UNIVERSIDAD DE MARGARITA
SUBSISTEMA DE DOCENCIA
DECANATO DE INGENIERÍA Y AFINES
COORDINACIÓN DE INVESTIGACIÓN Y PASANTÍA

DISEÑO DE UN PLAN DE SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO/IEC 27001 PARA LA UNIVERSIDAD DE MARGARITA (UNIMAR), UBICADA EN EL VALLE DEL ESPIRITU SANTO, ISLA DE MARGARITA, NUEVA ESPARTA, VENEZUELA

Elaborado por: Patricia Valentina Zacarías Rodríguez

Tutor: Ing. Gabriel Alejandro Delgado Sánchez

El Valle del Espíritu Santo, noviembre de 2022

ÍNDICE

ÍNDICE DE TABLAS

INDICE DE FIGURAS

UNIVERSIDAD DE MARGARITA

SUBSISTEMA DE DOCENCIA

COORDINACIÓN DE INVESTIGACIÓN

DISEÑO DE UN PLAN DE SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO/IEC 27001 PARA LA UNIVERSIDAD DE MARGARITA (UNIMAR), UBICADA EN EL VALLE DEL ESPIRITU SANTO, ISLA DE MARGARITA, NUEVA ESPARTA, VENEZUELA

Autor: Patricia Valentina Zacarías Rodríguez

Tutor: Ing. Gabriel Delgado

Noviembre de 2022

RESUMEN

Hoy en día, la evolución de la tecnología de la información y su relación directa con los procesos educativos es vital para el desarrollo y crecimiento de la sociedad, sin embargo, está lleno de amenazas y vulnerabilidades, por lo que es necesario proteger un activo tan importante como lo es la información que se transmite, almacena, gestiona y distribuye en las tecnologías de información y comunicación. La seguridad informática busca garantizar la confidencialidad, integridad y disponibilidad de los recursos y la organización en la que se implementa y se promueve, mediante la gestión de riesgos, aplicando controles y protocoles dispuestos por las normas ISO a nivel internacional, para la normalización y estandarización de los procesos activos de las organizaciones. La propuesta fue planteada y estructurada para diseñar un plan de seguridad informática basada en la norma ISO/IEC 27001:2013 en la Universidad de Margarita (UNIMAR).

Descriptores: Amenazas, Vulnerabilidades, Tecnología de la Información, Activos, Seguridad Informática, Gestión de riesgos, normas ISO.

INTRODUCCIÓN

La seguridad informática tiene como principal objetivo el preservar los recursos y activos de información en las organizaciones que implementan esta disciplina, así como sus técnicas y metodologías mediante normas estandarizadas y reconocidas internacionalmente por organizaciones referentes en esta materia, como la Organización Internacional de Estandarización (ISO), la cual brinda normas, protocolos y regulaciones en distintas áreas aplicables, las cuales mejoran las prácticas de las organizaciones que las implementan. Asimismo, dispone de un apartado de seguridad informática en la ISO 27001, para las buenas prácticas de seguridad informática, la cual permite el aseguramiento de las operaciones que realiza la institución, así como la confidencialidad, integridad y disponibilidad de los datos y de los sistemas que los procesan dentro de la organización.

Con la finalidad de resguardar la confidencialidad, integridad y disponibilidad gestión de la información, la seguridad informática se ha convertido en un tema de importancia para las organizaciones de cualquier índole. Permitiendo un crecimiento continuo al promover las buenas prácticas de seguridad en las distintas áreas de las organizaciones. Del mismo modo ocurre con las instituciones educativas, las cuales gestionan activos informáticos de carácter vital y sensible, por lo que es necesario contar con las herramientas correctas para su gestión.

La Universidad de Margarita (UNIMAR) no escapa de esta realidad y, al evidenciar que hay una ausencia de normas y políticas, es preciso establecer una adecuada gestión de la seguridad de la información, mediante la implantación de la norma ISO/IEC 27001:2013, realizando una valoración de riesgos, de los controles y protocolos de Tecnología de la Información (TI) de la UNIMAR, mediante la recolección de información con distintas técnicas apropiadas para la gestión de riesgos. Por lo tanto, con el análisis realizado, se procedió a la aplicación de la Norma ISO/IEC 27001:2013 con sus respectivos controles, teniendo como resultado un Plan de Gestión de Seguridad Informática en donde se describen políticas de seguridad de la información y tener un mejor uso de las Tecnologías de la información y Comunicación (TIC) que la institución maneja internamente.

Consecuentemente, la presente investigación se lleva a cabo bajo un enfoque cuantitativo, mediante el que se estudiará la realidad de los hechos de manera objetiva, de acuerdo al objetivo de diseñar un plan de seguridad basado en la norma ISO/IEC 27001:2013, se establece que el tipo de investigación es descriptiva y un proyecto factible, complementado con el diseño de campo del

estudio; lo cual permite proponer una solución viable a la problemática expuesta desde un enfoque general. Así pues, para cumplir lo establecido anteriormente, el trabajo se encuentra conformado por cinco (5) partes que, a su vez, se componen como se expresa a continuación:

En la Parte I, se presenta la descripción general del problema, en la cual se formula de forma detallada el problema bajo un enfoque deductivo, partiendo desde el nivel macro al nivel micro. Asimismo, se establecen las interrogantes y los objetivos generales y específicos de la investigación, los cuales sirven de norte para el estudio; y, por último, se expone el valor académico de la misma.

En la Parte ll, que enmarca la descripción teórica, se presentan los trabajos que sirven de antecedentes de la presente investigación, además de las bases teóricas y legales y la definición de términos que sustentan a nivel teórico las temáticas tratadas y que se pueden encontrar a lo largo del trabajo.

En la Parte III, se vislumbra la descripción metodológica, por medio de la cual se define la naturaleza, tipo y diseño de la investigación, se delimita la población y muestra con la que se trabaja, y se detallan las técnicas de recolección y análisis de datos implementados.

En la Parte IV, se realiza el análisis y presentación de los datos obtenidos mediante la aplicación de las técnicas previamente seleccionadas y se agrupan de acuerdo a los objetivos que satisfacen previamente definidos en el trabajo.

En la Parte V, se desarrolla la propuesta, comenzando con el planteamiento de la importancia de aplicación de la misma, seguido de la presentación de la viabilidad de aplicación de la propuesta, así como de las factibilidad técnica, operativa y económica de la misma; al igual que se define el objetivo general y los específicos de dicha propuesta y su representación gráfica y estructura.

Finalmente, se expone las Conclusiones y Recomendaciones obtenidas tras la culminación del proceso investigativo, al mismo tiempo que se muestra el listado de las fuentes que sirvieron de referencias consultadas en la investigación.

PARTE I

DESCRIPCIÓN GENERAL DEL PROBLEMA

En este primer capítulo se describe detalladamente el problema planteado en la investigación, en el cual se ejemplifica la problemática del objeto de estudio y el contexto de la misma. De igual forma, se expondrán las interrogantes del estudio, así como también los objetivos, tanto el objetivo general, como los objetivos específicos, además, se expone el valor académico que implica esta investigación.

1.1 Formulación del problema

Los métodos aplicables y la estandarización de sistemas en el área de seguridad informática han adquirido un alto valor para las organizaciones, dada la cantidad de ataques a los sistemas informáticos que estas sufren y al alto porcentaje de vulnerabilidad existente. En tal sentido, la información, como uno de los activos de una organización, posee un nivel de importancia imposible de ignorar y, por tanto, se emplean sistemas que manejen la información y la comunicación para el funcionamiento de los distintos procesos que se desarrollan dentro de la entidad. Es evidente que la incidencia de ataques informáticos a nivel mundial va en pleno ascenso, inclusive gobiernos destinan grandes cantidades de recursos en materia de ciberseguridad y crean leyes para penalizar a los agresores. Según Gómez, A (2006), en su obra Enciclopedia de la Seguridad Informática, define la seguridad informática como:

> (…) cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema.

El desarrollo tecnológico, la innovación en el área de informática y las telecomunicaciones, y especialmente el efecto sinérgico entre ambas, está suponiendo un cambio trascendental en la sociedad actual, lo cual implica un aumento en el ámbito de ciberseguridad. El impacto de la globalización, acompañado de la creciente implantación de las tecnologías, trae consigo beneficios paras las organizaciones y empresas de toda índole, pero a la vez producen grandes problemas de seguridad, como la protección de datos y privacidad, con los cuales las organizaciones tendrán que enfrentarse. Aguinaga, H (2013), expresa que:

> Al hacer uso de las tecnologías para almacenar, mantener, transmitir y recobrar información, las amenazas existentes podrían afectar la confidencialidad,

> disponibilidad e integridad de la información vital para la organización, el negocio y los clientes, provocando de esta forma graves pérdidas económicas, y de tiempo para la organización.

Se entiende que existen diferentes tipos de amenazas que atentan contra el buen funcionamiento de estos entes, como los virus, malware, cibercriminales, spyware y un sinfín de amenazas existentes. No obstante, para la implementación de estrategias no solo se estudian y clasifican los ataques intencionados, dado que en promedio un 85% de las infracciones de seguridad cibernética son causadas por errores humanos, de acuerdo a un estudio realizado por la empresa Verizon en 2021. De hecho, la revista Cybersegurity Ventures y sus analistas expertos, predicen que los costos asociados con los delitos cibernéticos crecerán anualmente un 15% durante los próximos cinco años.

Así pues, en términos generales, la seguridad informática se encarga de la seguridad del medio informático, también se le denomina como la ciencia administradora de los procesos, técnicas y métodos que buscan procesar almacenar y transmitir la información. De modo que, al implementar este tipo de seguridad, se busca minimizar los riesgos, en este caso provienen de muchas partes y factores, ya sea de la entrada de datos, del medio que transporta la información, del hardware empleado para transmitir y recibir, los usuarios en sí mismos e incluso pueden ser los mismos protocolos implementados. Según la Asociación de Auditoría y Control de Sistemas de Información (ISACA, por sus siglas en inglés) (2017), definen la ciberseguridad como “una capa de protección para los archivos de información. Las cuales ponen en riesgo la información que es procesada, transportada y almacenada en cualquier dispositivo”. En concordancia con lo expuesto, no se trata solo de prevenir ataque. También significa desarrollar estrategias de capacitación a empleados y usuarios para evitar estos ataques.

Consecuentemente, existe un organismo no gubernamental el cual se encuentra presente en más de 200 países, el cual tiene por misión la promoción del uso de estándares industriales y comerciales a nivel internacional. Las Normas ISO, tienen su origen en la denominada Organización Internacional para la Estandarización (ISO), por la cual llevan el mismo nombre. En principio, la ISO designó distintos comités técnicos para que trabajaran en el desarrollo de normas comunes que fuesen aceptadas en todo el mundo. Posteriormente, en 1987 se publicó un trabajo que luego se conocería como Norma ISO 9000, Sistema de Gestión de Calidad. En términos estrictamente técnicos, las Normas ISO se crearon con la finalidad de ofrecer orientación, coordinación, simplificación y unificación de criterios a las empresas y organizaciones con el objeto de reducir

costos, aumentar la efectividad y establecer criterios comunes referidos a productos y servicios internacionales.

La ISO 27001 tiene el objeto de proteger la confidencialidad, disponibilidad e integridad de los datos de una empresa, mediante un sistema de análisis de los principales riesgos y amenazas que podrían afectar a la información. Es importante entender que, hoy en día, la información engloba diferentes aspectos, como es el caso de la ciberseguridad, las tecnologías de la información y la protección de datos. En Venezuela, esta norma es conocida como FONDONORMA ISO/IEC 27001, y funciona bajo FONDONORMA, una asociación civil sin fines de lucro la cual cuenta con personalidad jurídica y patrimonio propio.

Según la norma ISO 27000 (2013), "la información constituye un activo de las entidades, organizaciones o empresas cualquiera sea su tamaño o función social". Definirse como activo, requiere hacer una medida de valoración que debe ser proporcional al impacto de su pérdida o manipulación mal intencionada. De acuerdo a esto, la ISO 27001 (2013) expresa que: "Los activos son los recursos del Sistema de Seguridad de la Información, necesarios para que la empresa funciones y consiga los objetivos que se ha propuesto la alta dirección". A fin de que se maneje la seguridad informática, se emplea un Sistema de Gestión de Seguridad Informática (SGSI) el cual se basa en un proceso sistemático, protocolizado y manejado por todos los miembros de la entidad, lo que permite una mayor confiabilidad, integridad y disponibilidad de la información en sí misma. Cabe destacar que la creación de un sistema de gestión de este tipo se basa en la identificación de los datos importantes, sus propietarios y el lugar donde se encuentran, así como el conocimiento de las amenazas.

