOS DE VULENRABILIDAD**	**IMPACTO**	**ÁREAS**	**HITOS DE VULENRABILIDAD**	**IMPACTO**	**ÁREAS**	**HITOS DE VULENRABILIDAD**	**IMPACTO**
UCCI	¿Tienen políticas de seguridad de la información aprobadas por la dirección de la ULEAM?	MUY GRAVE	UCCI	¿Se ha realizado auditoría interna a las áreas de la UCCI?	GRAVE	UCCI	De acuerdo con los requisitos de continuidad de seguridad de la información, la unidad establece, documenta, implanta y mantiene:	MENOR
UCCI	¿Estas políticas de seguridad son publicadas y comunicadas a los empleados de TI y partes externas relevantes?	MUY GRAVE	UCCI	¿Existen activos o grupos de activos que no tienen custodios asignados?	GRAVE	UCCI	¿Cuál es el nivel de seguridad de la información que tiene la unidad:	MENOR
UCCI	Dentro de las políticas de seguridad de la información, ¿está incluida la seguridad física de TI y las copia de respaldo de la información?	MUY GRAVE	UCCI	¿Se proporcionan las instrucciones de los requisitos de seguridad del área y los procedimientos de emergencia a los visitantes?	GRAVE	REDES	Se ha considerado medidas adicionales para sistemas sensibles o críticos como:	MENOR

PRIORIZACIÓN DE PROCESOS CRÍTICOS MUY SENSIBLES			PRIORIZACIÓN DE PROCESOS CRÍTICOS SENSIBLES		
ÁREAS	**HITOS DE VULENRABILIDAD**	**IMPACTO**	**ÁREAS**	**HITOS DE VULENRABILIDAD**	**IMPACTO**

UCCI	¿Se revisan las políticas de seguridad de la información con el fin de mejorar la misma y así responder a los cambios del entorno de la universidad y de la UCCI?	MUY GRAVE	UCCI	¿Se proporcionan las instrucciones de los requisitos de seguridad del área y los procedimientos de emergencia a los visitantes?	GRAVE
UCCI	La Dirección toma en cuenta los resultados de las revisiones de las políticas de seguridad?	MUY GRAVE	UCCI	¿Todos los empleados, contratistas y terceros y a todos los visitantes que llegan a la unidad, llevan una identificación visible?	GRAVE
UCCI	¿Tienen un sistema de gestión de Continuidad del Negocio?	MUY GRAVE	UCCI	¿Se notifica al personal de seguridad que se encuentran visitantes sin autorización o alguna persona sin llevar visible la identificación?	GRAVE

PRIORIZACIÓN DE PROCESOS CRÍTICOS MUY SENSIBLES **PRIORIZACIÓN DE PROCESOS CRÍTICOS SENSIBLES**

ÁREAS	HITOS DE VULENRABILIDAD	IMPACTO	ÁREAS	HITOS DE VULENRABILIDAD	IMPACTO
UCCI	¿La UCCI clasifica los activos y los protege debidamente para asegurar su cuidado?	MUY GRAVE	UCCI	¿Las áreas seguras vacías están físicamente cerradas y son comprobadas periódicamente que lo están?	GRAVE

UCCI	¿Se registra la fecha y la hora de entrada y salida de los visitantes o personas externas a la unidad?	MUY GRAVE	UCCI	¿Se permite el ingreso de equipos de fotografía, video, audio u otros equipos de grabación sin autorización?	GRAVE
UCCI	¿Se diseña y aplica seguridad física a las oficinas, despachos y recursos de la unidad?	MUY GRAVE	UCCI	¿Se establecen directrices para comer, beber y fumar en las proximidades de las instalaciones de tratamiento de la información?	GRAVE

PRIORIZACIÓN DE PROCESOS CRÍTICOS MUY SENSIBLES **PRIORIZACIÓN DE PROCESOS CRÍTICOS SENSIBLES**

ÁREAS	HITOS DE VULENRABILIDAD	IMPACTO	ÁREAS	HITOS DE VULENRABILIDAD	IMPACTO
UCCI	¿La unidad cuenta con un diseño aplicable de protección física contra desastres naturales, ataques provocados por el hombre o accidentes?	MUY GRAVE	UCCI	La unidad realiza inspecciones al azar a los usuarios internos y externos para detectar salida de activos no autorizados o entrada de dispositivos de grabación no autorizados, armas, entre otros?	GRAVE
UCCI	¿La unidad tiene un plan de contingencia y de emergencia contra amenazas externas y ambientales?	MUY GRAVE	UCCI	¿Tienen políticas de puesto de trabajo despejado de papeles y pantalla limpia para los recursos de	GRAVE

				tratamiento de la información?	

PRIORIZACIÓN DE PROCESOS CRÍTICOS MUY SENSIBLES			PRIORIZACIÓN DE PROCESOS CRÍTICOS SENSIBLES		
ÁREAS	**HITOS DE VULENRABILIDAD**	**IMPACTO**	**ÁREAS**	**HITOS DE VULENRABILIDAD**	**IMPACTO**
UCCI	¿Se han diseñado e implementados procedimientos para trabajar en las áreas seguras?	MUY GRAVE	UCCI	¿La información de negocio sensible o crítica (documentos, almacenamiento electrónico) es guardada en caja fuerte, armario u otro tipo de mueble de seguridad, cuando no se necesita, especialmente cuando la oficina está vacía?	GRAVE
UCCI	¿Las áreas seguras vacías están físicamente cerradas y son comprobadas periódicamente que lo están?	MUY GRAVE	UCCI	¿Los directivos o responsables utilizan los resultados de los sistemas de control y tendencias de uso para evitar posibles cuellos de botellas o dependencias de personal clave que represente una	GRAVE

				amenaza para el sistema de seguridad o para los servicios y de esta manera planificar las acciones adecuadas?	

PRIORIZACIÓN DE PROCESOS CRÍTICOS MUY SENSIBLES **PRIORIZACIÓN DE PROCESOS CRÍTICOS SENSIBLES**

ÁREAS	HITOS DE VULENRABILIDAD	IMPACTO	ÁREAS	HITOS DE VULENRABILIDAD	IMPACTO
UCCI	El material que entra a la unidad ¿Es inspeccionado para evitar amenazas potenciales como explosivos, productos químicos y otros materiales de riesgo?	MUY GRAVE	UCCI	¿Tiene la unidad un plan de gestión de la demanda de capacidad?	GRAVE
UCCI	¿El material (equipos tecnológicos) que entra a la unidad es registrado de acuerdo a los procedimientos de gestión de activos?	MUY GRAVE	UCCI	¿Tiene un plan documentado de gestión de la capacidad para los sistemas de misión crítica?	GRAVE
UCCI	¿Los interruptores y válvulas de emergencia para cortar el suministro de energía, agua, gas u otro servicio están ubicados fuera de las salidas de emergencia o de las salas de equipos?	MUY GRAVE	UCCI	¿La unidad ha determinado el tiempo de conservación para la información esencial tomando en cuenta cualquier requisito para las copias de archivo que hayan de	GRAVE

				ser conservadas de manera permanente?	

