UNIVERSIDAD TÉCNICA DE AMBATO

CENTRO DE POSGRADOS

PROGRAMA DE MAESTRÍA EN TECNOLOGÍAS DE LA INFORMACIÓN MENCIÓN SEGURIDAD DE REDES Y COMUNICACIONES

COHORTE 2021

Tema: SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA UNIVERSIDAD ESTATAL AMAZÓNICA.

Trabajo de titulación, previo a la obtención del Título de Cuarto Nivel de Magister en Tecnologías de la Información Mención Seguridad de Redes y Comunicaciones

Modalidad del Trabajo de Titulación: Proyecto de Titulación con Componente de Investigación Aplicada.

Autora: Ingeniera Verónica De las Mercedes Villarreal Morales

Director: Ingeniero Oscar Fernando Ibarra Torres Magister

Ambato – Ecuador

2023

A la Unidad Académica de Titulación del Centro de Posgrados

El Tribunal receptor del Trabajo de Titulación, presidido por el Ingeniero Héctor Fernando Gómez Alvarado. PhD, e integrado por los señores: Ingeniero Marcos Raphael Benítez Aldas Master e Ingeniero Leonardo Gabriel Ballesteros López Magister, designados por la Unidad Académica de Titulación del Centro de Posgrados de la Universidad Técnica de Ambato, para receptar el Trabajo de Titulación con el tema: "*IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA UNIVERSIDAD ESTATAL AMAZÓNICA"* elaborado y presentado por la señora Ingeniera Verónica De las Mercedes Villarreal Morales, para optar por el Grado Académico de Magíster en Tecnologías de la Información una vez escuchada la defensa oral del Trabajo de Titulación, el Tribunal aprueba y remite el trabajo para uso y custodia en las bibliotecas de la UTA.

Ing. Héctor Fernando Gómez Alvarado. PhD.
Presidente y Miembro del Tribunal

Ing. Marcos Raphael Benítez Aldas MSc.
Miembro del Tribunal

Ing. Leonardo Gabriel Ballesteros López Mg.
Miembro del Tribunal

AUTORÍA DEL TRABAJO DE TITULACIÓN

La responsabilidad de las opiniones, comentarios y críticas emitidas en el Trabajo de Titulación presentado con el tema: IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA UNIVERSIDAD ESTATAL AMAZÓNICA, le corresponde exclusivamente a: Ingeniera Verónica De las Mercedes Villarreal Morales, Autora bajo la Dirección del Ingeniero Oscar Fernando Ibarra Torres Magister, Director del Trabajo de Titulación, y el patrimonio intelectual a la Universidad Técnica de Ambato.

Ingeniera Verónica De las Mercedes Villarreal Morales
c.c.:1600537698
AUTORA

Ingeniero Oscar Fernando Ibarra Torres Magister
c.c.: 1804003497
DIRECTOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que el Trabajo de Titulación, sirva como un documento disponible para su lectura, consulta y procesos de investigación, según las normas de la Institución.

Cedo los Derechos de mi trabajo, con fines de difusión pública, además apruebo la reproducción de este, dentro de las regulaciones de la Universidad.

Ingeniera Verónica De las Mercedes Villarreal Morales
c.c.:1600537698

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

AGRADECIMIENTO

El proyecto de investigación para la Implementación de Sistema de Gestión de Seguridad de la Información en la Universidad Estatal Amazónica fue preparado originalmente por Verónica Villarreal Morales, con la notable ayuda del Mgs. Oscar Fernando Ibarra Torres,

DEDICATORIA

El presente trabajo está dedicado a Dios ya que en sus manos está cada paso dado. A mi esposo por su apoyo, a mi hija Camilita por ser el motivo para alcanzar cada meta y sueño y a mis padres quienes con su amor, ejemplo y apoyo han inculcado en mí, la perseverancia para alcanzar mis metas.

UNIVERSIDAD TÉCNICA DE AMBATO
CENTRO DE POSGRADOS
MAESTRÍA EN TECNOLOGÍAS DE LA INFORMACIÓN MENCIÓN SEGURIDAD DE REDES Y COMUNICACIONES
COHORTE 2021

TEMA:

IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA UNIVERSIDAD ESTATAL AMAZÓNICA

MODALIDAD DE TITULACIÓN: *Proyecto de Titulación con Componente de Investigación Aplicada.*

AUTOR: *Ingeniera. Verónica De las Mercedes Villarreal Morales*

DIRECTOR: *Ingeniero Oscar Fernando Ibarra Torres Magister*

FECHA: S*iete de diciembre de dos mil veinte y dos*

RESUMEN EJECUTIVO

La Universidad Estatal Amazónica, maneja información académica, de gestión financiera, proyectos de investigación y vinculación, que se generan en el transcurso de cada semestre académico, almacenados en bases de datos y gestionados a través de plataformas informáticas. El no aplicar metodologías de seguridad de la información podría ocasionar pérdida de confianza en los datos, incurriendo en delitos como fraude académico, estados financieros erróneos o manipulados, y/o proyectos vulnerados, esto puede evidenciar la fragilidad de la información institucional.

El mantener niveles aceptables de riesgo en el área de Tecnologías es responsabilidad del Director de Gestión de Tecnologías de la Información y Comunicación, por tal motivo, actualmente la seguridad de la información se la realiza de manera empírica, sin procedimientos, documentación y/o guía en estándares que garanticen la aplicabilidad de

una metodología estructurada de mejora continua para la gestión de la seguridad de la información en la UEA.

Según información recopilada en el trabajo de investigación, para la implementación de un Modelo de Gestión y Gobierno de Tecnologías de la Información en la Universidad Estatal Amazónica, Villarreal (2018), menciona el estado de la seguridad de la información con un nivel de capacidad de 1 sobre 5, lo que evidencia que el área de TI de la UEA no realiza sus procesos cumpliendo con parámetros estandarizados.

Por tal motivo el trabajo de investigación tiene como objetivo la implementación del Sistema de Gestión de la Información, permita garantizar la confidencialidad, integridad y disponibilidad de la información institucional, a través de la aplicación de Estándar ISO 27001 y la metodología Magerit para el análisis de riesgos. Adicional se busca evaluar el impacto que el Sistema de Seguridad de la Información tendrá para mejorar los niveles de capacidad del Gobierno y Gestión de las Tecnologías de la Información implementado en la Universidad Estatal Amazónica. El trabajo de investigación tiene un enfoque cuali-cuantitativo, es cuantitativa porque se utiliza parámetros de medición en la variable independiente; también es cualitativa porque se emite juicios de valor respecto al riesgo y seguridad de la información en miras de mejorar el Gobierno y Gestión de Tecnologías de la Información.

DESCRIPTORES: *GESTIÓN DE SEGURIDAD, TIC, ISO 27000, UNIVERSIDAD, RIESGOS DE TI, COBIT , MAGERIT.*

CAPÍTULO I
EL PROBLEMA DE INVESTIGACIÓN

1.1. Introducción

La dependencia de la tecnología para procesos empresariales u organizacionales ha aumentado de manera acelerada. La movilidad de la comunicación y el acceso a información desde cualquier lugar del planeta ha permitido escalar altos niveles en la transformación digital de las pequeñas, medianas y grandes instituciones públicas y privadas. Sin embargo, la gran importancia que ha adquirido la información digital la ha convertido en vulnerable ante ataques de terceros que buscan un lucro propio y beneficiarse de la vulnerabilidad de los usuarios que usan las plataformas y sistemas, dichos ataques en muchos casos termina en la pérdida de la información de grandes empresas.

Las Instituciones de Educación Superior (IES) no se encuentran ajenas a la transformación digital y a la dependencia de la información, siendo clara la responsabilidad de la custodia de datos y seguimiento académico de miles de profesionales a nivel nacional, además de información financiera, de proceso de compras públicas y todas las inherentes a las IES del Ecuador.

La Universidad Estatal Amazónica cuenta con un aproximado de 5000 usuarios entre estudiantes, docentes y administrativos que generan a diario información de alto valor, razón por la cual se ha generado la motivación de cambio y mejora de sus procesos y seguridad de la información.

Por lo antes indicado surge la necesidad del presente trabajo de investigación, a través del cual se propone la implementación de un Sistema de Gestión de la Seguridad de la Información que permita mitigar riesgos y fortalecer la conservación de la información

sensible de la Universidad Estatal Amazónica a fin de evitar problemas de pérdida de información y mejorar los niveles de seguridad.

El presente trabajo de investigación tiene un enfoque cuali-cuantitativo, es cuantitativo porque se utiliza parámetros de medición en la variable independiente; también es cualitativo porque se emite juicios de valor respecto al riesgo y seguridad de la información en miras de mejorar el Gobierno y Gestión de Tecnologías de la Información en la Universidad Estatal Amazónica.

Como limitantes para el proyecto de investigación se considera al Talento Humano, que debe contar con la predisposición para la aplicación de las políticas, normativas y demás lineamientos que se adopten para la implementación de un Sistema de Gestión de Seguridad de la Información en la Universidad Estatal Amazónica.

El CAPÍTULO I, EL PROBLEMA contiene: el tema de investigación, el planteamiento del problema, su contexto, análisis crítico, prognosis, formulación del problema, interrogantes, delimitación, justificación y objetivos.

El CAPÍTULO II MARCO TEÓRICO contiene: antecedentes de la investigación, fundamentación filosófica, fundamentación legal, categorías fundamentales, hipótesis y señalamiento de variables.

El CAPÍTULO III METODOLOGÍA contiene: el enfoque de investigación, modalidad básica de la investigación, nivel o tipo de investigación, población y muestra, operacionalización de variables, plan de recolección de información y plan de procesamiento de la información.

El CAPÍTULO IV RESULTADOS Y DISCUSIÓN contiene: El análisis del estado de situación inicial del objeto de estudio, factibilidad, resultados obtenidos mediante el proyecto.

El CAPÍTULO V CONCLUSIONES, RECOMENDACIONES, BIBLIOGRAFÍA Y ANEXOS contiene: Conclusiones, recomendaciones, bibliografía y los respectivos Anexos.

1.2. Justificación

En la actualidad los avances en las Tecnologías de la Información y Comunicación (TIC) ha ocasionado que los directivos de las organizaciones y/o empresas otorguen mayor atención a la protección de sus activos de información, con el objetivo de brindar resguardo a los datos sensibles y generar confianza en sus proveedores, clientes y socios. Las amenazas tecnológicas se han vuelto una preocupación para las organizaciones a nivel mundial, debido al alto impacto que las mismas pueden ocasionar. Por ello el Gobierno de la República del Ecuador a través de la Secretaría de la Administración Pública (2013), mediante decreto Nº 166, dispone el Artículo 1.- Disponer a las Entidades de la Administración Pública Central … el uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN –ISO/IEC 2700 para la Gestión de la Seguridad de la Información con la finalidad de implementar controles que puedan ser gestionados a través de un adecuado enfoque de seguridad de la información.

Para administrar sus riesgos las instituciones deben contar con procesos formales de administración integral de riesgos, es por ello que, dentro de los proyectos aplicados a la Universidad Estatal Amazónica (UEA), Villarreal (2018), menciona dos procesos importantes para gestionar la Seguridad de la Información, como son los procesos EDM03: Asegurar la Optimización del Riesgo y DSS05: Gestionar los Servicios de Seguridad, dichos procesos mantienen un nivel de madurez 0.4 y 1 respectivamente, sobre 5 puntos.

Tarazona (2007) menciona que la información debe ser manejada y protegida adecuadamente de los riesgos o amenazas que enfrente. La información valiosa se puede

encontrar en diferentes formas: impresa, almacenada electrónicamente, transmitida por diferentes medios de comunicación o de transporte, divulgada por medios audiovisuales, en el conocimiento de las personas, entre otros.

Ramírez Camargo & Rinconc Pinzon (2022), manifiesta que las instituciones públicas tienen la obligación constitucional de proteger la información que se maneja de los ciudadanos, ya sean funcionarios públicos que contribuyen con el desarrollo del objetivo de la entidad pública o el usuario que llega a depositar sus datos personales en busca de acceso a la justicia o al gobierno en general, dado que existe peligro de difusión o mala utilización de los datos. La información es un activo vital dentro de cualquier institución, la seguridad de la información y la ciberseguridad está definidas por un compuesto de instrucciones y elementos, que tienen como misión brindar las tres características fundamentales de la misma las cuales son: disponibilidad, confidencialidad, integridad

La ausencia de políticas y buenas prácticas en la seguridad de la información puede convertir a dispositivos móviles y/o equipos de escritorios, en medios para la vulneración de información, lo que ocasionen daños irreparables en la información institucional de la UEA.

Es importante mencionar, que la información se encuentra procesada y almacenada en el Centro de Datos de la UEA, el mismo que a la fecha no cuenta con políticas establecidas y documentadas que garanticen la seguridad informática de los equipos.

Luego de la implementación de un Sistema de Gestión de Seguridad de la Información se obtendrá el resultado del análisis de riesgos de los activos de información y si su aplicación incide en mejorar la Seguridad de la Información en la Universidad Estatal Amazónica.

1.3. Objetivos

1.3.1. General

Implementar un sistema de Gestión de Seguridad de la Información en la Universidad Estatal Amazónica que garantice la confidencialidad, integridad y disponibilidad de la información institucional.

1.3.2. Específicos

- Identificar los mecanismos para el análisis de riesgos de los activos de información aplicados en la Universidad Estatal Amazónica.
- Desarrollar políticas, buenas prácticas y niveles de riesgo de los activos de información de responsabilidad de la Dirección de Gestión de las Tecnologías de la Información que garantice la aplicabilidad de la gestión de Seguridad de la Información.
- Evaluar el impacto de la aplicabilidad de un Sistema de Seguridad de la Información dentro del Gobierno y Gestión de las Tecnologías de la Información en la Universidad Estatal Amazónica

CAPITULO II
ANTECEDENTES INVESTIGATIVOS

Luego de efectuar una revisión y análisis bibliográfico, en el repositorio de la Universidad se encontró que existe un trabajo relacionado, pero desde un enfoque diferente al planteado, el cual citamos a continuación:

Según Guevara (2017), en el proyecto de investigación intitulado "Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001 para el departamento de Tecnologías de la Información y Comunicación del Distrito 18D01 de Educación" desarrollado en el año 2017, se detalla la importancia del análisis de riesgos y la aplicabilidad de la Norma Internacional ISO 27001, que permita el mejoramiento de la seguridad de la información en el distrito 18D01 de Educación, en dicha investigación obtiene los siguientes resultados:

- El proyecto de investigación detalla directrices a tomarse en cuenta para una posterior aplicación relevantes de la norma ISO 27001. En el marco del cumplimiento del control "Políticas de Seguridad de la Información" el distrito de Educación no cuenta con un documento específico referentes a políticas de seguridad. Los diferentes procesos que se llevan a cabo no se los realiza en base a lineamientos establecidos, únicamente se aplican ciertas normativas para gestionar la información, pero éstas son hasta cierto punto básicas las cuales no son suficientes para garantizar que la información esté asegurada.
- El demás control tiene un cumplimiento parcial y empírico, entre ellos se destacan los controles que conforman el dominio "Seguridad física y ambiental", el proyecto refleja porcentajes de cumplimiento de los controles referentes a la seguridad física y ambiental, donde la ubicación y protección de los equipos son los tópicos donde el departamento de tecnología hace mayor énfasis en cuanto a su cuidado y aplicación.
- Los controles "Gestión de incidentes y mejoras en seguridad de la información" tienen un porcentaje de cumplimiento del 65%, lo cual da la pauta de la correcta

aplicabilidad de responsabilidades y procedimientos relacionados a la información de la institución.

Al realizar la investigación bibliografía en otras universidades se encuentran varios trabajos relacionados que servirán de apoyo para la presente investigación.

Zapata Chasiguasin (2020), en la investigación "SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LAS NORMAS ISO/IEC 27001, EN EL DEPARTAMENTO DE TECNOLOGIAS DE LA INFORMACION DEL GOBIERNO AUTONOMO DESCENTRALIZADO DE LA MUNICIPALIDAD DE AMBATO", trabajo realizado como tesis de la carrera Ingeniería en Sistemas Computacionales e Informáticos, detalla la importancia de analizar el estado actual de la seguridad con la que se mantiene la información dentro del GAD Municipalidad de Ambato., y se concluye lo siguiente:

- Se diseñó un Sistema de Gestión de la Seguridad de la Información en el que se aplican los estándares establecidos en la norma ISO 27001 de acuerdo a las necesidades institucionales, como consecuencia mejorará la seguridad en cuanto a disponibilidad confidencialidad e integridad de la información en la institución
- El Sistema de Gestión de Seguridad de la Información que se elaboró, servirá como base para una guía completa en la que se detallarán políticas que abarquen la seguridad de los departamentos del GADMA y del departamento de Tecnologías de la Información como tal.

En el proyecto de investigación, Escobar Meléndez (2020), plantea la implementación de un SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN APLICANDO LAS NORMAS ISO/IEC 27001 EN EL DATACENTER DE LA EMPRESA AMBACAR-AMBATO en dicha investigación obtiene los siguientes resultados:

- El resultado muestra que es imperativo el apoyo y compromiso real de la gerencia o administración para el proceso de implementación de un SGSI de acuerdo al

análisis realizado. Además, se debe formalizar los procesos y procedimientos que así lo requieran y documentarlos, ya que en la mayoría de casos se verificó la carencia de procesos de control, por lo cual se debe definir los procedimientos faltantes; también se debe implementar un sistema de control de seguridad informático estableciendo mecanismos que permitan el monitoreo permanente, orientando los protocolos hacia la mejora de la seguridad de la información.

- Como resultado del análisis se encontró que frente a los requerimientos de la norma ISO/IEC 27001, la empresa analizada (AMBACAR) obtuvo una calificación promedio de 2, lo que se interpreta que se encuentra en un nivel de madurez Repetible, es decir, que se han adelantado actividades para la implementación de controles y buenas prácticas, que en su mayoría siguen un patrón regular, pero que no se han formalizado y por tanto sus procedimientos ejecutorios dependen de cada persona.

2.1 Marco teórico

2.1.1 Categorías de la Variable Independiente

- **Activos de Información**

Tarazona (2007) menciona que la información debe ser manejada y protegida adecuadamente de los riesgos o amenazas que enfrente. La información valiosa se puede encontrar en diferentes formas: impresa, almacenada electrónicamente, transmitida por diferentes medios de comunicación o de transporte, divulgada por medios audiovisuales, en el conocimiento de las personas, entre otros.

Con la evolución de los sistemas de información y de la forma de hacer negocios, la información se ha convertido en uno de los activos de mayor valor para las personas y especialmente para las organizaciones. Los sistemas, redes y servicios de información afines, deben ser fiables y seguros, dado que los participantes son cada más dependientes de estos. Sólo un enfoque que tenga en cuenta los intereses de todos los participantes y la naturaleza de los sistemas, redes y servicios afines, puede proporcionar una seguridad efectiva.

Según la ISO (2005), la gestión de activos es la responsabilidad sobre los activos; clasificación de la información, lo que permite la identificación de un inventario de activos que incluye todos aquellos activos de información que tienen algún valor para la organización y que quedan dentro del alcance del SGSI.

- **Análisis de riesgos**

El análisis de riesgos es uno de los trabajos más importantes a la hora de definir proyectos e iniciativas para la mejora de la seguridad de la información. Identificar los riesgos a los que están sometidos los activos de información de una empresa es indispensable para poder gestionarlos de manera óptima.

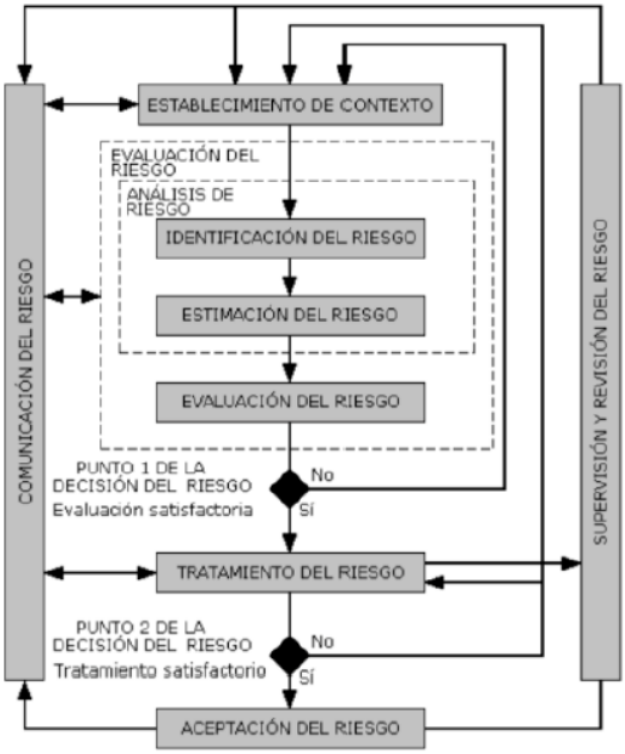
Para el análisis de riesgos la Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración (2012), desarrolla la metodología de Análisis de Riesgos, Magerit, en la cual se define al riesgo como: la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización. El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente.

Los riesgos de TI, y su necesidad de un análisis optimo que permita identificar vulnerabilidades y amenazas, ha permitido que Gobierno Central del ecuador en el 2020, mediante la defina una Guía para la Gestión de Riesgos de Seguridad de la Información, esto evidencia la importancia que significa la información en el Gobierno Central.

La Subsecretaría de Estado Gobierno Electrónico (2020), menciona que el análisis del riesgo consiste en utilizar métodos cuantitativos o cualitativos para obtener una cuantificación de los riesgos identificados, tomando en cuenta los activos, las amenazas y las políticas.

Luego de identificar los riesgos, el marco de trabajo debe considerar una metodología de análisis de riesgo. El análisis de riesgo cualitativo usa una escala de calificación de atributos para describir la magnitud de las consecuencias potenciales (por ejemplo, baja, media y alta) y la probabilidad de esas consecuencias.

Figura 1.- Proceso de gestión del riesgo en la seguridad de la información



Nota. El gráfico representa una visión amplia de la gestión de los Riesgos de las Tecnologías de la Información.

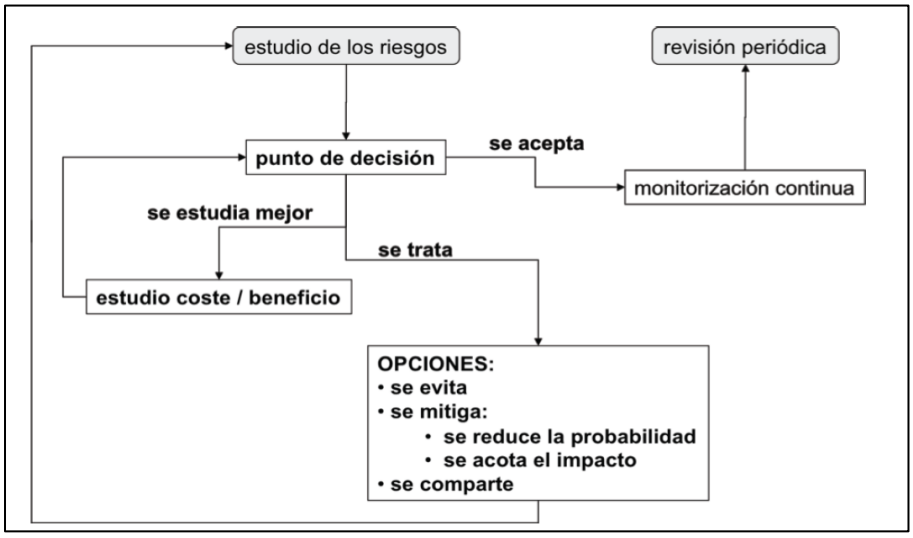
La Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración (2012), enfatiza que el análisis de riesgos determina impactos y riesgos. Los impactos recogen daños absolutos, independientemente de que sea más o menos probable que se dé la circunstancia. En cambio, el riesgo pondera la probabilidad de que ocurra. El impacto refleja el daño posible (lo peor que puede ocurrir), mientras que el

riesgo refleja el daño probable (lo que probablemente ocurra). El resultado del análisis es sólo un análisis. A partir de él se dispone de información para tomar decisiones conociendo lo que se quiere proteger (activos valorados=, de qué se quiere proteger (amenazas valoradas) y qué se ha hecho por protegerlo (salvaguardas valoradas). Todo ello sintetizado en los valores de impacto y riesgo. A partir de aquí, las decisiones son de los órganos de gobierno de la institución que actuarán en 2 pasos:

- Paso 1: evaluación
- Paso 2: tratamiento

La figura 6, resume las posibles decisiones que se pueden tomar tras estudiar los riesgos. La caja 'estudio de los riesgos' pretende combinar el análisis con la evaluación:

Figura 2.- Tratamiento de Riesgo.



Nota. La figura representa el flujo de acciones y las posibles decisiones que se pueden tomar tras estudiar los riesgos y proceder con su tratamiento.

En el marco de trabajo COBIT 5 desarrollado por ISACA (2012), se detalla el proceso catalizador EDM03: Asegurar la Optimización del Riesgo, donde se enfatiza las siguientes buenas prácticas:

EDM03.01 Evaluar la gestión de riesgos: Examinar y evaluar continuamente el efecto del riesgo sobre el uso actual y futuro de las TI en la empresa. Considerar si el apetito de riesgo de la empresa es apropiado y el riesgo sobre el valor de la empresa relacionado con el uso de TI es identificado y gestionado.

EDM03.02 Orientar la gestión de riesgos: Orientar el establecimiento de prácticas de gestión de riesgos para proporcionar una seguridad razonable de que son apropiadas para asegurar que riesgo TI actual no excede el apetito de riesgo del Consejo.

EDM03.03 Supervisar la gestión de riesgos: Supervisar los objetivos y las métricas clave de los procesos de gestión de riesgo y establecer cómo las desviaciones o los problemas serán identificados, seguidos e informados para su resolución.

- **Evaluación de Riesgos**

A continuación de la elaboración de los activos de información, amenazas e impacto es importante determinar y medir los niveles de riesgo de cada activo. Instituto Nacional de Ciberseguridad (2016), menciona que el nivel de riesgo es una estimación de lo que puede ocurrir y se valora, de forma cuantitativa, como el producto del impacto, (consecuencia), asociado a una amenaza (suceso), por la probabilidad de la misma.

El impacto, y por tanto el riesgo, se valoran en términos del coste derivado del valor de los activos afectados considerando, además de los daños producidos en el propio activo:

Impacto x Probabilidad = Riesgo

Si bien es posible, y en ocasiones necesario, realizar un análisis cualitativo, trabajar con magnitudes facilita a las organizaciones establecer el llamado umbral de riesgo, también llamado «apetito al riesgo»: el nivel máximo de riesgo que la empresa está dispuesta a soportar.

La gestión de riesgos debe mantener el nivel de riesgo siempre por debajo del umbral. Por otro lado, se denomina coste de protección al coste que supone para las organizaciones los

recursos y esfuerzos que dedican para mantener el nivel de riesgo por debajo del umbral deseado. Las organizaciones deben vigilar de no emplear más recursos de los necesarios para cumplir ese objetivo.

- **Tratamiento de riesgos**

Para aquellos riesgos cuyo nivel está por encima del valor deseado, es esencial decidir el tratamiento adecuado que permita disminuirlos. Esta decisión siempre ha de pasar un filtro económico donde el coste del tratamiento, o coste de protección, no supere el coste de riesgo disminuido.

El Instituto Nacional de Cyberseguridad (2016), identifica opciones para el tratamiento del riesgo que coincide con los expuestos en la metodología Magerit:

- **Evitar o eliminar el riesgo**: Por ejemplo, sustituyendo el activo por otro que no se vea afectado por la amenaza o eliminando la actividad que lo produce.
- **Reducirlo o mitigarlo:** Tomando las medidas oportunas para que el nivel de riesgo se sitúe por debajo del umbral. Para conseguirlo se puede:
    - Reducir la probabilidad o frecuencia de ocurrencia: tomando, por ejemplo, medidas preventivas
    - Reducir el impacto de la amenaza o acotar el impacto, estableciendo por ejemplo controles y revisando el funcionamiento de las medidas preventivas
- **Transferirlo, compartirlo o asignarlo a terceros**: En ocasiones la empresa no tiene la capacidad de tratamiento y precisa la contratación de un tercero con capacidad para reducir y gestionar el riesgo dejándolo por debajo del umbral.
- **Aceptarlo**: Se asume el riesgo, bien porque está debajo del umbral aceptable de riesgo, bien en situaciones en las que los costes de su tratamiento son elevados y aun siendo riesgos de impacto alto su probabilidad de ocurrencia es baja o porque aun a pesar del riesgo la empresa no quiere dejar de aprovechar la oportunidad que para su negocio supone esa actividad arriesgada.

2.1.2 Categorías de la Variable Dependiente

- **Políticas de seguridad**

Debido a la gran transformación digital que han sufrido las empresas tanto públicas como privadas, es necesario controlar todos los aspectos relacionados con la tecnología, ya que cualquier error o riesgo no considerado y gestionado, puede ocasionar grandes pérdidas.

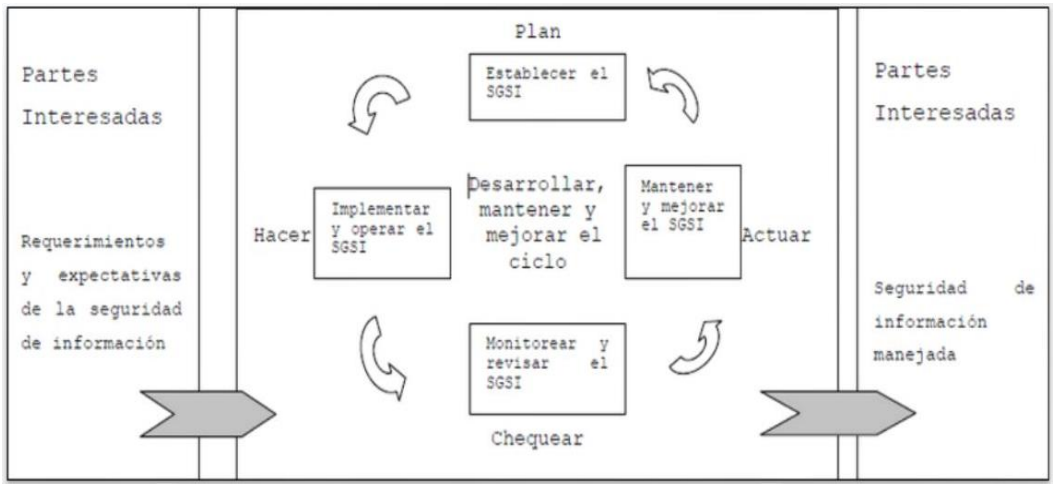
Aunque en teoría el proceso de administración estratégica se caracteriza por una toma de decisiones racional, en la práctica la política organizacional desempeña un rol clave. La política es endémica para las organizaciones. Los diferentes subgrupos (departamentos o divisiones) dentro de una organización tienen sus propias agendas y típicamente, estos conflictos. Por tanto, los departamentos pueden competir entre sí por una mayor participación en los recursos escasos y finitos de la organización. Tales conflictos se pueden resolver mediante la distribución relativa del poder entre las subunidades o bien a través de una evaluación racional de la necesidad relativa. De manera similar, los gerentes individuales con frecuencia participan en discusiones entre sí acerca de las decisiones políticas correctas.

En este contexto la Organización Internacional para la Estandarización ISO (2005), crea la ISO/IEC 27001, un estándar internacional para proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI), dicho estándar es aplicable para el desarrollo de políticas que garanticen la seguridad de la Información.

El diseño e implementación del SGSI de una organización está influenciado por las necesidades y objetivos, requerimientos de seguridad, los procesos empleados y el tamaño y estructura de la organización.

Para la aplicación del estándar ISO (2005), sugiere el modelo PDCA aplicado a los procesos de un Sistema de Gestión de Seguridad de la Información, como lo detalla la Figura

Figura 3.- Modelo PDCA.



Nota. La figura representa el Modelo PDCA, que permite contar con un ciclo la implementación de un SGSI.

- **Métricas de seguridad**

Para evaluar los procesos catalizadores EDM03 y DSS05, se establecen métricas que permitan identificar, puntos conflictivos o críticos al momento de presentar los servicios.