Las ISO son susceptibles a ser aplicadas en diversos ámbitos, y las instituciones educativas no son la excepción, dado que, como todos los ambientes institucionales, se caracterizan por contener reglas o requisitos a los que se deben ajustar los participantes para recibir el apoyo y legitimidad. Como organización, la universidad tiene tres fines fundamentales: el desarrollo de la enseñanza, la investigación y la extensión y por ende en ella se realizan actividades acordes a esos fines. De acuerdo a Mintzberg, H. (1984), "La estructura de la organización puede definirse simplemente como el conjunto de todas las formas en que se divide el trabajo en tareas distintas consiguiendo luego la coordinación de las mismas". De modo que, en el caso de las universidades, las dimensiones académicas**,** administrativa y de gobierno conviven manteniendo interconexiones múltiples y diversas. Las actividades académicas, que constituyen la razón de ser de la institución,

requieren soporte administrativo para poder desarrollarse y deben enmarcarse en las finalidades que se formulan desde el plano político.

Paralelamente, para las universidades se ha convertido en un requisito primordial la gestión de servicios de tecnología de la información, dado que requieren que la prestación de sus servicios se realice con la máxima calidad posible. En todo caso, gracias al estándar ISO 27001, se lleva a cabo la implantación de un SGSI de forma eficiente. Su objetivo es otorgar valor a la información, debido a que se trata de un activo clave para las universidades, para garantizar el éxito de las mismas y la continuidad de su negocio en el mercado, puesto que el principal objetivo para las universidades es asegurar lo mencionado con anterioridad y llevar a cabo los sistemas que procesan esa información.

En efecto, el implementar un SGSI basado en la norma ISO 27001 tiene el objeto de asegurar que la entidad cuente con todos los controles adecuados sobre la confidencialidad, integridad y disponibilidad de la información. De modo que el cumplimiento de esta norma puede ayudar a la institución a demostrar a sus participantes, la seriedad con la que abordan la seguridad de la información. Desde luego, una inversión en seguridad informática le ahorra tiempo y dinero, dado que cuando un equipo ha sido vulnerado y es dañado, el tiempo que lleva solucionar el desperfecto es prolongado; cuando hay un sistema de seguridad diseñado a la medida, los costos en mantenimiento preventivo son menores.

Inclusive, aunque en su mayoría los ciberataques abarcan a la institución en sí, también cabe la posibilidad de que se extienda a los integrantes que tengan alguna relación directa, dada la facilidad de infección en las redes y sistemas adyacentes. Como fue el caso de la Universidad Experimental de las Artes (UNEARTE) quien, en 2017, denunció ante la División Contra Delitos Informáticos del Cuerpo de Investigaciones Científicas Penales y Criminalísticas (CICPC), que el sistema de registro de información académico de la universidad, fue atacado por fuentes desconocidas y toda la información que contenía la base de datos fue secuestrada, pidiendo una recompensa por parte de los ciberdelicuentes.

Tal es el caso de la Universidad de Margarita, una institución que requiere resguardar sus posesiones informáticas, tangibles e intangibles, teniendo en cuenta que el riesgo de perder información podría significar una amenaza a todos los procesos sistemáticos que realiza la universidad, lo cual afectaría a los elementos que lo integran y participan activamente en la entidad. De igual forma, las preocupaciones existentes en relación a la privacidad y gestión de datos

personales es otro de los aspectos destacados del estudio, dado que la accesibilidad al reporte de notas y otras opciones del sistema web oficial de la universidad requieren el mínimo conocimiento de los datos personales de los estudiantes para ingresar.

Muchos de los ataques se presentan como campañas de suplantación por correo electrónico, con las que los atacantes tratan de aumentar su acceso a la red, lo cual ocasiona problemas a sus usuarios. El porqué de los ataques a institutos de educación superior como la Universidad de Margarita viene dado a que las universidades cuentan con amplias bases de datos de miles de estudiantes y personal, que incluyen activos muy valiosos para los ciberatacantes, como información personal, financiera y de investigación y desarrollo.

La importancia de crear un plan estratégico en seguridad informática y cómo debe implementarse en la Universidad de Margarita empieza con establecer los criterios básicos. En este ámbito, la estrategia permite aprovechar y focalizar los recursos disponibles en las áreas de mayor riesgo para que sean rentables. El objetivo siempre debe ser la disminución de riesgos, debido a que no existe el riesgo cero. Por tanto, el plan estratégico de seguridad informática propone una serie de medidas que ayudan a reducir los riesgos en torno a los activos informáticos de la universidad, abarcando aspectos técnicos, legales y organizativos que se deben llevar a cabo para reducir los riesgos provocados por las amenazas que afectan a la institución hasta un nivel aceptable.

1.2 Interrogantes

Respecto a la cuestión central de la investigación, se formula la siguiente pregunta: ¿Cómo diseñar un plan de seguridad informática, basado en la Norma ISO/IEC 27001:2013, permitirá la preservación de confidencialidad, integridad y disponibilidad de los activos de la Universidad de Margarita (UNIMAR)?

En relación a la interrogante principal de la investigación, se desglosan las siguientes interrogantes específicas:

1. ¿Cuáles son los riesgos asociados al sistema de información en la Universidad de Margarita (UNIMAR), mediante la estructura de la norma ISO 27001?
2. ¿Cuáles son los recursos que destina la Universidad de Margarita para la preservación de los activos informáticos?

3. ¿Cómo los departamentos dentro de la Universidad de Margarita implementan los protocolos o normas para la preservación, confidencialidad, integridad y disponibilidad de los activos informáticos?

1.3 Objetivo General

Diseñar un plan de seguridad informática basado en la norma ISO/IEC 27001:2013 para la Universidad de Margarita (UNIMAR), ubicada en El Valle del Espíritu Santo, Isla de Margarita, Nueva Esparta, Venezuela.

1.4 Objetivos Específicos

1. Identificar los riesgos asociados al sistema de información en la Universidad de Margarita (UNIMAR), mediante la estructura de la norma ISO/IEC 27001.
2. Evaluar los recursos que destina la Universidad de Margarita para la preservación de los activos informáticos.
3. Elaborar políticas y normas basadas en la ISO/IEC 27001 para gestionar, monitorear, supervisar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información (SGSI) dentro de los departamentos de la Universidad de Margarita.

1.5 Valor académico de la investigación

El estándar ISO 27001 para los Sistemas de Gestión de la Seguridad de la Información permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos. Es importante destacar que la aplicación de la ISO 27001 significa una diferenciación respecto al resto, que mejora la competitividad y la imagen de una organización. Así pues, la gestión de la Seguridad de la Información se complementa con las buenas prácticas o controles establecidos en la norma ISO 27002.

Para el fin de preservar la información, se ha demostrado que no es suficiente la implantación de controles y procedimientos de seguridad realizados frecuentemente sin un criterio común establecido. Notablemente, los requisitos de la Norma ISO 27001 nos aportan un Sistema de Gestión de la Seguridad de la Información (SGSI), consistente en medidas orientadas a proteger la información, indistintamente del formato de la misma, de forma que se garantice en todo momento la continuidad de las actividades de la entidad.

Una institución como la Universidad de Margarita se beneficiaria de implementar estas estrategias basadas en normas y estándares internacionales, como lo es la ISO 27001 para la gestión de riesgos dentro de la entidad dado que, con un marco de gestión de riesgos sólido, se podrá evitar

la exposición a los distintos tipos de amenazas informáticas. Del mismo modo, la implementación de un SGSI, se tiene un enfoque sistemático para la gestión de la información confidencial de la entidad para que siga siendo seguro. Abarca las personas, procesos y sistemas de Tecnología de la Información (TI). Consecuentemente, el diseño y la implementación de un SGSI (ISO/IEC 27001) dará confianza a los participantes que la seguridad de la información se toma en serio dentro de la organización, estando a la vanguardia en la aplicación de la técnica de procesos para hacer frente a las amenazas de la información y a los problemas de la seguridad.

PARTE II

DESCRIPCIÓN TEÓRICA

En esta parte se hace referencia a la teoría relacionada con el problema previamente planteado, de modo que se pueden evidenciar antecedente a la investigación que sustenten el trabajo actual, así como la descripción de las variables que lo conforman de acuerdo a su importancia y; además, las bases legales que sustentan la investigación de acuerdo al área asociada y por último un glosario de términos asociados al área de estudio.

2.1 Antecedentes

Guamán, J. (2017). DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL DEPARTAMENTO DE INFORMÁTICA DE LA DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DEL COMANDO CONJUNTO DE LAS FF.AA, UTILIZANDO LA NORMA ISO 27001:2013. El estudio realizado se basa en el diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) implementando la norma para establecer políticas de seguridad estandarizadas a nivel internacional, enfocándolas al campo militar y el avance e innovación tecnológica, utilizando metodologías para evaluar y minimizar riesgos, dados los hallazgos de fuga de activos de información. Así pues, el desarrollo de este estudio fue bajo el ciclo Deming, es decir, Planificar, Hacer, Verificar, Actuar (PHVA), dada la estructura organizativa y sus operaciones sistemáticas.

De tal forma que, tiene relevancia en la actual investigación en curso ya que permite ver los distintos enfoques que puede tomar norma ISO en base a la gestión de riesgos y seguridad informática, así como la versatilidad de diseño e implementación de Sistemas de Gestión de Seguridad de la Información (SGSI) en distintas ámbitos, de modo que se busque un desenvolvimiento, transmisión, resguardo y disponibilidad de activos informáticos para los involucrados, siendo propietarios, colaboradores o integrantes de los entes en los que se desarrolla el SGSI.

Espinoza, H. (2013). ANÁLISIS Y DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001:2005 PARA UNA EMPRESA DE PRODUCCIÓN Y COMERCIALIZACIÓN DE PRODUCTOS DE CONSUMO MASIVO. El trabajo plantea la necesidad de protección de activos informáticos en el rubro de producción y distribución de alimentos, tomando los aspectos que plantea la norma

ISO/IEC 27001:2005, buscando desarrollar cada una de las etapas asociadas al diseño del SGSI para la empresa dedicada a la producción de alimentos de consumo masivo en Perú. Además, el diseño planteado está enfocado a adaptarse a los objetivos del proceso de producción, así como a los objetivos estratégicos y de gobierno de la empresa en sí misma, los cuales pueden varias, por tanto, se establecen políticas y normas dentro de la entidad que permitían alcanzar las metas y objetivos.

De acuerdo a esto, la relación a destacar con el presente trabajo es que, sin importar el tipo de organización, estructura organizativa e incluso sus dimensiones, la implementación de un SGSI busca darle importancia a la seguridad de la información, así como facilitar normas y políticas que permitan alcanzar un mejor desenvolvimiento laboral, así como ser críticos en distintas áreas de la entidad. De igual forma, le permitirá alcanzar un mayor nivel de confiabilidad para con el mercado o, en tal caso, el área en el que se desenvuelva la entidad.

Baca, V. (2016). DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA LA UNIDAD DE GESTIÓN EDUCATIVA LOCAL-CHICLAYO. El presente trabajo tiene por objetivo fundamental el diseño de un SGSI basado en las normas ISO/IEC 27001:2013 e ISO/IEC 27002:2013, adoptando el marco de trabajo COBIT 5 para proveer gobierno y gestión para la función de Tecnología de la Información. Así mismo, busca el establecimiento de políticas y controles de seguridad que ayudarán a gestionar los riesgos en la seguridad de la información que maneja la Unidad de Gestión Educativa Local de Chiclayo, mejorando de esta forma la gestión de los incidentes de seguridad que se detecten.

El trabajo de grado previamente mencionado posee similitudes con respecto al trabajo actual en curso, dado que busca y permite mejorar cualquier situación en materia de seguridad de la información, dada la implementación de estándares internacionales y buenas prácticas gracias a las normas 27001 y 27002, dado que estas ISO repercuten directamente en una gestión optima y efectiva con respecto a la organización objeto de estudio, garantizando el cumplimiento de los principios básicos de seguridad de la información.

2.2 Bases Teóricas

2.2.1 Seguridad Informática

Ríos, J. (2015). Define la seguridad informática como "(…) la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas, orientados a proveer condiciones seguras y confiables, para el procesamiento de datos en sistemas informáticos". De acuerdo a esto, la

seguridad informática consiste en garantizar la integridad, disponibilidad y acceso a la información perteneciente a un sistema informático, mediante la implementación de normas, políticas o métodos que permitan la continuidad operativa de este tipo de sistemas dentro de una entidad, con la finalidad de preservar datos informáticos para mantener la confiabilidad en base a los principios de seguridad.

2.2.2 Principios de seguridad informática

Según Bradanovic, T. (2006, pág. 12), en referencia a los principios de la seguridad informática, estos conceptos son analizados como principios elementales:

- La confidencialidad o privacidad se refiere a que la información solo puede ser conocida por individuos autorizados.
- La integridad se refiere a la seguridad de que una información no ha sido alterada, borrada, reordenada o copiada, durante el proceso de transmisión o en su propio equipo de origen.
- La disponibilidad de la información se refiere a la seguridad de que la información pueda ser recuperada en el momento que se necesite. Bradanovic, T. (2006, pág. 13).