PRIORIZACIÓN DE PROCESOS CRÍTICOS MUY SENSIBLES			PRIORIZACIÓN DE PROCESOS CRÍTICOS SENSIBLES		
ÁREAS	**HITOS DE VULENRABILIDAD**	**IMPACTO**	**ÁREAS**	**HITOS DE VULENRABILIDAD**	**IMPACTO**
UCCI	¿La unidad ha establecido las funciones y responsabilidades asociadas a la gestión de las vulnerabilidades técnicas, incluyendo la supervisión de las mismas, la evaluación de los riesgos de la vulnerabilidad, el parcheo, el seguimiento de activos y cualquier responsabilidad de coordinación necesaria?	MUY GRAVE	UCCI	¿Se ha definido una escala temporal para reaccionar a las notificaciones de vulnerabilidades técnicas que puedan resultar relevantes?	GRAVE
OPERACIONES	¿La unidad tiene un plan de recuperación de desastres?	MUY GRAVE	DESARROLLO	¿Llevan los inventarios de los activos de soporte de software?	GRAVE
OPERACIONES	¿Las copias de respaldo están protegidas mediante cifrado, sobre todo en aquellas donde es importante la confidencialidad?	MUY GRAVE	DESARROLLO	¿Se han implantado controles de detección de fallos para identificar la existencia de problemas a su debido tiempo?	GRAVE

PRIORIZACIÓN DE PROCESOS CRÍTICOS MUY SENSIBLES			PRIORIZACIÓN DE PROCESOS CRÍTICOS SENSIBLES		
ÁREAS	**HITOS DE VULENRABILIDAD**	**IMPACTO**	**ÁREAS**	**HITOS DE VULENRABILIDAD**	**IMPACTO**
OPERACIONES	¿Se ha desarrollado y aprobado planes documentados y procedimientos de respuesta y recuperación que detallan como la Universidad gestionará un evento disruptivo y mantendrá la seguridad de su información en un nivel predeterminado?	MUY GRAVE	DESARROLLO	¿Se identifican las tendencias de uso, en lo particular a las aplicaciones de negocio o a las herramientas del sistema de gestión de la información?	GRAVE
OPERACIONES	¿Los controles de seguridad de la información que han sido implantados continúan operativos durante una situación adversa?	MUY GRAVE	DESARROLLO	¿El software de desarrollo y explotación se ejecuta en diferentes sistemas o procesadores de ordenador y en diferentes dominios o directorios?	GRAVE
MANTENIMIENTO	¿Se comprueban los controles establecidos e implementados a intervalos regulares para asegurar que son válidos y eficaces durante situaciones adversas?	MUY GRAVE	DESARROLLO	¿Existen parches disponibles de fuente legítima para tratar algún sistema vulnerable?	GRAVE

PRIORIZACIÓN DE PROCESOS CRÍTICOS MUY SENSIBLES			PRIORIZACIÓN DE PROCESOS CRÍTICOS SENSIBLES		
ÁREAS	**HITOS DE VULENRABILIDAD**	**IMPACTO**	**ÁREAS**	**HITOS DE VULENRABILIDAD**	**IMPACTO**
MANTENIMIENTO	¿Las instalaciones de la unidad están configuradas para prevenir que las actividades o la información de tipo confidencial sean visibles o audibles desde el exterior?	MUY GRAVE	DESARROLLO	¿La instalación incontrolada de software en equipos informáticos ha causado fugas de información, pérdidas de integridad u otros incidentes de seguridad de la información o violación de derechos de propiedad intelectual?	GRAVE
MANTENIMIENTO	¿Se ha aplicado sistemas de protección contra rayos en la unidad?	MUY GRAVE	DESARROLLO	¿Se separa la prueba y verificación general de la seguridad de la información con el de la prueba de los cambios?	GRAVE

PRIORIZACIÓN DE PROCESOS CRÍTICOS MUY SENSIBLES			PRIORIZACIÓN DE PROCESOS CRÍTICOS SENSIBLES		

ÁREAS	HITOS DE VULENRABILIDAD	IMPACTO	ÁREAS	HITOS DE VULENRABILIDAD	IMPACTO
MANTENIMIENTO	¿Se han colocado filtros de protección contra rayos en todas las entradas de corriente eléctrica y en todas las líneas de comunicación?	MUY GRAVE	MANTENIMIENTO	¿Se utilizan métodos de protección especial para los equipos?	GRAVE
MANTENIMIENTO	¿Tienen los recursos adecuados para realizar las copias de respaldo para que toda la información y los softwares esenciales puedan ser recuperados después de un desastre o fallo de los soportes?	MUY GRAVE	OPERACIONES	Los procedimientos operativos especifican las instrucciones para la ejecución detallada de cada tarea como:	GRAVE
MANTENIMIENTO	¿Se llevan registros precisos y completos de las copias de respaldo, así como de los procedimientos de recuperación documentados?	MUY GRAVE	OPERACIONES	¿Se han tomado medidas adecuadas de protección de la privacidad en los registros de eventos?	GRAVE

PRIORIZACIÓN DE PROCESOS CRÍTICOS MUY SENSIBLES **PRIORIZACIÓN DE PROCESOS CRÍTICOS SENSIBLES**

ÁREAS	HITOS DE VULENRABILIDAD	IMPACTO	ÁREAS	HITOS DE VULENRABILIDAD	IMPACTO

	OPERACIONES	¿Se ha definido un procedimiento para considerar la situación donde la vulnerabilidad ha sido identificada pero no es posible adoptar una contramedida?	GRAVE
	REDES	¿Existen procedimientos para el uso de los servicios de red para restringir el acceso a los mismos o a las aplicaciones, donde sea necesario?	GRAVE
	REDES	¿La unidad tiene una política de control de red?	GRAVE

Elaborado por: Las autoras.

Así mismo se tomaron en cuenta los impactos producidos en ataques informáticos a los sistemas de la ULEAM, de acuerdo a informes donde se detalla la descripción del ataque, la acción de mitigación, el nivel de riesgo en impacto y el área al que pertenecen (Tabla 22).

Tabla 22. Informes de ataques

ÁREA	AFECTACIÓN (VULNERABILIDAD)	ACCIÓN	IMPACTO
UCCI	Aplicación mal intencionada en el servidor, cifrando los archivos del disco completamente.	Elaborar indicadores de prevención y respuestas para tomar medidas de seguridad frente a ataques cibernéticos.	Alto
	Ataque Ransomware.	Actualizar semestralmente los antivirus, firewall contra código malicioso.	Alto
	Ataque Backdoor.	Elaborar indicadores de prevención y respuestas para tomar medidas de seguridad frente a ataques cibernéticos.	Alto
Desarrollo	Ataque Ransomware en un equipo de Windows server.	Actualizar semestralmente los antivirus, firewall contra código malicioso.	Alto
	Servidor con servicios RDP inseguros, que vulnera las contraseñas del administrador, con el fin de poder cifrar la información y pedir rescate por la misma.	Elaborar un protocolo de autoevaluación de control para la efectividad de la seguridad de las aplicaciones.	Alto
Mantenimiento	El sistema de contenido Wordpress no se encuentra actualizado	Actualizar el gestor de contenido a una versión superior	Medio
	Vulnerabilidad SOME en la librería PlubLoad que emplea WordPress para subir ficheros.	Corregir error de librería	Bajo
	Fallo en seguridad XXS, explotable usando URLs manipuladas a través de MediaElment.js, librería usada por los reproductores multimedia.	Elaborar indicadores de prevención y respuestas para tomar medidas de seguridad frente a ataques cibernéticos.	Alto
Redes	Ataque aplicación web institucional	Elaborar indicadores de prevención y respuestas para tomar medidas de seguridad frente a ataques cibernéticos.	Alto

Elaborado por: Las autoras.

12.3. CRITERIO DE EVALUACIÓN DE PROCESOS CRÍTICOS.

Toda vez que se analizaron los puntos anteriores, se llevó a cabo la elaboración de la matriz de los procesos críticos, que se obtuvieron en base a los métodos y procesos del modelo, en el cual califica procesos no crítico, moderados, medianamente alto, alto y crítico, y a su vez se evalúa los indicadores: sin impacto relevante, bajo impacto, impacto medio, impacto alto e impacto crítico respetivamente.