Dichas métricas van en concordancia con los procesos definidos por la técnica de cascada aplicada al presente proyecto de investigación y son seleccionadas de los procesos catalizadores de ISACA (2012) como se detalla a continuación:

Tabla 1.- Métricas de seguridad y optimización de riesgos

	PROCESO	**META DEL PROCESO**	**METRICA**
EDM03	Asegurar la Optimización del Riesgo	Los umbrales de riesgo son definidos y comunicados y los riesgos clave relacionados con la TI son conocidos.	Número de potenciales riesgos TI identificados y gestionados
		La empresa gestiona el riesgo crítico empresarial relacionado con las TI eficaz y eficientemente.	Porcentaje de proyectos de la empresa que consideran el riesgo TI
		Los riesgos empresariales relacionados con las TI no exceden el apetito de riesgo y el impacto del riesgo TI en el valor de la empresa es identificado y gestionado.	*Porcentaje de riesgos TI que exceden el riesgo empresarial tolerado

DSS05	Gestionar los Servicios de Seguridad	La seguridad de las redes y las comunicaciones cumple con las necesidades del negocio.	Número de vulnerabilidades descubiertas Número de rupturas (breaches) de cortafuegos
		La información procesada, almacenada y transmitida en los dispositivos de usuario final está protegida.	Porcentaje de individuos que reciben formación de concienciación relativa al uso de dispositivos de usuario final
		Todos los usuarios están identificados de manera única y tienen derechos de acceso de acuerdo con sus roles en el negocio.	Número de cuentas (con respecto al número de usuarios/empleados autorizados)
		Se han implantado medidas físicas para proteger la información de accesos no autorizados, daños e interferencias mientras es procesada, almacenada o transmitida.	Porcentaje de pruebas periódicas de los dispositivos de seguridad del entorno
		La información electrónica tiene las medidas de seguridad apropiadas mientras está almacenada, transmitida o destruida.	Políticas de seguridad para evitar incidentes relacionados con accesos no autorizados a la información.

Nota. La tabla permite identificar las metas del proceso para Asegurar la Optimización del Riesgo y Gestionar los Servicios de Seguridad, como lo indica el proyecto de Villarreal (2018).

- **Sistema de Gestión de Seguridad de la Información:**

Para la correcta administración de la seguridad de la información, se deben establecer y mantener acciones que busquen cumplir con los tres requerimientos canónicos para la seguridad de la información, que menciona la Organización Internacional para la Estandarización ISO (2005), los cuales son:

Confidencialidad: La propiedad que esa información esté disponible y no sea divulgada a personas, entidades o procesos no autorizados.

Integridad: La propiedad de salvaguardar la exactitud e integridad de los activos.

Disponibilidad: La disponibilidad de estar disponible y utilizable cuando lo requiera una entidad autorizada.

Para los propósitos del estándar 27001, sobre el Sistema de Gestión de Seguridad de la Información, la Organización Internacional para la Estandarización ISO (2005), los procesos utilizados se basan en el modelo PDCA que son los siguientes:

1. Estableces y manejar el SGSI
2. Implementar y operar el SGSI
3. Monitorear y revisar el SGSI
4. Mantener y mejorar el SGSI

Es importante destacar que en el marco de trabajo COBIT 5 desarrollado por ISACA (2012), se detalla el proceso catalizador DSS05 Gestionar Servicios de Seguridad, donde se enfatiza en las siguientes buenas prácticas:

> **DSS05.01 Proteger contra software malicioso (*malware*):** Implementar y mantener efectivas medidas, preventivas, de detección y correctivas (especialmente parches de seguridad actualizados y control de virus) a lo largo de la empresa para proteger los sistemas de información y tecnología del software malicioso (por ejemplo, virus, gusanos, software espía –spyware- y correo basura).
>
> **DSS05.02 Gestionar la seguridad de la red y las conexiones:** Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
>
> **DSS05.03 Gestionar la seguridad de los puestos de usuario final:** Asegurar que los puestos de usuario final (es decir, portátil, equipo sobremesa, servidor y otros dispositivos y software móviles y de red) están asegurados a un nivel que es igual o mayor al definido en los requerimientos de seguridad de la información procesada, almacenada o transmitida.
>
> **DSS05.04 Gestionar la identidad del usuario y el acceso lógico:** Asegurar que todos los usuarios tengan derechos de acceso a la información de acuerdo con los requerimientos de negocio y coordinar con las unidades de negocio que gestionan sus propios derechos de acceso con los procesos de negocio.

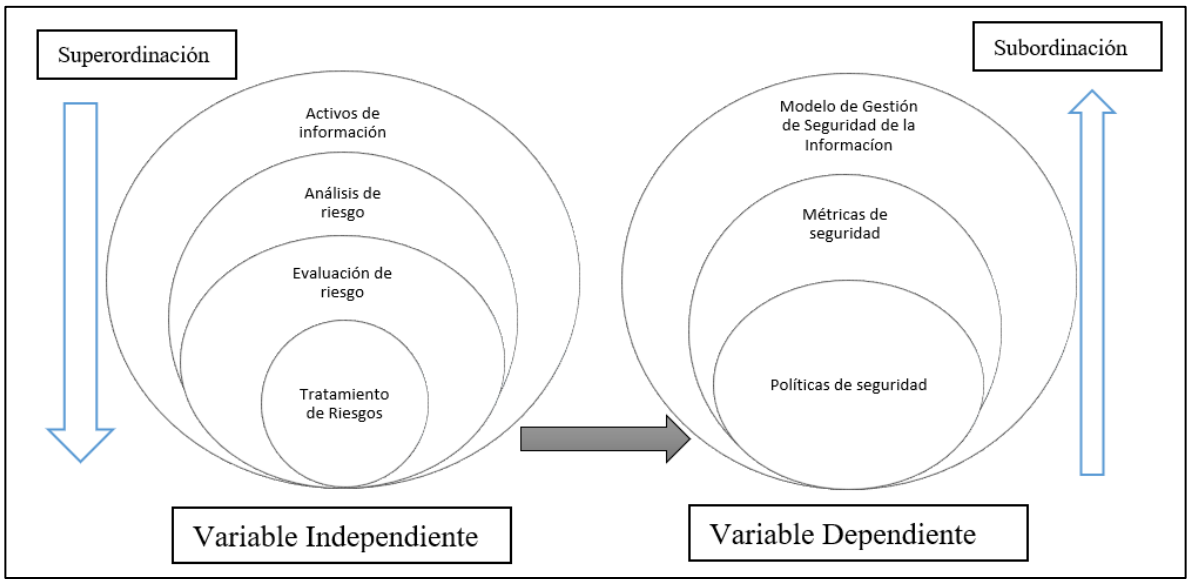
DSS05.05 Gestionar el acceso físico a los activos de TI: Definir e implementar procedimientos para conceder, limitar y revocar acceso a locales, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo emergencias. El acceso a locales, edificios y áreas debe estar justificado, autorizado, registrado y supervisado. Esto aplicará a todas las personas que entren en los locales, incluyendo empleados, empleados temporales, clientes, vendedores, visitantes o cualquier otra tercera parte.

DSS05.06 Gestionar documentos sensibles y dispositivos de salida: Establecer salvaguardas físicas apropiadas, prácticas de contabilidad y gestión del inventario para activos de TI sensibles, tales como formularios especiales, títulos negociables, impresoras de propósito especial o credenciales (*token*) de seguridad.

DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad: Usando herramientas de detección de intrusiones, supervisar la infraestructura para detectar accesos no autorizados y asegurar que cualquier evento esté integrado con la supervisión general de eventos y la gestión de incidentes.

2.2 Categorías Fundamentales

Figura 4.- Categorías fundamentales



Nota. La figura muestra las categorías fundamentales de las variables dependientes e independientes.

CAPITULO III
MARCO METODOLÓGICO

3.1. Ubicación

La Universidad Estatal Amazónica fue creada mediante Ley Nº 2002-85, publicada en el Registro Oficial Nº 686, del 18 octubre de 2002, con domicilio en la ciudad de Puyo, Provincia de Pastaza es una persona jurídica, autónoma de educación superior y de investigación científica, de derecho público, laica, sin fines de lucro, y como tal, garantiza la libertad de pensamiento y expresión y la libertad de cátedra. Con 20 años de vida institucional la UEA, cuenta actualmente con su campus principal, dos sedes académicas en las provincias de Sucumbíos y Zamora Chinchipe respectivamente, y un Centro Experimental de Investigación y Producción Amazónica (CEIPA) ubicado en los límites de las provincias de Pastaza y Napo.

3.2. Equipos y materiales

Institucionales:	Universidad Técnica de Ambato Universidad Estatal Amazónica
Humanos:	Investigador: Verónica de las Mercedes Villarreal Morales Director de Tesis: Mgs. Fernando Ibarra
Materiales:	Tecnológicos: Computador, Impresora. De escritorio: Materiales de oficina.
Bibliográficos:	Libros, revistas, artículos científicos, sitios web oficiales, entre otros.

3.3. Tipo de investigación

El presente trabajo de investigación tiene un enfoque cuali-cuantitativo, es cuantitativa porque se utiliza parámetros de medición en la variable independiente; también es cualitativa porque se emite juicios de valor respecto al riesgo y seguridad de la información en miras de mejorar el Gobierno y Gestión de Tecnologías de la Información, con diseño metodológico Pre - experimental y cuasi - experimental.

Investigación Bibliográfica

La investigación será bibliográfica porque se apoya en libros, documentos técnicos, tesis del área seguridad de la información e informática, revistas, artículos y leyes existentes para la elaboración del marco teórico sobre análisis de datos, así como también del riesgo y seguridad de la información en miras de mejorar el Gobierno y Gestión de Tecnologías de la Información.

Investigación de Campo

Se emplea la investigación de campo ya que se buscará obtener información respecto a los procesos de gestión de la información que se realiza, así como de los requeridos y del riesgo de TI dentro de la institución y con el personal involucrado en el tema.

Investigación Exploratoria

La investigación será de nivel exploratorio porque se acudirá directamente con las personas encargadas del área de Tecnologías de la Información y Comunicaciones, y se revisarán los procesos de gestión de la información.

3.4. Prueba de Hipótesis - pregunta científica – idea a defender

3.4.1 Hipótesis de investigación

Implementar un sistema de Gestión de Seguridad de la Información en la Universidad Estatal Amazónica garantizará la confidencialidad, integridad y disponibilidad de la información institucional.

3.4.2 Hipótesis nula

Implementar un sistema de Gestión de Seguridad de la Información en la Universidad Estatal Amazónica no garantizará la confidencialidad, integridad y disponibilidad de la información institucional.

3.5. Población o muestra:

El presente proyecto trabaja con la población total, que es el grupo de profesionales que laboran en el área de Tecnologías de la Información en la UEA.

Tabla 2.- Población

Población	**Número**
Director de Tecnologías de la Información	1
Analista de Tecnologías de la Información	4
Asistente de Tecnologías de la Información	3
Total	**8**

Nota. La tabla detalla la población que brinda información para el desarrollo del proyecto de investigación.

La población a ser investigada es de 8 personas, al ser una población reducida se trabajará con la totalidad del universo sin que sea necesario el cálculo de muestras representativas.

3.6 Recolección de información:

La recolección de información se realizará por medio de la técnica de encuestas (Anexo 1.1), mediante de aplicación de un cuestionario estructurado y entrevista (Anexo 1.2), instrumentos que permitirán determinar el estado inicial de la seguridad de la información, la problemática y el proceso que realiza la institución con el manejo de la información

Para la implementación del Sistema de Gestión de Seguridad de la Información se utilizará como técnica para la recolección de datos el análisis documental, ya que se basará en las políticas y estándares de las normas ISO.

Posterior a la implementación del Sistema de gestión de Seguridad de la Información por medio de la observación se definirá el cumplimiento del objetivo de mejorar la Seguridad de la Información.

3.7 Procesamiento de la información y análisis estadístico:

Se realizará un trabajo pre-experimental de un solo grupo, pues se aplicará un diseño de preprueba y otro de postprueba, con la utilización del método de la observación para evaluar los resultados.

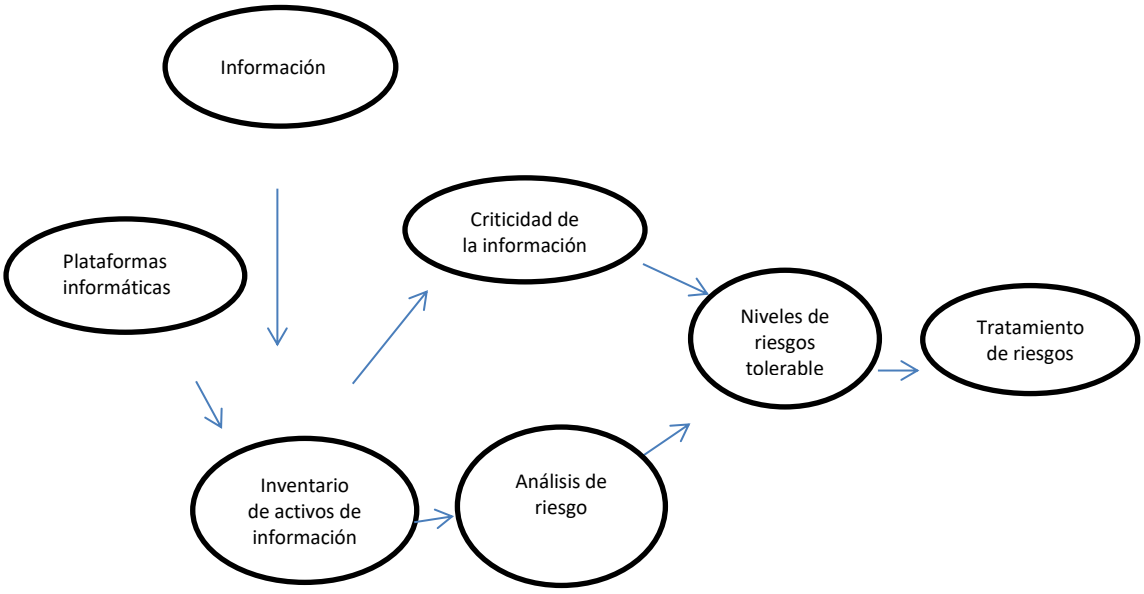
3.8 Variables respuesta o resultados alcanzados

Variable Independiente: Análisis de riesgos de activos de información.

Variable Dependiente: Seguridad de la Información en la Universidad Estatal Amazónica.

Constelación de Ideas, Mándala Variable Independiente u otros

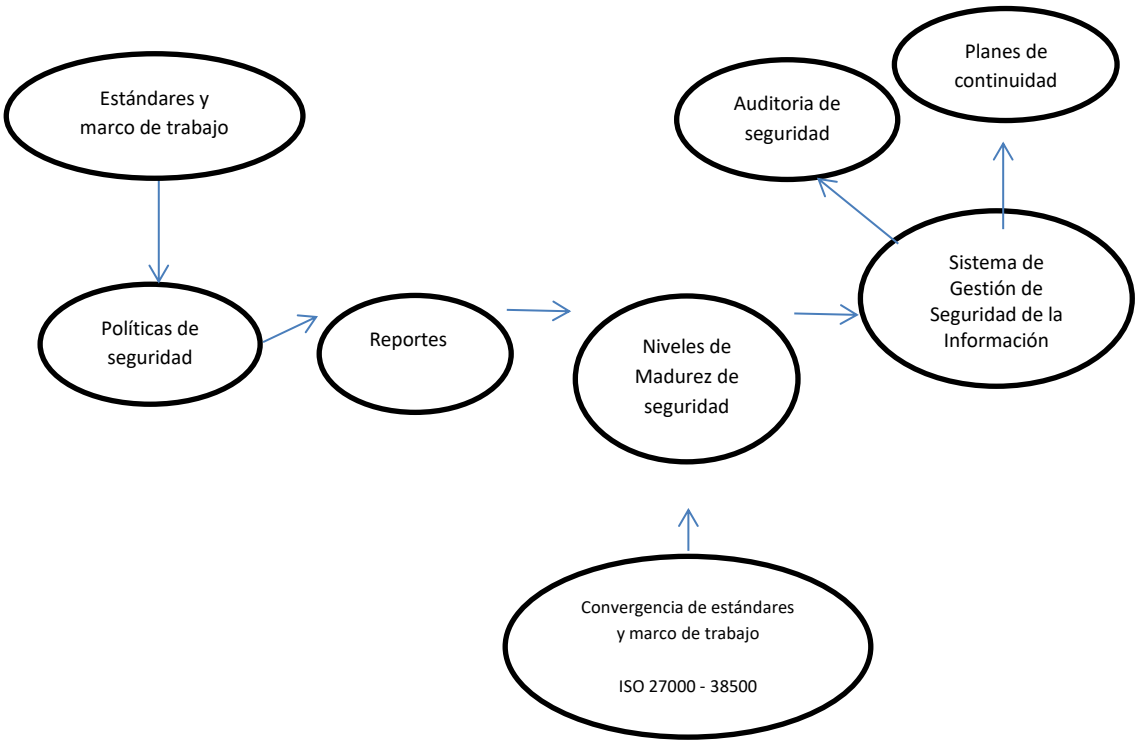
Figura 5.- Constelación de Ideas de la Variable Independiente



Nota. La figura presenta el flujo de información para el análisis de la variable independiente

Constelación de Ideas, Mándala Variable Dependiente u otros

Figura 6.- Constelación de Ideas de la Variable Dependiente



Nota. La figura presenta el flujo de información para el análisis de la variable dependiente

3.8.1 Variable Independiente:

Cuadro No. 1: Análisis de Riesgos

Tabla 3.- Variable Independiente: Análisis de riesgos

Conceptualización o Descripción	Dimensiones	Indicadores	Ítems Básicos	Técnicas e Instrumentos
El análisis de riesgos es uno de los trabajos más importantes a la hora de definir proyectos e iniciativas para la mejora de la seguridad de la información. Identificar los riesgos a los que están sometidos los activos de información de una empresa es indispensable para poder gestionarlos de manera óptima.	- Activos de información - Análisis de riesgos - Evaluación de riesgos - Tratamiento de riesgos.	- Inventario de activos de información - Criticidad de activos de información - Amenazas e impacto de riesgo - Medidas de prevención y manejo del riesgo - Niveles aceptables de riesgo - Desarrollo de medidas de prevención	- Tiene acceso a la información requerida. - La información que dispone es confiable. - Que estándares y metodologías se utiliza - Cómo calificaría el tiempo que emplea procesar los datos. - La información que obtiene es la que necesita. - La información llega a todos los involucrados. -	- Encuesta con Cuestionario - Entrevista con Cuestionario

Nota. La tabla representa un amplio análisis de la variable independiente, en el cual se detalla dimensiones, indicadores y técnicas.

3.8.2 Variable Dependiente:

Cuadro No. 2: Sistema de Gestión de Seguridad de la Información

Tabla 4.- Variable dependiente: Sistema de Gestión de Seguridad de la Información

Conceptualización o Descripción	Dimensiones	Indicadores	Ítems Básicos	Técnicas e Instrumentos
La seguridad de la información es una disciplina asociada tradicionalmente a la Gestión de TIC, cuyo propósito es mantener niveles aceptables de riesgo de la información organizacional y de los dispositivos tecnológicos que permiten su recolección, procesamiento, acceso, intercambio, almacenamiento, transformación y adecuada presentación	- Estándares - Políticas de seguridad - Métricas de seguridad - Modelo de Gestión de Seguridad - Toma de decisiones.	- Controles aplicados a la institución - Políticas aprobadas por Honorable Consejo Universitario - Evaluación de controles aplicados - Plan de mejoras - Decisiones en base a información obtenida	- Controles de seguridad. - La información que obtiene es la que necesita. - La información permite el análisis de datos. - Cuadros de resultados y niveles. - La información llega a todos los involucrados. - La información obtenida sirve de apoyo para la toma de decisiones.	- Encuesta con Cuestionario - Entrevista con Cuestionario

Nota. La tabla representa un amplio análisis de la variable dependiente, en el cual se detalla dimensiones, indicadores y técnicas.

CAPITULO IV
RESULTADOS Y DISCUSIÓN

4.1 ANÁLISIS SITUACIÓN INICIAL

En la actualidad los avances en las Tecnologías de la Información y Comunicación han ocasionado que los directivos de las organizaciones y/o empresas otorguen mayor atención a la protección de sus activos de información, con el objetivo de brindar resguardo a los datos sensibles y generar confianza en sus proveedores, clientes y socios. Las amenazas tecnológicas se han vuelto una preocupación para las organizaciones a nivel mundial, debido al alto impacto que las mismas pueden ocasionar. Por ello el Gobierno de la República del Ecuador a través de la Secretaria de la Administración Pública (2013), mediante decreto Nº 166, dispone el Artículo 1.- Disponer a las Entidades de la Administración Publica Central … el uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN –ISO/IEC 2700 para la Gestión de la Seguridad de la Información con la finalidad de implementar controles que puedan ser gestionados a través de un adecuado enfoque de seguridad de la información.

La seguridad de la información es una disciplina asociada tradicionalmente a la Gestión de TIC, cuyo propósito es mantener niveles aceptables de riesgo de la información organizacional y de los dispositivos tecnológicos que permiten su recolección, procesamiento, acceso, intercambio, almacenamiento, transformación y adecuada presentación. Su convergencia con la implementación de normas para el Gobierno y la Gestión de Tecnologías de la Información, ha permitido empoderar a las TIC en decisiones importantes en las empresas, tomando en cuenta metodologías y estándares como la norma 27000 de ISO/IEC (2014), en la cual se define que es necesario la reserva de la confidencialidad, integridad y disponibilidad de la información.

La implementación de políticas y estándares que garanticen la seguridad y privacidad de la información, adoptadas por las organizaciones en los últimos años, pone de manifiesto la importancia que ha tomado la seguridad de la información. El estándar internacional ISO presenta la familia de las normas 27000, las cuales son una guía para la

implementación de un Sistema de Gestión de Seguridad de la Información, no obstante, las normas establecen el deber ser, y no la forma como se logra, de allí la importancia de establecer metodologías que permitan orientar a las organizaciones en la forma como se debe abordar este tipo de procesos, con el respaldo de las normas internacionales promulgadas para tal fin.

Para administrar sus riesgos las instituciones deben contar con procesos formales de administración integral de riesgos, es por ello que, dentro de los procesos aplicados a la Universidad Estatal Amazónica (UEA), Villarreal (2018), menciona dos procesos importantes para gestionar la Seguridad de la Información, los cuales se detallan a continuación:

Tabla 5.- Proceso relacionados a la Seguridad de la Información

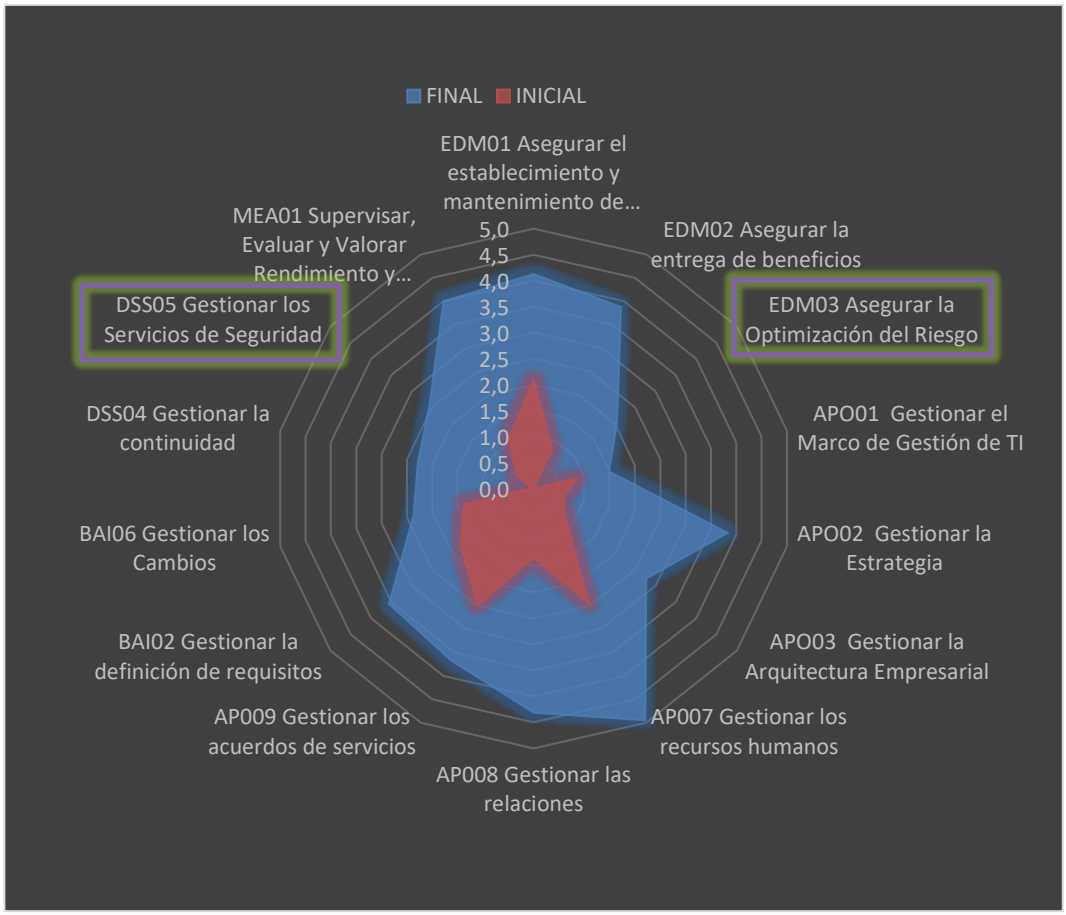
PROCESO	**PRACTICA**
EDM03.- Asegurar la Optimización del Riesgo	**EDM03.01** Evaluar la gestión de riesgos. **EDM03.02** Orientar la gestión de riesgos. **EDM03.03** Supervisar la gestión de riesgos.
DSS05.- Gestionar los Servicios de Seguridad	**DSS05.01** Proteger contra *software* malicioso (malware). **DSS05.02** Gestionar la seguridad de la red y las conexiones. **DSS05.03** Gestionar la seguridad de los puestos de usuario final. **DSS05.04** Gestionar la identidad del usuario y el acceso lógico. **DSS05.05** Gestionar el acceso físico a los activos de TI. **DSS05.06** Gestionar documentos sensibles y dispositivos de salida. **DSS05.07** Supervisar la infraestructura para detectar eventos relacionados con la seguridad.

Nota. La tabla detalla las practicas recomendadas por el Marco de trabajo COBIT para el cumplimiento de los procesos catalizadores EDM03 y DSS05.

En el trabajo de investigación realizado por Villarreal (2018), se menciona que los procesos EDM03 y DSS05 detallados en la tabla, evidencia un nivel de madurez final de

2,1 y 2,6 respectivamente, evidenciando que son procesos gestionados, pero que pueden tener desviaciones no controladas por el personal de TI de la UEA, los niveles obtenidos para cada proceso se pueden apreciar en la figura 1:

Figura 7.- Nivel de madurez de Gobierno y Gestión de TI en la UEA



Nota. La figura presenta de manera detallada el estado de madurez del Gobierno y Gestión de TI en la Universidad Estatal Amazónica, como lo indica Villarreal (2018), en la figura se puntualiza los procesos EDM03 y DSS05, proceso objeto de la presente investigación.

De los datos obtenidos se puede evidenciar la necesidad de fortalecer procesos que permitan asegurar la confidencialidad, integridad y disponibilidad de la información.

4.2 Análisis de los Resultados

Para el análisis e interpretación de resultados se consideran el momento respecto al proceso de investigación sobre la seguridad de la información:

- Encuestas a personal de TI.– Para analizar desde la visión del usuario su percepción, conocimiento y comprometimiento respecto a la seguridad de la información a la que accede. Complementario al proceso de investigación.

4.3 Interpretación de datos

Después de la aplicación de la encuesta, se realiza el análisis de los datos recopilados, emitiendo los siguientes resultados con los cuales se puede identificar el estado actual de la Gestión de Seguridad de la Información en la Universidad Estatal Amazónica:

1. **¿La UEA cuenta con un inventario actualizado de hardware y software de la institución?**

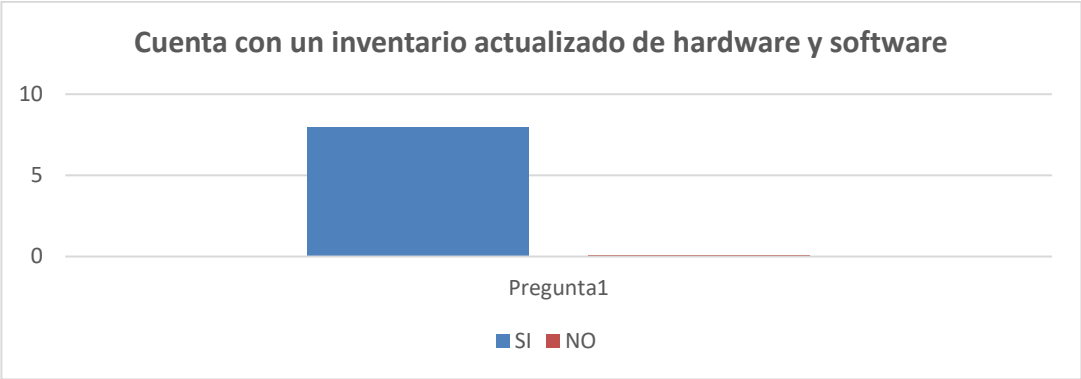
Tabulación:

Tabla 6.- Tabulación pregunta 1

DETALLE	VALORES
SI	8
NO	0
TOTAL	**8**

Gráfico:

Figura 8: Gráfico pregunta 1.



Análisis:

La totalidad de encuestados coinciden que la Universidad Estatal Amazónica cuenta con un inventario de hardware y software, lo que permite identificar que se cuenta con detalles de los bienes tangibles e intangibles que posee la institución para la administración de las Tecnologías de la Información y disponibilidad de los servicios administrados por el personal de TI.

2. **¿La UEA mantienen un inventario actualizado de los activos de información de la institución?**

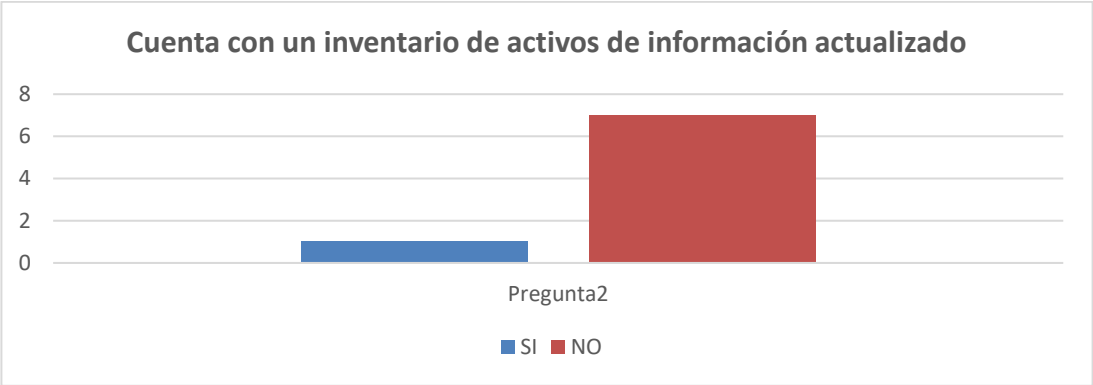
Tabulación:

Tabla 7: Tabulación pregunta 2

DETALLE	VALORES
SI	1
NO	7
TOTAL	8

Gráfico:

Figura 9: Gráfico pregunta 2



Análisis:

Un alto porcentaje de encuestados coinciden que la Universidad Estatal Amazónica, al momento no cuenta con un inventario de activos de información actualizado, lo que nos permite identificar que la institución de educación superior no ha considerado un manejo adecuado de los activos de información, lo que corrobora que la Dirección de Gestión de las Tecnologías de la Información y Comunicación, no administra de manera adecuada y estandarizada los activos de información a su cargo.

3. **¿Con relación al acceso a la información, que permisos son retirados después de la culminación del contrato con el empleado? Puede seleccionar varias opciones**
    a. **Acceso a Correo electrónico**
    b. **Acceso a Sistemas y Plataformas**
    c. **Acceso a documentación digital**
    d. **Acceso a documentación física**
    e. **Acceso a cuenta institucional**

Tabulación:

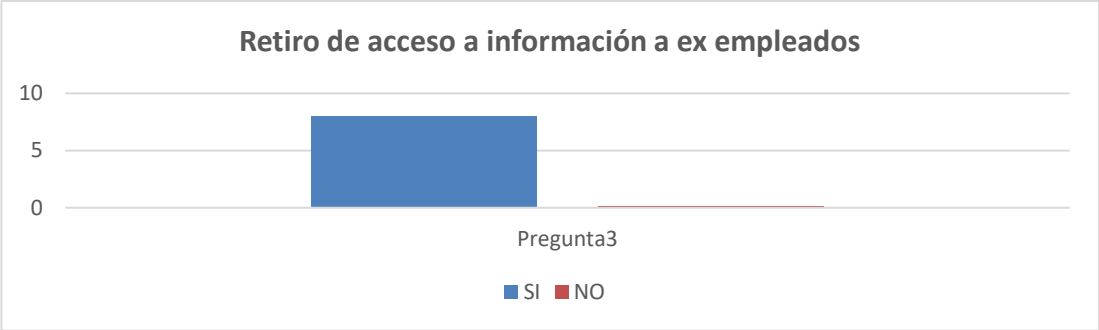
Tabla 8.- Tabulación pregunta 3

DETALLE	VALORES
Acceso a Correo electrónico	8
Acceso a Sistemas y Plataformas	8
Acceso a documentación digital	8

Acceso a documentación física	8
Acceso a cuenta institucional	8

Gráfico:

Figura 10: Gráfico pregunta 3



Análisis:

Como medida de seguridad de la información aplicada de forma empírica, los encuestados indican que la Universidad Estatal Amazónica, maneja una política de seguridad relacionada a la desactivación de cuentas institucionales, la misma que inhabilita el acceso a los recursos tecnológicos e información alojada en los mismos, a los empleados que han terminado su relación laboral con la institución de educación superior, esta restricción incluye también la negación de acceso a información física.