Estos principios están orientados a cumplir con los objetivos de la seguridad informática, de modo que permitan minimizar, gestionar, detectar y garantizar la seguridad de los datos. Entendiendo que, además de ser principios elementales, también están directamente relacionados con los distintos ámbitos que integran una entidad, como es el caso del marco legal en el que se incluye la autenticación para el control de acceso de los usuarios, la auditabilidad para el registro y monitoreo, así como la reclamación de propiedad y los demás servicios que ofrecen estos principios.

2.2.3 Riesgos y amenazas asociadas a sistemas de información

Corda et al. (2017) define el riesgo informático como "(…) aquella eventualidad que imposibilita el cumplimiento de un objetivo, es decir, todo aquel peligro o daño que puede afectar el funcionamiento directo o los resultados esperados de un sistema informático".

En tal sentido, Fournier, S. (1985) expone que la diferencia fundamental entre la amenaza y el riesgo está en que:

> (…) la amenaza está relacionada con la probabilidad de que se manifieste un evento natural o un evento provocado, mientras que el riesgo está relacionado con la probabilidad de que se manifiesten ciertas consecuencias, las cuales están íntimamente

relacionadas no sólo con el grado de exposición de los elementos sometidos sino con la vulnerabilidad que tienen dichos elementos a ser afectados por el evento.

Dentro de los sistemas informáticos siempre existirán amenazas que pongan en riesgo al sistema, dado que no existe el riesgo nulo. En la actualidad, y con un entorno altamente digitalizado y dependiente de los servicios de tecnología, las amenazas asociadas a la tecnología son inevitables. Estas atentan contra la seguridad de la información, dado que estas surgen al detectar las vulnerabilidades dentro de los sistemas informáticos. No obstante, los riesgos existen a partir del usuario en sí mismo y el uso incorrecto de la tecnología, así como por vulnerabilidades generadas desde medios internos o externos. De modo que deben tenerse en cuenta:

- Los usuarios pueden generar riesgos, ya sea accidental o intencionadamente dado que son ellos quienes manejan los equipos y, por tanto, una mala implementación puede poner en riesgo al equipo.
- Programas maliciosos, conocidos como malware que están destinados a perjudicar un ordenados cuando se instala o se hace uso ilícito de datos, de modo que, existen los virus, gusanos, troyanos, ransomware, keyloggers, entre otros tipos de amenazas.
- Errores de programación, son considerados vulnerabilidades dentro del sistema, lo que podrá generar una amenaza sobre este y la información que contiene, es decir, son la puerta de entrada para recibir ataques externos o internos. Siendo las principales vulnerabilidades los errores de configuración, de gestión de recursos, en los sistemas de validación, de acceso a los directorios, de gestión y asignación de permisos, entre otras vulnerabilidades.
- Los intrusos son individuos no autorizados que logran acceder a programas o datos que no deberían.
- Siniestro, implica la pérdida o deterioro de material informático por una mala manipulación o mala intención, lo que implicaría situaciones de robo, incendio o inundación.
- Las fallas electrónicas afectan al sistema informático y a todos sus componentes, lo que llevaría a errores lógicos dentro del dispositivo e incluso la perdida de componentes importantes dentro de la arquitectura.
- Catástrofes naturales.

2.2.4 Vulnerabilidades dentro del sistema informático

De acuerdo al Grupo de Informática y Comunicaciones Avanzadas (ICA) (2020), las vulnerabilidades son definidas como "(…) debilidades de un sistema que permite a los atacantes comprometer la confidencialidad, integridad y disponibilidad de los mismos y la información y servicios soportados". Un sistema informático necesita ser eficiente y eficaz para un desarrollo óptimo de procesos operativos, de modo que la presencia de debilidades dentro del mismo puede implicar convertirse en potenciales riesgos. Sin embargo, una o varias vulnerabilidades no causan daño por sí mismas, dado que es necesario que exista una amenaza concisa para poder ocasionar problemas dentro del sistema. No obstante, dado que los sistemas informáticos pertenecen en su mayoría a entidades u organizaciones y son controlados por los usuarios, las áreas que se pueden identificar como vulnerables son:

- La organización en la que se desenvuelve el sistema informático.
- Los procesos y procedimientos que participan en el manejo de la información.
- El personal puede provocar las vulnerabilidades, dado que son los encargados de gestionar y manipular la información física o lógica.
- El ambiente también se verá afectado cuando no se sigan los lineamientos o normas para mantener el espacio estable y libre de riesgos y amenazas.
- Configuraciones de los sistemas de información, si no existe una correcta configuración dentro del sistema en sí, se abre la puerta a vulnerabilidades con posibilidad de ser explotadas por amenazas internas o externas.
- Hardware y Software, de acuerdo a los procesos que realiza la empresa, debe ser el adecuado, entendiendo que emplear programas no aptos ni destinados a tareas en específico, afecta directamente a los principios de seguridad informática de integridad, autenticación y disponibilidad.

2.2.5 Administración de riesgos

Maxitana, J y Naranjo, B (2005, pág. 3) hacen referencia a la administración y los riesgos en el área de Tecnología de la Información (TI) expresando que:

> Mientras la seguridad y los controles de sistemas de información ayudan a administrar los riesgos sin eliminarlos, surge la necesidad de administrar esos riesgos, puesto que el exacto nivel de riesgo nunca puede ser conocido ya que siempre existe un grado de incertidumbre.

Al administrar los riesgos se busca asegurar que las probabilidades y eventos positivos se maximicen y llevar al mínimo la probabilidad y consecuencia de eventos negativos que perjudiquen, en este caso, sistemas informáticos. No obstante, se entiende que no existe el riesgo cero por lo que se debe reducir bajo un criterio crítico y tener entre quien administra los riesgos y estos en sí mismos. De modo que se pueda definir un nivel de riesgo en el que se esté dispuesto a reconocer, de acuerdo al análisis y estudio de los riesgos y lo que estos puedan provocar en la posibilidad de convertirse en amenazas.

2.2.6 Activos informáticos

Orozco, M (2013) define los activos informáticos como "aquellos recursos (hardware y software) con los que cuenta una empresa, es decir, todo elemento que compone el proceso completo de comunicación, partiendo desde la información, el emisor, el medio de transmisión y receptor". Los datos, como información, son partes vitales de los sistemas, lo que los vuelve elementos primordiales en una organización, es decir, que un activo de información es algo que una organización valora y por lo tanto debe proteger. Así pues, los datos, ya sean creados o utilizados por un proceso de la entidad ya sea digital, en papel o en otros medios, son activos informáticos. De igual forma los componentes, como el hardware y el software, que son utilizados para el procesamiento, transporte y almacenamiento de información, por tanto, se incluyen todos aquellos servicios utilizados para la transmisión, recepción y control de estos activos.

Consecuentemente, todas las herramientas, utilidades o funcionalidades empleadas por la organización para el desarrollo y soporte de los sistemas de información que la integran, son activos. También se deben incluir a las personas que manejen dicha información, o los métodos específicos para la gestión de los mismos dentro de la organización; ya sea para realizar cualquier tipo de actividad u operación.

2.2.7 Plan de Gestión de Seguridad Informática

Sevillano, F. (2021) define un plan de gestión de seguridad informática como "(…) documento en el que se describe de forma detallada cómo implementar los sistemas de seguridad y las acciones a ejecutar para conseguir la mayor seguridad cibernética posible dentro de una compañía". Un plan de gestión permite organizar la información recabada, conociendo el contexto de la organización, así como reconocer los riesgos a evaluar, fijar niveles de acuerdo a la estructura organizacional de modo que se puedan tratar y gestionar los riesgos con eficacia.

Dado que el objetico es evaluar todos los riesgos asociados con los activos informáticos que se gestionan en una empresa, su principal meta es alcanzar, cumplir y nunca contradecir los principios de seguridad informática. Un plan de estas características sirve de herramienta para garantizar la privacidad e integridad de los datos que maneja la entidad lo que incrementará su grado de confiabilidad para con los participantes, es decir, los clientes o integrantes de la organización, así como el cumplir y respetar las normativas legales en relación con la protección de datos.

2.2.8 Seguridad de la información

TECON (2018) expone que la seguridad de la información es, dentro de la seguridad informática "(…) el conjunto de medidas preventivas y reactivas que permiten resguardar y proteger la información. (…) son todas aquellas políticas de uso y medidas que afectan al tratamiento de los datos que se utilizan en una organización". La seguridad de la información implica la implementación de técnicas, métodos, normas y políticas críticas y objetivas dirigidas al resguardo de la información. Es aquí en donde se hace presente la gestión y administración de riesgos, así como también de las amenazas, los análisis de escenarios, las buenas prácticas y los esquemas normativos de acuerdo a los estándares existentes. Esta disciplina se encarga de proporcionar toda la información que permita diseñar y trazar un plan de acción y adecuación, siempre con el objetivo de minimizar los riesgos y la incertidumbre, de modo que garantice los principios de seguridad para con la información; confidencialidad, integridad, autenticidad y disponibilidad.

No obstante, no debe confundirse seguridad informática con seguridad de la información, dado que la primera se trata del resguardo de las instalaciones o medios informáticos, así como de la información en medios digitales o lógicos, mientras que la segunda integra los datos como información, independientemente del medio en el que esta se encuentre. Así pues, la seguridad de la información se apoya en la seguridad informática, dado que es la que le permite conocer los riesgos, amenazas y vulnerabilidades existentes dentro de la entidad, lo que permitirá estudiar y evaluar los sistemas informáticos. De modo que, gracias a la seguridad de la información, la seguridad informática puede realizar un mejor trabajo en la parte operativa de la seguridad.

2.2.9 Sistema de Gestión de Seguridad de la Información (SGSI)

La ISO/IEC 27001 (2013) define un sistema de gestión de seguridad de la información (SGSI) como "un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización y lograr sus objetivos comerciales y/o de servicio". Dado que toda la información almacenada y procesada por una organización está

expuesta a amenazas, errores, catástrofes naturales, fallas en el sistema, además de vulnerabilidades, el poder implementar acciones de protección de datos de acuerdo a políticas, normas y objetivos de acuerdo a la seguridad de la información, y el poder utilizar herramientas tecnológicas gracias a la seguridad informática, es lo que da vida a un SGSI.

Las claves de un SGSI es el diseño, implantación y mantenimiento de todos los procesos a gestionar eficientemente, de modo que exista accesibilidad a la información, así como el poder asegurar la confidencialidad, integridad, autenticidad y disponibilidad de los activos de la información para minimizar la incertidumbre y todos los riesgos asociados a la seguridad de la información.

2.2.10 Normas o Estándares internos

La EAE Business School (2021), define las normas o estándares internos como "procedimientos disciplinarios, diseñados para garantizar que los empleados reciben un trato justo. (…) deben dividirse en dos categorías: unas cuya infracción daría lugar a una acción disciplinaria; y otras que resultarán en una destitución sumaria". Las normas o estándares internos son acuerdos documentados para las distintas áreas de una organización, conteniendo especificaciones técnicas o criterios precisos, implementándolos como reglas que buscan asegurar que se cumplan los procesos y servicios en la misma. Su finalidad es regular las acciones de las partes involucradas de modo que exista un buen entendimiento y comunicación entre los participantes.

En las organizaciones es importante contar con una regulación que permita un correcto funcionamiento interno, dispuestas para los distintos departamentos que conforman la organización, de modo que se establezcan las funciones de cada uno de los integrantes de la organización o institución. Estos criterios brindarán validez y promoverán el buen actuar y las buenas prácticas en el desarrollo laboral de los empleados, así como la calidad de servicios prestados, pero su principal virtud es el de funcionar como reglas para los usuarios participantes.

2.2.11 Organización Internacional de Estandarización (ISO)

La Organización Internacional de Estandarización (ISO) (1947), es una organización sin ánimo de lucro de carácter no gubernamental, la cual expresa que:

> (…) promueve el desarrollo y la implementación de normas a nivel internacional, tanto de fabricación como de servicios. El objetivo de esta organización es brindar herramientas para facilitar las transacciones a nivel internacional tanto de objetos, bienes y servicios como de desarrollos científicos, actividades intelectuales, tecnológicas y económicas.

La ISO es una organización voluntaria y sus miembros son autoridades reconocidas en normalización, cada uno representando a un país. Además, se trata de auditores y expertos en materia de evaluación y control de acuerdos a las normas y estándares internacionales que, a su vez, publica la ISO. De igual forma, esta organización registra todas aquellas publicaciones que cumplan con sus objetivos, tratándose de estándares internacionales, informes técnicos, erratas técnicas, guías ISO, entre otras. De modo que la ISO es una buena ayuda para las organizaciones y empresas al momento de abordar normas dirigidas a la normalización y estandarización.