	Matriz de definición de procesos críticos									
	Criterios de evaluación		**Calificación de procesos**							
	1	Sin impacto relevante	**Procesos no crítico**					**Entre 1 y 2**		
	3	Bajo impacto	**Procesos moderados**					**Entre 3 y 4**		
	5	Impacto medio	**Proceso medianamente alto**					**Entre 5 y 6**		
	7	Impacto alto	**Proceso alto**					**Entre 7 – 8**		
	10	Impacto crítico	**Proceso crítico**					**Entre 9 – 10**		
Métodos	**Procesos**	**Criterios de análisis Área**						**Ponderación**	**Calificación**	
		Infraestructura y Redes	**Desarrollo**	**Mantenimiento y soporte a usuarios**	**Operaciones**	**Gestión de Riesgos de TI (INHABILITADO)**				
		21%	18%	17%	21%	22%				
Seguridad de la información en el proceso de Gestión de la Continuidad del Negocio	Considerar los requerimientos de seguridad de la información obligatorios para la Continuidad del Negocio.	10	10	5	10	10		9	Impacto crítico	
	Ejecutar y proteger los activos para la Continuidad del Negocio.	10	7	10	10	10		9	Impacto crítico	

Evaluación del riesgo	Identificar los sucesos que originan dificultades en los métodos en relación con la probabilidad de impacto.	10	10	10	10	10	10	Impacto crítico
	Análisis y evaluación de riegos.	10	10	10	10	10	10	Impacto crítico
Análisis de Impacto	Establecer aspectos críticos	10	10	10	10	10	10	Impacto crítico
	Comprender las actividades de la Continuidad de Negocios.	10	7	7	10	10	9	Impacto crítico
	Correlación entre áreas y usuarios.	10	7	7	10	10	9	Impacto crítico
	Concordancia de los procesos.	10	10	5	10	10	9	Impacto crítico
Estrategias de recuperación	Desarrollar alternativas de estrategias.	10	7	7	10	10	9	Impacto crítico
	Clarificar los requerimientos mínimos para la recuperación.	10	10	7	10	10	9	Impacto crítico
	Establecer capacidad del sitio de recuperación.	7	5	7	7	10	7	Impacto alto
Desarrollo del Plan de Continuidad	Desarrollar el Plan de Continuidad para conservar o restituir las operaciones.	10	7	7	10	10	9	Impacto crítico
	Asegurar la disponibilidad de la información en el nivel requerido y en tiempo establecido requerida después de la interrupción o falta en los procesos de negocios críticos.	7	5	5	7	7	6	Impacto medio
Marco referencial para la planeación de la Continuidad del Negocio	Conservar el marco referencial del plan de Continuidad de Negocio y la certificación del plan que cumpla con los requerimientos de la seguridad de la información.	10	10	10	10	10	10	Impacto crítico
	Prevalecer la calidad de los activos e información de la infraestructura tecnológica de la UCCI.	7	7	7	7	7	7	Impacto alto

Continuando con el análisis de la investigación es importante hacer énfasis en los criterios de análisis por área, dando por resultado los siguiente: Que el área que tuvo mayor impacto fue la de Gestión de Riesgos con 22%; continúa con 21% las áreas de Operaciones y de Infraestructura y Redes que si bien vendrían siendo las áreas con mayor impacto en procesos críticos, tomando en cuenta que las demás áreas como Desarrollo con 18% y Mantenimiento y Soporte a Usuario con 17% no son áreas de influencias críticas en algunos de los procesos (Gráfico 3).

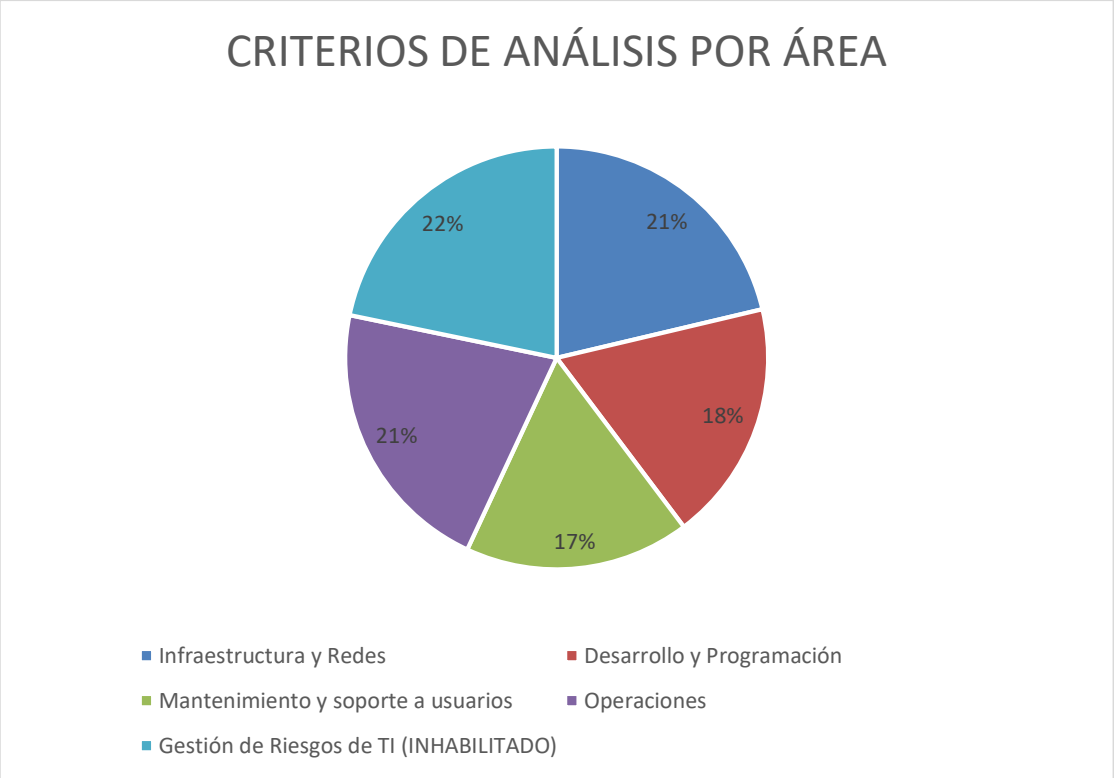


Gráfico 3. Criterio de análisis por áreas de la UCCI.
Elaborado por: Las autoras.

Cabe recalcar que el área de Gestión de Riesgos de TI, vendría siendo el de mayor influencia con un porcentaje del 22% según el análisis de riesgos en cuanto a procesos críticos, y que se lo tomaría en cuenta, pero se cuenta inhabilitado por cuestiones administrativas y de gestión, cumpliendo la funciones el director de la UCCI, pero es un área que debería ser implementada a futuro para llevar el debido control de los riesgos de manera general en la UCCI como estrategia dentro los modelos y planes que emergen o se asocian en esta investigación.

13. MEDIDAS PREVENTIVAS Y CORRECTIVAS

En este apartado se podrá observar las medidas preventivas y correctivas de la Continuidad del Negocio (Tabla 23).

Tabla 23. Medidas preventivas correctivas y acción

RIESGO	MEDIDAS PREVENTIVAS	MEDIDAS CORRECTIVAS	ACCIÓN
Interrupción eléctrica	Fuentes alternas de generación eléctrica	Optar por fuentes alternas de generación eléctrica como Ups y plantas eléctricas.	Elabora un plan que permita proteger los equipos contra interrupciones eléctricas.
	Mantenimiento en la fuente de generación eléctrica.	Realizar mantenimiento en las fuentes alternas de generación eléctrica.	
	Lámparas de emergencias.	Optar Lámparas de emergencias.	
Fallos en hardware	Monitorear equipos.	Realizar monitoreo de los equipos de cómputo y servidores de manera periódica.	Elaborar un diseño aplicable al mantenimiento correctivo y preventivo de los equipos de computación y servidores.
	Espacios limpio, ambiente recomendado.	Mantener los equipos de cómputos y servidores en áreas recomendadas.	
	Mantenimiento.	Realizar mantenimiento correctivo y preventivo en los equipos.	
Fallas en software	Actualizar protocolos	Mantener actualizado protocolos de seguridad.	Elaborar un plan, que indiquen el buen uso de estándares, protocolos de seguridad para obtener aplicaciones seguras.
	Uso de metodologías.	Emplear metodologías / estándares en el desarrollo de aplicaciones.	
Fallas en comunicación	Soporte técnico.	Realizar soporte técnico de los equipos.	Elaborar un diseño aplicable al mantenimiento correctivo y preventivo de los equipos de comunicación.
	Mantenimiento de lo equipo.	Realizar mantenimiento correctivo y preventivo en los equipos de comunicación.	