4. ¿El área de servidores está protegida por controles apropiados de entrada para asegurar que sólo el personal autorizado tenga acceso?

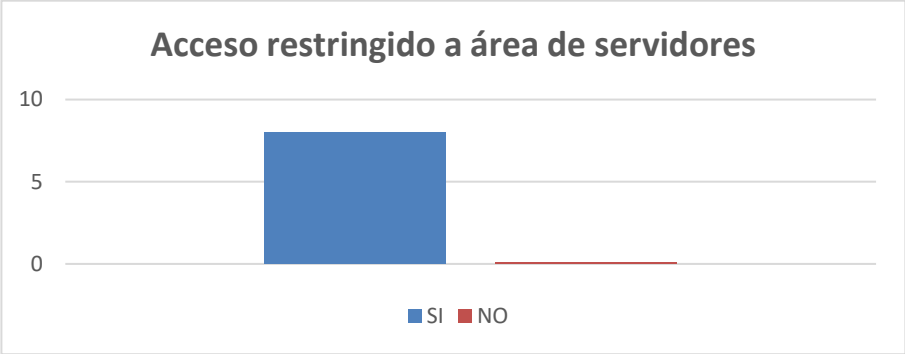
Tabulación:

Tabla 9.- Tabulación pregunta 4

DETALLE	**VALORES**
SI	8
NO	0
TOTAL	8

Gráfico:

Figura 11: Gráfico pregunta 4



Análisis:

La totalidad de encuestados indica que la Universidad Estatal Amazónica, cuenta con un Centro de Datos, que restringe el acceso a los equipos servidores a personal no autorizado, asegurando que solo el personal autorizado tenga acceso a dichos espacios físicos y equipos tecnológicos, tomando en cuenta la importancia de los datos que se encuentran alojados en dichas unidades de almacenamiento.

5. ¿Disponen de políticas para la seguridad de la Información, socializada con todos los actores involucrados de la comunidad universitaria?

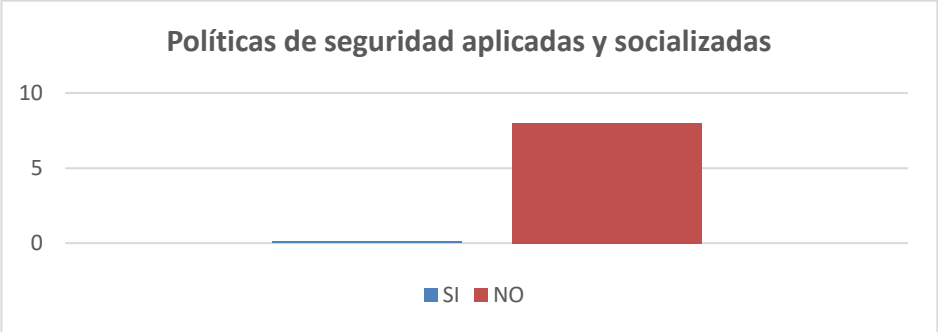
Tabulación:

Tabla 10.- Tabulación pregunta 5

DETALLE	VALORES
SI	0
NO	8
TOTAL	8

Gráfico:

Figura 12: Gráfico pregunta 5



Análisis:

El 100% de los encuestados concuerda que la Universidad Estatal Amazónica, al momento no cuenta con políticas de Seguridad de la Información, que le permita gestionar de manera segura sus activos de información, por tal motivo al no contar con políticas, es ausente también la socialización a la comunidad universitaria acerca de buenas prácticas alineadas a estándares que concienticen los riesgos de los activos de información y la forma como mitigar estos riesgos dentro del campus universitario esencialmente en el área de Tecnologías de Información.

6. ¿Conoce de manera clara y detallada los riesgos y niveles de criticidad de los activos de información relacionados a las tecnologías de la información?

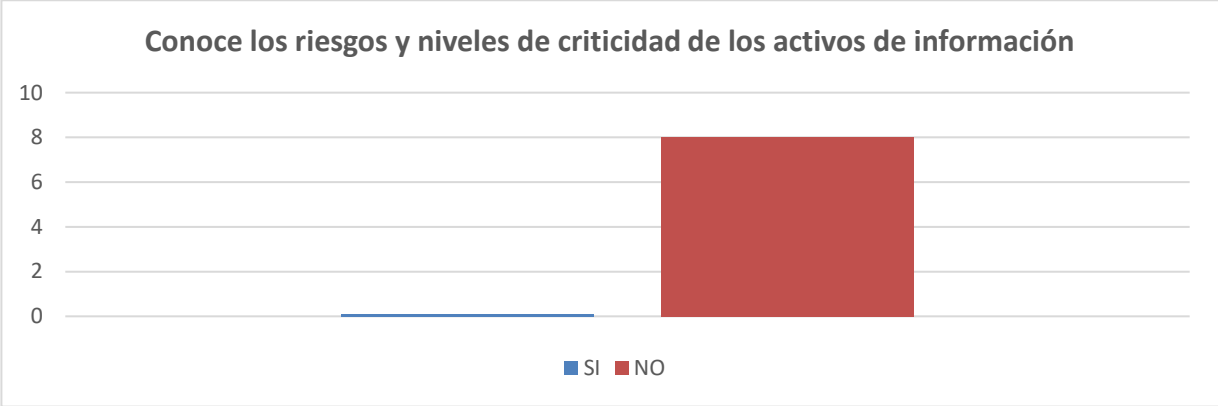
Tabulación:

Tabla 11.- Tabulación pregunta 6

DETALLE	VALORES
SI	0
NO	8
TOTAL	8

Gráfico:

Figura 13: Gráfico pregunta 6



Análisis:

El personal de la DGTIC de la Universidad Estatal Amazónica, mencionan que actualmente la institución no cuenta con un análisis de Riesgo relacionado al área de Tecnologías de la Información, por lo tanto, desconocen de manera clara y detallada sobre los niveles de criticidad en los que se encuentra cada Activos de Información, y por ende no cuenta con un plan que permita el tratamiento y mitigación de daños que puede sufrir los recursos tecnológicos de la UEA.

7. **¿La UEA, cuenta con datos sobre el estado de madurez del Gobierno y Gestión de TI? Si su respuesta es SI, detalle el nivel de madurez.**

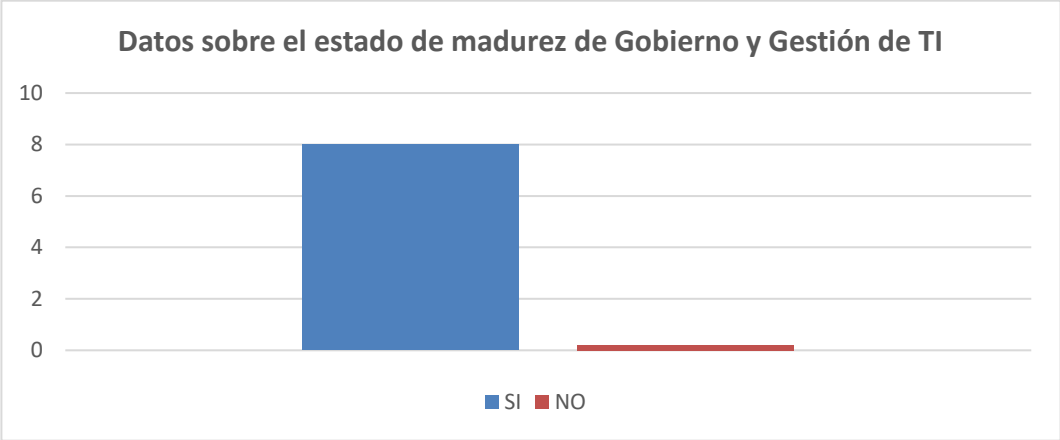
Tabulación:

Tabla 12.- Tabulación pregunta 7

DETALLE	VALORES
SI	8
NO	0
TOTAL	8

Gráfico:

Figura 14: Gráfico pregunta 7



Análisis:

Un alto porcentaje de encuestados coincide que cuenta con datos sobre el nivel de madures del Gobierno y Gestión de TI de la Universidad Estatal Amazónica, debido a que en fechas anteriores se realizó un trabajo de investigación en el cual se detalla los procesos y buenas prácticas relacionadas a la aplicación de un GTI, la respuesta el mismo que aún se encuentra en un nivel de madurez 3, y se encuentra en trámites de aprobación procesos y otros en desarrollo y mejora.

8. ¿En el Gobierno de TI aplicado en su institución, considera procesos encargados de la seguridad y riesgo de los activos de la información de la institución, fueron atendidos y elevaron su nivel de madurez?

Tabulación:

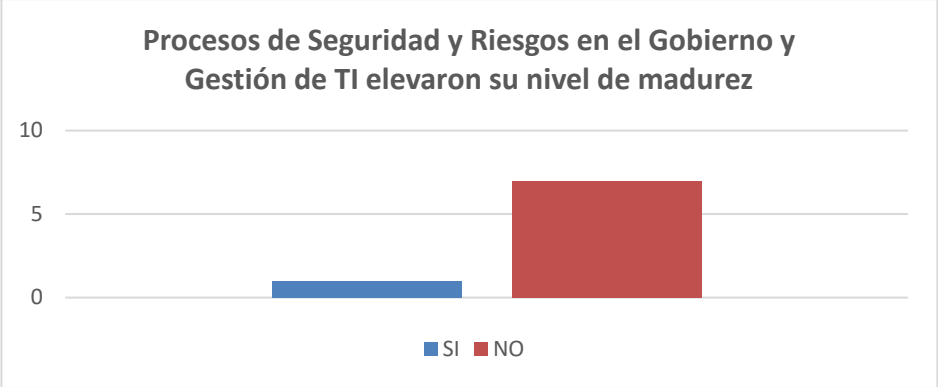
Tabla 13.- Tabulación pregunta 8

DETALLE	VALORES
SI	1
NO	7

TOTAL	8

Gráfico:

Figura 15: Gráfico pregunta 8



Análisis:

El Modelo de Gobierno y Gestión de TI, aplicado en la Universidad Estatal Amazónica, contempla procesos catalizadores relacionados con la seguridad y riesgo de la Tecnologías de la Información. Es importante mencionar que, si bien los encuestados concuerdan que se encuentra aplicadas buenas prácticas del Gobierno y Gestión del TI, en esta preguntan la mayoría indican que existen procesos como los de Seguridad y Riegos que no evidenciaron ser atendidos o mejoraron su nivel de madurez, lo que no ha permitido establecer buenas prácticas en estas áreas que mejoren la Seguridad de la Información.
Después de la aplicación de la encuesta, se realiza el análisis de los datos recopilados, emitiendo los siguientes resultados con los cuales se puede identificar el estado actual de la Gestión de Seguridad de la Información en la Universidad Estatal Amazónica:

Adicional se detalla a continuación la aplicación de la entrevista realizada al Director de Gestión de Tecnologías de la Información, concomitante se realiza el análisis de los datos recopilados, emitiendo los siguientes resultados con los cuales se puede identificar el

estado inicial de la Gestión de Seguridad de la Información en la Universidad Estatal Amazónica:

1.- ¿Cómo administra la DGTIC el inventario actualizado de hardware, software y de activos de la información en la Universidad Estatal Amazónica?

El Director de Gestión de las Tecnologías de la Información y Comunicación, manifiesta que la UEA cuenta con procesos establecidos que permiten la actualización constante del inventario de hardware y software, sin embargo, a la fecha no se cuenta con un inventario detallado de los activos de información detallado.

2.- ¿Qué prácticas de protección de seguridad de la información se aplican al momento de desvincular al personal de la Universidad?

El entrevistado indica que, al contar con autenticación federada, esto permite que al deshabilitar el acceso a la cuenta institucional, automáticamente el ex funcionario no contará con acceso a correo institucional, sistemas de información, plataformas y demás información digital, para el acceso a la información física la restricción la controlan los Directores departamentales.

3.- ¿Qué tipo de políticas de seguridad se utilizan para proteger la información almacenada en los diferentes sistemas, plataformas, bases de datos alojadas en los equipos servidores de la institución?

El Director de la DGTIC, menciona que la Universidad Estatal Amazónica cuenta con un Centro de Datos que cuenta con controles de acceso biométrico, sistema de detección de incendios, control de temperatura y humedad, cámaras de seguridad y detección de movimiento, lo que permite garantizar el acceso restringida solo a personal autorizado hacia le centro de datos.

4.- ¿Las políticas detalladas en la pregunta anterior se encuentran definidas formalmente y socializada con todos los actores involucrados de la comunidad universitaria? Argumente

El entrevistado responde que a la interrogante con una negativa y menciona que, todas la políticas han sido establecidas de manera empírica, por conocimiento del personal que labora en la DGTIC, sin embargo no se encuentra formalizada, y no responde a estándares

o normas nacionales o internacionales, al no contar con políticas documentadas, no se ha socializado las mismas con la comunidad universitaria, sin embargo como una buena práctica se mantiene envío de correos electrónico informativos que permite mantener a los usuarios informados sobre posibles riesgos a los que están expuestos como usuarios finales.

5.- ¿La DGTIC ha elaborado el análisis de claro y detallado de los riesgos a los que se encuentran expuestos los activos de información que son de su responsabilidad, identificando riesgos, niveles de criticidad y tratamiento de los mismos? Argumente

En las diferentes reuniones de trabajo realizada con el equipo de trabajo de la DGTIC, el Director de la DGITC indica que se establece conversaciones donde se identifica posibles riesgos a los diferentes usuarios, sistemas y equipos, la forma de tratarlos y mitigarlos. Estos riesgos no se encuentran detallados o documentados, ya que se realice el análisis al momento de la identificación de problemas.

6.- ¿La aplicación de un Gobierno y Gestión de TI permitió la aplicación de buenas prácticas en la administración de las Tecnologías de la Información? Argumente

El Director de la DGTIC indica que, la Aplicación de un modelo de Gestión y Gobierno de TI en la Universidad Estatal Amazónica, permitió la aplicación de buenas prácticas en la administración de las Tecnologías de la Información, esto significa que se identificó 14 procesos catalizadores, que de un nivel 1 puede llegar a un nivel de madurez 3, lo que sin duda alguna ha mejorado la forma de ver las tecnologías de la información y como estas pueden estar alineadas a los objetivos institucionales y responder a las necesidades de la institución.

7.- ¿La aplicación de un Gobierno y Gestión de TI mejoró la seguridad de la información y la optimización del riesgo en la Universidad Estatal Amazónica? Argumente

El entrevistado manifiesta que, lamentablemente, entre los 14 procesos de catalizadores que mejoraron mediante la implementación de un modelo de gestión y gobierno de TI en la UEA, no se logro mejorar el nivel de madurez en los procesos que administran la

seguridad y la optimización del riego, lo que de alguna manera conlleva no tener definidos parámetros que garanticen la seguridad de la información en la Universidad Estatal Amazónica.

4.4 Análisis de factibilidad

4.4.1 Factibilidad Técnica

Se determina que técnicamente es factible de realizar, ya que se cuenta con los recursos tecnológicos requeridos, haciendo referencia a la infraestructura, herramientas tecnológicas o software, acceso a datos e información requerida.

4.4.2 Factibilidad Operativa

El presente proyecto es factible operativamente porque cuenta con el apoyo de las autoridades de la UEA y responsables de TI, lo cual también permite tener la apertura necesaria con el personal que labora en la institución para proporcionar la información necesaria y asegurar que los resultados del presente proyecto por su beneficio y utilidad sean aplicados.

4.4.3 Factibilidad Económica

Se puede mencionar que económicamente el presente proyecto es factible ya que los costos que implican el análisis, estudio, tiempo empleado en estos temas son asumidos por el investigador, mientras que los tiempos del personal de la institución involucrados son asumidos por la UEA

4.5 Metodología, Modelo operativo

El presente proyecto de investigación basado en la investigación bibliográfica realizada en apartados anteriores, usa el modelo PCDA y toma como punto de partida que la Universidad Estatal Amazónica, cuenta con información almacenada en diferentes medios físicos y digitales.

4.5.1 Inventario de activos de información

Los activos de información con los que cuenta la Universidad Estatal Amazónica y que son gestionados, administrados o custodiados por la Dirección de Gestión de Tecnologías de la Información y Comunicación se enlistan en la siguiente tabla:

Tabla 14.- Activos de Información

Nº	ID	CATEGORIA	ACTIVOS DE INFORMACION PURA	DESCRIPCION DEL ACTIVO
1	SA-01	Software de aplicación	Siad Pregrado	Sistema informático para la gestión de información académica de docentes, estudiantes y área académica de las Facultades de Ciencias de la Tierra y Ciencias de la Vida
2	SA-02	Software de aplicación	Siad Posgrado	Sistema informático para la gestión de información académica de docentes, estudiantes y área académica de Posgrado
3	SA-03	Software de aplicación	Siad Educación continua	Sistema informático para la gestión de información académica de docentes, estudiantes y área académica de la Unidad de Educación Continua
4	SA-04	Software de aplicación	Sisges	Sistema informático para la gestión documental, en el area financiera, planificación, compras publicas y diferentes dependencias relacionadas a la adquisición de bienes y servicios
5	SA-05	Software de aplicación	SITIC	Sistemas informático para la gestión de tecnologías de la información
6	SA-06	Software de aplicación	Entorno Virtual de Aprendizaje	Aplicación para la despliegue de entornos virtuales de aprendizaje
7	SA-07	Software de aplicación	Balcón de servicios	Sistemas informático para la gestión de becas y seguimiento estudiantil relacionado a bienestar universitario
8	SO-01	Sistema Operativo	Sistema Operativo de Equipos de escritorio	Información alojada en los equipos de escritorio de las diferentes dependencias de la UEA, Campus Central y extensiones
9	SO-02	Sistema Operativo	Sistema Operativo de Servidores	Información alojada en los equipos servidores de la UEA, Campus Central y extensiones
10	SO-03	Sistema Operativo	Sistema Operativo de Dispositivos de red (Switch, AP, router)	Configuraciones y trafico de información de los equipos de red de la UEA, Campus Central y extensiones
11	DG-01	Datos digitales	Datos personales (Directorio Activo)	Datos personales administrados en el Directorio de Dominio institucional

12	DG-02	Datos digitales	Correo electrónico	Información de envío y recepción de correos electrónicos
13	DG-03	Datos digitales	Gestor de copia de seguridad	Almacenamiento de backup de imágenes y configuración de servicios
14	DG-04	Datos digitales	Gestor de base de datos	Administración de base de datos
15	DG-05	Datos digitales	Gestor de virtualización	Administración de virtualización
16	DOC-01	Documentación	Cartera de proyectos	Documentación de etapas de proyectos de tecnologías de la Información
17	DOC-02	Documentación	Gestión de Tecnologías	Documentación realcionada a la gestión de TI, servicios, equipamiento, licencias entre otros
18	INF-TI-01	Infraestructura de TI	Centro de datos	Espacio físico, donde se alojan los equipos servidores, y core de distribuidores.
19	INF-TI-02	Infraestructura de TI	Rack de comunicaciones	Espacio físico, donde se alojan los equipos de comutación de datos.
20	INF-TI-03	Infraestructura de TI	Oficina DGTIC	Espacio físico, donde se aloja, documentación y equipos de administración
21	CE-01	Controles de entorno TI	Equipos de alarma	Sistema de detección movimiento en el Centro de Datos y oficina UTIC
22	CE-02	Controles de entorno TI	Supresion contra incendio	Sistema de supresión de incendio, activación de ductos de agua para el Centro de datos
23	CE-03	Controles de entorno TI	Sistema de alimentación ininterrumpida	Sistema de respaldo de energia, que permite la alimentación de energia electrica
24	CE-04	Controles de entorno TI	Aire acondicionado	Sistema de climatización presurizada para el Centro de datos
25	CE-05	Controles de entorno TI	Deshumificador	Sistema de control de humedad para el Centro de datos
26	HW-01	Hardware de TI	Dispositivos de almacenamiento	Equipos de almacenamiento de información sensible de la UEA, ubicado en el Centro de datos
27	HW-02	Hardware de TI	Ordenadores de escritorio	Estaciones de trabajo para usuario final, procesamiento y almacenamiento de información
28	HW-03	Hardware de TI	Ordenadores portatiles, tablet y celulares	Equipos portátiles para usuario final, procesamiento y almacenamiento de información
29	HW-04	Hardware de TI	Dispositivos de comunicación	Equipos de comutación de red, access point, entre otros
30	HW-05	Hardware de TI	Equipos de impresión	Equipos de impresión en red, ubicadas en as diferentes dependencias
31	SERV-01	Servicio de TI	Servicio de autenticación de usuario	Autenticación de usuario a traves de dominio uea.edu.ec

32	SERV-02	Servicio de TI	Cortafuego	Software que permite gestionar y filtrar el trafico entrante y saliente de la red
33	SERV-03	Servicio de TI	Servidor Proxy	Software que se usan como un puente entre el origen y el destino de una solicitud
34	SERV-04	Servicio de TI	Servicio de red	Red interna de cableado estructurado que permite la conexión de toda la infraestructura de TI en el campus principal y sedes académicas
35	SERV-05	Servicio de TI	Servicio de red inalambrico	Red internade conexión analámbrica que permite la conexión de toda la infraestructura de TI en el campus principal y sedes académicas
36	SERV-06	Servicio de TI	Antivirus	Sistema de detección de amanezas e infección de softawre malicioso en equipos de ususario final
37	SERV-07	Servicio de TI	Sistema de monitoreo de redes	Zabbix Sistema de monitoreo de red interna y servidores
38	SERV-08	Servicio de TI	VPN - enlaces de datos	Enlaces troncaes que permites la conectividad entre el campus principal y las sedes académicas
39	SERV-09	Servicio de TI	Sistema de Telefonía	Servicio de telefonía de VoIP para el campus principal y sedes académicas
40	SERV-10	Servicio de TI	Servicio Web	Serviciso de acceso web a información isntitucional y acceso a aplicativos universitarios
41	TH-I-01	Talento Humano Internos	Personal administrativo y trabajadores	Personal que labora en la institución
42	TH-I-02	Talento Humano Internos	Autoridades y directores	Autoridades y directores de la institución
43	TH-I-03	Talento Humano Internos	Docentes	Docentes que laboran en la institución
44	TH-I-04	Talento Humano Internos	Estudiantes	Estudiantes que cursan sus estudios en la institución
45	TH-E-01	Talento Humano Externos	Contratistas	Personal de transito temporal, mientras dure su relacion con la UEA
46	TH-E-02	Talento Humano Externos	Proveedores	Personal de transito temporal, mientras dure su relacion con la UEA
47	TH-E-03	Talento Humano Externos	Visitantes temporales	Personal de transito temporal en la UEA

Nota. La tabla muestra los activos de información que son de responsabilidad de la Dirección de Gestión de Tecnologías de la Información y Comunicación de la Universidad Estatal Amazónica.

Los activos de información en el anexo 2 del presente documento se encuentran detallados de manera amplia donde consta información relacionada a sus procesos, custodios y

responsables, además de los niveles aceptables de las características de la información como son confiabilidad, integridad, disponibilidad, autenticidad y trazabilidad.

4.5.2 Gestión de Riesgos

Poseer el inventario de activos de información, permite efectivizar el análisis de riesgos que contemplan analizar las amenazas, probabilidad, riesgo y a aplicación de salvaguardas, como lo menciona Magerit v3, las todas las consideraciones anteriores desembocan en una calificación de cada riesgo significativo, determinándose si el riesgo es crítico, grave, apreciable, asumible. Por la amplitud de la información, la matriz de información se encuentra detallada en el Anexo Nº 3.

Tabla 15.- Análisis del riesgo

ACTIVOS DE INFORMA-CION PURA	DESCRIPCION DEL ACTIVO	CANT	RESPONSABLE ANALISIS DE RIESGO	ID RIESGO	AMENAZAS	PROBA-BILIDAD	IMPAC-TO	RIES-GO	CALIFICACION DE RIESGO
Siad Pregrado	Sistema informático para la gestión de información académica de docentes, estudiantes y area académica de las Facultades de Ciencias de la Tierra y Ciencias de la Vida	1	Ing. Verónica Villarreal	R1	Introducción de falsa información	2	3	6	ASUMIBLE
				R2	Fallo de servicios de comunicaciones	1	4	4	ASUMIBLE
				R3	Degradación de los soportes de almacenamiento de la información	2	5	10	APRECIABLE
				R4	Indisponibilidad del personal	3	5	15	GRAVE
				R5	Errores de los usuarios	3	4	12	GRAVE
				R6	Errores de configuración	1	4	4	ASUMIBLE
Siad Posgrado	Sistema informatico para la gestión de información	1	Ing. Verónica Villarreal	R1	Introducción de falsa información	2	3	6	ASUMIBLE

	académica de docentes, estudiantes y area académica de Posgrado			R2	Fallo de servicios de comunicaciones	1	4	4	ASUMIBLE
				R3	Degradación de los soportes de almacenamiento de la información	2	5	10	APRECIABLE
				R4	Indisponibilidad del personal	3	5	15	GRAVE
				R5	Errores de los usuarios	3	4	12	GRAVE
				R6	Errores de configuración	1	4	4	ASUMIBLE
Siad Educacion continua	Sistema informatico para la gestión de información académica de docentes, estudiantes y area académica de la Unidad de Educación Continua	1	Ing. Verónica Villarreal	R1	Introducción de falsa información	2	3	6	ASUMIBLE
				R2	Fallo de servicios de comunicaciones	1	4	4	ASUMIBLE
				R3	Degradación de los soportes de almacenamiento de la información	2	5	10	APRECIABLE
				R4	Indisponibilidad del personal	3	5	15	GRAVE
				R5	Errores de los usuarios	3	4	12	GRAVE
				R6	Errores de configuración	1	4	4	ASUMIBLE
Sisges	Sistema informático para la gestión documental, en el área fiannciera, planificación, compras publicas y diferentes dependencias	1	Ing. Verónica Villarreal	R1	Fuga de información	2	3	6	ASUMIBLE
				R2	Introducción de falsa información	2	3	6	ASUMIBLE
				R3	Fallo de servicios de comunicaciones	1	4	4	ASUMIBLE

	relacionadas a la adquisición de bienes y servicios			R4	Degradación de los soportes de almacenamiento de la información	2	5	10	APRECIABLE
				R5	Caída del sistema por sobrecarga	2	4	8	ASUMIBLE
				R6	Indisponibilidad del personal	3	5	15	GRAVE
				R7	Errores de los usuarios	3	3	9	APRECIABLE
SITIC	Sistemas informático para la gestión de tecnologías de la información	1	Ing. Verónica Villarreal	R1	Introducción de falsa información	2	3	6	ASUMIBLE
				R2	Fallo de servicios de comunicaciones	1	4	4	ASUMIBLE
				R3	Degradación de los soportes de almacenamiento de la información	2	5	10	APRECIABLE
				R4	Caída del sistema por sobrecarga	2	4	8	ASUMIBLE
				R5	Indisponibilidad del personal	3	3	9	APRECIABLE
				R6	Errores de los usuarios	3	3	9	APRECIABLE
Entorno Virtual de Aprendizaje	Aplicación para la despliegue de entornos virtuales de aprendizaje	4	Ing. Verónica Villarreal	R1	Fallo de servicios de comunicaciones	1	4	4	ASUMIBLE
				R2	Degradación de los soportes de almacenamiento de la información	2	5	10	APRECIABLE
				R3	Caída del sistema por sobrecarga	2	4	8	ASUMIBLE
				R4	Errores de los usuarios	3	3	9	APRECIABLE

				R5	Errores de configuración	2	2	4	ASUMIBLE
Balcon de servicios	Sistemas informático para la gestión de becas y seguimiento esudiantil relacionado a bienestar universitario	1	Ing. Verónica Villarreal	R1	Fuga de información	2	3	6	ASUMIBLE
				R2	Introducción de falsa información	2	3	6	ASUMIBLE
				R3	Fallo de servicios de comunicaciones	1	4	4	ASUMIBLE
				R4	Degradación de los soportes de almacenamiento de la información	2	5	10	APRECIABLE
				R5	Caída del sistema por sobrecarga	2	4	8	ASUMIBLE
				R6	Indisponibilidad del personal	3	3	9	APRECIABLE
				R7	Errores de los usuarios	3	3	9	APRECIABLE
Sistema Operativo de Equipos de escritorio	Información alojada en los equipos de escritorio de las diferentes dependencias de la UEA, Campus Central y extensiones	465	Ing. Verónica Villarreal	R1	Fuga de información	1	1	1	ASUMIBLE
				R2	Destrucción de información	3	5	15	GRAVE
				R3	Interceptación de información (escucha)	2	3	6	ASUMIBLE
				R4	Corte del suministro eléctrico	2	2	4	ASUMIBLE
				R5	Interrupción de otros servicios y suministros esenciales	1	4	4	ASUMIBLE
				R6	Degradación de los soportes de almacenamiento de la información	2	5	10	APRECIABLE

				R7	Difusión de software dañino	2	4	8	ASUMIBLE
				R8	Abuso de privilegios de acceso	2	3	6	ASUMIBLE
				R9	Errores de los usuarios	3	3	9	APRECIABLE
				R10	Ingeniería social	3	4	12	GRAVE
Sistema Operativo de Servidores	Información alojada en los equipos servidores de la UEA, Campus Central y extensiones	15	Ing. Verónica Villarreal	R1	Interceptación de información (escucha)	2	3	6	ASUMIBLE
				R2	Corte del suministro eléctrico	3	3	9	APRECIABLE
				R3	Interrupción de otros servicios y suministros esenciales	2	3	6	ASUMIBLE
				R4	Degradación de los soportes de almacenamiento de la información	2	5	10	APRECIABLE
				R5	Difusión de software dañino	2	4	8	ASUMIBLE
				R6	Errores de mantenimiento / actualización de programas (software)	2	3	6	ASUMIBLE
				R7	Caída del sistema por sobrecarga	2	3	6	ASUMIBLE
				R8	Errores de configuración	2	3	6	ASUMIBLE
Sistema Operativo de Dispositivo	Configuraciones y tráfico de información de los equipos de	32	Ing. Verónica Villarreal	R1	Interceptación de información (escucha)	2	4	8	ASUMIBLE

s de red (Switch, AP, router)	red de la UEA, Campus Central y extensiones			R2	Corte del suministro eléctrico	3	3	9	APRECIABLE
				R3	Interrupción de otros servicios y suministros esenciales	3	3	9	APRECIABLE
				R4	Degradación de los soportes de almacenamiento de la información	2	4	8	ASUMIBLE
				R5	Difusión de software dañino	2	5	10	APRECIABLE
				R6	Errores de mantenimiento / actualización de programas (software)	2	5	10	APRECIABLE
				R7	Caída del sistema por sobrecarga	2	5	10	APRECIABLE
				R8	Errores de configuración	2	5	10	APRECIABLE
Datos personales (Directorio Activo)	Datos personales administrados en el Directorio de Dominio institucional	5200	Ing. Verónica Villarreal	R1	Fallo de servicios de comunicaciones	2	4	8	ASUMIBLE
				R2	Interrupción de otros servicios y suministros esenciales	3	4	12	GRAVE
				R3	Degradación de los soportes de almacenamiento de la información	2	4	8	ASUMIBLE
				R4	Caída del sistema por sobrecarga	2	4	8	ASUMIBLE