2.2.12 Comisión Electrotécnica Internacional (IEC)

La Comisión Electrotécnica Internacional (IEC) (1906), es una organización de normalización de carácter global no gubernamental, la cual está dirigida a los campos: eléctrico, electrónico y todas las tecnologías relacionadas. Por lo que tiene como finalidad:

> (…) promover entre sus miembros la cooperación internacional en todas las áreas de la normalización electrotécnica. (…) bajo los siguientes objetivos: Promover el uso de sus normas y esquemas de aseguramiento de la conformidad a nivel mundial. Asegurar e implementar la calidad de producto y servicios mediante sus normas. Establecer las condiciones de interoperabilidad de sistemas complejos. Incrementar la eficiencia de los procesos industriales. Contribuir a la implementación del concepto de salud y seguridad humana. Contribuir a la protección del ambiente. Dar a conocer los nuevos campos electrónicos.

En la actualidad las normas de la IEC son un elemento clave para el comercio internacional de productos y servicios relacionados con las tecnologías nombradas anteriormente, debido a que permiten reducir barreras técnicas al ser adoptadas en los países que producen o importan esos productos y servicios, por lo que es considerada líder a nivel mundial e internacionalmente reconocida. Estas normas son usadas por diseñadores, fabricantes, laboratorios, entidades de regulación, normalización, y entidades públicas (gobiernos), para que los productos operen de manera segura y eficiente el cualquier parte del mundo.

2.2.13 Norma ISO/IEC 27001

La ISO en 2005 emitió este estándar internacional haciendo referencia a un compendio de requisitos que exige que los sistemas de seguridad de la información en la organización garanticen la mejora continua y la administración adecuada de la información. Así pues, la Escuela Europea de Excelencia (2019) define su función de la siguiente manera:

> (…) funciona con un enfoque de arriba hacia abajo, tecnológico neutral y basado en el riesgo. La norma ayuda a comprender la organización y su contexto en relación al uso de la información. Define para ello procesos de planificación, que incluyen la

> definición de una política de seguridad, la determinación del alcance del sistema de gestión, la realización de una evaluación de riesgos, la gestión de los riesgos evaluados, la selección de los objetivos de control que se implementarán y la preparación de una declaración de aplicabilidad.

Esta norma en última versión actualizada, 2013, proporciona un marco de trabajo para los SGSI con el fin de proporcionar los principios de seguridad informática; confidencialidad, integridad, autenticidad y disponibilidad continuada de la información, así como el cumplimiento legal bajo la certificación de la ISO 27001 para la protección de activos. Este estándar permite evaluar el riesgo y aplicar controles necesarios para aminorar o eliminar los riesgos en una organización, empresa o entidad. Además, su aplicación significa una diferenciación con respecto al resto, lo que mejora la competitividad y la imagen de la organización.

Entre las funcionalidades de la ISO 27001:2013 se encuentran la Evaluación de Seguridad de la información; los Controles de la norma 27002 para autoevaluación de controles y ver el estado actual de la organización; las salvaguardas, Métricas e Indicadores, Cuadro de Mando, Objetivos y Metas, Gestor documental para la revisión, aprobación, control de cambios y versiones, así como de todos los documentos en vigor u obsoletos; Recursos Humanos, Capacitación y, por último, los Procesos y el enfoque en estos, su descripción y la interacción de todos los procesos u operaciones que integran y se desarrollan dentro de la organización.

2.3 Bases Legales

2.3.1 Norma ISO/IEC 27001. Emitida en octubre de 2005. Actualizada en 2013

De acuerdo a ISOTools Excellence (2013: párr.6), la ISO 27001 tiene sus cimientos en la entidad normalizadora británica, British Standards Institution (BSI) (1901), con carácter internacional publicaba las nomas bajo el prefijo “BS” y, por tanto:

> (…) su origen fue la BS 7799-1, publicada en 1995 de. Se trataba de una serie de mejores prácticas para ayudar a las empresas británicas a administrar la Seguridad de la Información. Se trataba de recomendaciones que no daban opción a ningún tipo de certificación ni establecía la forma de conseguirla.

Así pues, la norma tuvo varias modificaciones que significaron actualizaciones hasta alcanzar, en 2005, el estándar ISO 2700, donde la versión más actual es la ISO/IEC 27001:2013, la cual se basa en el cumplimiento de requisitos legales en seguridad desde el funcionamiento como el diseño de un SGSI, los cuales sirven como sistema de control en caso de incidencias en ámbito de seguridad y resguardo de información de cualquier carácter y forma, física o lógica.

2.3.2 Constitución de la República Bolivariana de Venezuela

Art. 60.- Toda persona tiene derecho a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos.

2.3.3 Ley Especial Contra los Delitos Informáticos

2.3.3.1 De los Delitos Contra los Sistemas que Utilizan Tecnologías de Información

Art. 6.- Acceso indebido. Toda persona que sin la debida autorización o excediendo la que hubiere obtenido, acceda, intercepte, interfiera o use un sistema que utilice tecnologías de información (…).

Art. 7.- Sabotaje o daño a sistemas. Todo aquel que con intención destruya, daño, modifique o realice cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologías de información o cualesquiera de los componentes que lo conforman (…).

Art. 11.- Espionaje informático. Toda persona que indebidamente obtenga, revele o difunda la data o información contenidas en un sistema que utilice tecnologías de información o en cualesquiera de sus componentes (…).

2.3.3.2 De los Delitos Contra la Privacidad de las Personas y de las Comunicaciones

Art. 20.- Violación de la privacidad de la data o información de carácter personal. Toda persona que intencionalmente se apodere, utilice, modifique o elimine por cualquier medio, sin el consentimiento de su dueño, la data o información personales de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de información (…).

Art. 21.- Violación de la privacidad de las comunicaciones. Toda persona que mediante el uso de tecnologías de información acceda, capture, intercepte, interfiera, reproduzca, modifique, desvíe o elimine cualquier mensaje de datos o señal de transmisión o comunicación ajena (…).

Art. 22. Revelación indebida de data o información de carácter personal. Quien revele, difunda o ceda, en todo o en parte, los hechos descubiertos, las imágenes, el audio o, en general, la data o información obtenidos por alguno de los medios indicados en los artículos 20 y 21 (…).

2.3.4 Decreto N° 825, del 10 de mayo de 2000 sobre Internet como prioridad de la república Bolivariana de Venezuela. (Publicado en Gaceta Oficial de la República Bolivariana de Venezuela Nº 36.955 del 22 de mayo de 2000)

Art. 1.- Se declara el acceso y uso de Internet como política prioritaria para el desarrollo cultural, económico, social y político de la República bolivariana de Venezuela.

Art. 11.- El Estado, a través del Ministerio de Ciencia y Tecnología promoverá activamente el desarrollo del material académico, científico y cultural para lograr un acceso adecuado y uso efectivo de Internet, a los fines de establecer un ámbito para la investigación y el desarrollo del conocimiento en el sector de las tecnologías de la información.

2.3.5 Ministerio de Ciencia y Tecnología. Resolución N° 320. (2 de enero de 2006)

Art. 1.- El Ministerio de Ciencia y Tecnología a través de sus respectivos órganos, dictaminará las políticas, normas y procedimientos de seguridad informática física y lógica, en los bienes informáticos de los Órganos y Entes de la Administración Pública, así mismo asistirá a los órganos competentes de la Administración Pública Nacional en la implementación de las mismas.

Art. 3.- El Ministerio de Ciencia y Tecnología establecerá los acuerdos y convenios de cooperación que tengan lugar para viabilizar el cumplimiento de las políticas en materia de seguridad informática en los Órganos y Entes de la Administración Pública Nacional.

Art. 6.- Todas las infraestructuras y los servicios de seguridad informática de la Administración Pública Nacional deben cumplir con normas y estándares nacionales e internacionales, orientados a su uso, diseño y mantenimiento.

Art. 7.- Los Órganos y Entes de la Administración Pública Nacional deben tener un área de seguridad informática con personal calificado.

Art. 9.- Los Órganos y Entes de la Administración Pública Nacional deben realizar simulacros de operatividad en sus sistemas de redundancia, respaldo y recuperación.

2.3.6 Ley de Infogobierno. Principio de seguridad

Art. 23.- En las actuaciones electrónicas que realicen el Poder Público y el Poder Popular se debe garantizar la integridad, confidencialidad, autenticidad y disponibilidad de la información, documentos y comunicaciones electrónicas, en cumplimiento a las normas y medidas que dicte el órgano con competencia en materia de seguridad de la información.

2.4 Definición de Términos

Activo informático:

"Hace referencia a recursos tecnológicos del entorno de la información comunicativa que forman parte de las empresas y tienen como objetivo la difusión de información". (Perito Judicial GROUP, 2022).

Amenaza:

"Cosa o persona que constituye una posible causa de riesgo o perjuicio para alguien o algo". (Diccionario Oxford Languages).

Análisis de riesgo:

"El análisis de riesgo es el uso sistemático de la información disponible para determinar la frecuencia con la que determinados eventos se pueden producir y la magnitud de sus consecuencias". (EALDE, 2017).

Antivirus:

"Es un tipo de software que se utiliza para evitar, buscar, detectar y eliminar virus de una computadora. Una vez instalados, la mayoría de los software antivirus se ejecutan automáticamente en segundo plano para brindar protección en tiempo real contra ataques de virus". (VERIZON, 2022).

Administrador:

"Es la persona que se ocupa de realizar la tarea administrativa por medio de la planificación, organización, dirección y control de todas las tareas dentro de un grupo social o de una organización para lograr los objetivos mediante el uso eficiente de los recursos". Quiroa, M (2020).

Auditoría:

"Revisión sistemática de una actividad o de una situación para evaluar el cumplimiento de las reglas o criterios objetivos a que aquellas deben someterse". (RAE).

Autenticidad:

"Se refiere a la capacidad de un software de verificar que un usuario o el remitente de un mensaje sea realmente quien dice ser". KeepCoding (2022).

Banear:

"Limitar las acciones de un usuario en un sistema informático en el que interaccionan diversas personas". (Diccionario Oxford Languages).

Bloqueo:

"Un bloqueo o ban es una restricción (total, parcial, permanente o temporal) que se impone a un usuario dentro de un sistema informático". Pérez, J y Gardey, A (2013).

Confidencialidad:

"Es una propiedad que ostenta algún tipo de información y mediante la cual se garantizará el acceso a la misma solamente a aquellas personas que estén autorizadas a conocerla, y por consiguiente no será revelada ante aquellos que no cuenten con la autorización de conocerla". Ucha, F (2010).

Computador:

"Es una máquina electrónica que está diseñada para realizar tareas específicas". (GCFGlobal, 2022).

Copia de seguridad:

"Se entiende por copia de seguridad, respaldo de información, copia de reserva o back up (en inglés), una copia que se realiza de los datos y archivos originales con el fin de prevenir la pérdida parcial o total de la información del disco duro o en cualquier otro dispositivo". (Significados, 2022).

Correo electrónico:

"Sistema de transmisión de mensajes o archivos de un terminal a otro a través de redes informáticas". (RAE).

CPU:

"Sigla de la expresión inglesa central processing unit, unidad central de procesamiento, que es la parte de una computadora en la que se encuentran los elementos que sirven para procesar datos". (Diccionario Oxford Languages).

Datos:

"Información dispuesta de manera adecuada para su tratamiento por una computadora". (RAE).

Departamento de seguridad informática:

Es una unidad o división que existe dentro de una organización, empresa o entidad, destinada a proteger a la organización de ataques o incidentes informáticos mediante métodos y técnicas que minimicen el riesgo. (Definición propia).

Disponibilidad:

"Es la medición de la frecuencia con la que los datos y las aplicaciones están preparados para que puede accederse a ellos cuando se les necesite". (IBM, 2021).

Evaluación del riesgo:

“La evaluación de riesgos es la actividad fundamental que la ley establece que debe llevarse a cabo inicialmente y cuando se efectúen determinados cambios, para poder detectar los riesgos que puedan existir en todos y cada uno de los puestos de trabajo de la empresa y que puedan afectar a la seguridad y salud de los trabajadores”. (Instituto de Seguridad y Salud Laboral ,2007).

Evento:

En informática, un evento se define como “una acción que es detectada por un programa; éste, a su vez, puede hacer uso del mismo o ignorarlo”. Pérez, J y Gardey, A (2021).

Firewall:

“Sistema que protege redes y terminales privadas de accesos no autorizados, especialmente durante la navegación por internet”. (RAE).

Gestión del riesgo:

“Proceso de identificar, analizar y cuantificar las probabilidades de pérdidas y efectos secundarios que se desprenden de desastres, así como las acciones preventivas, correctivas y reductivas correspondientes que deben emprenderse”. Benavides, L (2010)

Hacker:

“Persona con grandes conocimientos de informática que se dedica a detectar fallos de seguridad en sistemas informáticos”. (Diccionario Oxford Languages).

Hardware:

“Son aquellos elementos físicos o materiales que constituyen una computadora o un sistema informático. Es decir, son aquellas partes físicas de un sistema operativo tales como sus componentes eléctricos, electrónicos, electromecánicos, mecánicos y cualquier elemento físico que esté involucrado”. (Apen, 2021).

Integridad:

En informática, se define la integridad como “Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada”. (RAE).