Desastres naturales	Pólizas seguros.	Contratar aseguradas confiables.	Elaborar un plan de recuperación de desastres.
	Personal informado.	Mantener a personal capacitado.	
	Rutas de evacuación.	Implementar rutas de evacuación.	
	Áreas iluminadas.	Mantener las áreas de emergencias iluminadas.	
Incendios	Usos de sensores.	Implementar sensores contra incendios.	Elaborar un plan de contingencia y de emergencia contra amenazas externas y ambientales.
	Pólizas seguros.	Contratar aseguradas confiables.	
	Sistemas automáticos y manuales.	Implementar sistemas automáticos y manuales (Extintores, gabinetes, aspersores).	
	Material resistente al fuego.	Hacer uso de materiales retar dantes del fuego.	
Fallas en respaldos	Respaldos.	Realizar respaldo periódicamente.	Elaborar las políticas de copia de respaldo de la información.
	Respaldos alternativos.	Realizar respaldo fuera y dentro de la institución servicio en la nube.	
	Actualización de documentación (respaldo y recuperación).	Mantener actualizada la documentación sobre procedimiento de respaldo y recuperación	
Virus	Actualización de Antivirus.	Tener antivirus actualizados con licencias originales.	Actualizar semestralmente los antivirus, firewall contra código malicioso.
	Policías de seguridad.	Establecer políticas de seguridad, para ataques de virus.	

Elaborado por: Las autoras.

14. ESTRATEGIAS DE RECUPERACIÓN

Para la continuidad es importante establecer estrategias de recuperación basadas en el resultado del análisis de impacto y la evaluación de los riesgos, de igual manera cumplir con un cronograma definido, así como mitigar, responder y gestionar los impactos. También se debe estabilizar, continuar, reanudar y recuperar las actividades, instaurando los recursos necesarios para su aplicación, y a la vez instaurar medidas proactivas para reducir la probabilidad de interrupción.

Estos procedimientos abarcan una estructura de respuesta a incidente y los protocolos de comunicación, por lo consiguiente se determinará la forma de continuar o recuperar las actividades dentro un plazo establecido; detallado de la siguiente manera (Figura 6):

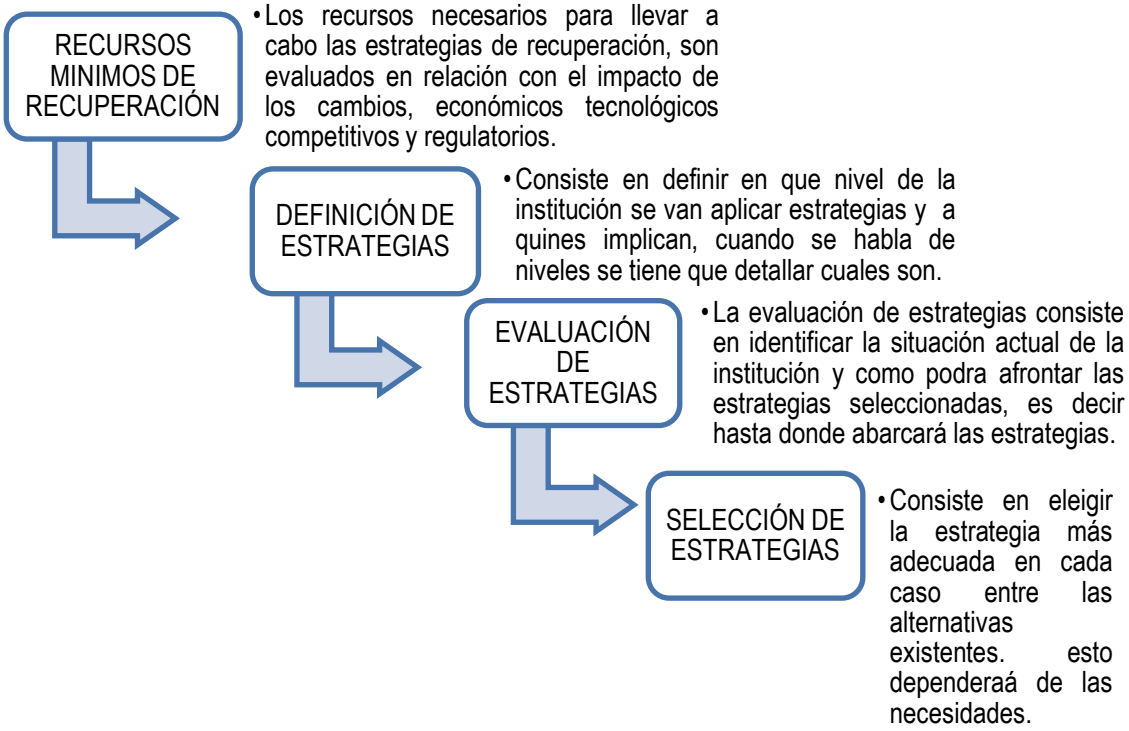


Figura 6. Selección de estrategias.
Elaborado por: Las autoras.

15. PLANIFICACIÓN Y POLÍTICAS PARA LA CONTINUIDAD DE NEGOCIOS DE TI

En este aparatado podemos visualizar como se encuentra detallado el compromiso de la dirección de manera secuencial (Figura 7).

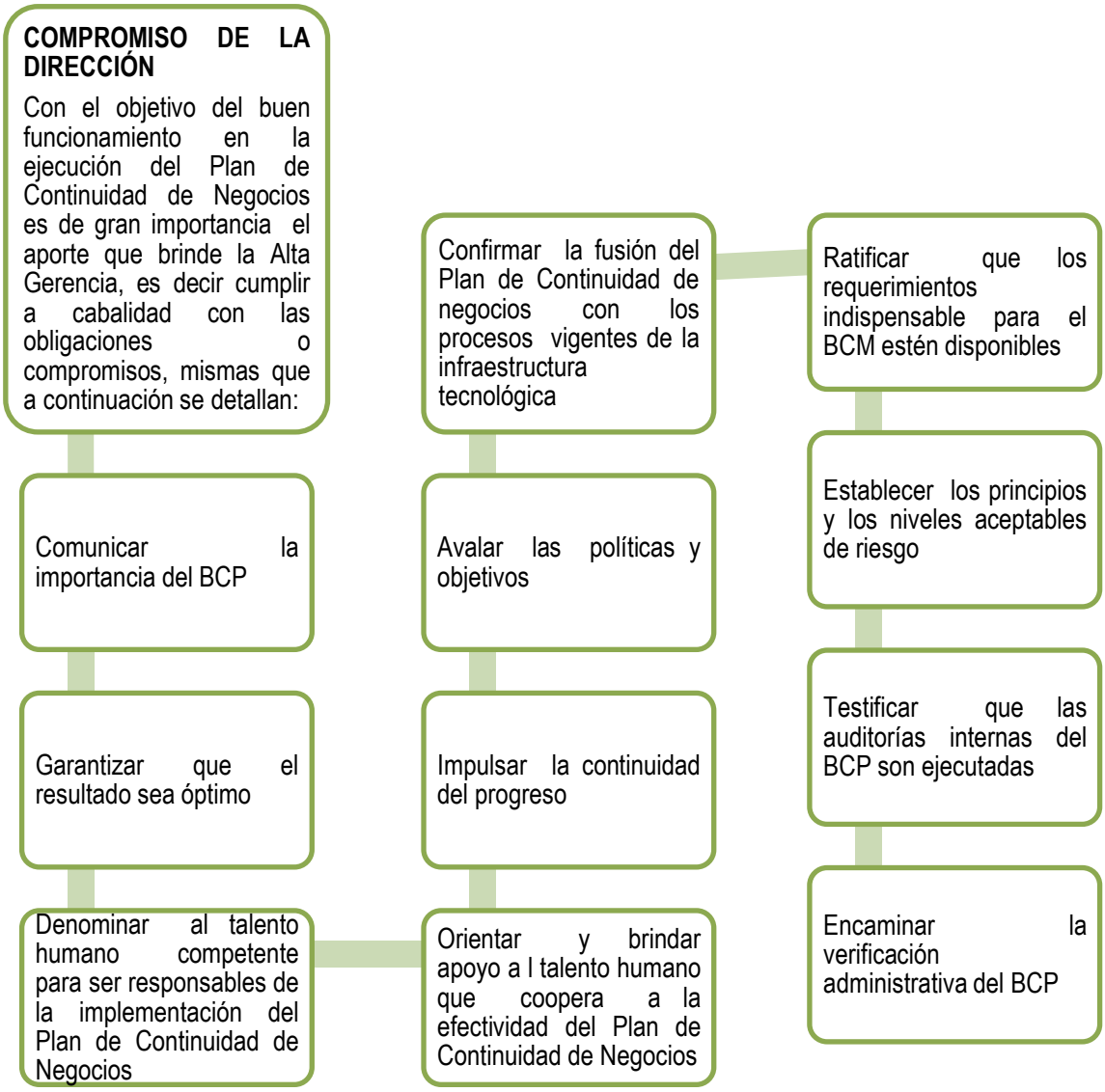


Figura 7. Modelo de compromiso de la dirección.
Elaborado por: Las autoras.