				R5	Indisponibilidad del personal	2	4	8	ASUMIBLE
				R6	Errores de configuración	2	4	8	ASUMIBLE
Correo electronico	Información de envio y recepción de correos electrónicos	5200	Ing. Verónica Villarreal	R1	Fallo de servicios de comunicaciones	2	3	6	ASUMIBLE
				R2	Interrupción de otros servicios y suministros esenciales	2	3	6	ASUMIBLE
				R3	Caída del sistema por sobrecarga	2	3	6	ASUMIBLE
				R4	Indisponibilidad del personal	2	4	8	ASUMIBLE
Gestor de copia de seguridad	Almacenamiento de backup de imágenes y configuración de servicios	32	Ing. Verónica Villarreal	R1	Fallo de servicios de comunicaciones	2	3	6	ASUMIBLE
				R2	Interrupción de otros servicios y suministros esenciales	2	3	6	ASUMIBLE
				R3	Caída del sistema por sobrecarga	2	3	6	ASUMIBLE
				R4	Indisponibilidad del personal	2	4	8	ASUMIBLE
Gestor de base de datos	Administración de base de datos	7	Ing. Verónica Villarreal	R1	Fallo de servicios de comunicaciones	2	3	6	ASUMIBLE
				R2	Interrupción de otros servicios y suministros esenciales	2	3	6	ASUMIBLE
				R3	Caída del sistema por sobrecarga	2	3	6	ASUMIBLE
				R4	Indisponibilidad del personal	2	4	8	ASUMIBLE

Gestor de virtualización	Administración de virtualización	32	Ing. Verónica Villarreal	R1	Fallo de servicios de comunicaciones	2	3	6	ASUMIBLE
				R2	Interrupción de otros servicios y suministros esenciales	2	3	6	ASUMIBLE
				R3	Caída del sistema por sobrecarga	2	3	6	ASUMIBLE
				R4	Indisponibilidad del personal	2	4	8	ASUMIBLE
Cartera de proyectos	Documentación de etapas de proyectos de tecnologías de la Información	40	Ing. Verónica Villarreal	R1	Fuga de información	**2**	**3**	6	ASUMIBLE
				R2	Indisponibilidad del personal	**2**	**4**	8	ASUMIBLE
				R3	Corrupción de la información	2	4	8	ASUMIBLE
Gestión de Tecnologías	Documentación realcionada a la gestión de TI, servicios, equipamiento, licencias entre otros	6	Ing. Verónica Villarreal	R1	Fuga de información	**2**	**3**	6	ASUMIBLE
				R2	Indisponibilidad del personal	**2**	**4**	8	ASUMIBLE
				R3	Corrupción de la información	2	4	8	ASUMIBLE
Centro de datos	Espacio físico, donde se alojan los equipos servidores, y core de distribuidores.	1	Ing. Verónica Villarreal	R1	Fuego	2	5	10	APRECIABLE
				R2	Desastres Naturales	2	5	10	APRECIABLE
				R3	Condiciones inadecuadas de temperatura o humedad	2	4	8	ASUMIBLE
				R4	Fallo de servicios de comunicaciones	2	5	10	APRECIABLE
				R5	Corte del suministro eléctrico	2	5	10	APRECIABLE
	Espacio físico, donde se alojan	12	Ing. Verónica Villarreal	R1	Fuego	2	5	10	APRECIABLE

Rack de comunicaciones	los equipos de comutación de datos.			R2	Desastres Naturales	2	5	10	APRECIABLE
				R3	Condiciones inadecuadas de temperatura o humedad	2	4	8	ASUMIBLE
				R4	Fallo de servicios de comunicaciones	2	5	10	APRECIABLE
Oficina DGTIC	Espacio físico, donde se aloja, documentación y equipos de administración	1	Ing. Verónica Villarreal	R1	Fuego	2	5	10	APRECIABLE
				R2	Desastres Naturales	2	5	10	APRECIABLE
Equipos de alarma	Sistema de detección movimiento en el Centro de Datos y oficina UTIC	2	Ing. Verónica Villarreal	R1	Fallo de servicios de comunicaciones	2	5	10	APRECIABLE
				R2	Errores de configuración	2	5	10	APRECIABLE
				R3	Caída del sistema por sobrecarga	2	5	10	APRECIABLE
Supresion contra incendio	Sistema de supresión de incendio, activación de ductos de agua para el Centro de datos	1	Ing. Verónica Villarreal	R1	Fallo de servicios de comunicaciones	2	5	10	APRECIABLE
				R2	Errores de configuración	2	5	10	APRECIABLE
				R3	Caída del sistema por sobrecarga	2	5	10	APRECIABLE
Sistema de alimentación ininterrumpida	Sistema de respaldo de energia, que permite la alimentación de energia electrica	1	Ing. Verónica Villarreal	R1	Fallo de servicios de comunicaciones	2	5	10	APRECIABLE
				R2	Errores de configuración	2	5	10	APRECIABLE
				R3	Caída del sistema por sobrecarga	2	5	10	APRECIABLE
Aire acondicionado	Sistema de climatización presurizada para	1	Ing. Verónica Villarreal	R1	Fallo de servicios de comunicaciones	2	5	10	APRECIABLE

	el Centro de datos			R2	Errores de configuración	2	5	10	APRECIABLE
				R3	Caída del sistema por sobrecarga	2	5	10	APRECIABLE
Deshumificador	Sistema de control de humedad para el Centro de datos	1	Ing. Verónica Villarreal	R1	Fallo de servicios de comunicaciones	2	5	10	APRECIABLE
				R2	Errores de configuración	2	5	10	APRECIABLE
				R3	Caída del sistema por sobrecarga	2	5	10	APRECIABLE
Dispositivos de almacenamiento	Equipos de almacenamiento de información sensible de la UEA, ubicado en el Centro de datos	2	Ing. Verónica Villarreal	R1	Errores de configuración	2	5	10	APRECIABLE
				R2	Degradación de los soportes de almacenamiento de la información	3	5	15	GRAVE
Ordenadores de escritorio	Estaciones de trabajo para usuario final, procesamiento y almacenamiento de información	465	Ing. Verónica Villarreal	R1	Errores de configuración	2	5	10	APRECIABLE
				R2	Degradación de los soportes de almacenamiento de la información	3	5	15	GRAVE
				R3	Fallo de servicios de comunicaciones	2	5	10	APRECIABLE
Ordenadores portatiles, tablet y celulares	Equipos portátiles para usuario final, procesamiento y almacenamiento de información	20	Ing. Verónica Villarreal	R1	Errores de configuración	2	5	10	APRECIABLE
				R2	Degradación de los soportes de almacenamiento de la información	3	5	15	GRAVE
				R3	Fallo de servicios de comunicaciones	2	5	10	APRECIABLE

Dispositivos de comunicación	Equipos de comutación de red, access point, entre otros	32	Ing. Verónica Villarreal	R1	Errores de configuración	2	5	10	APRECIABLE
				R2	Degradación de los soportes de almacenamiento de la información	3	5	15	GRAVE
				R3	Fallo de servicios de comunicaciones	2	5	10	APRECIABLE
Equipos de impresión	Equipos de impresión en red, ubicadas en as diferentes dependencias	104	Ing. Verónica Villarreal	R1	Errores de configuración	2	5	10	APRECIABLE
				R2	Degradación de los soportes de almacenamiento de la información	3	5	15	GRAVE
				R3	Fallo de servicios de comunicaciones	2	5	10	APRECIABLE
Servicio de autenticación de usuario	Autenticación de usuario a traves de dominio uea.edu.ec	1	Ing. Verónica Villarreal	R1	Errores de configuración	2	5	10	APRECIABLE
				R2	Fallo de servicios de comunicaciones	2	5	10	APRECIABLE
Cortafuego	Software que permite gestionar y filtrar el trafico entrante y saliente de la red	1	Ing. Verónica Villarreal	R1	Errores de configuración	2	5	10	APRECIABLE
				R2	Fallo de servicios de comunicaciones	2	5	10	APRECIABLE
Servidor Proxy	Software que se usan como un puente entre el origen y el destino de una solicitud	1	Ing. Verónica Villarreal	R1	Errores de configuración	2	5	10	APRECIABLE
				R2	Fallo de servicios de comunicaciones	2	5	10	APRECIABLE
Servicio de red	Red interna de cableado estructurado que permite la	4	Ing. Verónica Villarreal	R1	Errores de configuración	2	5	10	APRECIABLE

	conexión de toda la infraestructura de TI en el campus principal y sedes académicas			R2	Fallo de servicios de comunicaciones	2	5	10	APRECIABLE
Servicio de red inalambrico	Red internade conexión analámbrica que permite la conexión de toda la infraestructura de TI en el campus principal y sedes académicas	4	Ing. Verónica Villarreal	R1	Errores de configuración	2	5	10	APRECIABLE
				R2	Fallo de servicios de comunicaciones	2	5	10	APRECIABLE
Antivirus	Sistema de detección de amanezas e infección de softawre malicioso en equipos de ususario final	1	Ing. Verónica Villarreal	R1	Errores de configuración	2	5	10	APRECIABLE
Sistema de monitoreo de redes	Zabbix Sistema de monitoreo de red interna y servidores	1	Ing. Verónica Villarreal	R1	Errores de configuración	2	5	10	APRECIABLE
VPN - enlaces de datos	Enlaces troncaes que permites la conectividad entre el campus principal y las sedes académicas	4	Ing. Verónica Villarreal	R1	Errores de configuración	2	5	10	APRECIABLE
Sistema de Telefonía	Servicio de telefonía de VoIP para el campus principal y sedes académicas	4	Ing. Verónica Villarreal	R1	Errores de configuración	2	5	10	APRECIABLE
Servicio Web	Serviciso de acceso web a información isntitucional y acceso a aplicativos universitarios	1	Ing. Verónica Villarreal	R1	Errores de configuración	2	5	10	APRECIABLE
Personal administrativo y trabajadores	Personal que labora en la institución	140	Ing. Verónica Villarreal	R1	Errores de los usuarios	2	5	10	APRECIABLE
				R2	Indisponibilidad del personal	2	5	10	APRECIABLE

				R3	Victimas de Ingeniería social	3	4	12	GRAVE
Autoridades y directores	Autoridades y directores de la institución	10	Ing. Verónica Villarreal	R1	Victimas de Ingeniería social	3	4	12	GRAVE
Docentes	Docentes que laboran en la institución	150	Ing. Verónica Villarreal	R1	Victimas de Ingeniería social	3	4	12	GRAVE
Estudiantes	Estudiantes que cursan sus estudios en la institución	4800	Ing. Verónica Villarreal	R1	Victimas de Ingeniería social	3	4	12	GRAVE
Contratistas	Personal de transito temporal, mientras dure su relacion con la UEA	5	Ing. Verónica Villarreal	R1	Victimas de Ingeniería social	3	4	12	GRAVE
Proveedores	Personal de transito temporal, mientras dure su relacion con la UEA	2	Ing. Verónica Villarreal	R1	Victimas de Ingeniería social	3	4	12	GRAVE
Visitantes temporales	Personal de transito temporal en la UEA	100	Ing. Verónica Villarreal	R1	Victimas de Ingeniería social	3	4	12	GRAVE

Nota. La tabla muestra el análisis de riesgos de los activos de información que son de responsabilidad de la Dirección de Gestión de Tecnologías de la Información y Comunicación de la Universidad Estatal Amazónica, en el cual se identifica el riesgo de cada activo de información, el impacto, probabilidad y nivel de riesgo y criticidad.

Como resultado del análisis de riesgo, se puede definir el tratamiento que se dará a cada riesgo identificando las acciones que se tomará por cada riesgo que represente un alto nivel de criticidad.

Ejemplo:

Tabla 16.- Ejemplo Análisis de riesgos

			El riesgo crece con el impacto y con la probabilidad			
ACTIVOS DE INFORMACION PURA	**ID-RIESGO**	**AMENAZAS**	**PROBAB-ILIDAD**	**IMPAC-TO**	**RIES-GO**	**CALIFICACION DE RIESGO**
Sisges	R1	Fuga de información	2	3	6	ASUMIBLE

	R2	Introducción de falsa información	2	3	6	ASUMIBLE
	R3	Fallo de servicios de comunicaciones	1	4	4	ASUMIBLE
	R4	Degradación de los soportes de almacenamiento de la información	2	5	10	APRECIABLE
	R5	Caída del sistema por sobrecarga	1	4	4	ASUMIBLE
	R6	Indisponibilidad del personal	3	5	15	GRAVE
	R7	Errores de los usuarios	3	4	12	GRAVE

Nota. La tabla muestra un ejemplo del análisis de los riesgos de los activos de información que permite conocer la calificación del riesgo.

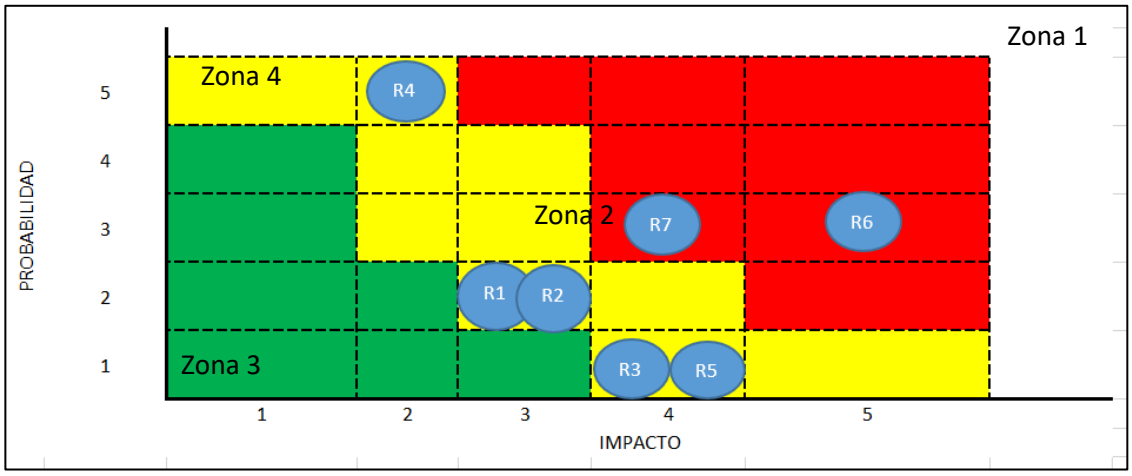
En términos de las zonas de riesgo, Magerit v3 identifica las siguientes para analizarlas visualmente en la figura 16.

• Zona 1 – riesgos muy probables y de muy alto impacto; posiblemente nos planteemos sacarlos de esta zona

• Zona 2 – riesgos de probabilidad relativa e impacto medio; se pueden tomar varias opciones • Zona 3 – riesgos improbables y de bajo impacto; o los dejamos como están, o permitimos que suban a mayores si ello nos ofreciera alguna ventaja o beneficio en otro terreno

• Zona 4 – riesgos improbables pero de muy alto impacto; suponen un reto de decisión pues su improbabilidad no justifica que se tomen medidas preventivas, pero su elevado impacto exige que tengamos algo previsto para reaccionar; es decir, hay que poner el énfasis en medidas de reacción para limitar el daño y de recuperación del desastre si ocurriera.

Figura 16.- Análisis de riesgo



Nota. La figura permite visualizar de manera gráfica la calificación del riesgo lo que permite identificar la criticidad de cada riesgo y conocer que riesgos requieren mayor atención.

4.5.3 Implementación de Sistema de Gestión de Seguridad de Información

La metodología para la implementación de un Sistema de Gestión de Seguridad de la Información, utilizada en el presente proyecto es PDCA, que define sus etapas de la siguiente manera:

a) Establecer el SGSI

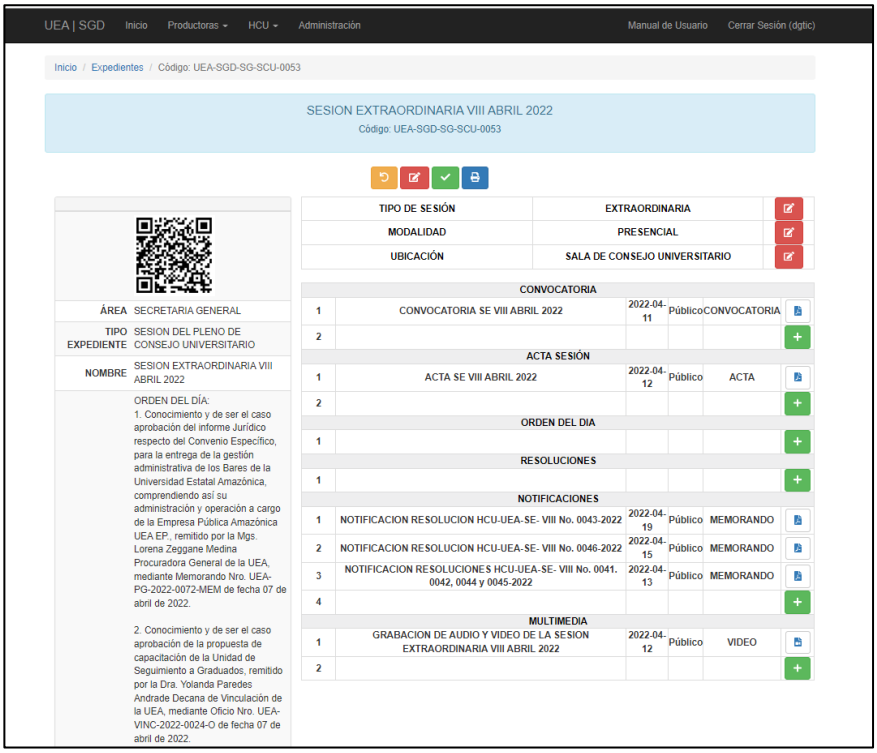
En el anexo Nº 4 se presenta la carta de compromiso de la máxima autoridad de la UEA, con el presente proyecto, que permite establecer el SGSI en la Universidad Estatal Amazónica.

b) Implementar y operar el SGSI

Seguido del análisis de riesgos, se viabilizó la creación de políticas de seguridad que permita mitigar las amenazas más altas, cumpliendo con los 14 dominios de la norma ISO27001, para lo cual se ha generado el manual de políticas de Seguridad de la Información en la Universidad Estatal Amazónica, la misma que por su longitud se encuentra en el anexo Nº 5.

Adicional se ha implementado el Sistema de Gestión documental de la UEA, en el cual se digitaliza y automatiza el procesamiento de expedientes y documentación sensible de la UEA, con esto se garantiza que las dependencias de la UEA, cuenten con el archivo físico y digital, garantizando la disponibilidad, integridad y confiabilidad de la información.

Figura 17.- Sistema de Gestión Documental



Nota. La figura muestra la interface del Sistema de Gestión documental de la UEA, lo que ha permitido digitalizar la información sensible garantizando la disponibilidad, integridad y confiablidad de la misma.

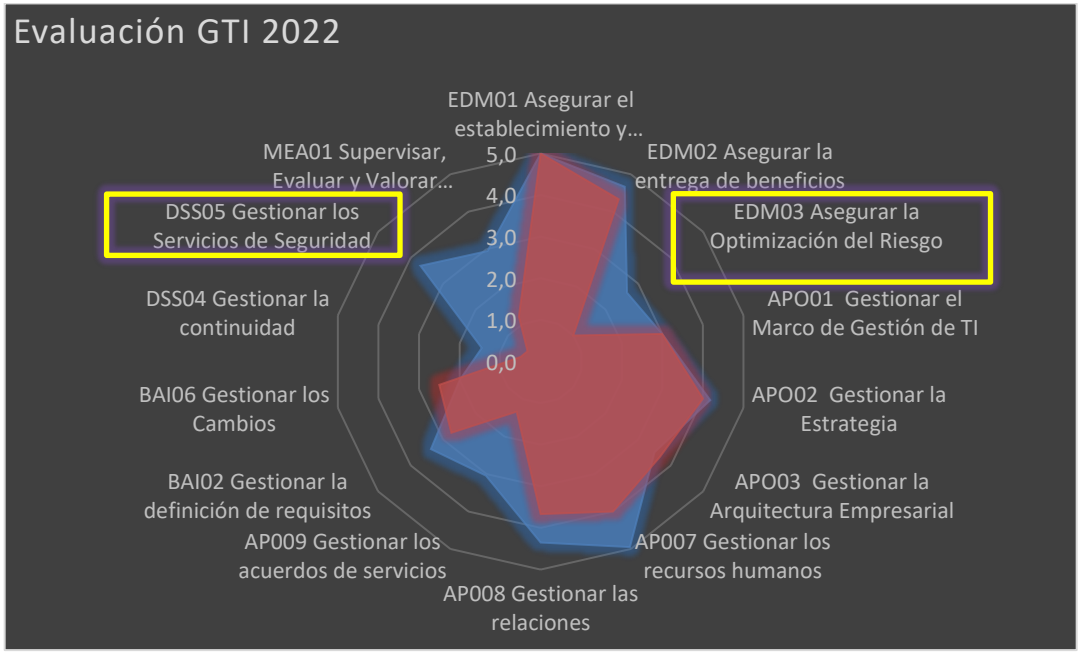
c) Monitorear y revisar el SGSI

Para el monitoreo y revisión del Sistema de Gestión de la Seguridad de la Información, se aplicará, encuestas a los actores involucrados, con la finalidad de conocer la adaptabilidad y los problemas que pueden emerger del sistema.

El SGSI converge de maneja significativa con el Gobierno y Gestión de la Tecnologías de la información, por lo que a través del monitoreo y evaluación anual realizado al Gobierno y Gestión de Tecnologías de la Información, de un nivel 2.1 en los procesos EDM03: Asegurar la Optimización del Riesgo, después de la aplicación del SGSI de un nivel 1 ha

alcanzado una valoración de 2,7, mientras que en el proceso catalizador DSS05: Gestionar los Servicios de Seguridad, de un nivel valorado en 2,6, ha alcanzado el nivel de 3,7, según las métricas aplicadas en el Gobierno y Gestión de Tecnologías de la Información, basada en la norma ISO 38500 y COBIT 5, aplicado en la Universidad Estatal Amazónica a partir del año 2018.

Figura 18.- Evaluación Gobierno y Gestión de TI correspondiente al año 2022



Nota. La figura muestra el avance en el ámbito de gestión de riesgos y seguridad de la información dentro del GTI, evidenciando un cambio significante en la realidad de la UEA.

d) Mantener y mejorar el SGSI

La evaluación del Sistema de Gestión de Seguridad de la Información junto a la Evaluación del Gobierno y Gestión de las Tecnologías de la Información en la Universidad Estatal Amazónica, permitió identificar los puntos que requieren ser fortalecidos y mejorados, identificándoles a continuación:

En el SGSI, las mejoras son:

De la mano el Gobierno y Gestión de TI, si bien ha superado en gran medida los procesos catalizadores EDM03 y DSS05, existen los siguientes procesos que aun merecen mayor atención:

Tabla 17.- Procesos para mejora continua del Gobierno y Gestión de TI

PROCESO	DETALLE	NIVEL DE CUMPLIMIENTO
EDM03	Asegurar la Optimización del Riesgo	2,7
BAI06	Gestionar los Cambios	2,0
DSS04	Gestionar la continuidad	1,5
MEA01	Supervisar, Evaluar y Valorar Rendimiento y Conformidad	2,9

Nota. La tabla muestra los procesos que después de la aplicación de SGSI aun requieren un proceso de mejora continua, que si bien aun se mantiene el proceso EDM03, se puede identificar que actualmente tiene un nivel mejorado a 2,7.

CAPÍTULO V
CONCLUSIONES, RECOMENDACIONES, BIBLIOGRAFÍA Y ANEXOS

5.1.Conclusiones

Ecuador es un país que ha fortalecido su legislación y reglamentos para fomentar la Seguridad de la información en las diferentes dependencias del Ejecutivo, en las empresas públicas y privadas.

Para la aplicación de un buen Sistema de seguridad de la información es fundamental un buen análisis y evaluación de riesgos que garantice conocer el estado actual de la organización.

Por otro lado, la seguridad de la información es la disciplina que nos habla de los riesgos, de las amenazas, de los análisis de escenarios, de las buenas prácticas y los esquemas normativos, que nos exigen niveles de aseguramiento de procesos y de tecnología para elevar el nivel de confianza en la creación, utilización, almacenaje, transmisión, recuperación y disposición final de la información.

El análisis y evaluación de riesgos propicia que las organizaciones conozcan e identifican riesgos que conocían o que desconocían y de esta manera comunicar a la alta gerencia, la cual convencida de la necesidad de precautelar su información sensible, creará políticas que eliminen o mitiguen el riesgo, garantizando de esta manera la aplicabilidad de medidas que permitan la seguridad de la información

5.2.Recomendaciones

La normativa y leyes contempladas desde la constitución hasta normas locales e internacionales, deben ser el fundamento para que las empresas públicas y privadas implementen un análisis de riesgos y posterior sistema de gestión de la seguridad de la información.

Es importante ejecutar un análisis de riesgo inicial que permita conocer el estado inicial de la organización y con la aceptación de la alta gerencia, aplicar normativas.

Es fundamental arrancar definiendo los activos de información ya que los mismos son el punto de partida para iniciar un cambio sustancial en la organización en relación con el conocimiento de los riesgos y la aplicabilidad de medidas para la seguridad de la información.

El análisis y evaluación de riesgo es un proceso repetitivo que debe ser ejecutado en cualquier momento, con la finalidad de adaptar los nuevos riesgos y vulnerabilidades, de esta manera garantizar que la empresa pueda mitigar los riesgos que pueden afectar gravemente su desempeño

5.3. BIBLIOGRAFÍA

Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid: Ministerio de Hacienda y Administraciones Públicas.

Escobar Meléndez, J. S. (2020). *SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN APLICANDO LAS NORMAS ISO/IEC 27001 EN EL DATACENTER DE LA EMPRESA AMBACAR-AMBATO.* Ambato: UNIVERSIDAD TÉCNICA DE AMBATO.

Guevara, R. (2017). Sistema de Gestión de Seguridad de la Információn basado en la Norma ISO/IEC 27000 para el departamento de Tecnologías de la Información y Comunicación del Distrito 18D01 de Educación. Ambato, Ecuador.

Instituto Nacional de Ciberseguridad. (2016). *Gestión de riesgos.* España: INCIBE.

International Standar. (2008). *Corporate Governance of Information Technology.* ISO/IEC .

ISACA. (2012). *Un marco de negocio para el gobierno y la gestion de las TI en las empresas.* Estados Unidos.

ISACA. (2018). *MARCO DE REFERENCIA COBIT 2019: OBJETIVOS DE GOBIERNO Y GESTIÓN.* Estados Unidos: ISACA.

ISO. (2005). Tecnologías de la Información - Tecnicas de Seguridad - SIstema de Gestión de la Seguridad de la Información - Requerimientos. Ginebra, Suiza.

Ramírez Camargo, E. A., & Rinconc Pinzon, M. A. (2022). La importancia de la seguridad de la información en el sector público en Colombia. *Revista lbérica de Sistemas y Tecnologías de Información*, 87 - 99.

Secretaria de la Administración Pública. (19 de Septiembre de 2013). Decreto 166 - Seguridad de la Información. Quito.

Subsecretaría de Estado Gobierno Electrónico. (2020). *GUIA PARA LA GESTIÓN DE RIESGOS PARA LA SEGURIDAD DE LA INFORMACIÓN.* Quito: Gobierno Electrónico.

Tarazona, C. (2007). *Amenazas informáticas y seguridad de la información.* Colombia: Universidad Externado.

Villarreal, V. (2018). Modelo de Gestión y Gobierno de Tecnologías de la Información en la Universidad Estatal Amazónica. Ambato.

Zapata Chasiguasin, K. B. (2020). *SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LAS NORMAS ISO/IEC 27001, EN EL DEPARTAMENTO DE TECNOLOGIAS DE LA INFORMACION DEL GOBIERNO AUTONOMO DESCENTRALIZADO DE LA MUNICIPALIDAD DE AMBATO.* Ambato: Universidad Técnica de Ambato.

.

5.4.ANEXOS

Anexo 1.-

ENCUESTA

Fecha:	
Cargo que desempeña:	
Genero	

Dirigida a: Personal que labora en la Dirección de Tecnologías de la Información y comunicación de la Universidad Estatal Amazónica.

Objetivo: Conocer la situación actual de la seguridad de la información en la Dirección de Tecnologías de la Información y Comunicación de la Universidad Estatal Amazónica.

Instrucciones: Marque con una x la alternativa que considera adecuada.

Nº	PREGUNTAS	SI	NO
1	**¿La UEA cuenta con un inventario actualizado de hardware y software de la institución?**		
2	**¿La UEA mantienen un inventario actualizado de los activos de información de la institución?**		

3	**¿Con relación al acceso a la información, que permisos son retirados después de la culminación del contrato con el empleado? Puede seleccionar varias opciones**	**SI**	**NO**
	Acceso a Correo electrónico		
	Acceso a Sistemas y Plataformas		
	Acceso a documentación digital		
	Acceso a documentación física		
	Acceso a cuenta institucional		

Nº	PREGUNTAS	SI	NO
4	**¿El área de servidores está protegida por controles apropiados de entrada para asegurar que sólo el personal autorizado tenga acceso?**		
5	**¿Disponen de políticas para la seguridad de la Información, socializada con todos los actores involucrados de la comunidad universitaria?**		

6	**¿Conoce de manera clara y detallada los riesgos y niveles de criticidad de los activos de información relacionados a las tecnologías de la información?**		
7	**¿La UEA, cuenta con datos sobre el estado de madurez del Gobierno y Gestión de TI?**		
Si su respuesta a la pregunta 7 es SI, detalle el nivel de madurez			

GRACIAS POR LA COLABORACIÓN

Anexo 1.2.-

ENTREVISTA

Fecha:	
Nombres y Apellidos:	
Cargo que desempeña:	

Dirigida: Al Director de Gestión de Tecnologías de la Información y comunicación de la Universidad Estatal Amazónica.

Objetivo: Conocer la situación actual de la seguridad de la información en la Dirección de Tecnologías de la Información y Comunicación de la Universidad Estatal Amazónica.

1.- ¿Cómo administra la DGTIC el inventario actualizado de hardware, software y de activos de la información en la Universidad Estatal Amazónica?

_____
_____
_____
_____

2.- ¿Qué prácticas de protección de seguridad de la información se aplican al momento de desvincular al personal de la Universidad?

_____
_____
_____
_____

3.- ¿Qué tipo de políticas de seguridad se utilizan para proteger la información almacenada en los diferentes sistemas, plataformas, bases de datos alojadas en los equipos servidores de la institución?