Internet:

“Internet es una red de computadoras interconectadas a nivel mundial en forma de tela de araña. Consiste de servidores (o "nodos") que proveen información a aproximadamente 100 millones de personas que están conectadas entre ellas a través de las redes de telefonía y cable”. Ramírez, H (1999).

ISO:

“Sigla de la expresión inglesa International Organization for Standardization, 'Organización Internacional de Estandarización', sistema de normalización internacional para productos de áreas diversas”. (Diccionario Oxford Languages).

Malware:

Es la abreviatura de “software malicioso”, es un término general que se refiere a una amplia variedad de programas diseñados para dañar o realizar acciones no deseadas en una computadora, servidor o red informática. (VERIZON, 2022).

Mantenimiento:

“Conservación de una cosa en buen estado o en una situación determinada para evitar su degradación”. (Diccionario Oxford Languages).

Monitoreo:

“Es el proceso continuo y sistemático mediante el cual se verifica la eficiencia y la eficacia de un proyecto mediante la identificación de sus logros y debilidades y, en consecuencia, se recomiendan medidas correctivas para optimizar los resultados esperados del proyecto”. Ortegón, E (2005).

Organización:

“Una organización es una estructura ordenada donde coexisten e interactúan personas con diversos roles, responsabilidades o cargos que buscan alcanzar un objetivo particular”. Roldán, N (2017).

PDCA:

“Es un acrónimo de cada uno de los pasos que comprende: Planear, Hacer, Comprobar y Actuar. La metodología PDCA tiene un carácter cíclico, que garantiza la atención continua sobre la mejora de la calidad”. (Escuela Europea de Excelencia, 2020).

Política:

Dentro de una organización, una política se define como “pautas o criterios que se tienen en cuenta para la consecución de objetivos en la misma. Sirven para gobernar la acción en el caminar hacia un objetivo, ayudando a delegar y mantener la buena relación entre personas”. (EALDE Business School, 2020).

Protocolos:

“Es el conjunto de reglas que, ya sea por norma o por costumbre, se establecen para actos oficiales o solemnes, ceremonias y otros eventos”. Morales, F (2020).

Red inalámbrica:

"Tipo de conexión entre sistemas informáticos, computadoras, que se lleva a cabo mediante diversas ondas del espectro electromagnético". (Editorial Etecé, 2021).

Revisión:

"Análisis o examen atento y cuidadoso de una cosa". (Diccionario Oxford Languages).

Riesgo:

"Posibilidad de que se produzca un contratiempo o una desgracia, de que alguien o algo sufra perjuicio o daño". (Diccionario Oxford Languages).

Servicios:

"Organización y personal destinados a cuidar intereses o satisfacer necesidades del público o de alguna entidad oficial o privada". (RAE).

Servidor:

"Unidad **informática** que proporciona diversos servicios a computadoras conectadas con ella a través de una red". (RAE).

Sistema de Control de Acceso:

"Hace referencia al mecanismo que en función de la identificación ya autentificada permite acceder a datos o recursos". (TECNOSeguro, 2021).

Sistema de Gestión de Seguridad de la Información SGSI:

Según la ISO 27001 (2013), "consiste en preservar la confidencialidad, integridad y disponibilidad, además de todos los sistemas implicados en el tratamiento dentro de la organización".

Universidad:

"Institución destinada a la enseñanza superior (aquella que proporciona conocimientos especializados de cada rama del saber), que está constituida por varias facultades y que concede los grados académicos correspondientes". (Diccionario Oxford Languages).

Usuario:

"Un usuario es aquel individuo que utiliza de manera habitual un producto, o servicio. Es un concepto muy utilizado en el sector informático y digital". Peiró, R (2020).

Validación:

Se trata de confirmar la autenticidad de acceso a usuarios o de algún archivo que se encuentra en proceso de ejecución. (Definición propia).

Virus informático:

"Programa introducido subrepticiamente en la memoria de una computadora que, al activarse, afecta a su funcionamiento destruyendo total o parcialmente la información almacenada". (RAE).

Vulnerabilidad

Hace referencia a que algo o alguien corre el riesgo de sufrir un incidente o evento asociado a debilidades. (Definición propia).

PARTE III

DESCRIPCIÓN METODOLÓGICA

En esta parte se expone todo lo concerniente a la naturaleza de la investigación, el tipo de investigación, el diseño de la misma, la población y muestra del estudio; así como las fuentes de información, con lo cual se estructuran las técnicas de recolección de datos y la forma científica de analizar los mismos, de acuerdo a la relación existente con los objetivos presentes en la investigación.

3.1 Naturaleza de la investigación

Fernández, P. y Díaz, P. (2002) exponen que "la investigación cuantitativa trata de determinar la fuerza de asociación o correlación entre variables, la generalización y objetivación de los resultados a través de una muestra para hacer inferencia a una población de la cual toda muestra procede". Por tanto, la investigación cuantitativa, como una metodología en el proceso científico, es una estrategia de investigación centrada en cuantificar la recopilación y análisis de datos, partiendo desde un enfoque deductivo, lo que le adjudica el nombre de investigación empírico-analítica, dado que se hace énfasis en la comprobación teórica, moldeada por filosofías empiristas y positivas, por esto, también se le conoce como racional o positivista. De modo que, la presente investigación posee una naturaleza cuantitativa, dado que consistió en la obtención de información a través de diversas fuentes, utilizando herramientas de análisis matemático y estadístico al momento de describir, explicar y predecir fenómenos mediante datos numéricos.

3.1.1 Tipo de investigación

De acuerdo a Tamayo y Tamayo, M (1994), una investigación descriptiva "comprende la descripción, registro, análisis e interpretación de la naturaleza actual y la composición o procesos de los fenómenos". En tal sentido, este tipo de investigación busca describir y explicar lo que se investiga, mediante un análisis de las características del objeto de estudio, es decir que define, clasifica, divide o resume la información. De acuerdo a esto, el presente estudio es descriptivo dado que busca describir la naturaleza del objeto de estudio, recopilando datos de la población, por tanto, es un método de investigación observacional.

Balestrini, M (2002) define los proyectos factibles como "(…) aquellos proyectos o investigaciones que proponen la formulación de modelos, sistemas, entre otros, que dan soluciones a una realidad o problemática real planteada, la cual fue sometida con anterioridad o estudios de

las necesidades a satisfacer". Se entiende entonces que, el tipo de investigación denominada proyecto factible hace referencia a propuestas o modelos que, de acuerdo a sus características, pueden materializarse y brindar soluciones a problemas. Así pues, el presente trabajo pertenece a este tipo de investigación, que permite satisfacer una necesidad en concreto o solucionar algún problema, detectado tras un análisis y posteriormente la creación de un diseño para la propuesta de acción, teniendo como resultado un modelo aplicable sin necesidad de una inversión externa a este estudio.

3.1.2 Diseño de la investigación

Con respecto a la definición del diseño de campo, Arias (2006) expone que "la investigación o diseño de campo es aquella que consiste en la recolección de datos directamente de los sujetos investigados, o de la realidad donde ocurren los hechos (datos primarios)". De tal forma, este diseño de investigación trata de una planificación estructurada aplicada al estudio de la realidad existente en la Universidad de Margarita con respecto a la seguridad informática, para que se puedan identificar los instrumentos y técnicas a implementar en la recolección de datos.

3.1.3 Población y muestra

Arias (2006) define la población como "un conjunto finito o infinito de elementos con características comunes para los cuales serán extensivas las conclusiones de la investigación. Esta queda delimitada por el problema y por los objetivos del estudio". En el presente estudio la población está representada por todos aquellos departamentos que integran la Universidad de Margarita (UNIMAR) y que se relacionan directamente con la gestión de la información y con el objeto de estudio, conformados por tres (3) departamentos: la Comisión de Sistemas y Tecnología de la UNIMAR, Control de Estudios, Dirección de Administración.

DEPARTAMENTO	**CANTIDAD DE PERSONAS**
Comisión de Sistemas y Tecnología	4 personas, 1 encargado
Control de Estudios	5 personas, 1 encargado
Dirección de Administración	8 personas, 2 encargados; 1 para Contabilidad y 1 para Administración

Tabla 1. *Población y muestra*

Fuente. *Elaboración propia (2022).*

Por tanto, Tamayo y Tamayo, M (2006), definen la muestra como "el conjunto de operaciones que se realizan para estudiar la distribución de determinados caracteres en totalidad de una

población universo, o colectivo partiendo de la observación de una fracción de la población considerada". De modo que, se seleccionó una muestra de la población total que es representativa en cuanto a la relación con la gestión de la información en los departamentos de la Universidad de Margarita (UNIMAR), siendo esta la Comisión de Sistemas y Tecnología de la UNIMAR, encargada del sistema de la universidad como de la gestión de activos informáticos.

Según Cuesta (2009), el muestreo no probabilístico es definido como "una técnica de muestreo donde las muestras se recogen en un proceso que no brinda a todos los individuos de la población iguales oportunidades de ser seleccionados". Así mismo, dentro de los tipos de muestreo no probabilísticos, está el de tipo intencional y, de acuerdo con Dzib, A (2022), en el cual la selección de las muestras ocurre "(…) basándose únicamente en el conocimiento y la credibilidad del investigador. (…) los investigadores eligen solo a aquellos que estos creen que son los adecuados para participar en un estudio de investigación".

En el presente trabajo, el análisis de muestro no probabilístico es de tipo intencional debido a que de la población total, representada por 17 personas del personal de la Universidad de Margarita, específicamente de los departamentos de la Comisión de Sistemas y Tecnología, Control de estudios y Dirección de Administración, se seleccionó intencionadamente la muestra que responde directamente a las interrogantes del estudio de investigación, es decir, 4 personas pertenecientes a la Comisión de Sistemas y Tecnología, debido a que responden a los aspectos técnicos acerca de la seguridad informática.

3.2.3 Técnicas de recolección de datos

Sabino, C (2002) expone que la entrevista estructurada "Se caracteriza por estar rígidamente estandarizada, se plantean idénticas preguntas y en el mismo orden a cada uno de los participantes, quienes deben escoger la respuesta entre dos, tres o más alternativas que se les ofrecen". Con base en lo anterior, se realizó una entrevista al personal que integra la Comisión de Sistemas y Tecnología de la Universidad de Margarita (UNIMAR) encargado de la gestión del sistema, específicamente el Ing. Silvestre Cárdenas. Del mismo modo, se entrevistó al personal de los departamentos de Control de Estudios y Dirección de Administración respectivamente, para identificar los riesgos asociados al sistema de información en la UNIMAR, mediante la estructura normativa del estándar internacional ISO/IEC 27001:2013

Asimismo, este tipo de entrevista formal permitió recopilar toda la información relevante en cuestión de seguridad y preservación de los activos informáticos, así como el poder evaluar los

recursos destinados por la Universidad de Margarita para realizar estas actividades. Consecuentemente, se aplicó como instrumento de recolección de datos una guía de entrevista basada en la seguridad informática y de la información.

Hernández (2012) expresa que un cuestionario consiste en:

> (…) diseñar un instrumento para medir las variables conceptualizadas al plantear su problema de investigación (…) en éste las variables están operacionalizadas como preguntas. Éstas no solo deben tomar en cuenta el problema que se investiga sino también la población que las contestará y los diferentes métodos de recolección de información.

El cuestionario es un documento formado y estructurado por preguntas formales, redactadas lógica y coherentemente, de acuerdo con la planificación de la investigación, teniendo como finalidad que las respuestas obtenidas satisfagan la esencia de las preguntas en sí mismas. En tal sentido, se realizó un cuestionario estructurado por preguntas asociadas a la gestión de la información, así como a la seguridad de los activos informáticos.

Según Hurtado (2008) con respecto a la revisión documental afirma que "una revisión documental es una técnica en donde se recolecta información escrita sobre un determinado tema, teniendo como fin proporcionar variables que se relacionan indirectamente o directamente con el tema establecido". Así pues, se consultaron guías de implantación para la seguridad de la información basadas en la ISO/IEC 27001:2013 abaladas por la Organización Internacional de Normalización (ISO), asimismo, se consultaron artículos, entradas y trabajos publicados en la página oficial de la ISO. Además, se complementó la información, con publicaciones sobre la ISO 27002 la cual va dirigida a las buenas prácticas en la Gestión de la Seguridad de la Información. Igualmente, el libro MAGERIT v.3 para la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de los Administradores. En tal sentido, la información recopilada es fundamental para el diseño del Sistema de Gestión de Seguridad de la Información (SGSI) que permitirá asegurar que se cumplan los principios de seguridad informática.