Adicionalmente se observa las funciones y competencias que debe poseer el Talento Humano que coordinará el Plan de Continuidad de Negocios (Figura 8).

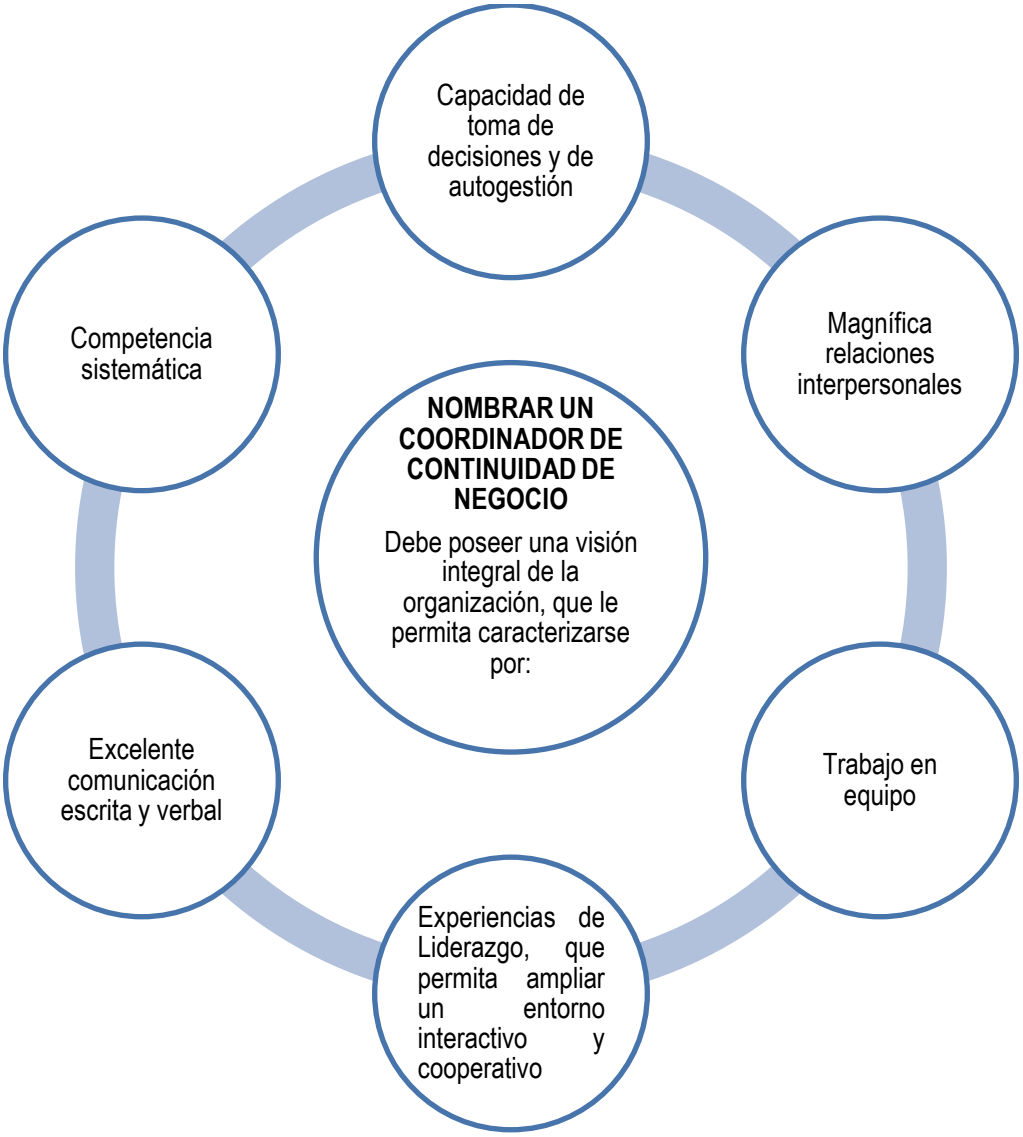


Figura 8. Modelo de planificación de Continuidad de Negocio.
Elaborado por: Las autoras.

Luego del análisis exhaustivo de las investigaciones de varios autores se estableció que el líder de Gestión de Negocios, es la persona encargada de trabajar en equipo con todo el comité para la ejecución BCP; a continuación se detalla el responsable con cada una de sus funciones (Figura 9).

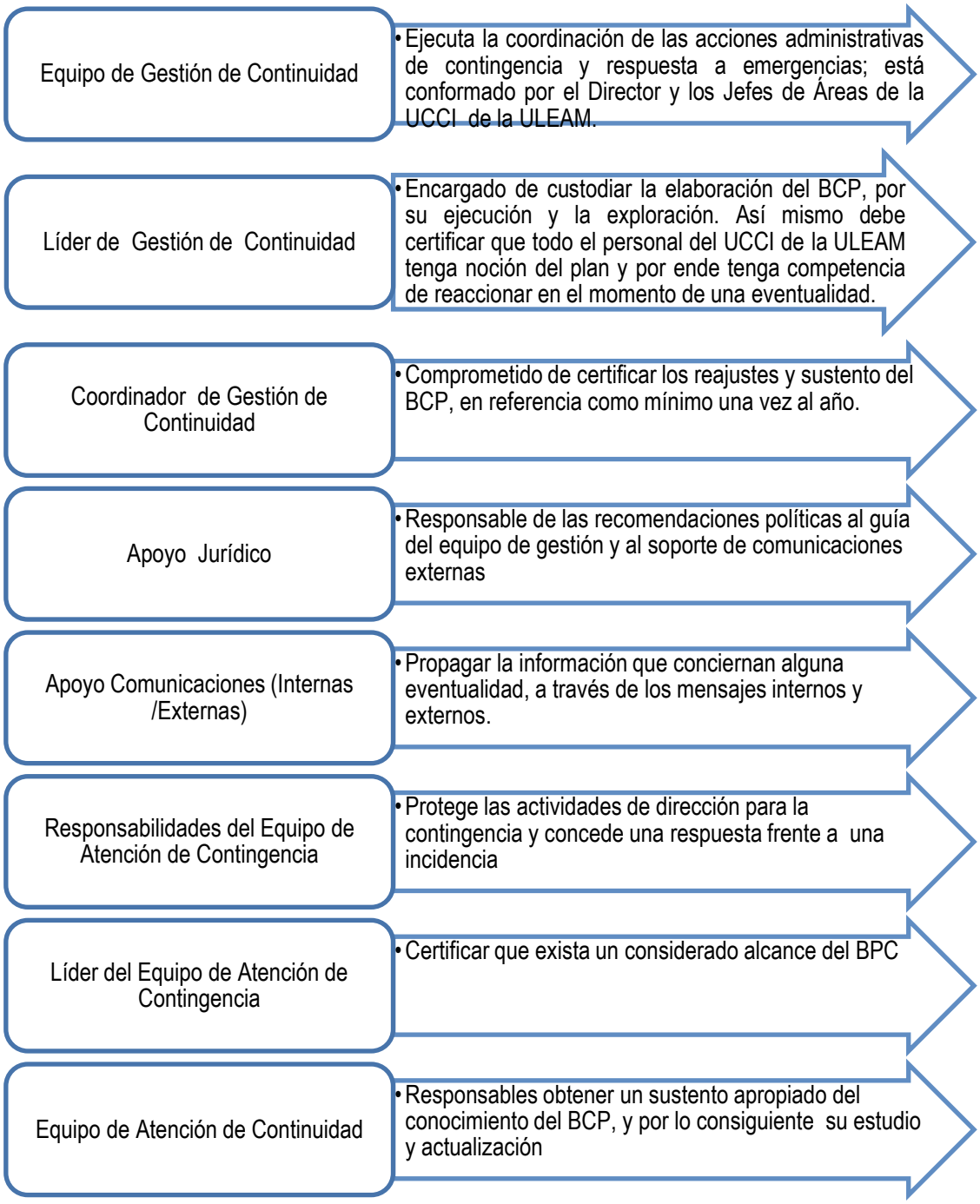


Figura 9. Coordinación o Equipo para la llevar a cabo la planificación del modelo de Continuidad de Negocio.
Elaborado por: Las autoras.