_____
_____
_____
_____

4.- ¿Las políticas detalladas en la pregunta anterior se encuentran definidas formalmente y socializada con todos los actores involucrados de la comunidad universitaria? Argumente

_____
_____
_____
_____

5.- ¿La DGTIC ha elaborado el análisis de claro y detallado de los riesgos a los que se encuentran expuestos los activos de información que son de su responsabilidad, identificando riesgos, niveles de criticidad y tratamiento de los mismos? Argumente

_____
_____
_____
_____

6.- ¿La aplicación de un Gobierno y Gestión de TI permitió la aplicación de buenas prácticas en la administración de las Tecnologías de la Información? Argumente

_____
_____
_____
_____

7.- ¿La aplicación de un Gobierno y Gestión de TI mejoro la seguridad de la información y la optimización del riesgo en la Universidad Estatal Amazónica? Argumente

_____
_____
_____
_____

FIRMA DEL ENCUESTADOR

Nº	ID	CATEGORIA	ACTIVOS DE INFORMACION PURA	DESCRIPCION DEL ACTIVO	CANTIDAD	IDIOMA	MEDIO DE CONSERVACION O SOPORTE	FORMA DE CONSULTA O ACCESO	FECHA DE GENERACION	CONTENEDOR	PROCESO QUE PRODUCE LA INFORMACIÓN	PROPIETARIO	CUSTODIO	RESPONSABLE TÉCNICO	AUTENTICIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	TRAZABILIDAD
ACTIVOS LÓGICOS																			
1	SA-01	Software de aplicación	Siad Pregrado	Sistema informatico para la gestión de información académica de docentes, estudiantes y area académica de las Facultades de Ciencias de la Tierra y Ciencias de la Vida	1	Español	Documentación fisica y digital	Acceso Web	2009	Servidores Datacenter Bloque D	Gestión académica Facultades	Facultad Ciencias de la Vida y Ciencias de la Tierra	Decanatos	Ing. Patricio Ochoa	Crítica	Protegida	Alto	Diaria	Si
2	SA-02	Software de aplicación	Siad Posgrado	Sistema informatico para la gestión de información académica de docentes, estudiantes y area académica de Posgrado	1	Español	Documentación fisica y digital	Acceso Web	2009	Servidores Datacenter Bloque D	Gestión académica Posgrado	Posgrado	Decano Posgrado	Ing. Patricio Ochoa	Crítica	Protegida	Alto	Diaria	Si
3	SA-03	Software de aplicación	Siad Educacion continua	Sistema informatico para la gestión de información académica de docentes, estudiantes y area académica de la Unidad de Educación Continua	1	Español	Documentación fisica y digital	Acceso Web	2009	Servidores Datacenter Bloque D	Gestión académica Educación Continua	Educación continua	Director Vibculación	Ing. Patricio Ochoa	Crítica	Protegida	Alto	Diaria	Si
4	SA-04	Software de aplicación	Sisges	Sistema informático para la gestión documental, en el area fianciera, planificación, compras publicas y diferentes dependencias relacionadas a la adquisición de bienes y servicios	1	Español	Documentación fisica y digital	Acceso Web	2009	Servidores Datacenter Bloque D	Gestión documental, proceso de compras publicas	Planificación, Financiero, Compras publicas	Director Planificación Director Financiero	Ing. Gustavo Fernandez	Crítica	Protegida	Alto	Diaria	Si
5	SA-05	Software de aplicación	SITIC	Sistemas informático para la gestión de tecnologías de la información	1	Español	Documentación fisica y digital	Acceso Web	2018	Servidores Datacenter Bloque D	Gestión de Tecnologías de la Información	Tecnologías de la Información	Director Gestión de TIC	Ing. Gustavo Fernandez	Crítica	Protegida	Alto	Diaria	Si
6	SA-06	Software de aplicación	Entorno Virtual de Aprendizaje	Aplicación para la despliegue de entornos virtuales de aprendizaje	4	Español	Docmentación digital	Acceso Web	2009	Servidores Datacenter Bloque D	Gestión docente	Docentes	Ing. Verónica Villarreal	Ing. Verónica Villarreal	Critica	Protegida	Alto	Diaria	Si
7	SA-07	Software de aplicación	Balcon de servicios	Sistemas informático para la gestión de becas y seguimiento esudiantil relacionado a bienestar universitario	1	Español	Documentación fisica y digital	Acceso Web	2009	Servidores Datacenter Bloque D	Gestión de becas y bienestar universitario	Bienestar Universitario	Director DBU	Ing. Gustavo Fernandez	Crítica	Protegida	Alto	Diaria	Si
8	SO-01	Sistema Operativo	Sistema Operativo de Equipos de escritorio	Información alojada en los equipos de escritorio de las diferentes dependencias de la UEA, Campus Central y extensiones	465	Español	Documentación digital	Remoto	2019	Servidores Datacenter Bloque D	Gestión docente y administrativa	Usuario Final	Usuario Final	Ing. Verónica Villarreal Ing. Gustavo Fernández Sr. Bladimir Asas	Crítica	Protegida	Alto	Diaria	Si
9	SO-02	Sistema Operativo	Sistema Operativo de Servidores	Información alojada en los equipos servidores de la UEA, Campus Central y extensiones	15	Español	Documentación digital	Remoto	2016	Servidores Datacenter Bloque D	Gestión de Tecnologías de la Información	Tecnologías de la Información	Ing. Gustavo Fernández	Ing. Gustavo Fernández	Crítica	Protegida	Alto	Diaria	Si
10	SO-03	Sistema Operativo	Sistema Operativo de Dispositios de red (Switch, AP, router)	Configuraciones y trafico de información de los equipos de red de la UEA, Campus Central y extensiones	32	Español	Documentación digital	Remoto	2009	Servidores Datacenter Bloque D	Gestión de Tecnologías de la Información	Tecnologías de la Información	Ing. Gustavo Fernández	Ing. Gustavo Fernández	Crítica	Protegida	Alto	Diaria	Si
11	DG-01	Datos digitales	Datos personales (Directorio Activo)	Datos personales administrados en el Directorio de Dominio institucional	5200	Español	Documentación digital	Acceso Web	2017	Servidores Datacenter Bloque D	Gestión de Tecnologías de la Información	Tecnologías de la Información	Ing. Gustavo Fernandez	Ing. Gustavo Fernandez	Crítica	Protegida	Alto	Diaria	Si
12	DG-02	Datos digitales	Correo electronico	Información de envio y recepción de correos electrónicos	5200	Español	Documentación digital	Acceso Web	2017	Servidores Datacenter Bloque D	Gestión de Tecnologías de la Información	Tecnologías de la Información	Ing. Gustavo Fernandez	Ing. Gustavo Fernandez	Crítica	Protegida	Alto	Diaria	Si
13	DG-03	Datos digitales	Gestor de copia de seguridad	Almacenamiento de backup de imágenes y configuración de servicios	32	Español	Documentación digital	Acceso Web	2017	Servidores Datacenter Bloque D	Gestión de Tecnologías de la Información	Tecnologías de la Información	Ing. Gustavo Fernandez	Ing. Gustavo Fernandez	Crítica	Protegida	Alto	Diaria	Si
14	DG-04	Datos digitales	Gestor de base de datos	Administración de base de datos	7	Español	Documentación digital	Acceso Web	2017	Servidores Datacenter Bloque D	Gestión de Tecnologías de la Información	Tecnologías de la Información	Ing. Gustavo Fernandez	Ing. Gustavo Fernandez	Crítica	Protegida	Alto	Diaria	Si
15	DG-05	Datos digitales	Gestor de virtualización	Administración de virtualización	32	Español	Documentación digital	Acceso Web	2017	Servidores Datacenter Bloque D	Gestión de Tecnologías de la Información	Tecnologías de la Información	Ing. Gustavo Fernandez	Ing. Gustavo Fernandez	Crítica	Protegida	Alto	Diaria	Si
ACTIVOS FÍSICOS																			
16	DOC-01	Documentación	Cartera de proyectos	Documentación de etapas de proyectos de tecnologías de la Información	40	Español	Documentación fisica y digital	Acceso Web	2017	Unidad de Tecnologías de la Información y Comunicación	Gestión de Tecnologías de la Información	Tecnologías de la Información	Ing. Verónica Villarreal	Ing. Verónica Villarreal	Crítica	Restringida	Alto	Semanal	Si
17	DOC-02	Documentación	Gestión de Tecnologías	Documentación realcionada a la gestión de TI, servicios, equipamiento, licencias entre otros	6	Español	Documentación fisica y digital	Acceso Web	2018	Unidad de Tecnologías de la Información y Comunicación	Gestión de Tecnologías de la Información	Tecnologías de la Información	Ing. Verónica Villarreal	Ing. Verónica Villarreal	Crítica	Restringida	Alto	Semanal	Si
18	INF-TI-01	Infraestructura de TI	Centro de datos	Espacio físico, donde se alojan los equipos servidores, y core de distribuidores.	1	Español	Espaco físico	Acceso Biométrico	2009	Unidad de Tecnologías de la Información y Comunicación	Gestión de Tecnologías de la Información	Tecnologías de la Información	Ing. Bernabé Ortega	Ing. Gustavo Fernández Ing. Verónica Villarreal	Crítica	Protegida	Alto	Inmediata	Si
19	INF-TI-02	Infraestructura de TI	Rack de comunicaciones	Espacio físico, donde se alojan los equipos de comutación de datos.	12	Español	Espaco físico	Acceso con lleva de seguridad	2009	Unidad de Tecnologías de la Información y Comunicación	Gestión de Tecnologías de la Información	Tecnologías de la Información	Ing. Gustavo Fernandez	Ing. Gustavo Fernández Ing. Verónica Villarreal	Crítica	Protegida	Alto	Inmediata	Si
20	INF-TI-03	Infraestructura de TI	Oficina DGTIC	Espacio físico, donde se aloja, documentación y equipos de administración	1	Español	Espaco físico	Acceso con lleva de seguridad	2009	Unidad de Tecnologías de la Información y Comunicación	Gestión de Tecnologías de la Información	Tecnologías de la Información	Sr. Carlos Gavidia	Ing. Gustavo Fernandez	Crítica	Protegida	Alto	Inmediata	Si
21	CE-01	Controles de entorno TI	Equipos de alarma	Sistema de detección movimiento en el Centro de Datos y oficina UTIC	2	Español	Control de entorno TI	Físico	2009	Datacenter Bloque D	Gestión de Tecnologías de la Información	Tecnologías de la Información	Sr. Cristian Arciniega	Sr. Cristian Arciniega	Crítica	Protegida	Alto	Inmediata	Si

22	CE-02	Controles de entorno TI	Supresion contra incendio	Sistema de supresión de incendio, activación de ductos de agua para el Centro de datos	1	Español	Control de entorno TI	Físico	2009	Datacenter Bloque D	Gestión de Tecnologías de la Información	Tecnologías de la Información	Sr. Cristian Arciniega	Sr. Cristian Arciniega	Crítica	Protegida	Alto	Inmediata	Si
23	CE-03	Controles de entorno TI	Sistema de alimentación ininterrumpida	Sistema de respaldo de energia, que permite la alimentación de energia electrica	1	Español	Control de entorno TI	Físico	2009	Datacenter Bloque D	Gestión de Tecnologías de la Información	Tecnologías de la Información	Sr. Cristian Arciniega	Sr. Cristian Arciniega	Crítica	Protegida	Alto	Inmediata	Si
24	CE-04	Controles de entorno TI	Aire acondicionado	Sistema de climatización presurizada para el Centro de datos	1	Español	Control de entorno TI	Físico	2009	Datacenter Bloque D	Gestión de Tecnologías de la Información	Tecnologías de la Información	Sr. Cristian Arciniega	Sr. Cristian Arciniega	Crítica	Protegida	Alto	Inmediata	Si
25	CE-05	Controles de entorno TI	Deshumificador	Sistema de control de humedad para el Centro de datos	1	Español	Control de entorno TI	Físico	2009	Datacenter Bloque D	Gestión de Tecnologías de la Información	Tecnologías de la Información	Sr. Cristian Arciniega	Sr. Cristian Arciniega	Crítica	Protegida	Alto	Inmediata	Si
26	HW-01	Hardware de TI	Dispositivos de almacenamiento	Equipos de almacenamiento de información sensible de la UEA, ubicado en el Centro de datos	2	Español	Hardware de TI	Cuenta de administración	2009	Datacenter Bloque D	Gestión de Tecnologías de la Información	Tecnologías de la Información	Ing. Gustavo Fernández	Ing. Gustavo Fernández	Crítica	Protegida	Alto	Inmediata	Si
27	HW-02	Hardware de TI	Ordenadores de escritorio	Estaciones de trabajo para usuario final, procesamiento y almacenamiento de información	465	Español	Hardware de TI	Cuenta de administración	2009	Datacenter Bloque D	Usuario Final	Usuario Final	Usuario Final	Ing. Bernabe Ortega Ing. Rafael De la Torre Sr. Bladimir Asas	Crítica	Protegida	Alto	Inmediata	Si
28	HW-03	Hardware de TI	Ordenadores portatiles, tablet y celulares	Equipos portátiles para usuario final, procesamiento y almacenamiento de información	20	Español	Hardware de TI	Cuenta de administración	2009	Datacenter Bloque D	Usuario Final	Usuario Final	Usuario Final	Ing. Bernabe Ortega Ing. Rafael De la Torre Sr. Bladimir Asas	Crítica	Protegida	Alto	Inmediata	Si
29	HW-04	Hardware de TI	Dispositivos de comunicación	Equipos de comutación de red, access point, entre otros	32	Español	Hardware de TI	Cuenta de administración	2009	Datacenter Bloque D	Gestión de Tecnologías de la Información	Tecnologías de la Información	Ing. Gustavo Fernández	Ing. Gustavo Fernández Ing. Verónica Villarreal	Crítica	Protegida	Alto	Inmediata	Si
30	HW-05	Hardware de TI	Equipos de impresión	Equipos de impresión en red, ubicadas en as diferentes dependencias	104	Español	Hardware de TI	Cuenta de administración	2009	Datacenter Bloque D	Usuario Final	Usuario Final	Usuario Final	Ing. Bernabe Ortega	Crítica	Protegida	Alto	Inmediata	Si
31	SERV-01	Servicio de TI	Servicio de autenticación de usuario	Autenticación de usuario a traves de dominio uea.edu.ec	1	Español	Servicio de TI	Cuenta de administración	2017	Servidores Datacenter Bloque D	Gestión de Tecnologías de la Información	Tecnologías de la Información	Ing. Gustavo Fernández	Ing. Gustavo Fernández	Crítica	Protegida	Alto	Inmediata	Si
32	SERV-02	Servicio de TI	Cortafuego	Software que permite gestionar y filtrar el trafico entrante y saliente de la red	1	Español	Servicio de TI	Cuenta de administración	2017	Servidores Datacenter Bloque D	Gestión de Tecnologías de la Información	Tecnologías de la Información	Ing. Gustavo Fernández	Ing. Gustavo Fernández	Crítica	Protegida	Alto	Inmediata	Si
33	SERV-03	Servicio de TI	Servidor Proxy	Software que se usan como un puente entre el origen y el destino de una solicitud	1	Español	Servicio de TI	Cuenta de administración	2009	Servidores Datacenter Bloque D	Gestión de Tecnologías de la Información	Tecnologías de la Información	Ing. Gustavo Fernández	Ing. Gustavo Fernández	Crítica	Protegida	Alto	Inmediata	Si
34	SERV-04	Servicio de TI	Servicio de red	Red interna de cableado estructurado que permite la conexión de toda la infraestructura de TI en el campus principal y sedes académicas	4	Español	Servicio de TI	Cuenta de administración	2009	Servidores Datacenter Bloque D	Gestión de Tecnologías de la Información	Tecnologías de la Información	Ing. Gustavo Fernández	Ing. Gustavo Fernández	Crítica	Protegida	Alto	Inmediata	Si
35	SERV-05	Servicio de TI	Servicio de red inalambrico	Red internade conexión analámbrica que permite la conexión de toda la infraestructura de TI en el campus principal y sedes académicas	4	Español	Servicio de TI	Cuenta de administración	2009	Servidores Datacenter Bloque D	Gestión de Tecnologías de la Información	Tecnologías de la Información	Ing. Gustavo Fernández	Ing. Gustavo Fernández	Crítica	Protegida	Alto	Inmediata	Si
36	SERV-06	Servicio de TI	Antivirus	Sistema de detección de amanezas e infección de softawre malicioso en equipos de ususario final	1	Español	Servicio de TI	Cuenta de administración	2009	Servidores Datacenter Bloque D	Gestión de Tecnologías de la Información	Tecnologías de la Información	Ing. Gustavo Fernández	Ing. Gustavo Fernández	Crítica	Protegida	Alto	Inmediata	Si
37	SERV-07	Servicio de TI	Sistema de monitoreo de redes	Zabbix Sistema de monitoreo de red interna y servidores	1	Español	Servicio de TI	Acceso Web	2009	Servidores Datacenter Bloque D	Gestión de Tecnologías de la Información	Tecnologías de la Información	Ing. Gustavo Fernández	Ing. Gustavo Fernández	Crítica	Protegida	Alto	Inmediata	Si
38	SERV-08	Servicio de TI	VPN - enlaces de datos	Enlaces troncaes que permites la conectividad entre el campus principal y las sedes académicas	4	Español	Servicio de TI	Acceso Web	2009	Servidores Datacenter Bloque D	Gestión de Tecnologías de la Información	Tecnologías de la Información	Ing. Gustavo Fernández	Ing. Gustavo Fernández	Crítica	Protegida	Alto	Inmediata	Si
39	SERV-09	Servicio de TI	Sistema de Telefonía	Servicio de telefonía de VoIP para el campus principal y sedes académicas	4	Español	Servicio de TI	Acceso Web	2009	Servidores Datacenter Bloque D	Gestión de Tecnologías de la Información	Tecnologías de la Información	Ing. Gustavo Fernández	Ing. Gustavo Fernández	Crítica	Protegida	Alto	Inmediata	Si
40	SERV-10	Servicio de TI	Servicio Web	Serviciso de acceso web a información isntitucional y acceso a aplicativos universitarios	1	Español	Servicio de TI	Acceso Web	2009	Servidores Datacenter Bloque D	Gestión de Tecnologías de la Información	Tecnologías de la Información	Ing. Gustavo Fernández	Ing. Gustavo Fernández	Crítica	Protegida	Alto	Inmediata	Si
ACTIVO HUMANO																			
41	TH-I-01	Talento Humano Internos	Personal administrativo y trabajadores	Personal que labora en la institución	140	Español	Talento Humano	Físco		Talento Humano	Talento Humano	Talento Humano	Talento Humano	Talento Humano	Normal	Libre	Normal	Diaria	No
42	TH-I-02	Talento Humano Internos	Autoridades y directores	Autoridades y directores de la institución	10	Español	Talento Humano	Físco		Talento Humano	Talento Humano	Talento Humano	Talento Humano	Talento Humano	Normal	Libre	Normal	Diaria	No
43	TH-I-03	Talento Humano Internos	Docentes	Docentes que laboran en la institución	150	Español	Talento Humano	Físco		Talento Humano	Talento Humano	Talento Humano	Talento Humano	Talento Humano	Normal	Libre	Normal	Diaria	No
44	TH-I-04	Talento Humano Internos	Estudiantes	Estudiantes que cursan sus estudios en la institución	4800	Español	Talento Humano	Físco		Talento Humano	Talento Humano	Talento Humano	Talento Humano	Talento Humano	Normal	Libre	Normal	Diaria	No
45	TH-E-01	Talento Humano Externos	Contratistas	Personal de transito temporal, mientras dure su relacion con la UEA	5	Español	Talento Humano	Físco		Talento Humano	Talento Humano	Talento Humano	Talento Humano	Talento Humano	Normal	Libre	Normal	Diaria	No
46	TH-E-02	Talento Humano Externos	Proveedores	Personal de transito temporal, mientras dure su relacion con la UEA	2	Español	Talento Humano	Físco		Talento Humano	Talento Humano	Talento Humano	Talento Humano	Talento Humano	Normal	Libre	Normal	Diaria	No
47	TH-E-03	Talento Humano Externos	Visitantes temporales	Personal de transito temporal en la UEA	100	Español	Talento Humano	Físco		Talento Humano	Talento Humano	Talento Humano	Talento Humano	Talento Humano	Normal	Libre	Normal	Diaria	No

Nº	ID	CATEGORIA	ACTIVOS DE INFORMACION PUR/	DESCRIPCION DEL ACTIVO	CANTIDAD	RESPONSABLE ANALISIS DE RIESGC	ID RIESGO	AMENAZAS	PROBABILIDAD	IMPACTO	RIESGO	CALIFICACION D RIESGC	SALVAGUARDAS	TRATAMIENTO DEL RIESGO	FECHA DE ULTIMA REVISION
ACTIVOS LÓGICOS															
1	SA-01	Software de aplicación	Siad Pregrado	Sistema informatico para la gestión de información académica de docentes, estudiantes y area académica de las Facultades de Ciencias de la Tierra y Cienci de la Vida	1	Ing. Verónica Villarreal	R1	Introducción de falsa información	2	3	6	ASUMIBLE	Filtros de validación	Mitigación del riesgo	20/09/2022
							R2	Fallo de servicios de comunicacione	1	4	4	ASUMIBLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
							R3	Degradación de los soportes de almacenamiento de la información	2	5	10	APRECIABLE	Backups diarios	Mitigación del riesgo	20/09/2022
							R4	Indisponibilidad del personal	3	5	15	GRAVE	Capacitación a más de 1 funcionario	Transferencia de riesgo	20/09/2022
							R5	Errores de los usuarios	3	4	12	GRAVE	Capacitación usuario	Transferencia de riesgo	20/09/2022
							R6	Errores de configuración	1	4	4	ASUMIBLE	Control de Pruebas en desarrollo y parametrizacion de SW	Transferencia de riesgo	20/09/2022
2	SA-02	Software de aplicación	Siad Posgrado	Sistema informatico para la gestión de información académica de docentes, estudiantes y area académica de Posgrad	1	Ing. Verónica Villarreal	R1	Introducción de falsa información	2	3	6	ASUMIBLE	Filtros de validación	Mitigación del riesgo	20/09/2022
							R2	Fallo de servicios de comunicacione	1	4	4	ASUMIBLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
							R3	Degradación de los soportes de almacenamiento de la información	2	5	10	APRECIABLE	Backups diarios	Mitigación del riesgo	20/09/2022
							R4	Indisponibilidad del personal	3	5	15	GRAVE	Capacitación a más de 1 funcionario	Transferencia de riesgo	20/09/2022
							R5	Errores de los usuarios	3	4	12	GRAVE	Capacitación usuario	Transferencia de riesgo	20/09/2022
							R6	Errores de configuración	1	4	4	ASUMIBLE	Control de Pruebas en desarrollo y parametrizacion de SW	Transferencia de riesgo	20/09/2022
3	SA-03	Software de aplicación	Siad Educacion continua	Sistema informatico para la gestión de información académica de docentes, estudiantes y area académica de la Unidad de Educación Continua	1	Ing. Verónica Villarreal	R1	Introducción de falsa información	2	3	6	ASUMIBLE	Filtros de validación	Mitigación del riesgo	20/09/2022
							R2	Fallo de servicios de comunicacione	1	4	4	ASUMIBLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
							R3	Degradación de los soportes de almacenamiento de la información	2	5	10	APRECIABLE	Backups diarios	Mitigación del riesgo	20/09/2022
							R4	Indisponibilidad del personal	3	5	15	GRAVE	Capacitación a más de 1 funcionario	Transferencia de riesgo	20/09/2022
							R5	Errores de los usuarios	3	4	12	GRAVE	Capacitación usuario	Transferencia de riesgo	20/09/2022
							R6	Errores de configuración	1	4	4	ASUMIBLE	Control de Pruebas en desarrollo y parametrizacion de SW	Transferencia de riesgo	20/09/2022
4	SA-04	Software de aplicación	Sisges	Sistema informático para la gestión documental, en el area fiannciera, planificación, compras publicas y diferentes dependencias relacionadas a la adquisición de bienes y servicios	1	Ing. Verónica Villarreal	R1	Fuga de información	2	3	6	ASUMIBLE	Firma de contratos de confidencialidad	Aceptación de riesgo	20/09/2022
							R2	Introducción de falsa información	2	3	6	ASUMIBLE	Filtros de validación	Mitigación del riesgo	20/09/2022
							R3	Fallo de servicios de comunicacione	1	4	4	ASUMIBLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
							R4	Degradación de los soportes de almacenamiento de la información	2	5	10	APRECIABLE	Backups diarios	Mitigación del riesgo	20/09/2022
							R5	Caída del sistema por sobrecarga	2	4	8	ASUMIBLE	Balanceo de carga y monitoreo de servicios	Mitigación del riesgo	20/09/2022
							R6	Indisponibilidad del personal	3	5	15	GRAVE	Capacitación a más de 1 funcionario	Transferencia de riesgo	20/09/2022
							R7	Errores de los usuarios	3	3	9	APRECIABLE	Capacitación usuario	Transferencia de riesgo	20/09/2022
		Software de		Sistemas informático para la gestión de			R1	Introducción de falsa información	2	3	6	ASUMIBLE	Filtros de validación	Mitigación del riesgo	20/09/2022
							R2	Fallo de servicios de comunicacione	1	4	4	ASUMIBLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
							R3	Degradación de los soportes de almacenamiento de la información	2	5	10	APRECIABLE	Backups diarios	Mitigación del riesgo	20/09/2022

5	SA-05	aplicación	SITIC	tecnologías de la información	1	Ing. Verónica Villarrea	R4	Caída del sistema por sobrecarga	2	4	8	ASUMIBLE	Balanceo de carga y monitoreo de servicios	Mitigación del riesgo	20/09/2022
							R5	Indisponibilidad del personal	3	3	9	APRECIABLE	Capacitación a más de 1 funcionario	Transferencia de riesgo	20/09/2022
							R6	Errores de los usuarios	3	3	9	APRECIABLE	Capacitación usuario	Transferencia de riesgo	20/09/2022
6	SA-06	Software de aplicación	Entorno Virtual de Aprendizaje	Aplicación para la despliegue de entornos virtuales de aprendizaje	4	Ing. Verónica Villarreal	R1	Fallo de servicios de comunicaciones	1	4	4	ASUMIBLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
							R2	Degradación de los soportes de almacenamiento de la información	2	5	10	APRECIABLE	Backups diarios	Mitigación del riesgo	20/09/2022
							R3	Caída del sistema por sobrecarga	2	4	8	ASUMIBLE	Balanceo de carga y monitoreo de servicios	Mitigación del riesgo	20/09/2022
							R4	Errores de los usuarios	3	3	9	APRECIABLE	Capacitación usuario	Transferencia de riesgo	20/09/2022
							R5	Errores de configuración	2	2	4	ASUMIBLE	Control de Pruebas en desarrollo y parametrizacion de SW	Transferencia de riesgo	20/09/2022
7	SA-07	Software de aplicación	Balcon de servicios	Sistemas informático para la gestión de becas y seguimiento esudiantil relacionado a bienestar universitario	1	Ing. Verónica Villarreal	R1	Fuga de información	2	3	6	ASUMIBLE	Firma de contratos de c	Aceptación de riesgo	20/09/2022
							R2	Introducción de falsa información	2	3	6	ASUMIBLE	Filtros de validación	Mitigación del riesgo	20/09/2022
							R3	Fallo de servicios de comunicaciones	1	4	4	ASUMIBLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
							R4	Degradación de los soportes de almacenamiento de la información	2	5	10	APRECIABLE	Backups diarios	Mitigación del riesgo	20/09/2022
							R5	Caída del sistema por sobrecarga	2	4	8	ASUMIBLE	Balanceo de carga y monitoreo de servicios	Mitigación del riesgo	20/09/2022
							R6	Indisponibilidad del personal	3	3	9	APRECIABLE	Capacitación a más de 1 funcionario	Transferencia de riesgo	20/09/2022
							R7	Errores de los usuarios	3	3	9	APRECIABLE	Capacitación usuario	Transferencia de riesgo	20/09/2022
8	SO-01	Sistema Operativo	Sistema Operativo de Equipos de escritorio	Información alojada en los equipos de escritorio de las diferentes dependencias de la UEA, Campus Central y extensiones	465	Ing. Verónica Villarreal	R1	Fuga de información	1	1	1	ASUMIBLE	Firma de contratos de confidencialidad	Aceptación de riesgo	20/09/2022
							R2	Destrucción de información	3	5	15	GRAVE	Backups	Mitigación del riesgo	20/09/2022
							R3	Interceptación de información (escucha)	2	3	6	ASUMIBLE	Segmentación de red, VLAN	Mitigación del riesgo	20/09/2022
							R4	Corte del suministro eléctrico	2	2	4	ASUMIBLE	Planta de energía eléctrica	Mitigación del riesgo	20/09/2022
							R5	Interrupción de otros servicios y suministros esenciales	1	4	4	ASUMIBLE	Monitoreo de Servicio	Aceptación de riesgo	20/09/2022
							R6	Degradación de los soportes de almacenamiento de la información	2	5	10	APRECIABLE	Backups	Mitigación del riesgo	20/09/2022
							R7	Difusión de software dañino	2	4	8	ASUMIBLE	Sistema Antivirus actualizados y capacitacion a usuario final	Mitigación del riesgo	20/09/2022
							R8	Abuso de privilegios de acceso	2	3	6	ASUMIBLE	Capacitacion a usuario final	Aceptación de riesgo	20/09/2022
							R9	Errores de los usuarios	3	3	9	APRECIABLE	Capacitación usuario	Transferencia de riesgo	20/09/2022
							R10	Ingeniería social	3	4	12	GRAVE	Definición de roles y Capacitación usuario	Aceptación de riesgo	20/09/2022
9	SO-02	Sistema Operativo	Sistema Operativo de Servidores	Información alojada en los equipos servidores de la UEA, Campus Central y extensiones	15	Ing. Verónica Villarreal	R1	Interceptación de información (escucha)	2	3	6	ASUMIBLE	Segmentación de red, VLAN	Mitigación del riesgo	20/09/2022
							R2	Corte del suministro eléctrico	3	3	9	APRECIABLE	Planta de energía eléctrica	Mitigación del riesgo	20/09/2022
							R3	Interrupción de otros servicios y suministros esenciales	2	3	6	ASUMIBLE	Monitoreo de Servicio	Aceptación de riesgo	20/09/2022
							R4	Degradación de los soportes de almacenamiento de la información	2	5	10	APRECIABLE	Backups	Mitigación del riesgo	20/09/2022
							R5	Difusión de software dañino	2	4	8	ASUMIBLE	Sistema Antivirus actualizados y capacitacion a usuario final	Mitigación del riesgo	20/09/2022
							R6	Errores de mantenimiento / actualización de programas (software)	2	3	6	ASUMIBLE	Plan de mantenimiento	Mitigación del riesgo	20/09/2022

							R7	Caída del sistema por sobrecarga	2	3	6	ASUMIBLE	Balanceo de carga y monitoreo de servicios	Mitigación del riesgo	20/09/2022
							R8	Errores de configuración	2	3	6	ASUMIBLE	Control de Pruebas en desarrollo y parametrizacion de SW	Transferencia de riesgo	20/09/2022
10	SO-03	Sistema Operativo	Sistema Operativo de Dispositios de red (Switch, AP, router)	Configuraciones y trafico de información de los equipos de red de la UEA, Campus Central y extensiones	32	Ing. Verónica Villarreal	R1	Interceptación de información (escucha)	2	4	8	ASUMIBLE	Segmentación de red, VLAN	Mitigación del riesgo	20/09/2022
							R2	Corte del suministro eléctrico	3	3	9	APRECIABLE	Planta de energía eléctrica	Mitigación del riesgo	20/09/2022
							R3	Interrupción de otros servicios y suministros esenciales	3	3	9	APRECIABLE	Monitoreo de Servicio	Aceptación de riesgo	20/09/2022
							R4	Degradación de los soportes de almacenamiento de la información	2	4	8	ASUMIBLE	Backups	Mitigación del riesgo	20/09/2022
							R5	Difusión de software dañino	2	5	10	APRECIABLE	Sistema Antivirus actualizados y capacitacion a usuario final	Mitigación del riesgo	20/09/2022
							R6	Errores de mantenimiento / actualización de programas (software)	2	5	10	APRECIABLE	Plan de mantenimiento	Mitigación del riesgo	20/09/2022
							R7	Caída del sistema por sobrecarga	2	5	10	APRECIABLE	Balanceo de carga y monitoreo de servicios	Mitigación del riesgo	20/09/2022
							R8	Errores de configuración	2	5	10	APRECIABLE	Control de Pruebas en desarrollo y parametrizacion de SW	Transferencia de riesgo	20/09/2022
11	DG-01	Datos digitales	Datos personales (Directorio Activo)	Datos personales administrados en el Directorio de Dominio institucional	5200	Ing. Verónica Villarreal	R1	Fallo de servicios de comunicaciones	2	4	8	ASUMIBLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
							R2	Interrupción de otros servicios y suministros esenciales	3	4	12	GRAVE	Monitoreo de Servicio	Aceptación del riesgo	20/09/2022
							R3	Degradación de los soportes de almacenamiento de la información	2	4	8	ASUMIBLE	Backups diarios	Mitigación del riesgo	20/09/2022
							R4	Caída del sistema por sobrecarga	2	4	8	ASUMIBLE	Balanceo de carga y monitoreo de servicios	Mitigación del riesgo	20/09/2022
							R5	Indisponibilidad del personal	2	4	8	ASUMIBLE	Capacitación a más de 1 funcionario	Transferencia de riesgo	20/09/2022
							R6	Errores de configuración	2	4	8	ASUMIBLE	Capacitación usuario	Transferencia de riesgo	20/09/2022
12	DG-02	Datos digitales	Correo electronico	Información de envio y recepción de correos electrónicos	5200	Ing. Verónica Villarreal	R1	Fallo de servicios de comunicaciones	2	3	6	ASUMIBLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
							R2	Interrupción de otros servicios y suministros esenciales	2	3	6	ASUMIBLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
							R3	Caída del sistema por sobrecarga	2	3	6	ASUMIBLE	Balanceo de carga y monitoreo de servicios	Mitigación del riesgo	20/09/2022
							R4	Indisponibilidad del personal	2	4	8	ASUMIBLE	Capacitación a más de 1 funcionario	Transferencia de riesgo	20/09/2022
13	DG-03	Datos digitales	Gestor de copia de seguridad	Almacenamiento de backup de imágenes y configuración de servicios	32	Ing. Verónica Villarreal	R1	Fallo de servicios de comunicaciones	2	3	6	ASUMIBLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
							R2	Interrupción de otros servicios y sur	2	3	6	ASUMIBLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
							R3	Caída del sistema por sobrecarga	2	3	6	ASUMIBLE	Balanceo de carga y monitoreo de servicios	Mitigación del riesgo	20/09/2022
							R4	Indisponibilidad del personal	2	4	8	ASUMIBLE	Capacitación a más de 1 funcionario	Transferencia de riesgo	20/09/2022
14	DG-04	Datos digitales	Gestor de base de datos	Administración de base de datos	7	Ing. Verónica Villarreal	R1	Fallo de servicios de comunicaciones	2	3	6	ASUMIBLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
							R2	Interrupción de otros servicios y sur	2	3	6	ASUMIBLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
							R3	Caída del sistema por sobrecarga	2	3	6	ASUMIBLE	Balanceo de carga y monitoreo de servicios	Mitigación del riesgo	20/09/2022