3.3.4 Técnicas de análisis de datos

Según Dyson (2004), la matriz FODA o análisis FODA "consiste en realizar una evaluación de los factores fuertes y débiles que, en su conjunto, diagnostican la situación interna de una organización, así como su evaluación externa, es decir, las oportunidades y amenazas". Este tipo de matriz permite visualizar las características de una organización de cualquier índole y evaluarlas de modo que se pueda obtener una perspectiva general con respecto a la situación y la estrategia a llevar a cabo. Por tanto, en esta investigación, se empleó esta herramienta para estimar de manera

objetiva la situación estratégica y gestionar los posibles eventos mediante la evaluación de las variables y características de la universidad de Margarita con respecto a la seguridad informática, mediante la evaluación de sus fortalezas, oportunidades, debilidades y amenazas.

Wolinsky (2003) define la matriz de riesgo como "un elemento que posibilita cuantificar los riesgos disminuyendo el nivel de subjetividad al momento de su evaluación, siempre que la parametrización y asignación de valores a los indicadores esté debidamente fundamentada". Se considera una herramienta de gestión, dado que permite determinar y observar objetivamente cuáles son los riesgos relevantes, en el caso de esta investigación, para la seguridad informática mediante el diseño de un plan de seguridad informática para la Universidad de Margarita (UNIMAR).

La matriz de riesgo parte desde la identificación de las principales actividades y los riesgos asociados, considerando tanto los incidentes como riesgos o peligros, lo cual permitió realizar el proceso cuantitativo para el análisis y poder evaluar los riesgos mediante la identificación de los activos a proteger en el área de seguridad informática, de acuerdo a las probabilidades de incidencias, amenazas, vulnerabilidades y el impacto en la organización, en este caso la Universidad de Margarita (UNIMAR), mediante la estructura de la norma ISO/IEC 27001.

PARTE IV

RESULTADOS

El análisis de los resultados de la presente investigación está dirigido a relacionar, interpretar y buscar significado a toda aquella información obtenida mediante las técnicas de recolección y análisis de datos, las cuales permitirán presentar de manera ordenada y comprensible toda la información relevante, de acuerdo al trabajo de grado denominado: Diseño de un Plan de Seguridad Informática basado en la Norma ISO/IEC 27001 para la Universidad de Margarita (UNIMAR), ubicada en El Valle del Espíritu Santo, Isla de Margarita, Nueva Esparta, Venezuela.

4.1 Identificación de los riesgos asociados al sistema de información en la Universidad de Margarita (UNIMAR), mediante la estructura de la norma ISO/IEC 27001

La Universidad de Margarita (UNIMAR) es una universidad privada, ubicada en El Valle del Espíritu Santo en la Isla de Margarita, en el estado Nueva Esparta, Venezuela. La UNIMAR fue fundada el 20 de noviembre de 1998, mediante decreto presidencial Nª 3034, siendo una institución referente y prestigiosa de la Isla de Margarita, la cual busca forjar hombres de bien, brindando educación superior de calidad. Dicha institución, gestiona activos informáticos, los cuales se procesan, almacenan y transmiten en el sistema de información de la UNIMAR.

Los datos e información como activos dentro de un sistema de información son la base fundamental en la toma de decisiones, por lo que es importante cumplir con los principios de seguridad de la información; integridad, disponibilidad y confidencialidad, entendiendo que la información es el recurso más importante de todo sistema u organización. La Universidad de Margarita, está estructurada internamente por departamentos que gestionan información relevante de todos sus integrantes, tanto estudiantes como personal de cualquier índole, por tanto, es necesario que se gestione la información de manera óptima, tanto en su procesamiento como en el almacenamiento y transmisión de la misma. Los riesgos asociados a sistemas de información vienen dados por vulnerabilidades dentro del mismo, las cuales condicionan al sistema, lo que da paso a una amenaza que se aprovecha de esa debilidad. Consecuentemente, el riesgo nace de la probabilidad de que una amenaza explote la vulnerabilidad de un activo de información.

En este orden de ideas, para cumplir con el primer objetivo de, mediante la Norma ISO/IEC 27001, identificar los riesgos asociados al sistema de información en la Universidad de Margarita (UNIMAR), se aplicó una encuesta estructurada dividida en tres partes y dirigida a la totalidad de

población de la presente investigación (17 sujetos del personal de los tres departamentos; Comisión de Sistemas y Tecnología de la UNIMAR, Control de Estudios, Dirección de Administración), en donde las dos primeras secciones buscan evidenciar el conocimiento con respecto a la seguridad de la información, así como de la Norma ISO/IEC 27001 para la seguridad informática, de modo que se puedan identificar claramente los riesgos asociados y así definir la Matriz de Riesgo, en la cual se buscó determinar los niveles de riesgo asociados al sistema de información de la Universidad de Margarita (UNIMAR) que se encuentren presentes en el caso de estudio. Detallándolos a continuación:

ENCUESTA ESTRUCTURADA

PARTE I: CONOCIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

OBJETIVO: Determinar el nivel de conocimiento que dispone el personal de los tres departamentos con respecto a normas y políticas de la seguridad de la información, evaluando el nivel de conocimiento del 1 al 5.

1. **Nivel de conocimiento actual que posee el personal de los tres departamentos con respecto a la seguridad de la información.**

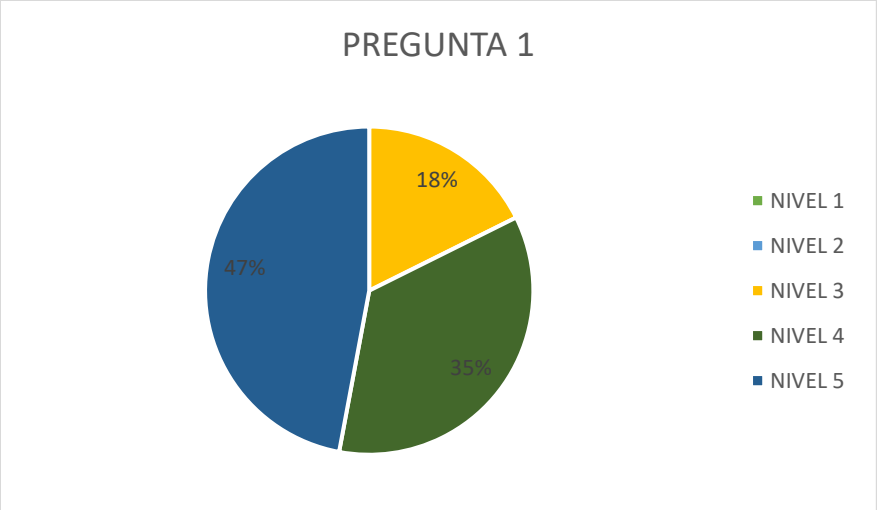

Figura 1. Encuesta Estructurada, Parte I: Conocimientos de Seguridad de la Información, Pregunta 1.

Fuente. *Elaboración propia (2022).*

En la Gráfica 1, se muestra que el 47% de la distribución porcentual corresponde al nivel 5, siendo este último el de más alto índice dentro de la escala, mientras que el segundo mayor porcentaje esta puntuado en un nivel medio-alto, es decir, un 35% con un nivel 4 de acuerdo a los

encuestados y, por último, el nivel con menor valor porcentual es de 18% de la población total, que se encuentra en el nivel 3 o nivel intermedio dentro de la escala.

De acuerdo a la estructura de la encuesta, se evaluó el nivel de conocimiento actual que posee la población total (17 personas entre los tres departamentos), con respecto a la seguridad de la información. Entendiendo que la seguridad de la información implica la implementación de técnicas, normas y políticas críticas y objetivas dirigidas al resguardo de la información, mediante las buenas prácticas en la gestión de los datos, indistintamente del medio en el que se encuentren los datos.

De modo que, con respecto a los resultados obtenidos, en base al conocimiento actual que posee la población total en materia de seguridad de la información, se observa que un porcentaje significativo y excelente (47%) posee un conocimiento alto sobre los distintos métodos a implementar en la gestión de información en sus respectivos departamentos dentro de la Universidad de Margarita, del mismo modo, el segundo porcentaje más alto (35%) posee un nivel de conocimiento bueno y aceptable sobre los activos de información que gestionan, aunque conociendo solo algunas de las técnicas sobre seguridad de la información. No obstante, el nivel intermedio está representado por un porcentaje bajo en materia de seguridad de la información, representado en un 18%, en el cual parte de la población conoce sobre el resguardo de la información, mas no hay un dominio total de las normas, técnicas y métodos que engloban la disciplina.

2. **Nivel de conocimiento adquirido el personal de los tres departamentos con respecto a normas o estándares internos que establece la seguridad de la información.**

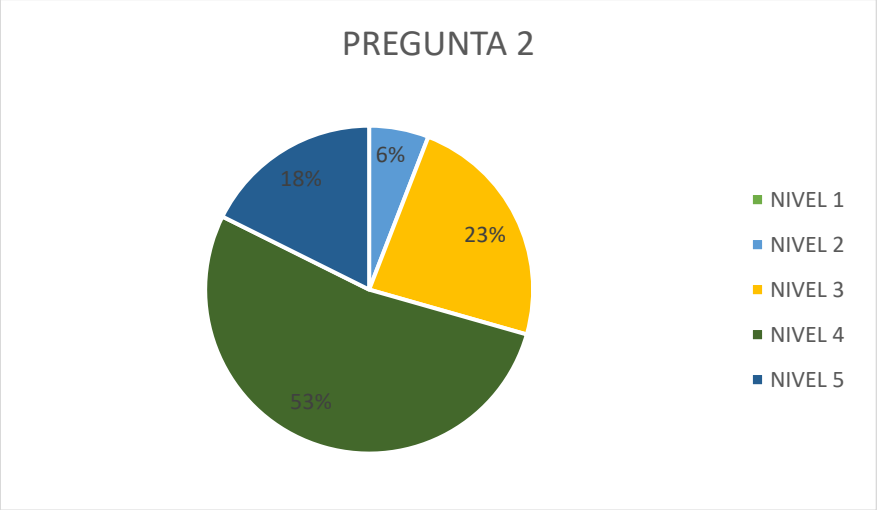

Figura 2. *Encuesta Estructurada, Parte I: Conocimientos de Seguridad de la Información, Pregunta 2.*

Fuente. *Elaboración propia (2022).*

En la Gráfica 2, el 53% de la población posee un nivel 4 de conocimiento sobre normas o estándares internos establecidos por la seguridad de la información, el 23% representa un nivel 3, es decir, tienen conocimiento sobre algunas normas internas. El tercer valor porcentual más elevado es de 18%, más este porcentaje posee un nivel de conocimiento alto sobre las normas o estándares interno y lo que significan dentro de la organización en sus distintas áreas. Por otro lado, el penúltimo nivel más bajo de la escala está representado en un 6%, con un nivel 2 de conocimiento con respecto a normas o estándares internos.

Las normas o estándares internos dentro de los departamentos tienen la finalidad de administrar y regular las funciones propias de los participantes, así como de los procesos que los departamentos desarrollan y el papel que estos cumplen dentro de la organización. Por lo tanto, los integrantes deben tener conocimiento sobre estas normas, para tener claros los principios, criterios y valores sobre los que se sustenta cada norma y exista un acuerdo tácito entre los participantes y las labores que desempeñan dentro de la organización. Por lo tanto, existen normas generales y normas específicas, en donde las primeras van orientadas a todos los trabajadores y todas las funciones sin distinción de sección, departamento o área; mientras que las segundas detallan elementos específicos del funcionamiento de la organización.

Según la evaluación, los conocimientos adquiridos con respecto a normas o estándares internos que establece la seguridad de la información por parte de la población total (17 personas entre los tres departamentos dentro de la Universidad de Margarita), el mayor valor dentro de la distribución porcentual (53%) posee un nivel de conocimiento bueno y aceptable sobre las normas o estándares internos que dispone la seguridad de la información para la gestión de activos de información de acuerdo a los procesos internos de la organización. El 23%, con un nivel intermedio (nivel 3), poseen cierta noción sobre las normas internas que deben existir en los departamentos; un 18% refleja que posee un conocimiento alto y excelente con respecto a las normas o estándares internos que permiten un desarrollo continuo en el desempeño de las áreas en las que se gestionan activos de información. No obstante, el nivel más bajo (6%), evidencia un porcentaje de la población que se encuentra en un rango por debajo de la media, por lo que poseen un conocimiento muy básico con respecto a las normas internas que deben existir en los departamentos a los que pertenecen.