Es importante recalcar que el comité para la ejecución del BCP debe estar apoyado por otras áreas de la institución que involucren la continuidad de todas las actividades como: Capacitación, Coordinador de Logística, Coordinadores Académicos, Coordinador Administrativo, Financiera, entre otras; seguidamente se adjunta el organigrama estructural con los responsables de cada proceso:

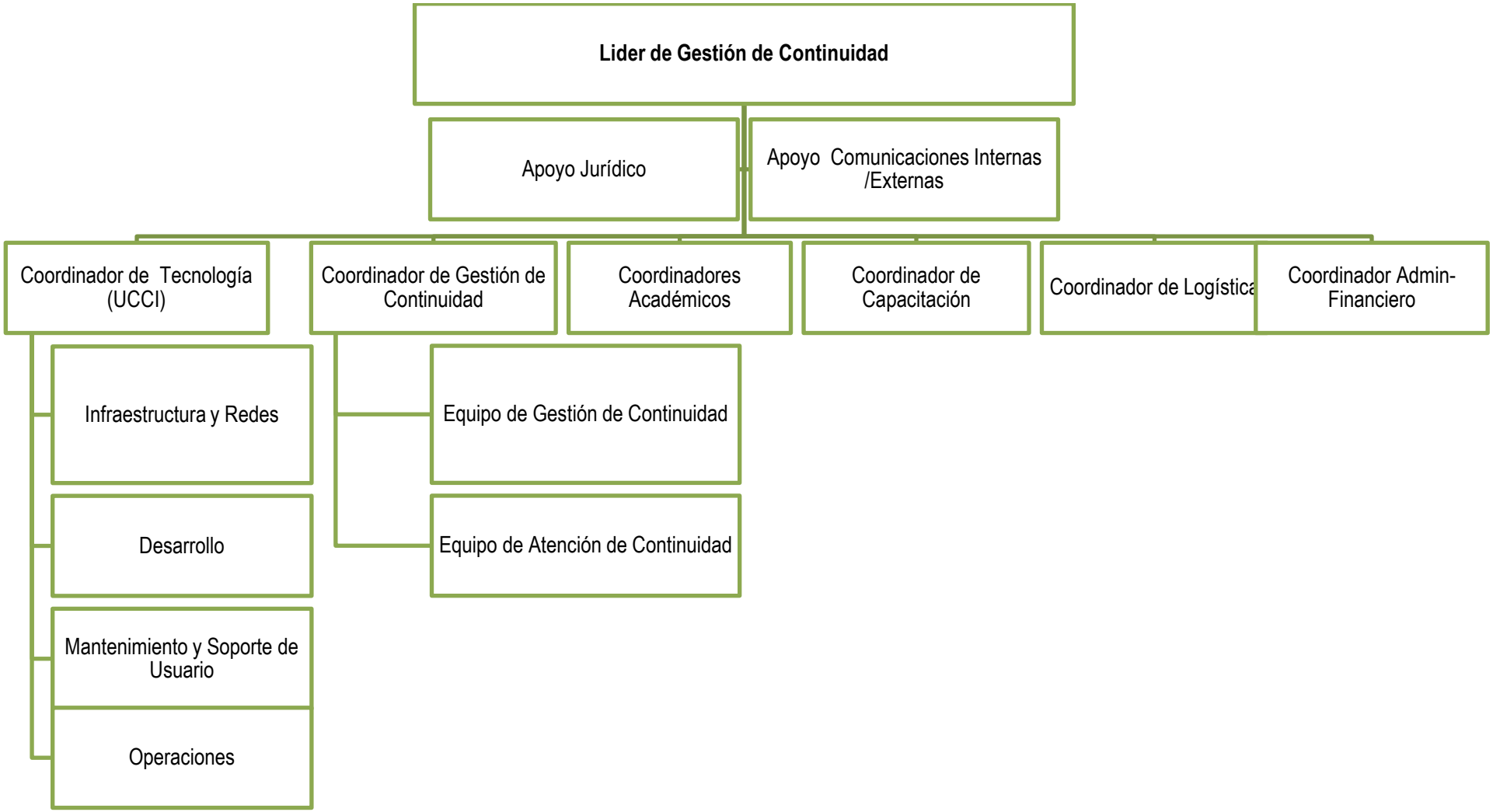


Figura 10. Estructura organizacional del modelo de planificación de Continuidad de Negocio.
Elaborado por:: Las autoras.

15.1. POLÍTICAS DE CONTINUIDAD DE NEGOCIO

- Garantizar que todos los procesos críticos de la Institución operen apropiadamente, de acuerdo a los escenarios de continuidad brindando eficacia y confiabilidad, en la infraestructura Tecnológica de la ULEAM, mediante la implementación de un Plan de Continuidad de Negocio.

- Valorizar la importancia de la aplicación del Plan de Continuidad de Negocio a través de los elementos primordiales implícitos en el BCP, tales son: salvaguarda del talento humano, amparo del entorno, proteger a los activos de la Institución, y la continuidad de las operaciones.

- Crear el Comité de Continuidad, quienes serán ente responsable de la prolongación de procesos Institucionales, mismos que estarán en concordancia con el Director de la UCCI, Jefes de Áreas, y Funcionarios de valoración de Riesgos.

- Establecer acciones primordiales a la asignación del Talento Humano, financieros y materiales para certificar el cumplimiento de las políticas, y el adecuado desenvolvimiento del Plan de Continuidad.

- Capacitar a personal para la gestión de la continuidad de las operaciones, con el propósito de cumplir con la normativa vigente, y por lo consiguiente de los requerimientos de los usuarios internos y externos.

Es indispensable resaltar que para la elaboración de las políticas del Plan de Continuidad de Negocio se tomó como referencia la norma ISO 22301, con la finalidad de afirmar el progreso y contar con un marco normativo que acceda a las mejores prácticas definidas en la norma aplicada a nivel mundial.

16. PROGRAMA DE CAPACITACIÓN DE RESPONSABILIDADES Y FUNCIONES

En este modelo se considera importante que se lleven programas de capacitación a los responsables y de acuerdo a sus funciones, para que se tome concientización con respecto a la Continuidad de Negocio en las diferentes áreas (Figura 11).