							R4	Indisponibilidad del personal	2	4	8	ASUMIBLE	Capacitación a más de 1 funcionario	Transferencia de riesgo	20/09/2022
15	DG-05	Datos digitales	Gestor de virtualización	Administración de virtualización	32	Ing. Verónica Villarreal	R1	Fallo de servicios de comunicacione	2	3	6	ASUMIBLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
							R2	Interrupción de otros servicios y sur	2	3	6	ASUMIBLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
							R3	Caída del sistema por sobrecarga	2	3	6	ASUMIBLE	Balanceo de carga y monitoreo de servicios	Mitigación del riesgo	20/09/2022
							R4	Indisponibilidad del personal	2	4	8	ASUMIBLE	Capacitación a más de 1 funcionario	Transferencia de riesgo	20/09/2022
ACTIVOS FÍSICOS															
16	DOC-01	Documentación	Cartera de proyectos	Documentación de etapas de proyectos de tecnologías de la Información	40	Ing. Verónica Villarreal	R1	Fuga de información	**2**	**3**	6	ASUMIBLE	Firma de contratos de confidencialidad	Aceptación de riesgo	20/09/2022
							R2	Indisponibilidad del personal	**2**	**4**	8	ASUMIBLE	Capacitación a más de 1 funcionario	Transferencia de riesgo	20/09/2022
							R3	Corrupción de la información	2	4	8	ASUMIBLE	Encryptación de información sensible	Mitigación del riesgo	20/09/2022
17	DOC-02	Documentación	Gestión de Tecnologías	Documentación realcionada a la gestión de TI, servicios, equipamiento, licencias entre otros	6	Ing. Verónica Villarreal	R1	Fuga de información	**2**	**3**	6	ASUMIBLE	Firma de contratos de confidencialidad	Aceptación de riesgo	20/09/2022
							R2	Indisponibilidad del personal	**2**	**4**	8	ASUMIBLE	Capacitación a más de 1 funcionario	Transferencia de riesgo	20/09/2022
							R3	Corrupción de la información	2	4	8	ASUMIBLE	Encryptación de información sensible	Mitigación del riesgo	20/09/2022
18	INF-TI-01	Infraestructura de TI	Centro de datos	Espacio físico, donde se alojan los equipos servidores, y core de distribuidores.	1	Ing. Verónica Villarreal	R1	Fuego	2	5	10	APRECIABLE	Sistema de incendios activado y funcional	Mitigación del riesgo	20/09/2022
							R2	Desastres Naturales	2	5	10	APRECIABLE	Centro de Datos de replicación	Aceptación del riesgo	20/09/2022
							R3	Condiciones inadecuadas de temperatura o humedad	2	4	8	ASUMIBLE	Sistema de control de temperatura y humedad	Mitigación del riesgo	20/09/2022
							R4	Fallo de servicios de comunicacione	2	5	10	APRECIABLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
							R5	Corte del suministro eléctrico	2	5	10	APRECIABLE	Planta de energía eléctrica	Mitigación del riesgo	20/09/2022
19	INF-TI-02	Infraestructura de TI	Rack de comunicaciones	Espacio físico, donde se alojan los equipos de comutación de datos.	12	Ing. Verónica Villarreal	R1	Fuego	2	5	10	APRECIABLE	Sistema de incendios activado y funcional	Mitigación del riesgo	20/09/2022
							R2	Desastres Naturales	2	5	10	APRECIABLE	Infraestructura nueva	Aceptación del riesgo	20/09/2022
							R3	Condiciones inadecuadas de temperatura o humedad	2	4	8	ASUMIBLE	Sistema de control de temperatura y humedad	Mitigación del riesgo	20/09/2022
							R4	Fallo de servicios de comunicacione	2	5	10	APRECIABLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
20	INF-TI-03	Infraestructura de TI	Oficina DGTIC	Espacio físico, donde se aloja, documentación y equipos de administración	1	Ing. Verónica Villarreal	R1	Fuego	2	5	10	APRECIABLE	Sistema de incendios activado y funcional	Mitigación del riesgo	20/09/2022
							R2	Desastres Naturales	2	5	10	APRECIABLE	Infraestructura nueva	Aceptación del riesgo	20/09/2022
21	CE-01	Controles de entorno TI	Equipos de alarma	Sistema de detección movimiento en el Centro de Datos y oficina UTIC	2	Ing. Verónica Villarreal	R1	Fallo de servicios de comunicacione	2	5	10	APRECIABLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
							R2	Errores de configuración	2	5	10	APRECIABLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
							R3	Caída del sistema por sobrecarga	2	5	10	APRECIABLE	Plan de mantenimiento	Mitigación del riesgo	20/09/2022
22	CE-02	Controles de entorno TI	Supresion contra incendio	Sistema de supresión de incendio, activación de ductos de agua para el Centro de datos	1	Ing. Verónica Villarreal	R1	Fallo de servicios de comunicacione	2	5	10	APRECIABLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
							R2	Errores de configuración	2	5	10	APRECIABLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
							R3	Caída del sistema por sobrecarga	2	5	10	APRECIABLE	Plan de mantenimiento	Mitigación del riesgo	20/09/2022
23	CE-03	Controles de entorno TI	Sistema de alimentación ininterrumpida	Sistema de respaldo de energia, que permite la alimentación de energia electrica	1	Ing. Verónica Villarreal	R1	Fallo de servicios de comunicacione	2	5	10	APRECIABLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
							R2	Errores de configuración	2	5	10	APRECIABLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
							R3	Caída del sistema por sobrecarga	2	5	10	APRECIABLE	Plan de mantenimiento	Mitigación del riesgo	20/09/2022
24	CE-04	Controles de entorno TI	Aire acondicionado	Sistema de climatización presurizada para el Centro de datos	1	Ing. Verónica Villarreal	R1	Fallo de servicios de comunicacione	2	5	10	APRECIABLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
							R2	Errores de configuración	2	5	10	APRECIABLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
							R3	Caída del sistema por sobrecarga	2	5	10	APRECIABLE	Plan de mantenimiento	Mitigación del riesgo	20/09/2022
25	CE-05	Controles de	Deshumificador	Sistema de control de humedad para el	1	Ing. Verónica Villarrea	R1	Fallo de servicios de comunicacione	2	5	10	APRECIABLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022

		entorno TI		Centro de datos			R2	Errores de configuración	2	5	10	APRECIABLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
							R3	Caída del sistema por sobrecarga	2	5	10	APRECIABLE	Plan de mantenimiento	Mitigación del riesgo	20/09/2022
26	HW-01	Hardware de TI	Dispositivos de almacenamiento	Equipos de almacenamiento de información sensible de la UEA, ubicado en el Centro de datos	2	Ing. Verónica Villarreal	R1	Errores de configuración	2	5	10	APRECIABLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
							R2	Degradación de los soportes de almacenamiento de la información	3	5	15	GRAVE	Backup y monitoreo de servicios	Mitigación del riesgo	20/09/2022
27	HW-02	Hardware de TI	Ordenadores de escritorio	Estaciones de trabajo para usuario final, procesamiento y almacenamiento de información	465	Ing. Verónica Villarreal	R1	Errores de configuración	2	5	10	APRECIABLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
							R2	Degradación de los soportes de almacenamiento de la información	3	5	15	GRAVE	Backup y monitoreo de servicios	Mitigación del riesgo	20/09/2022
							R3	Fallo de servicios de comunicaciones	2	5	10	APRECIABLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
28	HW-03	Hardware de TI	Ordenadores portatiles, tablet y celulares	Equipos portátiles para usuario final, procesamiento y almacenamiento de información	20	Ing. Verónica Villarreal	R1	Errores de configuración	2	5	10	APRECIABLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
							R2	Degradación de los soportes de almacenamiento de la información	3	5	15	GRAVE	Backup y monitoreo de servicios	Mitigación del riesgo	20/09/2022
							R3	Fallo de servicios de comunicaciones	2	5	10	APRECIABLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
29	HW-04	Hardware de TI	Dispositivos de comunicación	Equipos de comutación de red, access point, entre otros	32	Ing. Verónica Villarreal	R1	Errores de configuración	2	5	10	APRECIABLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
							R2	Degradación de los soportes de almacenamiento de la información	3	5	15	GRAVE	Backup y monitoreo de servicios	Mitigación del riesgo	20/09/2022
							R3	Fallo de servicios de comunicaciones	2	5	10	APRECIABLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
30	HW-05	Hardware de TI	Equipos de impresión	Equipos de impresión en red, ubicadas en as diferentes dependencias	104	Ing. Verónica Villarreal	R1	Errores de configuración	2	5	10	APRECIABLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
							R2	Degradación de los soportes de almacenamiento de la información	3	5	15	GRAVE	Backup y monitoreo de servicios	Mitigación del riesgo	20/09/2022
							R3	Fallo de servicios de comunicaciones	2	5	10	APRECIABLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
31	SERV-01	Servicio de TI	Servicio de autenticación de usuario	Autenticación de usuario a traves de dominio uea.edu.ec	1	Ing. Verónica Villarreal	R1	Errores de configuración	2	5	10	APRECIABLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
							R2	Fallo de servicios de comunicaciones	2	5	10	APRECIABLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
32	SERV-02	Servicio de TI	Cortafuego	Software que permite gestionar y filtrar el trafico entrante y saliente de la red	1	Ing. Verónica Villarreal	R1	Errores de configuración	2	5	10	APRECIABLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
							R2	Fallo de servicios de comunicaciones	2	5	10	APRECIABLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
33	SERV-03	Servicio de TI	Servidor Proxy	Software que se usan como un puente entre el origen y el destino de una solicitud	1	Ing. Verónica Villarreal	R1	Errores de configuración	2	5	10	APRECIABLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
							R2	Fallo de servicios de comunicaciones	2	5	10	APRECIABLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
34	SERV-04	Servicio de TI	Servicio de red	Red interna de cableado estructurado que permite la conexión de toda la infraestructura de TI en el campus principal y sedes académicas	4	Ing. Verónica Villarreal	R1	Errores de configuración	2	5	10	APRECIABLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
							R2	Fallo de servicios de comunicaciones	2	5	10	APRECIABLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
35	SERV-05	Servicio de TI	Servicio de red inalambrico	Red internade conexión analámbrica que permite la conexión de toda la infraestructura de TI en el campus principal y sedes académicas	4	Ing. Verónica Villarreal	R1	Errores de configuración	2	5	10	APRECIABLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
							R2	Fallo de servicios de comunicaciones	2	5	10	APRECIABLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
36	SERV-06	Servicio de TI	Antivirus	Sistema de detección de amanezas infección de softawre malicioso en equipos de ususario final	1	Ing. Verónica Villarreal	R1	Errores de configuración	2	5	10	APRECIABLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
37	SERV-07	Servicio de TI	Sistema de monitoreo de redes	Zabbix Sistema de monitoreo de red interna y servidores	1	Ing. Verónica Villarreal	R1	Errores de configuración	2	5	10	APRECIABLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022

38	SERV-08	Servicio de TI	VPN - enlaces de datos	Enlaces troncaes que permites la conectividad entre el campus principal y las sedes académica	4	Ing. Verónica Villarreal	R1	Errores de configuración	2	5	10	APRECIABLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
39	SERV-09	Servicio de TI	Sistema de Telefonía	Servicio de telefonía de VoIP para el campus principal y sedes académica	4	Ing. Verónica Villarreal	R1	Errores de configuración	2	5	10	APRECIABLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
40	SERV-10	Servicio de TI	Servicio Web	Serviciso de acceso web a información isntitucional y acceso a aplicativos universitarios	1	Ing. Verónica Villarreal	R1	Errores de configuración	2	5	10	APRECIABLE	Monitoreo de Servicio	Mitigación del riesgo	20/09/2022
ACTIVO HUMANO															
41	TH-I-01	Talento Humano Internos	Personal administrativo y trabajadores	Personal que labora en la institución	140	Ing. Verónica Villarreal	R1	Errores de los usuarios	2	5	10	APRECIABLE	Capacitación constante	Mitigación del riesgo	20/09/2022
							R2	Indisponibilidad del personal	2	5	10	APRECIABLE	Capacitación a más de 1 funcionario	Mitigación del riesgo	20/09/2022
							R3	Victimas de Ingeniería social	3	4	12	GRAVE	Capacitación constante	Mitigación del riesgo	20/09/2022
	TH-I-02	Talento Humano Internos	Autoridades y directores	Autoridades y directores de la institución	10	Ing. Verónica Villarreal	R1	Victimas de Ingeniería social	3	4	12	GRAVE	Capacitación constante	Mitigación del riesgo	20/09/2022
	TH-I-03	Talento Humano Internos	Docentes	Docentes que laboran en la institución	150	Ing. Verónica Villarreal	R1	Victimas de Ingeniería social	3	4	12	GRAVE	Capacitación constante	Mitigación del riesgo	20/09/2022
	TH-I-04	Talento Humano Internos	Estudiantes	Estudiantes que cursan sus estudios en la institución	4800	Ing. Verónica Villarreal	R1	Victimas de Ingeniería social	3	4	12	GRAVE	Capacitación constante	Mitigación del riesgo	20/09/2022
	TH-E-01	Talento Humano Externos	Contratistas	Personal de transito temporal, mientras dure su relacion con la UEA	5	Ing. Verónica Villarreal	R1	Victimas de Ingeniería social	3	4	12	GRAVE	Limitar permisos y roles	Mitigación del riesgo	20/09/2022
	TH-E-02	Talento Humano Externos	Proveedores	Personal de transito temporal, mientras dure su relacion con la UEA	2	Ing. Verónica Villarreal	R1	Victimas de Ingeniería social	3	4	12	GRAVE	Limitar permisos y roles	Mitigación del riesgo	20/09/2022
	TH-E-03	Talento Humano Externos	Visitantes temporales	Personal de transito temporal en la UEA	100	Ing. Verónica Villarreal	R1	Victimas de Ingeniería social	3	4	12	GRAVE	Limitar permisos y roles	Mitigación del riesgo	20/09/2022

Oficio Nro. UEA-REC-2021-0244-OFI

Puyo, 22 de julio de 2021

Asunto: Autorización para la aplicación del trabajo de grado titulado: Implementación de Sistema de Gestión de Seguridad de la Información en la UEA.

Señorita
Verónica de las Mercedes Villarreal Morales
En su Despacho

De mi consideración:

En respuesta al Documento s/n de 20 de julio del 2021, suscrito por Usted mediante el cual solicita lo siguiente: *"Con un atento y cordial saludo me dirijo a usted con la finalidad de solicitarle de la manera más comedida, se autorice la aplicación del trabajo de grado intitulado: "Implementación de Sistema de Gestión de Seguridad de la Información en la Universidad Estatal Amazónica", el mismo que se desarrollará como parte del programa de Maestría de Tecnologías de la Información que curso en la Universidad Técnica de Ambato".*

En virtud de lo solicitado, este Rectorado autoriza la aplicación del trabajo de grado de titulación: Implementación de Sistema de Gestión de Seguridad de la Información en la UEA. del programa de Maestría de Tecnologías de la Información.

Con sentimientos de distinguida consideración.

Atentamente,

Dr. David Sancho Aguilera
RECTOR

Referencias:
- UEA-SG-2021-0171-E

Anexos:
- solicitud_titulacioÌn_uea-signed.pdf

Copia:
Señor Ingeniero
Edwin Gustavo Fernández Sánchez
Director (E) de Gestión de Tecnologías de la Información y Comunicación

Oficio Nro. UEA-REC-2021-0244-OFI

Puyo, 22 de julio de 2021

ds

Seguridad de la Información

Proyecto DGTIC

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

UNIVERSIDAD ESTATAL AMAZÓNICA
2002
VITA ET SAPIENTIA

DIRECCIÓN DE GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN		Universidad Estatal Amazónica
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LA UNIVERSIDAD ESTATAL AMAZÓNICA		
Código: DGTIC-2022-03-001	**Versión:** 1.0	**Número de Páginas:** 40
Ing. Verónica Villarreal	Elaboración de proyecto. Revisión de Proyecto. Responsable de gestión y seguimiento de resultados del Proyecto.	
Ing. Daniel Mantilla	Revisión del ítem relacionados a la Dirección de Talento Humano	
Ing. Gustavo Fernández	Aprobación. Director de Gestión de Tecnologías de la Información	

VERSIONAMIENTO

Versión del documento	Fecha de revisión (MM/AAAA)	Cambio realizado
v1.0	30 de Septiembre del 2022	Documento Inicial

ÍNDICE

1. OBJETIVOS:

El objetivo de la presente política es alcanzar un grado aceptable y sostenido de seguridad de los computadores personales, los centros de datos, de la información almacenada en ellos y el uso de los sistemas e infraestructura tecnológica, en función del perfil de riesgos tecnológicos y las vulnerabilidades, para lo cual se requiere normar los aspectos relacionados con las seguridades físicas y lógicas.

En particular, se proporciona una guía a los funcionarios de la UEA, que por la naturaleza de sus funciones manejen información perteneciente a la institución, con la finalidad de propiciar la utilización segura, eficiente y efectiva de la información a su cargo, con el fin de racionalizar y optimizar el uso de recursos y servicios tecnológicos y asegurar una mayor calidad en el desarrollo de las funciones.

2. AUDIENCIA:

Los funcionarios, docentes, estudiantes, personal externo, proveedores y todos aquellos que tengan responsabilidades sobre las fuentes, repositorios y recursos de procesamiento de la información, deben adoptar los lineamientos contenidos en el presente documento y en los documentos relacionados con él, con el fin de mantener la confidencialidad, la integridad y asegurar la disponibilidad de la información.

3. ANTECEDENTES:

El artículo 226 de la Constitución de la República del Ecuador prevé que: “Las instituciones del Estado sus organismos y dependencias, y las servidoras o servidores públicos, tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución”;

En virtud de lo establecido en el numeral 19 del artículo 66 de la Norma Suprema se dispone: “Se reconoce y garantizará a las personas: (…) El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la Ley”;

El artículo 178 del Código Orgánico Integral Penal establece: “La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años…”;

El artículo 190 ibídem señala: “La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años(…)”;

El artículo 230 del Código Orgánico Integral Penal determina: "Será sancionada con pena privativa de libertad de tres a cinco años: (…) La persona que sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible. (…)";

La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, en los artículos 2 y 44, respectivamente, reconoce ante el Estado la validez jurídica de los mensajes de datos electrónicos, así como el valor y efecto jurídicos de cualquier actividad, transacción mercantil, financiera o de servicios que se realice con los mismos por medio de redes electrónicas;

La Carta Iberoamericana de Gobierno Electrónico, en la sección 24, recomienda a los gobiernos tomar en consideración la importancia de la interoperabilidad de las comunicaciones y servicios, así como disponer las medidas necesarias, para que todas las entidades públicas, cualquiera que sea su nivel y con independencia del respeto a su autonomía, establezcan sistemas que sean interoperables;

La Ley del Sistema Nacional de Registro de Datos Públicos publicada en el Registro Oficial No. 162 de 31 de marzo de 2010, en su artículo 4, cita: *"Las instituciones del sector público y privado y las personas naturales que actualmente o en el futuro administren bases o registros de datos públicos, son responsables de la integridad, protección y control de los registros y bases de datos a su cargo. Dichas instituciones responderán por la veracidad, autenticidad, custodia y debida conservación de los registros. La responsabilidad sobre la veracidad y autenticidad de los datos registrados, es exclusiva de la o el declarante cuando esta o este provee toda la información…";*

El artículo 27 de la Ley ibídem establece: *"Las Registradoras o Registradores y máximas autoridades, a quienes se autoriza el manejo de las licencias para el acceso a los registros de datos utilizados por la ley, serán las o los responsables directos administrativa, civil y penalmente por el mal uso de las mismas";*

4. DEFINICIONES:

Activo de información: Cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios de la institución, en consecuencia, debe ser protegido.

Acuerdo de Confidencialidad: Es un documento en los que los funcionarios de la UEA o los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información de la IES, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la misma.

Análisis de riesgos de seguridad de la información: Proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

Autenticación: Es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

Ducto de comunicación: Son habitaciones donde se deberán instalar los dispositivos de comunicación y la mayoría de los cables. Al igual que los centros de cómputo, los ductos de comunicaciones deben cumplir requisitos de acceso físico, materiales de paredes, pisos y techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.

Centro de datos: Es una zona específica para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos. El centro de datos debe cumplir ciertos estándares con el fin de garantizar los controles de acceso físico, los materiales de paredes, pisos y techos, el suministro de alimentación eléctrica y las condiciones medioambientales adecuadas.

Cifrado: Es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información.

Confidencialidad: Es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.

Control: Es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.

Criptografía: Es la disciplina que agrupa a los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación no detectada, prevenir su repudio, y/o prevenir su uso no autorizado.

Custodio del activo de información: Es la Dirección organizacional o proceso, designado por los propietarios, encargado de mantener las medidas de protección establecidas sobre los activos de información confiados.

Derechos de Autor: Es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.

Disponibilidad: Es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

Equipo de cómputo: Dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.

Clasificación de la información: Directrices para catalogar la información de la entidad y hacer una distinción entre la información que es crítica y aquella que lo es menos o no lo es y, de

acuerdo con esto, establecer diferencias entre las medidas de seguridad a aplicar para preservar los criterios de confidencialidad, integridad y disponibilidad de la información

Hacking ético: Es el conjunto de actividades para ingresar a las redes de datos y voz de la institución con el objeto de lograr un alto grado de penetración en los sistemas, de forma controlada, sin ninguna intensión maliciosa, ni delictiva y sin generar daños en los sistemas o redes, con el propósito de mostrar el nivel efectivo de riesgo a lo cual está expuesta la información, y proponer eventuales acciones correctivas para mejorar el nivel de seguridad.

Incidente de Seguridad: Es un evento adverso, confirmado o bajo sospecha, que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo).

Integridad: Es la protección de la exactitud y estado completo de los activos.

Inventario de activos de información: Es una lista ordenada y documentada de los activos de información pertenecientes a la institución.

Licencia de software: Es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.

Medio removible: Es cualquier componente extraíble de hardware que sea usado para el almacenamiento de información; los medios removibles incluyen cintas, discos duros removibles, CDs, DVDs y Direcciónes de almacenamiento USB, entre otras.

Perfiles de usuario: Son grupos que concentran varios usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información a los cuales se les concede acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios cobijados dentro de él.

Propiedad intelectual: Es el reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano. Este reconocimiento es aplicable a cualquier propiedad que se considere de naturaleza intelectual y merecedora de protección, incluyendo las invenciones científicas y tecnológicas, las producciones literarias o artísticas, las marcas y los identificadores, los dibujos y modelos industriales y las indicaciones geográficas.

Propietario de la información: Es la Dirección organizacional o proceso donde se crean los activos de información.

Recursos tecnológicos: Son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre

otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo.

Registros de Auditoría: Son archivos donde son registrados los eventos que se han identificado en los sistemas de información, recursos tecnológicos y redes de datos del instituto. Dichos eventos pueden ser, entre otros, identificación de usuarios, eventos y acciones ejecutadas, terminales o ubicaciones, intentos de acceso exitosos y fallidos, cambios a la configuración, uso de utilidades y fallas de los sistemas.

Responsable por el activo de información: Es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.

SGSI: Sistema de Gestión de Seguridad de la Información.

Sistema de información: Es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por la UEA o de origen externo ya sea adquirido por la entidad como un producto estándar de mercado o desarrollado para las necesidades de ésta.

Sistemas de control ambiental: Son sistemas que utilizan la climatización, un proceso de tratamiento del aire que permite modificar ciertas características del mismo, fundamentalmente humedad y temperatura y de manera adicional, también permite controlar su pureza y su movimiento.

Software malicioso: Es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.

Terceros: Todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la entidad.

Vulnerabilidades: Son las debilidades, hoyos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por la UEA (amenazas), las cuales se constituyen en fuentes de riesgo.

5. POLÍTICA GLOBAL DE SEGURIDAD DE LA INFORMACIÓN

En la Universidad Estatal Amazónica la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de sus propiedades más significativas como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad.

Consciente de las necesidades actuales, la UEA implementa un modelo de gestión de seguridad de la información como la herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información, ayuda a la reducción de costos operativos y financieros, establece una cultura de seguridad y garantiza el cumplimiento de los requerimientos legales, contractuales, regulatorios y de negocio vigentes.

La Política de Seguridad de la Información implementada en la UEA se encuentra soportada por políticas, normas y procedimientos específicos los cuales guiarán el manejo adecuado de la información de la institución. Adicionalmente, se establecerán políticas específicas de seguridad de la información las cuales se fundamentan en los dominios y objetivos de control del Anexo A de la norma internacional ISO 27001.

El Comité de Seguridad de la UTIC tendrá la potestad de modificar la Política Global o las Políticas Específicas de Seguridad de la Información de acuerdo con las necesidades de revisión establecidas periódicamente o a la aplicabilidad de las mismas, seguido de la aprobación de Consejo Universitario de la UEA.

6. SANCIONES PARA LAS VIOLACIONES A LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Las Políticas de Seguridad de la Información pretenden instituir y afianzar la cultura de seguridad de la información entre los usuarios. Por tal razón, es necesario que las violaciones a las Políticas Seguridad de la Información sean clasificadas, con el objetivo de aplicar medidas correctivas conforme con los niveles de clasificación definidos y mitigar posibles afectaciones contra la seguridad de la información. Las medidas correctivas pueden considerar desde acciones administrativas, hasta acciones de orden disciplinario o penal, de acuerdo con las circunstancias, si así lo ameritan.

7. POLÍTICAS DE LA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

7.1. POLITICA PARA USO DE DISPOSITIVOS MOVILES

La UEA proveerá las condiciones para el manejo de los dispositivos móviles (teléfonos, inteligentes y tabletas, entre otros) institucionales y personales que hagan uso de servicios de la UEA. Así mismo, velará porque los funcionarios hagan un uso responsable de los servicios y equipos proporcionados por la entidad.

7.1.1. Normas para uso de dispositivos móviles

Normas dirigidas a la Dirección de Tecnologías de la Información:

- La Dirección de Tecnologías debe investigar y probar las opciones de protección de los dispositivos móviles institucionales y personales que hagan uso de los servicios provistos por la institución.

- La Dirección de Tecnologías debe establecer las configuraciones aceptables para los dispositivos móviles institucionales que hagan uso de los servicios provistos por la IES.

- La Dirección de Tecnologías debe establecer un método de bloqueo (por ejemplo, contraseñas, biométricos, patrones, reconocimiento de voz) para los dispositivos móviles institucionales que serán entregados a los usuarios.
- La Dirección de Tecnologías debe activar la opción de cifrado de la memoria de almacenamiento de los dispositivos móviles institucionales haciendo imposible la copia o extracción de datos si no se conoce el método de desbloqueo.
- La Dirección de Tecnologías debe configurar la opción de borrado remoto de información en los dispositivos móviles institucionales, con el fin de eliminar los datos de dichos dispositivos y restaurarlos a los valores de fábrica, de forma remota, evitando así divulgación no autorizada de información en caso de pérdida o hurto.
- La Dirección de Tecnologías debe contar con una solución de copias de seguridad para la información contenida en los dispositivos móviles institucionales; dichas copias deben acogerse a la Política de Copias de Respaldo de la Información.
- La Dirección de Tecnologías debe instalar un software de antivirus en los dispositivos móviles institucionales.

Normas dirigidas a los usuarios finales:

- Los usuarios deben evitar usar los dispositivos móviles institucionales en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.
- Los usuarios no deben modificar las configuraciones de seguridad de los dispositivos móviles institucionales bajo su responsabilidad, ni desinstalar el software provisto con ellos al momento de su entrega.
- Los usuarios deben evitar la instalación de programas desde fuentes desconocidas; se deben instalar aplicaciones únicamente desde los repositorios oficiales de los dispositivos móviles institucionales.
- Los usuarios deben, cada vez que el sistema de sus dispositivos móviles institucionales notifique de una actualización disponible, aceptar y aplicar la nueva versión.
- Los usuarios deben evitar hacer uso de redes inalámbricas de uso público ajenos a la UEA.
- Los usuarios deben evitar conectar los dispositivos móviles institucionales asignados por puerto USB a cualquier computador público, de hoteles o cafés internet, entre otros.
- Los usuarios no deben almacenar videos, fotografías o información personal en los dispositivos móviles institucionales asignados.

7.2. POLITICA PARA USO DE CONEXIONES REMOTAS

La UEA establecerá las circunstancias y requisitos para el establecimiento de conexiones remotas a los equipos institucionales conectados a la red, con finalidad de brindar soporte técnico en el campus principal, CIPCA y sedes académicas; así mismo, suministrará las herramientas y controles necesarios para que dichas conexiones se realicen de manera segura.

7.2.1. Normas para uso de conexiones remotas:

- La Dirección de Tecnologías debe implantar los métodos y controles de seguridad para establecer conexiones remotas.

- La Dirección de Tecnologías debe restringir las conexiones remotas a los equipos institucionales; únicamente se deben permitir estos accesos a personal autorizado de acuerdo con las labores desempeñadas.
- La Dirección de Tecnologías debe verificar la efectividad de los controles aplicados sobre las conexiones remotas de manera permanente.

8. POLÍTICAS DE SEGURIDAD DEL PERSONAL

8.1. POLÍTICA RELACIONADA CON LA VINCULACIÓN Y DESVINCULACIÓN DE FUNCIONARIOS

La UEA reconoce la importancia que tiene el factor humano para el cumplimiento de sus objetivos institucionales y con el interés de contar con el personal mejor calificado, garantizará que la vinculación de nuevos funcionarios se realizará siguiendo un proceso formal de selección, acorde con la legislación vigente, el cual estará orientado a las funciones y roles que deben desempeñar los funcionarios en sus cargos.

8.1.1. Normas relacionadas con la vinculación de funcionarios

Normas dirigidas a la Dirección de Talento Humano:

- La Dirección de Talento Humano debe realizar las verificaciones necesarias para confirmar la veracidad de la información suministrada por el personal candidato a ocupar un cargo en la UEA, antes de su vinculación temporal o definitiva.
- La Dirección de Talento Humano debe certificar que los funcionarios de la UEA firmen un Acuerdo y/o Cláusula de Confidencialidad y un documento de Aceptación de Políticas de Seguridad de la Información; estos documentos deben ser anexados a los demás documentos relacionados con la ocupación del cargo.
- La Dirección de Talento Humano deberá notificar a la Dirección de Tecnologías, la vinculación de nuevo personal para la creación de cuentas de acceso a servicios institucionales.

8.1.2. Normas para la desvinculación, licencias, vacaciones o cambios de labores de los funcionarios:

- La Dirección de Talento Humano debe realizar el proceso de desvinculación de los funcionarios de la UEA llevando a cabo los procedimientos y ejecutando los controles establecidos para tal fin, acto seguido deberá emitir solicitud para la modificación o inhabilitación de usuarios a la Dirección de Tecnologías.

9. POLÍTICAS DE GESTIÓN DE ACTIVOS DE INFORMACIÓN

9.1. POLÍTICA DE RESPONSABILIDAD POR LOS ACTIVOS

La UEA como propietario de la información física, así como de la información generada, procesada, almacenada y transmitida con su plataforma tecnológica, otorgará responsabilidad a las áreas sobre sus activos de información, asegurando el cumplimiento de las directrices que regulen el uso adecuado de la misma.

La información, archivos físicos, los sistemas, los servicios y los equipos (ej. estaciones de trabajo, equipos portátiles, impresoras, redes, Internet, correo electrónico, herramientas de

acceso remoto, aplicaciones, teléfonos, entre otros) propiedad del UEA, son activos de la institución y se proporcionan a los funcionarios autorizados, para cumplir con los objetivos de la IES.

Toda la información sensible de la UEA, así como los activos donde ésta se almacena y se procesa deben ser asignados a un responsable, inventariados y posteriormente clasificados, de acuerdo con los requerimientos y los criterios que dicte la Dirección de Tecnologías. Los propietarios de los activos de información deben llevar a cabo el levantamiento y la actualización permanente del inventario de activos de información al interior de sus procesos o áreas.

9.1.1. Normas de responsabilidad por los activos

Normas dirigidas a propietarios de los activos de información:

- Consejo Universitario, Rectorado, Vicerrectorados y Direcciones de la UEA, deben actuar como propietarias de la información física y electrónica de la entidad, ejerciendo así la facultad de aprobar o revocar el acceso a su información con los perfiles adecuados para tal fin.
- Los propietarios de los activos de información deben generar un inventario de dichos activos para las áreas o procesos que lideran, acogiendo las indicaciones de las guías de clasificación de la información; así mismo, deben mantener actualizado el inventario de sus activos de información.
- Los propietarios de los activos de información deben monitorear periódicamente la validez de los usuarios y sus perfiles de acceso a la información.
- Los propietarios de los activos de información deben ser conscientes que los recursos de procesamiento de información de la institución, se encuentran sujetos a auditorías por parte de su inmediato superior, de la Dirección de Planificación y Evaluación y/o revisiones de cumplimiento por parte de la Dirección de Tecnologías.