3. **Inducción que ha recibido el personal de los tres departamentos por parte de la Universidad de Margarita (UNIMAR) en materia de seguridad de la información.**

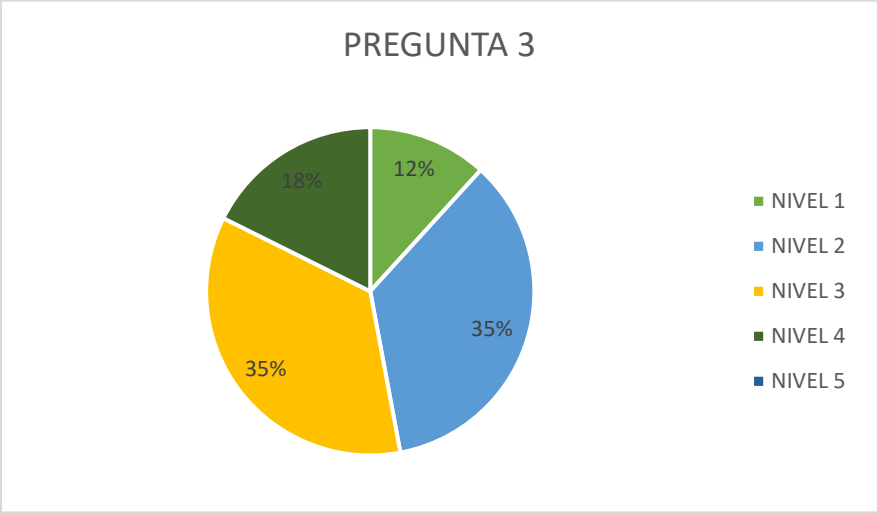

Figura 3. *Encuesta Estructurada, Parte I: Conocimientos de Seguridad de la Información, Pregunta 3.*

Fuente. *Elaboración propia (2022).*

En la distribución porcentual de la Gráfica 3, se evidencia existen dos porcentajes del mismo valor en el que; de acuerdo a la escala jerárquica, el mayor corresponde al 35% de la población con un nivel intermedio o nivel 3 (representado en amarillo) de inducción sobre materia de seguridad de la información por parte de la Universidad de Margarita (UNIMAR); a su vez, el otro 35% representa al personal que se ubica en un nivel más bajo o nivel 2, con respecto al anterior, en el que han recibido una inducción baja con respecto a las técnicas para gestionar datos e información por parte de la UNIMAR. Asimismo, el 18% muestra que posee un nivel 4 de inducción, resaltando que han recibido formación en materia de seguridad de la información para la gestión de activos. Por último, el 12% representa al porcentaje de la población que ha recibido el nivel más bajo de inducción sobre seguridad de la información.

La seguridad de la información abarca todas las medidas preventivas y reactivas dispuestas por las organizaciones, en conjunto con los sistemas y herramientas tecnológicas, para el resguardo y protección de la información de acuerdo a los principios de seguridad (confidencialidad, integridad y disponibilidad), por lo que la capacitación de los usuarios que van a desempeñar labores que incluyan activos de información es vital para una buena gestión de información en las áreas que integran la organización.

De acuerdo a los resultados obtenidos, el nivel intermedio, representado en un 35% de la población total (17 personas entre los tres departamentos), evidencia que dicho porcentaje posee una inducción normal con respecto a la seguridad de la información, específicamente con la gestión de los activos de información que existen en la Universidad de Margarita (UNIMAR), mientras que el otro 35% posee un nivel por debajo del anterior, lo que quiere decir que esta parte del personal ha recibido una inducción muy básica en materia de seguridad de la información, por lo que se evidencia una ausencia de conocimiento con respecto a las medidas preventivas a llevar a cabo en sus espacios de trabajo. El 18%, con nivel 4 de inducción, evidencia que esta parte del personal posee un nivel muy bueno de inducción y capacitación por parte de la Universidad de Margarita, es decir que manejan las metodologías dispuestas por la seguridad de la información que les ha facilitado la UNIMAR.

PARTE II: CONOCIMIENTOS DE SEGURIDAD DE LA NORMATIVA ISO/IEC 27001:2013

OBJETIVO: Determinar el nivel de conocimiento que dispone el personal de los tres departamentos con respecto a las nomas y estándares, específicamente la Norma ISO/IEC 27001, evaluando el nivel de conocimiento del 1 al 5.

4. **Nivel de conocimiento que posee el personal de los tres departamentos sobre Normas o Estándares Internacionales dirigidos a la seguridad informática.**

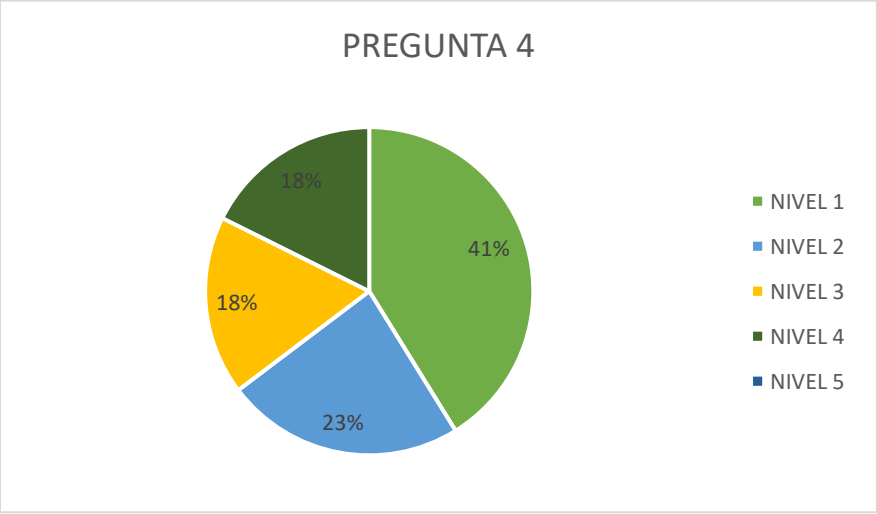

Figura 4. *Encuesta Estructurada, Parte II: Conocimientos de Seguridad de la Normativa ISO/IEC 27001:2013, Pregunta 4.*

Fuente. *Elaboración propia (2022).*

En la gráfica 4, se muestra que el 41% de la población posee un nivel muy bajo (nivel 1) de conocimiento sobre las normativas, desconociendo en un alto grado estos estándares internacionales, mientras que el 23% posee un nivel 2 con respecto a las normas, correspondiente a un nivel bajo. No obstante, en la gráfica 4, se muestra que el nivel medio (nivel 3) y el nivel bueno (nivel 4), están distribuidos porcentualmente en un 18% respectivamente, lo que equivale a un conocimiento bueno sobre las normativas de seguridad informática.

Las normas o estándares internacionales son los criterios o reglas documentadas, las cuales son producto de diferentes tipos de organizaciones de normalización que disponen de decenas de miles de normas que cubren casi cualquier tema concebible. Estas normas o estándares internacionales pueden emplearse mediante su aplicación directa o mediante su adopción, modificándola para adaptarla a las condiciones locales. La adopción de normas internacionales permite crear normas nacionales equivalentes, que son substancialmente las mismas en cuanto a su contenido técnico.

Según los resultados obtenidos, el 41% de la población posee un nivel muy bajo (nivel 1) de conocimiento sobre estas normativas, desconociendo en un alto grado estos estándares que rigen sobre la normalización en las organizaciones. El 23% posee un nivel 2 con respecto a las normas o estándares, siendo un nivel bajo, representa un porcentaje significativo de la población que presenta una ausencia de conocimiento sobre dichos estándares, así como de las organizaciones internacionales que las publican. Asimismo, se muestra que el nivel bueno (nivel 4) con un 18%, representa la parte de la población que tiene conocimiento sobre las organizaciones normalizadoras, así como las normas que estas emiten, por lo que el conocimiento sobre las técnicas que disponen es mejor y mayor. El nivel 3 con un 18% muestra un conocimiento normal sobre este tema, es decir, que el conocimiento es básico, pero siendo capaces de reconocer las técnicas y herramientas que brindan las organizaciones internacionales en materia de normalización.

5. **Nivel de conocimiento que posee el personal de los tres departamentos sobre la Norma ISO/IEC 27001:2013.**

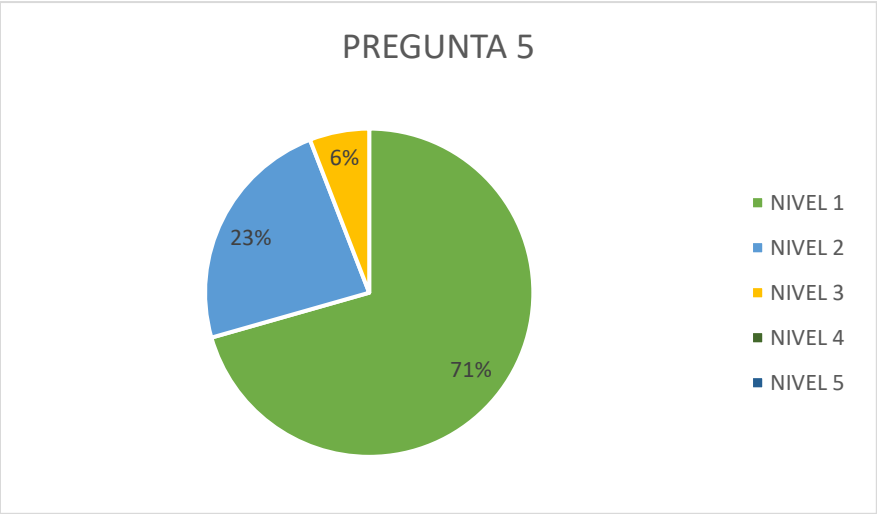

Figura 5. *Encuesta Estructurada, Parte II: Conocimientos de Seguridad de la Normativa ISO/IEC 27001:2013, Pregunta 5.*

Fuente. *Elaboración propia (2022).*

En la gráfica 5, el 71% de la población total posee el nivel más bajo de conocimiento sobre este estándar internacional de la Organización Internacional de Normalización (ISO). Mientras que solo el 23% de la población tiene un nivel 2 (bajo) sobre la norma y el 6% del personal entre los tres departamentos posee un nivel intermedio o nivel 3 de conocimiento sobre la Norma ISO/IEC 27001, en su edición de 2013.

La norma internacional ISO/IEC 27001:2013 tiene como finalidad el proporcionar un marco de trabajo para los Sistemas de Gestión de Seguridad de la Información (SGSI), buscando cumplir con los principios de seguridad (confidencialidad, integridad y disponibilidad), así como alcanzar un buen cumplimiento legal en base a las buenas prácticas de seguridad. La certificación en esta norma es esencial para proteger los activos de información más importantes de la organización, con un enfoque basado en procesos para lanzar, implantar, operar y mantener un SGSI.

Así pues, el 71% de la evidencian una ausencia de conocimiento bajo sobre la norma ISO/IEC 27001, en su edición 2013, por lo que desconocen los requisitos legislativos, las técnicas y metodologías para la gestión dispuestas por la norma para el resguardo de la información. El 23% que evidencia un nivel bajo en cuanto al conocimiento sobre la norma, muestra que esta parte de la población, a pesar de conocer sobre normas y estándares, desconoce los parámetros por los que se rige la ISO/IEC 27001:2013. No obstante, el 6% del personal posee un nivel intermedio de conocimiento sobre la norma, por lo que conocen las referencias normativas y la estructura de la norma, mas no poseen el nivel adecuado para la certificación de la misma.

6. **Nivel de conocimiento que posee el personal entre los tres departamentos acerca de un Sistema de Gestión de Seguridad de la Información (SGSI)**

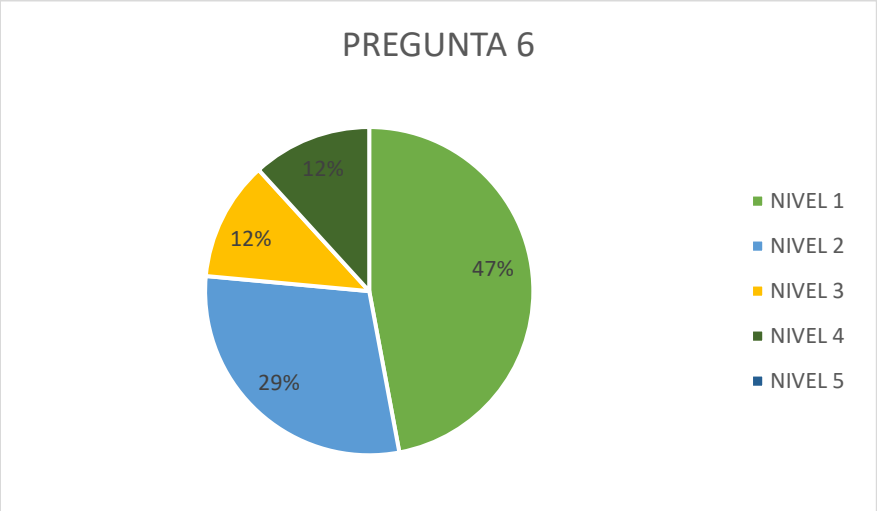

Figura 6. *Encuesta Estructurada, Parte II: Conocimientos de Seguridad de la Normativa ISO/IEC 27001:2013, Pregunta 6.*

Fuente. *Elaboración propia (2022).*

En la gráfica 6, un 47% posee el nivel más bajo dentro de la escala (nivel 1), un 29% posee el segundo nivel más bajo o nivel 2; evidenciando que existe un conocimiento muy básico sobre este tipo de sistemas de gestión de información. Por otro lado, el 12% perteneciente al nivel 4 muestra que este porcentaje de la población tiene conocimiento sobre los SGSI y su aplicación en las organizaciones, y el otro 12% con un nivel intermedio posee un conocimiento normal y básico sobre este tipo de sistemas.