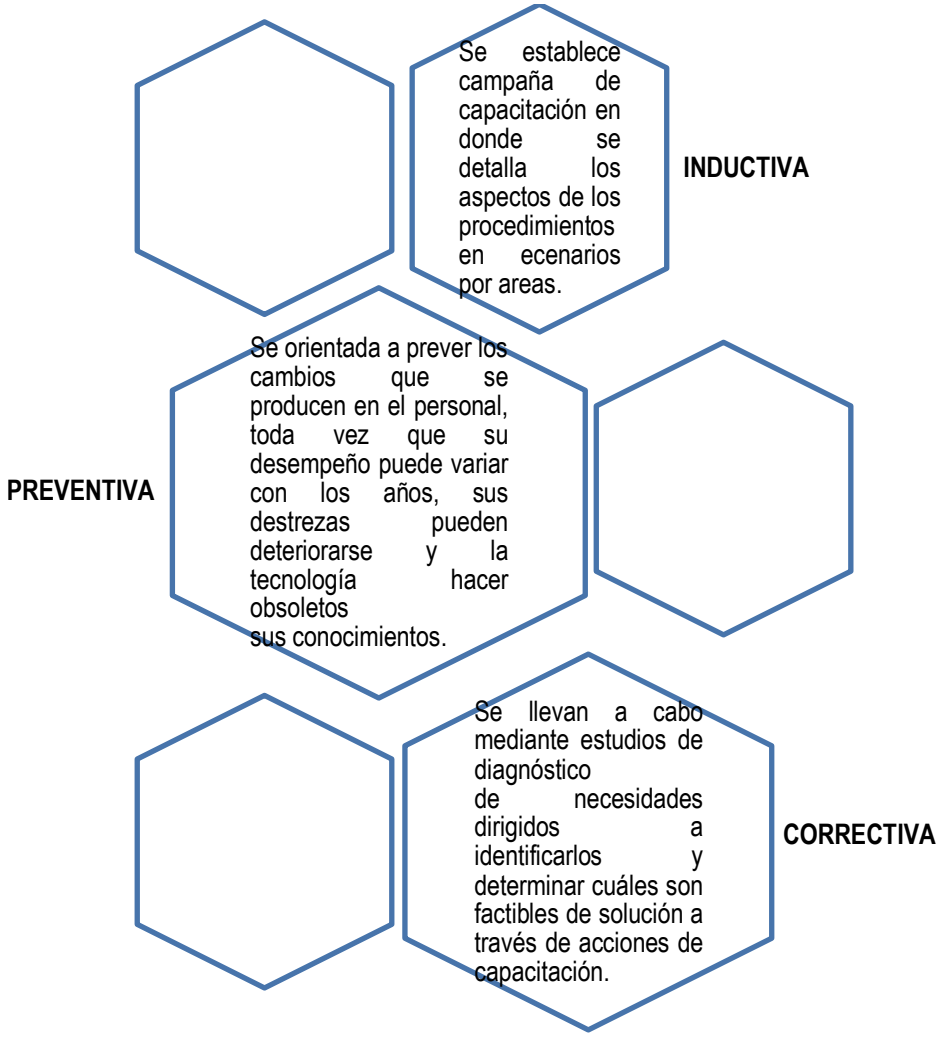


Figura 11. Modalidad de capacitación
Elaborado por: Las autoras

Para llevar a cabo el programa de capacitación de responsabilidades y funciones se tomó como referencia las áreas de trabajo de la ULEAM (2017) y los propósitos establecidos por Reynoso (2013), de las cuales se pueden observar en la siguiente manera (Tabla 24):

Tabla 24. Propósito de responsabilidades y funciones en la UCCI

ÁREAS DE TRABAJO	RESPONSABILIDADES	FUNCIONES / PRODUCCIÓN	PROPÓSITO DE LA CAPACITACIÓN
INFRAESTRUCTURA Y REDES	Son responsables de los componentes claves de la infraestructura: routers, switches, firewalls, segmentación de redes, gestión de desempeño de la red, acceso remoto, etc. Esta área es responsable del control técnico y administrativo de la LAN, WAN y redes inalámbricas, esto incluye asegurar que los enlaces de transmisión de datos estén funcionando correctamente, que las copias de respaldo de los sistemas se estén realizando y que las implementaciones en cuanto a HW y SW de red se lleven a cabo debidamente.	• Supervisar y monitorear los niveles de acuerdos de servicios de prestadores externos de infraestructura y telecomunicaciones. • Asegurar el adecuado desempeño de los servicios de transmisión de datos; VoIP y tráfico en general de la red. • Asesorarlas dependencias académicas y o administrativas en la adquisición y manejo de los sistemas de cómputo y comunicación emitiendo informes técnicos • Probar nuevas tecnologías y proponer su implementación de acuerdo a las necesidades, garantizando la funcionalidad, soporte y facilidad de administración; • Dotar de la infraestructura necesaria para cubrir las necesidades de interoperabilidad, interconexión o transmisión de datos con entes externos. • Mantener y dar soporte permanente al servicio telefónico IP.	• Mejorar la interacción entre el personal y, con ello, a elevar el interés por los procesos que se manejan en la Continuidad del Negocio por áreas. • Satisfacer más fácilmente requerimientos futuros sobre la planificación y ejecución del control de las actividades realizadas por áreas en la UCCI. • Generar conductas positivas y éticas en la toma de decisiones con respecto las acciones preventivas y correctivas de los activos y recursos de la UCCI. • Motivar a que el personal a que brinden ideas proactivas y creativas en los programas de capacitación con el fin de buscar soluciones eficientes y eficaces que tribuyan al modelo. • Mantener un ambiente de cooperación y de sano compartir entre los capacitados que permita la obsolescencia de la fuerza de trabajo.

DESARROLLO	Son responsables de desarrollar y mantener las aplicaciones. El desarrollo puede incluir; desarrollar un nuevo código o cambiar la configuración de las aplicaciones existentes. Los nuevos desarrollos o cambios que se generan en esta área son los que en última instancia correrán en los ambientes de producción.	1. Administración de Software. 2. Administración de las Bases de Datos. 3. Administración del Servidor de Aplicaciones. 4. Instalación de Software. 5. Mantenimiento y Modificación de Programas desarrollados en la Institución de acuerdo a las necesidades y cambios de ley. 6. Análisis de Software para Instalación en la Institución. 7. Asistencia técnica en software y hardware. 8. Obtención de Actualizaciones e Instalación de los Sistemas y aplicaciones que mantiene la Institución. 9. Subir a la página Institucional información proporcionada por las distintas oficinas. 10. Capacitación en software y hardware que la institución posee. 11. Elaboración de Informes. 12. Recepción de despacho de documentación.
MANTENIMIENTO Y SOPORTE A USUARIOS	Son responsables de responder preguntas y resolver problemas técnicos que enfrentan los usuarios e incluyen las siguientes actividades: Apoyar a los usuarios finales con las dificultades de hardware (HW) o software (SW). Capacitar a usuarios para utilizar HW, SW y base de datos. Responder consultas de usuarios finales.	1. Instalación, Configuración y Administración de la Red Informática. 2. Administración y configuración del servidor de internet y correo electrónico. 3. Instalación de programas 4. Mantenimiento y Modificación de Programa de 1.5 por mil de acuerdo a las necesidades y cambios de ley. 5. Formateo de equipos de cómputo. 6. Subir a la página situacional información

	Monitorear desarrollos técnicos e informar a los usuarios finales de desarrollos que podrían ser pertinentes para ellos. Gestión de incidentes. Gestión de revisiones. Gestión de la configuración; y, Gestión de Problemas. Planificar y ejecuta mantenimiento preventivos y correctivos a los equipos de la institución. Emisión de informes técnicos a los equipos de cómputo que estén presentando fallas o se dispongan para la baja. Instalación y configuración de periféricos. (Scanner, video beams e impresoras)	proporcionada la Oficina de Comunicación Institucional. 7. Asistencia técnica en software y hardware. 8. Eliminación de software innecesario e ilegal que impide el buen funcionamiento de los equipos de cómputo. 9. Capacitación en software y hardware que la institución posee. 10. Colaboración con la oficina en trabajos asignados d acuerdo a la necesidad. 11. Instalación de cableado estructurado.
OPERACIONES	Son responsables de: Gestión de continuidad de servicios. Gestión de la capacidad. Gestión de la disponibilidad; y, Gestión de los niveles de servicio. Esta área define y mantiene los sistemas en producción, la estructura de los datos en el sistema de base de datos institucional y es responsable de la seguridad de los datos compartidos y almacenados en la base de	• Asegurar que se asignen recursos adecuados para apoyar las operaciones de los Sistemas de Información. • Planificar para asegurar el uso más eficiente y efectivo de los recursos de TI basados en políticas institucionales. • Asegurar que existan programas detallados de la operación. • Revisar y coordinar la autorización de cambios en los cronogramas de las operaciones. • Revisar y coordinar los