Normas dirigidas a la Dirección de Tecnologías:

- La Dirección de Tecnologías es la propietaria de los activos de información correspondientes a los alojados en los servidores de la UEA y, en consecuencia, debe asegurar su apropiada operación y administración.
- La Dirección de Tecnologías son quienes deben autorizar y apoyar la instalación, cambio o eliminación de componentes en las plataformas tecnológicas de propiedad de la UEA.
- La Dirección de Tecnologías debe establecer una configuración adecuada para los recursos tecnológicos, con el fin de preservar la seguridad de la información y hacer un uso adecuado de ellos.
- La Dirección de Tecnologías es responsable de preparar las estaciones de trabajo fijas y/o portátiles de los funcionarios.
- La Dirección de Tecnologías es responsable de generar copias de seguridad de la información de los funcionarios que se retiran o cambian de labores, cuando les es formalmente solicitado.

Normas dirigidas a todos los usuarios:

- Los recursos tecnológicos de la UEA, deben ser utilizados de forma ética y en cumplimiento de las leyes y reglamentos vigentes, con el fin de evitar daños o pérdidas de información institucional.
- Los funcionarios no deben utilizar sus equipos de cómputo y dispositivos móviles personales para desempeñar las actividades laborales.
- Los funcionarios no deben utilizar software no autorizado o de su propiedad en los equipos institucionales.
- Todas las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos son asignados a un responsable, por lo cual es su compromiso hacer uso adecuado y eficiente de dichos recursos.
- En el momento de desvinculación o cambio de labores, los funcionarios deben realizar la entrega de los recursos tecnológicos en la Dirección de Activos Fijos de la UEA y otros activos de información suministrados en el momento de su vinculación.

9.2. POLÍTICA DE CLASIFICACIÓN Y MANEJO DE LA INFORMACIÓN

La UEA definirá los niveles más adecuados para clasificar su información de acuerdo con su sensibilidad y generará una guía de Clasificación de la Información para que los propietarios de la misma la cataloguen y determinen los controles requeridos para su protección.

Toda la información de la UEA debe ser identificada, clasificada y documentada de acuerdo con las guías de Clasificación de la Información establecidas por el Comité de Seguridad de la Información de la UTIC.

Una vez clasificada la información, la UEA proporcionará los recursos necesarios para la aplicación de controles en busca de preservar la confidencialidad, integridad y disponibilidad de la misma, con el fin de promover el uso adecuado de la información por parte de los funcionarios para la ejecución de sus actividades.

9.2.1. Normas para la clasificación y manejo de la información

Normas dirigidas a los propietarios de los activos de información

- Los propietarios de los activos de información deben clasificar su información de acuerdo con la guía de clasificación de la Información establecida.
- Los propietarios de los activos de información son responsables de monitorear periódicamente la clasificación de sus activos de información y de ser necesario realizar su re-clasificación.

Normas dirigidas a todos los usuarios

- Los usuarios deben acatar los lineamientos guía de clasificación de la Información para el acceso, divulgación, almacenamiento, copia, transmisión, etiquetado y eliminación de la información contenida en los recursos tecnológicos, así como de la información física de la UEA.
- Los usuarios deben tener en cuenta estas consideraciones cuando impriman, escaneen, saquen copias y envíen faxes: verificar las áreas adyacentes a impresoras, escáneres, fotocopiadoras y máquinas de fax para asegurarse que no quedaron documentos relacionados o adicionales; asimismo, recoger de las impresoras, escáneres, fotocopiadoras y máquinas de fax, inmediatamente los documentos confidenciales para evitar su divulgación no autorizada.

- Tanto los funcionarios deben asegurarse que, en el momento de ausentarse de su puesto de trabajo, sus escritorios se encuentren libres de documentos y medios de almacenamiento, utilizados para el desempeño de sus labores; estos deben contar con las protecciones de seguridad necesarias de acuerdo con su nivel de clasificación.
- La información que se encuentra en documentos físicos debe ser protegida, a través de controles de acceso físico y las condiciones adecuadas de almacenamiento y resguardo.

9.3. POLITICA PARA USO DE TOKENS DE SEGURIDAD

La UEA proveerá las condiciones de manejo de los tokens de seguridad para los procesos que los utilizan y velará porque los funcionarios hagan un uso responsable de los mismos.

9.3.1. Normas para uso de tokens de seguridad

Normas dirigidas a las áreas usuarias de tokens de seguridad

- Cada área usuaria de tokens de seguridad debe asignar un funcionario administrador de los mismos con la potestad para autorizar las solicitudes de acceso.

Normas dirigidas a los administradores de los tokens de seguridad

- Los Administradores de los tokens de seguridad deben procesar las solicitudes de dichos tokens según los requerimientos de cada entidad proveedora de éstos y adjuntar la documentación necesaria.
- Los Administradores de los tokens deben recibirlos y realizar la activación necesaria en los respectivos portales o sitios de uso para poder realizar operaciones por medio de ellos.
- Los Administradores de los tokens deben crear los usuarios y perfiles en cada portal o sitio de uso, según las actividades a realizar por cada funcionario creado.
- Los Administradores de los tokens deben entregar a los funcionarios designados los usuarios y seriales de los dispositivos que le son asignados para su uso, formalizando la entrega por medio de acta para custodia de los mismos.
- Los Administradores de los tokens deben dar avisos a las entidades emisoras en caso de robo o pérdida de estos con el fin de efectuar el bloqueo respectivo y la reposición de los mismos.
- Los Administradores de los tokens deben realizar el cambio de estos, cuando se presente mal funcionamiento, caducidad, cambio de funciones o cambio del titular, reportando a la entidad emisora y devolviendo los dispositivos asignados.

Normas dirigidas a los usuarios de tokens de seguridad

- Los usuarios que requieren utilizar los tokens de seguridad deben contar con una cuenta de usuario en los portales o sitios de uso de los mismos; dichos tokens harán parte del inventario físico de cada usuario a quien se haya asignado.
- Cada usuario de los portales o sitios de uso de los tokens debe tener su propio dispositivo, el cual es exclusivo, personal e intransferible, al igual que la cuenta de usuario y la contraseña de acceso.
- El almacenamiento de los tokens debe efectuarse bajo estrictas medidas de seguridad, dentro de caja fuerte o escritorios con llave al interior de las áreas

usuarias, de tal forma que se mantengan fuera del alcance de terceros no autorizados.

- Los usuarios deben notificar al Administrador de los tokens en caso de robo, pérdida, mal funcionamiento o caducidad para que este a su vez, se comunique con las entidades emisoras de dichos tokens.
- Los usuarios no deben permitir que terceras personas observen la clave que genera el token, así como no deben aceptar ayuda de terceros para la utilización del token.
- Los usuarios deben responder por las transacciones electrónicas que se efectúen con la cuenta de usuario, clave y el token asignado, en el desarrollo de las actividades como funcionarios de la UEA. En caso de que suceda algún evento irregular con los tokens los usuarios deben asumir la responsabilidad administrativa, disciplinaria y económica.
- Los usuarios deben mantener los tokens asignados en un lugar seco y no introducirlos en agua u otros líquidos.
- Los usuarios deben evitar exponer los tokens a campos magnéticos y a temperaturas extremas.
- Los usuarios deben evitar que los tokens sean golpeados o sometidos a esfuerzo físico.
- Los usuarios no deben abrir los tokens, retirar la batería o placa de circuitos, ya que ocasionará su mal funcionamiento.

9.4. POLÍTICA DE USO DE PERIFÉRICOS Y MEDIOS DE ALMACENAMIENTO

El uso de periféricos y medios de almacenamiento en la UEA será reglamentado por la Dirección de Tecnologías, considerando las labores realizadas por los funcionarios y su necesidad de uso.

9.4.1. Normas uso de periféricos y medios de almacenamiento

Normas dirigidas a la Dirección De Tecnologías:

- La Dirección de Tecnologías debe implantar los controles que regulen el uso de periféricos y medios de almacenamiento en los equipos institucionales, de acuerdo con los lineamientos y condiciones establecidas.
- La Dirección de Tecnologías debe generar y aplicar lineamientos para la disposición segura de los medios de almacenamiento, ya sea cuando son dados de baja o reasignados a un nuevo usuario.

Normas dirigidas a todos los usuarios:

- Los funcionarios deben acoger las condiciones de uso de los periféricos y medios de almacenamiento establecidos por la Dirección de Tecnologías.
- Los funcionarios no deben modificar la configuración de periféricos y medios de almacenamiento establecidos por la Dirección de Tecnologías.
- Los funcionarios son responsables por el custodio de los medios de almacenamiento institucionales asignados.

10. POLÍTICAS DE CONTROL DE ACCESO

10.1. POLÍTICA DE ACCESO A REDES Y RECURSOS DE RED

La Dirección de Tecnologías de la UEA, como responsables de las redes de datos y los recursos de red de la institución debe administrar dichas redes protegiéndolas contra accesos no autorizados a través de mecanismos de control de acceso lógico.

10.1.1. Normas de acceso a redes y recursos de red

Normas dirigidas a la Dirección de Tecnologías:

- La Dirección de Tecnologías debe establecer un procedimiento de autorización y controles para proteger el acceso a las redes de datos y los recursos de red de la UEA.
- La Dirección de Tecnologías debe asegurar que las redes inalámbricas cuenten con métodos de autenticación que evite accesos no autorizados.
- La Dirección de Tecnologías, debe establecer controles para la identificación y autenticación, así como formalizar la aceptación de las Políticas de Seguridad de la Información por parte de los usuarios.

Normas dirigidas a todos los usuarios:

- Los funcionarios, antes de contar con acceso lógico por primera vez a la red de datos deben contar con el formato de creación de cuentas de usuario debidamente autorizado por la Dirección de Talento Humano y el Acuerdo de Confidencialidad firmado previamente.
- Los equipos de cómputo de usuario final que se conecten o deseen conectarse a las redes de datos deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.

10.2. POLÍTICA DE ADMINISTRACIÓN DE ACCESO DE USUARIOS

La UEA establecerá privilegios para el control de acceso lógico de cada usuario o grupo de usuarios a las redes de datos, los recursos tecnológicos y los sistemas de información. Así mismo, velará que los funcionarios tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y que la asignación de los derechos de acceso esté regulada por normas y procedimientos establecidos para tal fin.

10.2.1. Normas de administración de acceso de usuarios

Normas dirigidas a la Dirección de Tecnologías:

- La Dirección de Tecnologías debe establecer un procedimiento formal para la administración de los usuarios en las redes de datos, los recursos tecnológicos y sistemas de información de la institución, que contemple la creación, modificación, bloqueo o eliminación de las cuentas de usuario.
- La Dirección de Tecnologías, previa solicitud de la Dirección de Talento Humano debe crear, modificar, bloquear o eliminar cuentas de usuarios sobre las redes de datos, los recursos tecnológicos y los sistemas de información administrados, acorde con el procedimiento establecido.
- La Dirección de Tecnologías, debe definir lineamientos para la configuración de contraseñas que aplicaran sobre la infraestructura tecnológica, los servicios de red y los sistemas de información; dichos lineamientos deben considerar aspectos como

longitud, complejidad, cambio periódico, control histórico, bloqueo por número de intentos fallidos en la autenticación y cambio de contraseña en el primer acceso, entre otros.

- La Dirección de Tecnologías debe establecer un procedimiento que asegure la eliminación, reasignación o bloqueo de los privilegios de acceso otorgados sobre los recursos tecnológicos, los servicios de red y los sistemas de información de manera oportuna, cuando los funcionarios se desvinculan, toman licencias, vacaciones, son trasladados o cambian de cargo.
- La Dirección de Tecnologías debe asegurarse que los usuarios o perfiles de usuario que tienen asignados por defecto los diferentes recursos tecnológicos sean inhabilitados o eliminados.

Normas dirigidas a los propietarios de los activos de información:

- Es responsabilidad de los propietarios de los activos de información, definir los perfiles de usuario y autorizar las solicitudes de acceso a dichos recursos de acuerdo con los perfiles establecidos.
- Los propietarios de los activos de información deben verificar y ratificar periódicamente todas las autorizaciones sobre sus recursos tecnológicos y sistemas de información.

10.3. POLÍTICA DE RESPONSABILIDADES DE ACCESO DE LOS USUARIOS

Los usuarios de los recursos tecnológicos y los sistemas de información realizarán un uso adecuado y responsable de dichos recursos y sistemas, salvaguardando la información a la cual les es permitido el acceso.

10.3.1. Normas de responsabilidades de acceso de los usuarios

Normas dirigidas a todos los usuarios:

- Los usuarios de los recursos tecnológicos, los servicios de red y los sistemas de información deben hacerse responsables de las acciones realizadas en los mismos, así como del usuario y contraseña asignados para el acceso a estos.
- Los funcionarios no deben compartir sus cuentas de usuario y contraseñas con otros funcionarios o terceras partes.
- Los funcionarios que posean acceso a los recursos tecnológicos, los servicios de red y los sistemas de información de la UEA deben acogerse a lineamientos para la configuración de contraseñas implantados por la Institución.

10.4. POLÍTICA DE USO DE ALTOS PRIVILEGIOS Y UTILITARIOS DE ADMINISTRACIÓN

La Dirección de Tecnologías velará porque los recursos tecnológicos y los servicios de red de la UEA sean operados y administrados en condiciones controladas y de seguridad, que permitan un monitoreo posterior de la actividad de los usuarios administradores, poseedores de los más altos privilegios sobre dichos recursos y servicios.

10.4.1. Normas de uso de altos privilegios y utilitarios de administración

Normas dirigidas a la Dirección de Tecnologías, administradores de los recursos tecnológicos y servicios de red:

- La Dirección de Tecnologías debe otorgar los privilegios para administración de recursos tecnológicos, servicios de red y sistemas de información sólo a aquellos funcionarios designados para dichas funciones.
- La Dirección de Tecnologías debe establecer cuentas personalizadas con altos privilegios para cada uno de los administradores de los recursos tecnológicos, servicios de red y sistemas de información.
- La Dirección de Tecnologías debe verificar que los administradores de los recursos tecnológicos y servicios de red no tengan acceso a sistemas de información en producción.
- La Dirección de Tecnologías debe restringir las conexiones remotas a los recursos tecnológicos; únicamente se deben permitir estos accesos a personal autorizado, de acuerdo con las labores desempeñadas.
- La Dirección de Tecnologías debe asegurarse que los usuarios o perfiles de usuario que traen por defecto los sistemas operativos, el firmware y las bases de datos sean suspendidos o renombrados en sus autorizaciones y que las contraseñas por defecto dichos usuarios o perfiles sean modificadas.
- La Dirección de Tecnologías debe establecer los controles para que los usuarios finales de los recursos tecnológicos, los servicios de red y los sistemas de información no tengan instalados en sus equipos de cómputo utilitarios que permitan accesos privilegiados a dichos recursos, servicios o sistemas.
- Los administradores de los recursos tecnológicos y servicios de red, funcionarios de la Dirección de Tecnologías, no deben hacer uso de los utilitarios que permiten acceso a los sistemas operativos, firmware o conexión a las bases de datos para pasar por alto la seguridad de los sistemas de información alojados sobre la infraestructura tecnológica de la UEA.
- Los administradores de los recursos tecnológicos deben deshabilitar las funcionalidades o servicios no utilizados de los sistemas operativos, el firmware y las bases de datos. Se debe configurar el conjunto mínimo requerido de funcionalidades, servicios y utilitarios.
- La Dirección de Tecnologías debe generar y mantener actualizado un listado de las cuentas administrativas de los recursos de la plataforma tecnológica.

10.5. POLÍTICA DE CONTROL DE ACCESO A SISTEMAS Y APLICATIVOS

La Dirección de Tecnologías, como responsable de la administración de sistemas de información y aplicativos, propenderá para que estos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico. Así mismo, velará porque los desarrolladores, tanto internos como externos, acojan buenas prácticas de desarrollo en los productos generados para controlar el acceso lógico y evitar accesos no autorizados a los sistemas administrados.

10.5.1. Normas de control de acceso a sistemas y aplicativos

Normas dirigidas a los propietarios de los activos de información:

- Los propietarios de los activos de información deben autorizar los accesos a sus sistemas de información o aplicativos, de acuerdo con los perfiles establecidos y las necesidades de uso, acogiendo los procedimientos establecidos.

- Los propietarios de los activos de información deben monitorear periódicamente los perfiles definidos en los sistemas de información y los privilegios asignados a los usuarios que acceden a ellos.

Normas dirigidas a la Dirección de Tecnologías:

- La Dirección de Tecnologías debe establecer un procedimiento para la asignación de accesos a los sistemas y aplicativos de la UEA.
- La Dirección de Tecnologías debe establecer ambientes separados a nivel físico y lógico para desarrollo, pruebas y producción, contando cada uno con su plataforma, servidores, aplicaciones, dispositivos y versiones independientes de los otros ambientes, evitando que las actividades de desarrollo y pruebas puedan poner en riesgo la integridad de la información de producción.
- La Dirección de Tecnologías debe asegurar, mediante los controles necesarios, que los usuarios utilicen diferentes perfiles para los ambientes de desarrollo, pruebas y producción, y así mismo que los menús muestren los mensajes de identificación apropiados para reducir los riesgos de error.
- La Dirección de Tecnologías debe establecer el procedimiento y los controles de acceso a los ambientes de producción de los sistemas de información; así mismo, debe asegurarse que los desarrolladores internos o externos, posean acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción.
- La Dirección de Tecnologías debe proporcionar repositorios de archivos fuente de los sistemas de información; estos deben contar con acceso controlado y restricción de privilegios, además de un registro de acceso a dichos archivos.

Normas dirigidas a desarrolladores (internos y externos)

- Los desarrolladores deben asegurar que los sistemas de información construidos requieran autenticación para todos los recursos y páginas, excepto aquellas específicamente clasificadas como públicas.
- Los desarrolladores deben certificar la confiabilidad de los controles de autenticación, utilizando implementaciones centralizadas para dichos controles.
- Los desarrolladores deben certificar que no se almacenen contraseñas, cadenas de conexión u otra información sensible en texto claro y que se implementen controles de integridad de dichas contraseñas.
- Los desarrolladores deben establecer los controles de autenticación de tal manera que cuando fallen, lo hagan de una forma segura, evitando indicar específicamente cual fue la falla durante el proceso de autenticación y, en su lugar, generando mensajes generales de falla.
- Los desarrolladores deben asegurar que no se despliegan en la pantalla las contraseñas ingresadas, así como deben deshabilitar la funcionalidad de recordar campos de contraseñas.
- Los desarrolladores deben certificar que se inhabilitan las cuentas luego de un número establecido de intentos fallidos de ingreso a los sistemas desarrollados.
- Los desarrolladores deben asegurar que, si se utiliza la reasignación de contraseñas, únicamente se envíe un enlace o contraseñas temporales a cuentas de correo electrónico previamente registradas en los aplicativos, los cuales deben tener un

periodo de validez establecido; se deben forzar el cambio de las contraseñas temporales después de su utilización.

- Los desarrolladores deben certificar que el último acceso (fallido o exitoso) sea reportado al usuario en su siguiente acceso exitoso a los sistemas de información.
- Los desarrolladores deben asegurar la re-autenticación de los usuarios antes de la realización de operaciones críticas en los aplicativos.
- Los desarrolladores deben, a nivel de los aplicativos, restringir acceso a archivos u otros recursos, a direcciones URL protegidas, a funciones protegidas, a servicios, a información de las aplicaciones, a atributos y políticas utilizadas por los controles de acceso y a la información relevante de la configuración.
- Los desarrolladores deben establecer que periódicamente se re-valide la autorización de los usuarios en los aplicativos y se asegure que sus privilegios no han sido modificados.

11. POLÍTICAS DE SEGURIDAD FISICA Y MEDIOAMBIENTAL

11.1. POLÍTICA DE AREAS SEGURAS

La Universidad Estatal Amazónica proveerá la implantación y velará por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones en todas sus sedes. Así mismo, controlará las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas. Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideras áreas de acceso restringido.

11.2. Normas de áreas seguras

Normas dirigidas a la Dirección de Tecnologías:

- Las solicitudes de acceso al centro de datos o ductos de comunicaciones deben ser aprobadas por funcionarios de la Dirección de Tecnologías autorizados; no obstante, los visitantes siempre deberán estar acompañados de un funcionario de dicha dependencia durante su visita al centro de datos o ductos de comunicaciones.
- La Dirección de Tecnologías debe descontinuar o modificar de manera inmediata los privilegios de acceso físico al centro de datos y ductos de comunicación que están bajo su custodia, en los eventos de desvinculación o cambio en las labores de un funcionario autorizado.
- La Dirección de Tecnologías debe proveer las condiciones físicas y medioambientales necesarias para certificar la protección y correcta operación de los recursos de la plataforma tecnológica ubicados en el centro de datos; deben existir sistemas de control ambiental de temperatura y humedad, sistemas de detección y extinción de incendios, sistemas de descarga eléctrica, sistemas de vigilancia y monitoreo y alarmas en caso de detectarse condiciones ambientales inapropiadas. Estos sistemas se deben monitorear de manera permanente.
- La Dirección de Tecnologías debe velar porque los recursos de la infraestructura tecnológica de la UEA ubicados en el centro de datos se encuentran protegidos contra fallas o interrupciones eléctricas.
- La Dirección de Tecnologías debe certificar que el centro de datos y ductos de comunicación que están bajo su custodia, se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.

- La Dirección de Tecnologías debe asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado; así mismo, se debe llevar control de la programación de los mantenimientos preventivos.

Normas dirigidas a la Dirección de Infraestructura y mantenimiento:

- La Dirección de Infraestructura y mantenimiento debe proporcionar los recursos necesarios para ayudar a proteger, regular y velar por el perfecto estado de los controles físicos implantados en las instalaciones de la UEA.
- La Dirección de Infraestructura y mantenimiento debe identificar mejoras a los mecanismos implantados y de ser necesario, la implementación de nuevos mecanismos, con el fin de proveer la seguridad física de las instalaciones.
- La Dirección de Infraestructura y mantenimiento debe certificar la efectividad de los mecanismos de seguridad física y control de acceso al centro de datos, ductos de comunicación y demás áreas de procesamiento de información.
- La Dirección de Infraestructura y mantenimiento debe cerciorarse de que los ductos de comunicación que están bajo su custodia, se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.
- La Dirección de Infraestructura y mantenimiento, con el acompañamiento de la Dirección de Tecnologías, debe verificar que el cableado se encuentra protegido con el fin de disminuir las intercepciones o daños.

Normas dirigidas a todos los usuarios

- Los ingresos y egresos de personal a centro de datos o ductos de comunicaciones deben ser registrados; por consiguiente, los funcionarios deben cumplir completamente con los controles físicos implantados.
- El personal provisto por terceras partes para los que aplique, en razón del servicio prestado, deben utilizar prendas distintivas que faciliten su identificación.
- Los funcionarios de la UEA y estudiantes no deben intentar ingresar a áreas a las cuales no tengan autorización.

11.3. POLÍTICA DE SEGURIDAD PARA LOS EQUIPOS INSTITUCIONALES

La UEA para evitar la pérdida, robo o exposición al peligro de los recursos tecnológicos que se encuentren dentro o fuera de sus instalaciones, proveerá los recursos que garanticen la mitigación de riesgos.

11.3.1. Normas de seguridad para los equipos institucionales

Normas dirigidas a la Dirección de Tecnología:

- La Dirección de Tecnologías debe proveer los mecanismos y estrategias necesarios para proteger la confidencialidad, integridad y disponibilidad de los recursos tecnológicos, dentro y fuera de las instalaciones de la UEA.
- La Dirección de Tecnologías debe realizar mantenimientos preventivos y correctivos de los recursos tecnológicos de la UEA.

- La Dirección de Tecnologías debe generar estándares de configuración segura para los equipos de cómputo de uso académico y administrativo y configurar dichos equipos acogiendo los estándares generados.
- La Dirección de Tecnologías debe establecer las condiciones que deben cumplir los equipos de cómputo personales autorizados para conectarse a la red de datos de la UEA y verificar el cumplimiento de dichas condiciones antes de conceder a estos equipos acceso a los servicios de red.
- La Dirección de Tecnologías debe aislar los equipos de áreas sensibles para proteger su acceso de los demás funcionarios.
- La Dirección de Tecnologías debe generar y aplicar lineamientos para la disposición segura de los equipos de cómputo de los funcionarios, ya sea cuando son dados de baja o cambian de usuario.

Normas dirigidas a todos los usuarios:

- La Dirección de Activos Fijos es la única área autorizada para realizar movimientos y asignaciones de recursos tecnológicos; por consiguiente, se encuentra prohibida la disposición que pueda hacer cualquier funcionario de los recursos tecnológicos de la UEA.
- Las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos asignados a los funcionarios deben acoger las instrucciones técnicas de proporcione la Dirección de Tecnologías.
- Cuando se presente una falla o problema de hardware o software en una estación de trabajo u otro recurso tecnológico propiedad de la UEA el usuario responsable debe informar a la Mesa de Ayuda en donde se atenderá o escalará al interior de la Dirección de Tecnologías, con el fin de realizar una asistencia adecuada.
- La instalación, reparación o retiro de cualquier componente de hardware o software de las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos de la UEA, solo puede ser realizado por los funcionarios de la Dirección de Tecnologías.
- Los funcionarios deben bloquear sus estaciones de trabajo en el momento de abandonar su puesto de trabajo.
- Los funcionarios no deben dejar encendidas las estaciones de trabajo u otros recursos tecnológicos en horas no laborables.
- Los equipos de cómputo, bajo ninguna circunstancia, deben ser dejados desatendidos en lugares públicos, en el caso de que estén siendo transportados.
- Los equipos de cómputo deben ser transportados con las medidas de seguridad apropiadas, que garanticen su integridad física.
- Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.
- En caso de pérdida o robo de un equipo de cómputo, se debe informar de forma inmediata al Responsable de la Dirección de Activos Fijos de la UEA para que se inicie el trámite interno correspondiente y se debe poner la denuncia ante la autoridad competente.

12. POLITICAS DE SEGURIDAD EN LAS OPERACIONES

12.1. POLÍTICA DE ASIGNACIÓN DE RESPONSABILIDADES OPERATIVAS

La Dirección de Tecnologías, encargada de la operación y administración de los recursos tecnológicos que apoyan los procesos de la UEA, asignará funciones específicas a sus funcionarios, quienes deben efectuar la operación y administración de dichos recursos

tecnológicos, manteniendo y actualizando la documentación de los procesos operativos para la ejecución de las actividades. Así mismo, velará por la eficiencia de los controles implantados en los procesos operativos asociados a los recursos tecnológicos con el objeto de proteger la confidencialidad, la integridad y la disponibilidad de la información manejada y asegurará que los cambios efectuados sobre los recursos tecnológicos, serán adecuadamente controlados y debidamente autorizados.

La Dirección de Tecnologías proveerá la capacidad de procesamiento requerida en los recursos tecnológicos y sistemas de información de la institución, efectuando proyecciones de crecimiento y provisiones en la infraestructura tecnológica con una periodicidad definida.

12.1.1. Normas de asignación de responsabilidades operativas

Normas dirigidas a la Dirección de Tecnologías:

- La Dirección de Tecnologías debe efectuar, a través de sus funcionarios, la documentación y actualización de los procedimientos relacionados con la operación y administración de la infraestructura tecnológica de la UEA.
- La Dirección de Tecnologías debe proporcionar a sus funcionarios manuales de configuración y operación de los sistemas operativos, firmware, servicios de red, bases de datos y sistemas de información a su cargo.
- La Dirección de Tecnologías debe proveer los recursos necesarios para la implantación de controles que permitan la separación de ambientes de desarrollo, pruebas y producción, teniendo en cuenta consideraciones como: controles para el intercambio de información entre los ambientes de desarrollo y producción, la inexistencia de compiladores, editores o fuentes en los ambientes de producción y un acceso diferente para cada uno de los ambientes.
- La Dirección de Tecnologías, a través de sus funcionarios, debe realizar estudios sobre la demanda y proyecciones de crecimiento de los recursos administrados de manera periódica, con el fin de asegurar el desempeño y capacidad de la infraestructura tecnológica. Estos estudios y proyecciones deben considerar aspectos de consumo de recursos de procesadores, memorias, discos, servicios de impresión, ancho de banda, internet y tráfico de las redes de datos, entre otros.
- La Dirección de Tecnologías debe emitir informes y generar recomendaciones acerca de las soluciones de seguridad seleccionadas para la infraestructura tecnológica de la UEA.

12.2. POLÍTICA DE PROTECCIÓN FRENTE A SOFTWARE MALICIOSO

La UEA proporcionará los mecanismos necesarios que garanticen la protección de la información y los recursos de la infraestructura tecnológica en donde se procesa y almacena, adoptando los controles necesarios para evitar la divulgación, modificación o daño permanente ocasionados por el contagio de software malicioso. Además, proporcionará los mecanismos para generar cultura de seguridad entre sus funcionarios frente a los ataques de software malicioso.

12.2.1. Normas de protección frente a software malicioso

Normas dirigidas a la Dirección de Tecnologías:

- La Dirección de Tecnologías debe proveer herramientas tales como antivirus, antimalware, antispam, antispyware, entre otras, que reduzcan el riesgo de contagio de software malicioso y respalden la seguridad de la información contenida y administrada en los recursos tecnológicos de la UEA y los servicios que se ejecutan en los mismos.
- La Dirección de Tecnologías debe asegurar que el software de antivirus, antimalware, antispam y antispyware cuente con las licencias de uso requeridas, certificando así su autenticidad y la posibilidad de actualización periódica de las últimas bases de datos de firmas del proveedor del servicio.
- La Dirección de Tecnologías, a través de sus funcionarios, debe asegurarse que los usuarios no puedan realizar cambios en la configuración del software de antivirus, antispyware, antispam, antimalware.
- La Dirección de Tecnologías, a través de sus funcionarios, debe certificar que el software de antivirus, antispyware, antispam, antimalware, posea las últimas actualizaciones y parches de seguridad, para mitigar las vulnerabilidades de los recursos e infraestructura tecnológica de la UEA.

Normas dirigidas a todos los usuarios:

- Los usuarios de recursos tecnológicos no deben cambiar o eliminar la configuración del software de antivirus, antispyware, antimalware, antispam definida por la Dirección de Tecnologías; por consiguiente, únicamente podrán realizar tareas de escaneo de virus en diferentes medios.
- Los usuarios de recursos tecnológicos deben ejecutar el software de antivirus, antispyware, antispam, antimalware sobre los archivos y/o documentos que son abiertos o ejecutados por primera vez, especialmente los que se encuentran en medios de almacenamiento externos o que provienen del correo electrónico
- Los usuarios deben asegurarse que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas y seguras para evitar el contagio de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos.
- Los usuarios que sospechen o detecten alguna infección por software malicioso deben notificar a la Mesa de Ayuda, para que, a través de ella, la Dirección de Tecnologías tome las medidas de control correspondientes.

12.3. POLÍTICA DE COPIAS DE RESPALDO DE LA INFORMACIÓN

La UEA certificará la generación de copias de respaldo y almacenamiento de su información crítica, proporcionando los recursos necesarios y estableciendo los procedimientos y mecanismos para la realización de estas actividades. Las áreas propietarias de la información, con el apoyo de la Dirección de Tecnologías, encargada de la generación de copias de respaldo, definirán la estrategia a seguir y los periodos de retención para el respaldo y almacenamiento de la información.

Así mismo, la UEA velará porque los medios magnéticos que contienen la información crítica sean almacenados en una ubicación diferente a las instalaciones donde se encuentra dispuesta. El sitio externo donde se resguarden las copias de respaldo debe contar con los controles de seguridad física y medioambiental apropiados.

12.3.1. Normas de copias de respaldo de la información

Normas dirigidas a la Dirección de Tecnologías:

- La Dirección de Tecnologías, a través de sus funcionarios, debe generar y adoptar los procedimientos para la generación, restauración, almacenamiento y tratamiento para las copias de respaldo de la información, velando por su integridad y disponibilidad.
- La Dirección de Tecnologías debe disponer de los recursos necesarios para permitir la identificación de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.
- La Dirección de Tecnologías, a través de sus funcionarios, debe llevar a cabo los procedimientos para realizar pruebas de recuperación a las copias de respaldo, para así comprobar su integridad y posibilidad de uso en caso de ser necesario.
- La Dirección de Tecnologías debe definir las condiciones de transporte o transmisión y custodia de las copias de respaldo de la información que son almacenadas externamente.
- La Dirección de Tecnologías debe proporcionar apoyo para la definición de las estrategias de generación, retención y rotación de las copias de respaldo de los activos información de la UEA.

Normas dirigidas a los propietarios de los activos de información:

- Los propietarios de los recursos tecnológicos y sistemas de información deben definir, en conjunto con la Dirección de Tecnologías, las estrategias para la generación, retención y rotación de las copias de respaldo de los activos de información.

Normas dirigidas a todos los usuarios:

- Es responsabilidad de los usuarios de los recursos tecnológicos identificar la información crítica que debe ser respaldada y almacenarla de acuerdo con su nivel de clasificación.

12.4. POLÍTICA DE REGISTRO DE EVENTOS Y MONITOREO DE LOS RECURSOS TECNOLÓGICOS Y LOS SISTEMAS DE INFORMACIÓN

La UEA realizará monitoreo permanente del uso que dan los funcionarios a los recursos de la infraestructura tecnológica y los sistemas de información. Además, velará por la custodia de los registros de auditoria cumpliendo con los periodos de retención establecidos para dichos registros. La Dirección de Tecnologías definirá la realización de monitoreo de los registros de auditoria sobre los aplicativos donde se opera los procesos estratégicos de la UEA y se encaragara de la revisión de logs para analizar los resultados del monitoreo efectuado.

12.4.1. Normas de registro de eventos y monitoreo de los recursos tecnológicos y los sistemas de información

Normas dirigidas a la Dirección de Tecnologías:

- La Dirección de Tecnologías, debe determinar los eventos que generarán registros de auditoría en los recursos tecnológicos y los sistemas de información.
- La Dirección de Tecnologías, debe definir los monitoreos se realizarán de los registros sobre los aplicativos donde se opera los procesos estratégicos de la UEA. Así mismo, se debe analizar los resultados de cada monitoreo efectuado.
- La Dirección de Tecnologías, a través de sus funcionarios, debe habilitar los registros de auditoría y sistemas de monitoreo de la plataforma tecnológica administrada, acorde con los eventos a auditar establecidos.
- La Dirección de Tecnologías debe certificar la integridad y disponibilidad de los registros de auditoria generados en la infraestructura tecnológica y los sistemas de información. Estos registros deben ser almacenados y solo deben ser accedidos por personal autorizado.

Normas dirigidas a desarrolladores (internos y externos):

- Los desarrolladores deben generar registros (logs) de auditoría de las actividades realizadas por los usuarios finales y administradores en los sistemas de información desarrollados. Se deben utilizar controles de integridad sobre dichos registros.
- Los desarrolladores deben registrar en los logs de auditoría eventos como: fallas de validación, intentos de autenticación fallidos y exitosos, fallas en los controles de acceso, intento de evasión de controles, excepciones de los sistemas, funciones administrativas y cambios de configuración de seguridad, entre otros, de acuerdo con las directrices establecidas por la Dirección de Tecnologías.
- Los desarrolladores deben evitar almacenar datos innecesarios de los sistemas construidos en los logs de auditoria que brinden información adicional a la estrictamente requerida.

12.5. POLITICA DE CONTROL AL SOFTWARE OPERATIVO

La UEA, a través de la Dirección de Tecnologías, designará responsables y establecerá procedimientos para controlar la instalación de software operativo, se cerciorará de contar con el soporte de los proveedores de dicho software y asegurará la funcionalidad de los sistemas de información que operan sobre la plataforma tecnológica cuando el software operativo es actualizado.

12.5.1. Normas de control al software operativo

Normas dirigidas a la Dirección de Tecnologías:

- La Dirección de Tecnologías debe establecer responsabilidades y procedimientos para controlar la instalación del software operativo.
- La Dirección de Tecnologías debe asegurarse que el software operativo instalado en los recursos tecnológicos de la UEA cuenta con soporte de los proveedores.
- La Dirección de Tecnologías debe validar los riesgos que genera la migración hacia nuevas versiones del software operativo. Se debe asegurar el correcto funcionamiento de sistemas de información y herramientas de software que se ejecutan sobre los recursos tecnológicos cuando el software operativo es actualizado.
- La Dirección de Tecnologías debe establecer las restricciones y limitaciones para la instalación de software operativo en los equipos de cómputo.

12.6. POLÍTICA DE GESTIÓN DE VULNERABILIDADES

La UEA, a través de la Dirección de Tecnologías revisará periódicamente la aparición de vulnerabilidades técnicas sobre los recursos de la tecnológica por medio de la realización periódica de pruebas de vulnerabilidades, con el objetivo de realizar la corrección sobre los hallazgos arrojados por dichas pruebas. Se designará un encargado de revisar, valorar y gestionar las vulnerabilidades técnicas encontradas.

12.6.1. Normas para la gestión de vulnerabilidades

Normas dirigidas a la Dirección de Tecnologías:

- La Dirección de Tecnologías debe revisar periódicamente la aparición de nuevas vulnerabilidades técnicas y reportarlas a los administradores de la infraestructura tecnológica y los desarrolladores de los sistemas de información, con el fin de prevenir la exposición al riesgo de estos.
- La Dirección de Tecnologías, a través de sus funcionarios, debe generar y ejecutar o monitorear planes de acción para la mitigación de las vulnerabilidades técnicas detectadas en la plataforma tecnológica.
- La Dirección de Tecnologías debe revisar, valorar y gestionar las vulnerabilidades técnicas encontradas, apoyándose en herramientas tecnológicas para su identificación.

13. POLÍTICAS DE SEGURIDAD EN LAS COMUNICACIONES

13.1. POLÍTICA DE GESTION Y ASEGURAMIENTO DE LAS REDES DE DATOS

La UEA establecerá, a través de la Dirección de Tecnologías, los mecanismos de control necesarios para proveer la disponibilidad de las redes de datos y de los servicios que dependen de ellas; así mismo, velará por que se cuente con los mecanismos de seguridad que protejan la integridad y la confidencialidad de la información que se transporta a través de dichas redes de datos.

De igual manera, propenderá por el aseguramiento de las redes de datos, el control del tráfico en dichas redes y la protección de la información reservada y restringida.

13.1.1. Normas de gestión y aseguramiento de las redes de datos

Normas dirigidas a la Dirección de Tecnologías:

- La Dirección de Tecnologías debe adoptar medidas para asegurar la disponibilidad de los recursos y servicios de red de la UEA.
- La Dirección de Tecnologías debe implantar controles para minimizar los riesgos de seguridad de la información transportada por medio de las redes de datos.
- La Dirección de Tecnologías debe mantener las redes de datos segmentadas por dominios, grupos de servicios, grupos de usuarios, ubicación geográfica o cualquier otra tipificación que se considere conveniente para la UEA.
- La Dirección de Tecnologías debe identificar los mecanismos de seguridad y los niveles de servicio de red requeridos e incluirlos en los acuerdos de servicios de red, cuando estos se contraten externamente.

- La Dirección de Tecnologías debe establecer los estándares técnicos de configuración de los dispositivos de seguridad y de red de la infraestructura tecnológica, acogiendo buenas prácticas de configuración segura.
- La Dirección de Tecnologías, a través de sus funcionarios, debe identificar, justificar y documentar los servicios, protocolos y puertos permitidos por la UEA en sus redes de datos e inhabilitar o eliminar el resto de los servicios, protocolos y puertos.
- La Dirección de Tecnologías debe instalar protección entre las redes internas de la UEA y cualquier red externa, que este fuera de la capacidad de control y administración de la UEA.
- La Dirección de Tecnologías debe velar por la confidencialidad de la información del direccionamiento y el enrutamiento de las redes de datos.

13.2. POLÍTICA DE USO DEL CORREO ELECTRÓNICO

La UEA, entendiendo la importancia del correo electrónico como herramienta para facilitar la comunicación entre funcionarios y terceras partes, proporcionará un servicio idóneo y seguro para la ejecución de las actividades que requieran el uso del correo electrónico, respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones a través de este medio.

13.2.1. Normas de uso del correo electrónico

Normas dirigidas a la Dirección de Tecnologías:

- La Dirección de Tecnologías debe generar y divulgar un procedimiento para la administración de cuentas de correo electrónico.
- La Dirección de Tecnologías debe diseñar y divulgar las directrices técnicas para el uso de los servicios de correo electrónico.
- La Dirección de Tecnologías debe proveer un ambiente seguro y controlado para el funcionamiento de la plataforma de correo electrónico.
- La Dirección de Tecnologías debe establecer procedimientos e implantar controles que permitan detectar y proteger la plataforma de correo electrónico contra código malicioso que pudiera ser transmitido a través de los mensajes.
- La Dirección de Tecnologías, debe generar campañas para concientizar a los funcionarios internos, respecto a las precauciones que deben adoptar en el intercambio de información sensible por medio del correo electrónico.

Normas dirigidas a todos los usuarios:

- La cuenta de correo electrónico asignada es de carácter individual; por consiguiente, ningún funcionario bajo ninguna circunstancia debe utilizar una cuenta de correo que no sea la suya.
- Los mensajes y la información contenida en los correos electrónicos deben ser relacionados con el desarrollo de las labores y funciones de cada usuario en apoyo a los objetivos institucionales. El correo institucional no debe ser utilizado para actividades personales.
- Los mensajes y la información contenida en los buzones de correo son propiedad de la UEA. Cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.

- Los usuarios de correo electrónico institucional tienen prohibido el envió de cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana y resulten ofensivas para los funcionarios de la UEA.
- No es permitido el envío de archivos que contengan extensiones ejecutables, bajo ninguna circunstancia.
- Todos los mensajes enviados deben respetar el estándar de formato e imagen institucional.

13.3. POLÍTICA DE USO ADECUADO DE INTERNET

La UEA consciente de la importancia de Internet como una herramienta para el desempeño de labores, proporcionará los recursos necesarios para asegurar su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias en la institución

13.3.1. Normas de uso adecuado de internet

Normas dirigidas a la Dirección de Tecnologías:

- La Dirección de Tecnologías debe proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet.
- La Dirección de Tecnologías debe diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.
- La Dirección de Tecnologías debe monitorear continuamente el canal o canales del servicio de Internet.
- La Dirección de Tecnologías debe establecer procedimientos e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos.
- La Dirección de Tecnologías debe establecer e implantar procedimientos de monitoreo sobre la utilización del servicio de Internet.
- La Dirección de Tecnologías debe generar campañas para concientizar tanto a los funcionarios como estudiantes respecto a las precauciones que deben tener en cuenta cuando utilicen el servicio de Internet.

Normas dirigidas a todos los usuarios:

- Los usuarios del servicio de Internet deben hacer uso del mismo en relación con las actividades laborales o académicas que así lo requieran.
- Los usuarios del servicio de Internet deben evitar la descarga de software desde internet, así como su instalación en las estaciones de trabajo o dispositivos móviles asignados para el desempeño de sus labores.
- No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas establecidas en este documento.
- No está permitido la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas

que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros. La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por su inmediato superior y la Dirección de Tecnología, o a quienes ellos deleguen de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.

- No está permitido el intercambio no autorizado de información de propiedad de la UEA, estudiantes y/o de sus funcionarios, con terceros

13.4. POLÍTICA DE INTERCAMBIO DE INFORMACIÓN

La UEA asegurará la protección de la información en el momento de ser transferida o intercambiada con otras entidades y establecerá los procedimientos y controles necesarios para el intercambio de información; así mismo, se establecerán Acuerdos de Confidencialidad y/o de Intercambio de Información con las terceras partes con quienes se realice dicho intercambio. La UEA propenderá por el uso de tecnologías informáticas y de telecomunicaciones para llevar a cabo el intercambio de información; sin embargo, establecerá directrices para el intercambio de información en medio físico

13.4.1. Normas de intercambio de información

Normas dirigidas a la Dirección de Planificación y Evaluación:

- La Dirección de Planificación y Evaluación debe definir y establecer el procedimiento de intercambio de información con terceros que reciben o envían información institucional, que contemple la utilización de medios de transmisión confiables y la adopción de controles, con el fin de proteger la confidencialidad e integridad de la misma.
- La Dirección de Planificación y Evaluación debe velar que el intercambio de información con entidades externas se realice en cumplimiento de las Políticas de seguridad para el intercambio de información aquí descritas, los Acuerdos de Intercambio de Información y el procedimiento definido para dicho intercambio de información.
- La Dirección de Planificación y Evaluación debe autorizar el establecimiento del vínculo de transmisión de información con terceras partes, para que posteriormente las áreas funcionales realicen las actividades de transmisión requeridas en cada caso.

Normas dirigidas a Propietarios de los Activos de Información:

- Los propietarios de los activos de información deben velar porque la información de la UEA sea protegida de divulgación no autorizada por parte de los terceros a quienes se entrega esta información, verificando el cumplimiento de las clausulas relacionadas en los contratos o Acuerdos de confidencialidad establecidos.
- Los propietarios de los activos de información deben asegurar que los datos requeridos sólo puedan ser entregada a terceros, previo autorización de la máxima autoridad, salvo en los casos que lo disponga una ley o sea una solicitud de los entes de control.
- Los propietarios de los activos de información, o a quien ellos deleguen, deben verificar que el intercambio de información con terceros deje registro del tipo de

información intercambiada, el emisor y receptor de la misma y la fecha de entrega/recepción.

- Los propietarios de los activos de información deben asegurarse que el Intercambio de información (digital) solamente se realice si se encuentra autorizada y dando cumplimiento a las Políticas de administración de redes, de acceso lógico y de protección de datos personales de la UEA así como del procedimiento de intercambio de información.

Normas dirigidas a Secretaria General:

- La Secretaria General debe acoger el procedimiento para el intercambio, de información (medios de almacenamiento y documentos) con terceras partes y la adopción de controles a fin de proteger la información sensible contra divulgación, pérdida o modificaciones.
- La Secretaria General debe certificar que todo envió de información física a terceros (documento o medio magnético) utilice únicamente los servicios de transporte o servicios de mensajería autorizados por la UEA, y que estos permitan ejecutar rastreo de las entregas.

Normas dirigidas a la Dirección de Tecnologías:

- La Dirección de Tecnologías debe ofrecer servicios o herramientas de intercambio de información seguros, así como adoptar controles como el cifrado de información, que permitan el cumplimiento del procedimiento para el intercambio de información (digital o medio magnético), con el fin de proteger dicha información contra divulgación o modificaciones no autorizadas.

Normas dirigidas a terceros con quienes se intercambia información de la UEA:

- Los terceros con quienes se intercambia información de la UEA deben darle manejo adecuado a la información recibida, en cumplimiento de las Políticas de seguridad de la UEA, de las condiciones contractuales establecidas y del Procedimiento de intercambio de información.

Normas dirigidas a todos los usuarios:

- No está permitido el intercambio de información sensible de la universidad por vía telefónica

14. POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

14.1. POLÍTICA PARA EL ESTABLECIMIENTO DE REQUISITOS DE SEGURIDAD

La UEA asegurará que el software adquirido y desarrollado tanto al interior de la UEA, como por terceras partes, cumplirá con los requisitos de seguridad y calidad establecidos por la UEA. Las áreas propietarias de sistemas de información y la Dirección de Tecnologías incluirán requisitos de seguridad en la definición de requerimientos y posteriormente se asegurarán que estos se encuentren generados a cabalidad durante las pruebas realizadas sobre los desarrollos del software construido

14.1.1. Normas para el establecimiento de requisitos de seguridad

Normas dirigidas a propietarios de los Sistemas de Información, Dirección de Tecnologías:

- Todos los sistemas de información o desarrollos de software deben tener un área propietaria dentro del UEA formalmente asignada.
- La Dirección de Tecnologías debe establecer metodologías para el desarrollo de software, que incluyan la definición de requerimientos de seguridad y las buenas prácticas de desarrollo seguro, con el fin de proporcionar a los desarrolladores una visión clara de lo que se espera.
- Las áreas propietarias de los sistemas de información, en acompañamiento con la Dirección de Tecnologías deben establecer las especificaciones de adquisición o desarrollo de sistemas de información, considerando requerimientos de seguridad de la información.
- Las áreas propietarias de los sistemas de información deben definir qué información sensible puede ser eliminada de sus sistemas y solicitar que estos soporten la eliminación de dicha información, como es el caso de los datos personales o financieros, cuando estos ya no son requeridos.
- La Dirección de Tecnologías debe liderar la definición de requerimientos de seguridad de los sistemas de información, teniendo en cuenta aspectos como la estandarización de herramientas de desarrollo, controles de autenticación, controles de acceso y arquitectura de aplicaciones, entre otros.

Normas dirigidas a desarrolladores (internos o externos):

- Los desarrolladores deben documentar los requerimientos establecidos y definir la arquitectura de software más conveniente para cada sistema de información que se quiera desarrollar, de acuerdo con los requerimientos de seguridad y los controles deseados.
- Los desarrolladores deben certificar que todo sistema de información adquirido o desarrollado utilice herramientas de desarrollo licenciadas y/o reconocidas en el mercado.
- Los desarrolladores deben deshabilitar las funcionalidades de completar automáticamente en formularios de solicitud de datos que requieran información sensible.
- Los desarrolladores deben establecer el tiempo de duración de las sesiones activas de las aplicaciones, terminándolas una vez se cumpla este tiempo.
- Los desarrolladores deben asegurar que no se permitan conexiones recurrentes a los sistemas de información construidos con el mismo usuario.
- Los desarrolladores deben usar los protocolos sugeridos por la Dirección de Tecnologías en los aplicativos desarrollados.

14.2. POLÍTICA DE DESARROLLO SEGURO, REALIZACION DE PRUEBAS Y SOPORTE DE LOS SISTEMAS

La UEA velará porque el desarrollo interno o externo de los sistemas de información cumpla con los requerimientos de seguridad esperados, con las buenas prácticas para desarrollo seguro de aplicativos, así como con metodologías para la realización de pruebas de aceptación y seguridad al software desarrollado. Además, se asegurará que todo software

desarrollado o adquirido, interna o externamente cuenta con el nivel de soporte requerido por la UEA.

14.2.1. Normas de desarrollo seguro, realización de pruebas y soporte de los sistemas

Normas dirigidas a propietarios de los sistemas de información:

- Los propietarios de los sistemas de información son responsables de realizar las pruebas para asegurar que cumplen con los requerimientos de seguridad establecidos antes del paso a producción de los sistemas, utilizando metodologías establecidas para este fin, documentado las pruebas realizadas y aprobando los pasos a producción. Estas pruebas deben realizarse por entrega de funcionalidades nuevas, por ajustes de funcionalidad o por cambios sobre la plataforma tecnológica en la cual funcionan los aplicativos.
- Los propietarios de los sistemas de información deben aprobar las migraciones entre los ambientes de desarrollo, pruebas y producción de sistemas de información nuevos y/o de cambios o nuevas funcionalidades.

Normas dirigidas a la Dirección de Tecnologías:

- La Dirección de Tecnologías debe implantar los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo, pruebas y producción han sido aprobadas, de acuerdo con el procedimiento de control de cambios.
- La Dirección de Tecnologías debe contar con sistemas de control de versiones para administrar los cambios de los sistemas de información.
- La Dirección de Tecnologías debe asegurarse que los sistemas de información adquiridos o desarrollados por terceros, cuenten con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.
- La Dirección de Tecnologías debe generar metodologías para la realización de pruebas al software desarrollado, que contengan pautas para la selección de escenarios, niveles, tipos, datos de pruebas y sugerencias de documentación.
- La Dirección de Tecnologías debe verificar que las pruebas de seguridad sobre los sistemas de información se realicen de acuerdo con las metodologías definidas, contando con pruebas debidamente documentadas.
- La Dirección de Tecnologías, a través de sus funcionarios, se debe asegurar que la infraestructura tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información estén actualizados con todos los parches generados para las versiones en uso y que estén ejecutando la última versión aprobada del sistema.
- La Dirección de Tecnologías debe incluir dentro del procedimiento y los controles de gestión de cambios el manejo de los cambios en el software aplicativo y los sistemas de información de la institución.

Normas dirigidas a desarrolladores (internos o externos):

- Los desarrolladores de los sistemas de información deben considerar las buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de los mismos, pasando desde el diseño hasta la puesta en marcha.

- Los desarrolladores deben proporcionar un nivel adecuado de soporte para solucionar los problemas que se presenten en el software aplicativo; dicho soporte debe contemplar tiempos de respuesta aceptables.
- Los desarrolladores deben construir los aplicativos de tal manera que efectúen las validaciones de datos de entrada y la generación de los datos de salida de manera confiable, utilizando rutinas de validación centralizadas y estandarizadas.
- Los desarrolladores deben asegurar que los sistemas de información construidos validen la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como: tipos de datos, rangos válidos, longitud, listas de caracteres aceptados, caracteres considerados peligrosos y caracteres de alteración de rutas, entre otros.
- Los desarrolladores deben suministrar opciones de desconexión o cierre de sesión de los aplicativos (logout) que permitan terminar completamente con la sesión o conexión asociada, las cuales deben encontrarse disponibles en todas las páginas protegidas por autenticación.
- Los desarrolladores deben asegurar el manejo de operaciones sensibles o críticas en los aplicativos desarrollados permitiendo el uso de dispositivos adicionales como tokens o el ingreso de parámetros adicionales de verificación.
- Los desarrolladores deben asegurar que los aplicativos proporcionen la mínima información de la sesión establecida, almacenada en cookies y complementos, entre otros.
- Los desarrolladores deben garantizar que no se divulgue información sensible en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios; así mismo, deben implementar mensajes de error genéricos.
- Los desarrolladores deben remover todas las funcionalidades y archivos que no sean necesarios para los aplicativos, previo a la puesta en producción.
- Los desarrolladores deben prevenir la revelación de la estructura de directorios de los sistemas de información construidos.
- Los desarrolladores deben remover información innecesaria en los encabezados de respuesta que se refieran a los sistemas operativos y versiones del software utilizado.
- Los desarrolladores deben evitar incluir las cadenas de conexión a las bases de datos en el código de los aplicativos. Dichas cadenas de conexión deben estar en archivos de configuración independientes, los cuales se recomienda que estén cifrados.
- Los desarrolladores deben certificar el cierre de la conexión a las bases de datos desde los aplicativos tan pronto como estas no sean requeridas.
- Los desarrolladores deben desarrollar los controles necesarios para la transferencia de archivos, como exigir autenticación, vigilar los tipos de archivos a transmitir, almacenar los archivos transferidos en repositorios destinados para este fin o en bases de datos, eliminar privilegios de ejecución a los archivos transferidos y asegurar que dichos archivos solo tengan privilegios de lectura.
- Los desarrolladores deben proteger el código fuente de los aplicativos construidos, de tal forma de que no pueda ser descargado ni modificado por los usuarios.
- Los desarrolladores deben asegurar que no se permite que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo.

14.3. POLÍTICA PARA LA PROTECCION DE LOS DATOS DE PRUEBA

La Dirección de Tecnologías de la UEA protegerá los datos de prueba que se entregarán a los desarrolladores, asegurando que no revelan información confidencial de los ambientes de producción.

14.3.1. Normas para la protección de los datos de prueba

Normas dirigidas a la Dirección de Tecnologías:

- La Dirección de Tecnologías debe certificar que la información a ser entregada a los desarrolladores para sus pruebas será enmascarada y no revelará información confidencial de los ambientes de producción.
- La Dirección de Tecnologías debe eliminar la información de los ambientes de pruebas, una vez estas han concluido.

15. POLÍTICAS DE GESTIÓN DE INCIDENTES DE SEGURIDAD

15.1. POLÍTICA PARA EL REPORTE Y TRATAMIENTO DE INCIDENTES DE SEGURIDAD

La UEA promoverá entre los funcionarios el reporte de incidentes relacionados con la seguridad de la información y sus medios de procesamiento, incluyendo cualquier tipo de medio de almacenamiento de información, como la infraestructura tecnológica, los sistemas de información, los medios físicos de almacenamiento y las personas.

De igual manera, asignará responsables para el tratamiento de los incidentes de seguridad de la información, quienes tendrán la responsabilidad de investigar y solucionar los incidentes reportados, tomando las medidas necesarias para evitar su reincidencia y escalando los incidentes de acuerdo con su criticidad.

La Máxima Autoridad o a quien delegue, son los únicos autorizados para reportar incidentes de seguridad ante las autoridades gubernamentales; así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante entidades externas.

15.1.1. Normas para el reporte y tratamiento de incidentes de seguridad

Normas dirigidas a propietarios de los activos de información:

- Los propietarios de los activos de información deben informar a la Dirección de Tecnologías los incidentes de seguridad que identifiquen o que reconozcan su posibilidad de materialización.

Normas dirigidas a la Dirección de Tecnologías:

- La Dirección de Tecnologías debe establecer responsabilidades y procedimientos para asegurar una respuesta rápida, ordenada y efectiva frente a los incidentes de seguridad de la información.
- La Dirección de Tecnologías debe evaluar todos los incidentes de seguridad de acuerdo a sus circunstancias particulares y escalar a la Máxima Autoridad aquellos en los que se considere pertinente.
- La Dirección de Tecnologías debe designar personal calificado, para investigar adecuadamente los incidentes de seguridad reportados, identificando las causas,

realizando una investigación exhaustiva, proporcionando las soluciones y finalmente previniendo su re-ocurrencia.

- La Dirección de Tecnologías, debe crear bases de conocimiento para los incidentes de seguridad presentados con sus respectivas soluciones, con el fin de reducir el tiempo de respuesta para los incidentes futuros, partiendo de dichas bases de conocimiento.

Normas dirigidas a todos los usuarios:

- Es responsabilidad de los funcionarios de la UEA reportar cualquier evento o incidente relacionado con la información y/o los recursos tecnológicos con la mayor prontitud posible.
- En caso de conocer la pérdida o divulgación no autorizada de información clasificada como uso interno, reservada o restringida, los funcionarios deben notificarlo a la Dirección de Tecnologías para que se registre y se le dé el trámite necesario.

16. POLÍTICAS DE INCLUSIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

16.1. POLÍTICA DE CONTINUIDAD, CONTINGENCIA, RECUPERACIÓN Y RETORNO A LA NORMALIDAD CON CONSIDERACIONES DE SEGURIDAD DE LA INFORMACIÓN

La UEA proporcionará los recursos suficientes para brindar una respuesta efectiva de funcionarios y procesos en caso de contingencia o eventos catastróficos que se presenten en la universidad y que afecten la continuidad de su operación.

Además, responderá de manera efectiva ante eventos catastróficos según la magnitud y el grado de afectación de los mismos; se restablecerán las operaciones con el menor costo y pérdidas posibles, manteniendo la seguridad de la información durante dichos eventos. La UEA mantendrá canales de comunicación adecuados hacia funcionarios, proveedores y terceras partes interesadas.

16.1.1. Normas de continuidad, contingencia, recuperación y retorno a la normalidad con consideraciones de seguridad de la información

Normas dirigidas a la Dirección de Tecnologías:

- La Dirección de Tecnologías, debe elaborar un plan de recuperación ante desastres para el centro de datos y un conjunto de procedimientos de contingencia, recuperación y retorno a la normalidad para cada uno de los servicios y sistemas prestados.
- La Dirección de Tecnologías debe participar activamente en las pruebas de recuperación ante desastres y notificar los resultados a la Máxima Autoridad de la UEA.

Normas dirigidas a Vicerrectores y Directores:

- Los Vicerrectores y Directores deben identificar y al interior de sus áreas, generar la documentación de los procedimientos de continuidad que podrían ser utilizados en caso de un evento adverso, teniendo en cuenta la seguridad de la información. Estos documentos deben ser probados para certificar su efectividad.

16.2. POLÍTICA DE REDUNDANCIA

La UEA propenderá por la existencia de una plataforma tecnológica redundante que satisfaga los requerimientos de disponibilidad aceptables para la universidad.

16.2.1. Normas de redundancia

Normas dirigidas a la Dirección de Tecnologías:

- La Dirección de Tecnologías debe analizar y establecer los requerimientos de redundancia para los sistemas de información críticos de la UEA y la infraestructura tecnológica que los apoya.
- La Dirección de Tecnologías debe evaluar y probar soluciones de redundancia tecnológica y seleccionar la solución que mejor cumple los requerimientos de la UEA.
- La Dirección de Tecnologías, a través de sus funcionarios, debe administrar las soluciones de redundancia tecnológica y realizar pruebas periódicas sobre dichas soluciones, para asegurar el cumplimiento de los requerimientos de disponibilidad de la UEA.

17. POLÍTICAS DE CUMPLIMIENTO

17.1. POLÍTICA DE CUMPLIMIENTO CON REQUISITOS LEGALES Y CONTRACTUALES

La UEA velará por la identificación, documentación y cumplimiento de la legislación relacionada con la seguridad de la información, entre ella la referente a derechos de autor y propiedad intelectual, razón por la cual propenderá porque el software instalado en los recursos tecnológicos cumpla con los requerimientos legales y de licenciamiento aplicables.

17.1.1. Normas de cumplimiento con requisitos legales y contractuales

Normas dirigidas a la Dirección de Procuraduría:

- La Dirección de Procuraduría debe identificar, documentar y mantener actualizados los requisitos legales, reglamentarios o contractuales aplicables a la UEA y relacionados con seguridad de la información.

Normas dirigidas a la Dirección de Tecnologías:

- La Dirección de Tecnologías debe certificar que todo el software que se ejecuta en la UEA esté protegido por derechos de autor y requiera licencia de uso o, en su lugar sea software de libre distribución y uso.
- La Dirección de Tecnologías debe establecer un inventario con el software y sistemas de información que se encuentran permitidos en las estaciones de trabajo o equipos móviles para el desarrollo de las actividades laborales, así como verificar periódicamente que el software instalado en dichas estaciones de trabajo o equipos móviles corresponda únicamente al permitido.

Normas dirigidas a todos los usuarios:

- Los usuarios no deben instalar software o sistemas de información en sus estaciones de trabajo o equipos móviles suministrados para el desarrollo de sus actividades.

- Los usuarios deben cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software. Es ilegal duplicar software o su documentación sin la autorización del propietario de los derechos de autor y, su reproducción no autorizada es una violación de ley; no obstante, puede distribuirse un número de copias bajo una licencia otorgada.

17.2. POLÍTICA DE PRIVACIDAD Y PROTECCION DE DATOS PERSONALES

En cumplimiento de la Constitución de la república, que en su artículo 66, literal 19, se reconoce y garantizará a las personas: El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La UEA a través de la Dirección de Tecnologías, propenderá por la protección de los datos personales de sus funcionarios, estudiantes, proveedores y demás terceros de los cuales reciba y administre información.

Se establecerán los términos, condiciones y finalidades para las cuales la UEA como responsable de los datos personales obtenidos a través de sus distintos procesos, tratará la información de todas las personas que, en algún momento, por razones de la actividad que desarrolla la universidad, hayan suministrado datos personales.

Así mismo, buscará proteger la privacidad de la información personal de sus funcionarios, estableciendo los controles necesarios para preservar aquella información que la institución conozca y almacene de ellos, velando porque dicha información sea utilizada únicamente para funciones propias de la institución y no sea publicada, revelada o entregada a funcionarios o terceras partes sin autorización

17.2.1. Normas de privacidad y protección de datos personales

Normas dirigidas a las áreas que procesan datos personales:

- Las áreas que procesan datos personales de funcionarios, estudiantes, proveedores y demás terceros deben obtener la autorización para el tratamiento de estos datos con el fin de recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar y transmitir dichos datos personales en el desarrollo de las actividades de la UEA.
- Las áreas que procesan datos personales de funcionarios, estudiantes, proveedores y demás terceros deben asegurar que solo aquellas personas que tengan una necesidad laboral legítima puedan tener acceso a dichos datos.

Normas dirigidas a la Dirección de Tecnologías:

- La Dirección de Tecnologías debe implantar los controles necesarios para proteger la información personal de los funcionarios, estudiantes, proveedores u otras terceras partes almacenada en bases de datos o cualquier otro repositorio y evitar su divulgación, alteración o eliminación sin la autorización requerida.

Normas dirigidas a todos los usuarios:

- Los usuarios deben guardar la discreción correspondiente, o la reserva absoluta con respecto a la información de la UEA o de sus funcionarios de cual tengan conocimiento en el ejercicio de sus funciones.

- Es deber de los usuarios, verificar la identidad de todas aquellas personas, a quienes se les entrega información por teléfono, por fax, por correo electrónico o por correo certificado, entre otros.

Normas dirigidas a usuarios de las plataformas y sistemas de información:

- Los usuarios de las plataformas y sistemas de información deben asumir la responsabilidad individual sobre la clave de acceso a dichos portales que les es suministrada; así mismo, deben cambiar de manera periódica esta clave de acceso.
- Los usuarios de las plataformas y sistemas de información deben contar con controles de seguridad en sus equipos de cómputo o redes privadas para acceder a los portales de la UEA.
- Los usuarios de las plataformas y sistemas de información deben aceptar el suministro de datos personales que pueda hacer la UEA a entidades judiciales y demás entes del Estado que, en ejercicio de sus funciones, solicitan esta información; de igual manera, deben aceptar que pueden ser objeto de procesos de auditoria interna o externa.