	datos, es responsable también del diseño real, la definición y el mantenimiento adecuado de los datos.	cambios a la red y sistemas de información y aplicaciones en general. • Asegurar que los cambios al HW y SW no ocasionen una interrupción indebida al procesamiento normal. • Monitorear el desempeño del sistema y el uso de recursos para optimizar la utilización de los recursos de los computadores. • Monitorear los acuerdos de nivel de servicio para asegurar una prestación de servicios de TI que satisfagan las necesidades institucionales. • Anticipar el reemplazo de equipos para maximizar el rendimiento de los trabajos en curso y planificar estratégicamente las adquisiciones futuras. • Mantener los reportes de registro de actividades y otros registros de auditoría. • Revisar los logs de todos los sistemas para detectar eventos críticos de sistema y establecer responsabilidad de las operaciones de sistemas de información. • Asegurar que todos los incidentes y problemas se gestionen de manera oportuna. • Asegurar que los procesamientos de los	

		sistemas de información pueden recuperarse de manera oportuna frente a interrupciones menores y mayores. • Ejecutar y monitorear trabajos programados. • Facilitar la creación oportuna de copias y respaldos. • Monitorear el acceso y el uso no autorizado de datos sensibles. • Participar en las pruebas de los planes de recuperación ante desastres. • Monitorear el desempeño, capacidad, disponibilidad y falla de los recursos de información. • Elaborar procedimientos que detallen las instrucciones y cursos de acción para la operación y supervisión de la gestión de sistemas de información.
GESTIÓN DE RIESGOS DE TI (INHABILITADA)	Son responsables de asegurar el cumplimiento de la política de seguridad de la información y que los controles sean los adecuados para prevenir el acceso no autorizado a los activos de información de la institución (datos, programas y equipos), son funciones de esta área: Mantener las reglas de accesos a los datos y otros recursos de TI.	• Documentar y mantener las políticas de seguridad la información y las normas y procedimientos relacionadas a seguridad de la información y uso aceptable de los recursos de TI. • Desarrollar un programa de gestión de riesgos de TI. • Ejecutar procesos de gestión de riesgos de TI. • Mantener las reglas de accesos a los datos y

	Mantener la seguridad y confidencialidad sobre la e misión y mantenimiento de usuarios y contraseñas. Monitorear las violaciones de seguridad y aplicar acciones. Revisar y evaluar periódicamente la política de seguridad y sugerir cambios.	otros recursos de TI. • Mantener la seguridad y confidencialidad sobre la emisión y mantenimiento de usuarios y contraseñas. • Monitorear las violaciones de seguridad y aplicar acciones. • Revisar y evaluar periódicamente la política de seguridad y sugerir cambios.	

Elaborado por: Las autoras

17. CONCLUSIONES Y RECOMENDACIONES

17.1. CONCLUSIONES

- La propuesta del BCP es un instrumento que permite crear controles de prevención y recuperación frente a eventualidades e incidentes, cuyo propósito es reiniciar de manera rápida ante una paralización de procesos en la institución.

- La consecución de la aplicación del BCP depende de la responsabilidad de la Alta Dirección y del soporte de los miembros de Comité encargados de cumplir con las políticas establecidas en el Modelo.

- Las capacitaciones deben ser enmarcadas en temas sobre Sistemas Gestión de Continuidad de Negocio y enfatizar en el BCP con sus respectivas políticas, mismo que conlleva a enriquecer de conocimientos al Talento Humano involucrado, es decir a desarrollar, evaluar y mejorar lo sugerido en el Plan, de esa manera se avala el reajuste y alcance del mismo.

- El análisis y evaluación de los riesgos y amenazas permitirá llevar un control sobre el progreso del Plan y de la responsabilidad en la aplicación de las estrategias de recuperación proyectadas en la institución.

- La observación permanente del BCP contribuirá al desarrollo de mejoras continuas y la convicción de que el Plan se encuentra activo en todo momento.

17.2. RECOMENDACIONES

- La Alta Dirección de la Institución, deberá priorizar la puesta en marcha de la propuesta del BCP con la finalidad de proteger los activos y recursos de información de la Institución.

- En las reuniones periódicas del comité encargado de dar continuidad a la Infraestructura Tecnológica es necesario que se involucre a los entes encargados de las diversas áreas para la correcta toma de decisiones.

- El Líder del BCP debe realizar capacitaciones sobre los temas relevantes a la Continuidad de Negocio, dirigido a todo el talento humano involucrado en el plan y por ende se difunda las políticas del mismo.

- El personal encargado del análisis y evaluación de los riesgos o amenazas deberá revisar permanentemente la situación actual de la Institución para definir a tiempo los controles de prevención.

- Aportes de mejores estratégicas para el Plan de Continuidad de Negocios, que permitirá tomar acciones de salvaguarda y recuperación en caso de nuevas eventualidades, todo esto con el fin de mantener el compromiso de la Institución y tomar protecciones continuas acerca de procesos críticos.

BIBLIOGRAFÍA

Betancourt, E., & Salguero , J. (2014). Propuesta de un Plan de Continuidad del Negocio (BCP) Caso de Aplicación.

Cordero (2015). MAGERIT. Disponible en; http://dspace.uazuay.edu.ec/bitstream/datos/5051/1/11490.pdf

ISO. (2012). Tecnología de la información - Técnicas de seguridad -. Estándar Internacional ISO / IEC 27032, Primera edición 2012-07-15. Revisado y confirmado en 2018.

González, Myer y Pachón. (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. Disponible en: http://www.scielo.org.co/pdf/recig/v15n19/1900-6586-recig-15-19-00269.pdf

Isotools. (2017). Norma ISO 22301. Disponible en: https://www.isotools.org/2017/07/23/iso-22301-gestion-continuidad-negocio-la-practica/

Nieto. (2013). BIA. Dispinible en https://www.icetex.gov.co/dnnpro5/Portals/0/Documentos/La%20Institucion/manuales/Manual_continuidad_negocio.pdf

Rajoy, M. (s.f.). ESTRATEGIA DE CIBERSEGURIDAD NACIONAL. Disponible enL: https://www.ccn-cert.cni.es/publico/dmpublidocuments/EstrategiaNacionalCiberseguridad.pdf

Ramírez. (2017). Eventos. Disponible en: https://intranet2.sbs.gob.pe/intranet/INT_CN/DV_INT_CN/1709/v1.0/Adjuntos/G-191-2017.pdf

Reynoso, H. (2013). Modelo de un plan de capacitación. Disponible en: https://www.eoi.es/blogs/mintecon/2013/05/14/modelo-de-un-plan-de-capacitacion-2/

Romero, M.; Figueroa, G.; Vera, D.; Álava, J.; Parrales, R.; Álava, J.; Murillo, A.; Castillo, M. (2018). VULNERABILIDAD. Disponible en: https://books.google.es/books?hl=es&lr=&id=5Z9yDwAAQBAJ&oi=fnd&pg=PA29&dq=vulnerabilidades+y+riesgos&ots=ylvQxRh7Pu&sig=XbzG-3bBLU1ZixqZJcSh7BIJa54#v=onepage&q=vulnerabilidades%20y%20riesgos&f=false

UOC. (s.f.). Infraestructura tecnológica. Disponible en: https://www.uoc.edu/portal/es/tecnologia_uoc/infraestructures/index.html ULEAM. (2013). PLAN DE CONTINGENCIA DE SERVICIOS DE TI.

ULEAM. (2017). Areas de Trabajo. Disponible en : http://departamentos.uleam.edu.ec/ucci/#

ULEAM. (2018). Plan Estratégico de Tecnologías de Información y Comunicación. Unidad Central de Coordinación Informática "U.C.C.I." Universidad Laica Eloy Alfaro de Manabí.

ULEAM. (2019). Plan de Contingencia de Servicios de TI . Unidad Central de Coordinación Informática "U.C.C.I." Universidad Laica Eloy Alfaro de Manabí.