Los Sistemas de Gestión de Seguridad de la Información permiten gestionar de manera adecuada la seguridad de la información de una organización de cualquier índole, a fin de hacer frente a amenazas de ataque o intromisión, error, actos fortuitos (desastres naturales), entre otros eventos. Por lo tanto, se basa en un conjunto de políticas para la administración de la información, proporcionando un modelo para crear, implementar, hacer funcionar, supervisar, revisar, mantener y mejorar la protección de los activos de información para alcanzar los objetivos de negocio.

En la gráfica 6, se evidencia que el mayor porcentaje (47%) del personal entre los tres departamentos posee un conocimiento muy bajo sobre SGSI, su definición, aplicación y atributos que contribuyen con las buenas prácticas de gestión de información, mediante dispositivos de Tecnología de la Información (TI), como por otros medios. El 29% representa un porcentaje de la población con un conocimiento muy básico sobre los SGSI y los equipos de TI que intervienen en

la gestión de activos de información. El 12% perteneciente al nivel 4 evidencia que existe un conocimiento bueno sobre los SGSI y su aplicación en las organizaciones, así como en las distintas áreas en donde se emplean equipos de TI, mientras que el otro 12%, con un nivel intermedio, posee un conocimiento normal y básico sobre este tipo de sistemas, conociendo las aplicaciones de los SGSI mas no la metodología para implementarlo por medios propios.

En concordancia con lo antes delineado, para el objetivo específico 4.1, sobre la identificación de los riesgos asociados al sistema de información en la Universidad de Margarita (UNIMAR), mediante la estructura de la norma ISO/IEC 27001:2013, se aplicó una matriz **F.O.D.A** (Fortalezas, Oportunidades, Debilidades y Amenazas). En la cual se buscó determinar los factores definidos como riesgos asociados al sistema de información en la UNIMAR, detallando lo siguiente:

FORTALEZAS	**OPORTUNIDADES**
• Reducción de riesgos que afecten la confiabilidad, integridad y disponibilidad. • Uso consiente de los activos de información. • Correcto uso de los activos informáticos (Software-Hardware). • Políticas internas de seguridad para los usuarios existentes. • Personal capacitado y estructurado para cada proceso tecnológico de la información y buen desenvolvimiento cotidiano en la UNIMAR.	• Capacitación periódica a los usuarios en la gestión y seguridad de la información. • Implementación de nuevas herramientas tecnológicas para la seguridad de la información. • Crecimiento profesional de los empleados en los departamentos. • Mejora de la calidad de servicio en base a la gestión de los activos. • Definir normas y políticas de seguridad para la organización. • Crecimiento y mejora de los procesos en sus distintas áreas dentro de la UNIMAR.
DEBILIDADES	**AMENAZAS**
• Falta de tiempo por parte del personal para recibir capacitaciones.	• Factores externos de alto riesgo (desastres naturales). • Desinformación interna o externa.

• Ausencia de conocimiento de la normativa ISO/IEC 27001. • Ausencia de capacitación en el uso de las herramientas tecnológicos y de los controles de seguridad. • Costos significativos al aplicar sistemas de seguridad más apropiados. • Ausencia de normas y políticas documentadas para los departamentos y la gestión de los activos. • Ausencia de jerarquización de los activos.	• Riesgo de pérdida, suplantación y ataques a los activos informáticos. • Ausencia de apoyo de la Alta Dirección para dirigir más recursos en ámbito de seguridad. • Falta de control sobre los equipos por parte de los administradores. • Ausencia de encargados para tomar acciones en el área de Tecnología de la Información.

Tabla 2. *Matriz F.O.D.A*

Fuente. *Elaboración propia (2022).*

En este orden de ideas, y con el fin de valorar la efectividad al identificar los riesgos asociados al sistema de información de la Universidad de Margarita (UNIMAR), se le asignó una puntuación a cada resultado de los aspectos de la Matriz F.O.D.A (Fortalezas, Oportunidades, Debilidades y Amenazas) basada en una escala numérica y apreciativa que va del uno (1) al cuatro (4) y que se desglosa de la siguiente manera:

Cualitativa	**Cuantitativa**
Irrelevante	1
Poca relevancia	2
Relevante	3
Muy relevante	4

Tabla 3. *Ponderación de la Matriz F.O.D.A*

Fuente. *Elaboración propia (2022).*

FORTALEZAS	**OPORTUNIDADES**
• Reducción de riesgos que afecten la confiabilidad, integridad y disponibilidad. **(2)**	• Capacitación periódica a los usuarios en la gestión y seguridad de la información. **(3)**

• Uso consiente de los activos de información. **(3)** • Correcto uso de los activos informáticos (Software-Hardware). **(3)** • Políticas internas de seguridad para los usuarios existentes. **(4)** • Personal capacitado y estructurado para cada proceso tecnológico de la información y buen desenvolvimiento cotidiano en la UNIMAR. **(4)**	• Implementación de nuevas herramientas tecnológicas para la seguridad de la información. **(4)** • Crecimiento profesional de los empleados en los departamentos. **(3)** • Mejora de la calidad de servicio en base a la gestión de los activos. **(4)** • Definir normas y políticas de seguridad para la organización. **(3)** • Crecimiento y mejora de los procesos en sus distintas áreas dentro de la UNIMAR. **(3)**
TOTAL: 16	**TOTAL: 20**
DEBILIDADES	**AMENAZAS**
• Falta de tiempo por parte del personal para recibir capacitaciones. **(2)** • Ausencia de conocimiento de la normativa ISO/IEC 27001. **(3)** • Ausencia de capacitación en el uso de las herramientas tecnológicos y de los controles de seguridad. **(4)** • Costos significativos al aplicar sistemas de seguridad más apropiados. **(2)** • Ausencia de normas y políticas documentadas para los departamentos y la gestión de los activos. **(3)** • Ausencia de jerarquización de los activos. **(2)**	• Factores externos de alto riesgo (desastres naturales). **(2)** • Desinformación interna o externa. **(2)** • Riesgo de pérdida, suplantación y ataques a los activos informáticos. **(4)** • Ausencia de apoyo de la Alta Dirección para dirigir más recursos en ámbito de seguridad. **(3)** • Falta de control sobre los equipos por parte de los administradores. **(3)** • Ausencia de encargados para tomar acciones en el área de Tecnología de la Información. **(3)**
TOTAL: 16	**TOTAL: 17**

Tabla 4. *Matriz F.O.D.A con ponderación Cualitativa - Cuantitativa*

Fuente. *Elaboración propia (2022).*

De acuerdo a las ponderaciones, se puede evidenciar que, en cada aspecto de la matriz F.O.D.A, las valoraciones de acuerdo a la Tabla 2, de Ponderación de la Matriz F.O.D.A. Los aspectos fueron puntuados Cuantitativa y Cualitativamente de la siguiente manera: Fortalezas con 16 puntos; mostrando que existen aspectos positivos en materia de seguridad y gestión de recursos de Tecnología de la Información (TI); Oportunidades con 20 puntos, da cabida a promover el crecimiento de las oportunidades laborales, tanto de los empleados individualmente, como de los departamentos en su totalidad, Debilidades con 16 puntos, también evidencia una ausencia en cuanto a gestión de recursos de TI, ya sea por ausencia de los conocimientos necesarios o por ausencia de documentación esencial para ejercer labores de seguridad y manejo de activos y, por último, las Amenazas con 17 puntos, muestran que existe un rango alto de vulnerabilidades que pueden convertirse en amenazas reales para los recursos de TI (equipos informáticos, data, entre otros).

4.2 Evaluación de los recursos que destina la Universidad de Margarita (UNIMAR) para la preservación de los activos informáticos.

La Universidad de Margarita (UNIMAR), desde el punto de vista de la gestión estratégica, es una organización compleja en la que se evidencian distintos tipos de procesos; estratégicos, misionales y de apoyo o soporte, que conforman la estructura de dicha institución y se ejecutan para el continuo desarrollo de la UNIMAR, como pilar fundamental para la sociedad en el ámbito educativo. De tal forma, que se evidencia un sistema de estructura compleja, en el que se manejan recursos que alimentan al sistema en sí. Dichos recursos, se manifiestan como activos para la organización, permitiendo que funcione de manera óptima y que sea posible alcanzar los objetivos propuestos por la alta dirección.

Los activos corresponden a una parte fundamental de las organizaciones en general, de cualquier índole y tamaño, y con una adecuada distribución pueden generar beneficios considerables a las instituciones. Los recursos como activos, constituyen una inversión significativa para la organización y, por tanto, necesitan de controles para su gestión, de manera que se genere información relevante para la toma de decisiones en torno a estos, lo que traería consigo un impacto positivo y otros beneficios que constituyen al desarrollo organizacional, es por esto que en esta parte de la investigación, la estructura de la encuesta es específica y técnica en el área se seguridad

informática, por lo que se llevó a cabo en la Comisión de Sistemas y Tecnología (4 personas en el departamento), de la que se obtuvieron los siguientes resultados:

ENTREVISTA ESTRUCTURADA

PARTE III: TÉCNICAS PARA LA PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN

OBJETIVO: Determinar el nivel de seguridad de la información en la UNIMAR, de acuerdo a preguntas estructuradas con respuestas de opción múltiple.

Preguntas	**Si**	**No**	**No lo se**
7. ¿La Universidad de Margarita (UNIMAR) cuenta con un Sistema de Gestión de la Seguridad de la Información (SGSI)?	(0)	(2)	(2)
8. ¿Se cuenta con un comité interno para establecer las Políticas de Seguridad?	(0)	(3)	(1)
9. ¿Existen políticas de seguridad documentadas y gestionadas?	(0)	(0)	(4)
10. ¿La alta dirección de la UNIMAR está involucrada en la iniciativa de Seguridad de la Información?	(0)	(2)	(2)

Tabla 5. *Encuesta Estructurada, Parte III: Técnicas para la Protección de Datos y Seguridad de la Información, Pregunta 7, 8, 9 y 10.*

Fuente. *Elaboración propia (2022).*

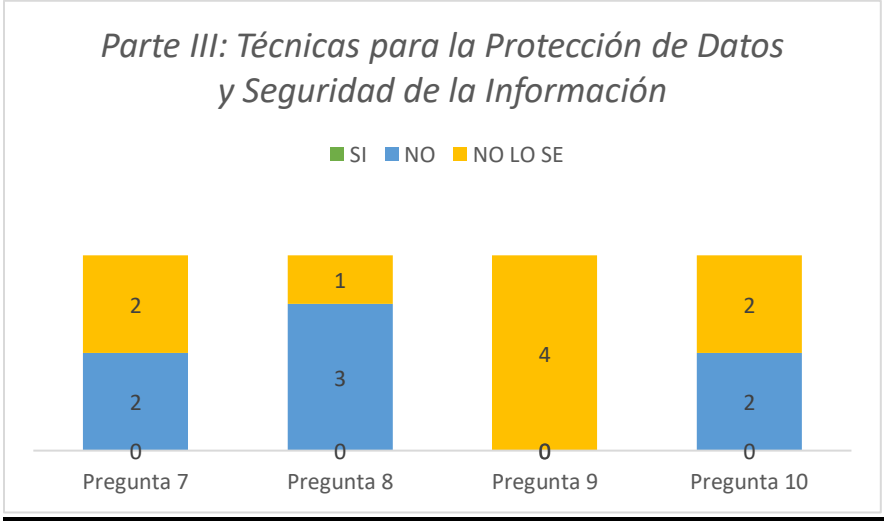

Figura 7. *Encuesta Estructurada, Parte III: Técnicas para la Protección de Datos y Seguridad de la Información, Pregunta 7, 8, 9 y 10.*

Fuente. *Elaboración propia (2022).*

Según lo expuesto en la tabla 1, las primeras cuatro (4) preguntas (7, 8, 9 y 10) realizadas a la muestra de la población total (4 personas de la Comisión de Sistemas y Tecnología de la Universidad de Margarita), se obtuvieron las siguientes respuestas:

Pegunta 7: de los encuestados, 2 negaron que exista un Sistema de Gestión de Seguridad de la Información (SGSI) y los otros 2 desconocen si existe un SGSI en la Universidad de Margarita.

Pregunta 8: de los encuestados, 3 negaron que la universidad cuente con un comité interno para establecer las Políticas de Seguridad y 1 desconoce si existe dicho comité interno.

Pregunta 9: la totalidad de los encuestados respondió que desconocen si en la Universidad de Margarita existen políticas de seguridad documentadas y gestionadas.

Pregunta 10: de los encuestados, 2 negaron que la Alta Dirección de la Universidad de Margarita está involucrada en la iniciativa de Seguridad de la Información y los otros 2 desconocen si están involucrados en materia de Seguridad de la Información.

11. Si la respuesta anterior es **SI,** del 1 al 5, ¿Qué tanta relevancia le da a la seguridad de la Información?

(1) (2) (3) (4) (5)

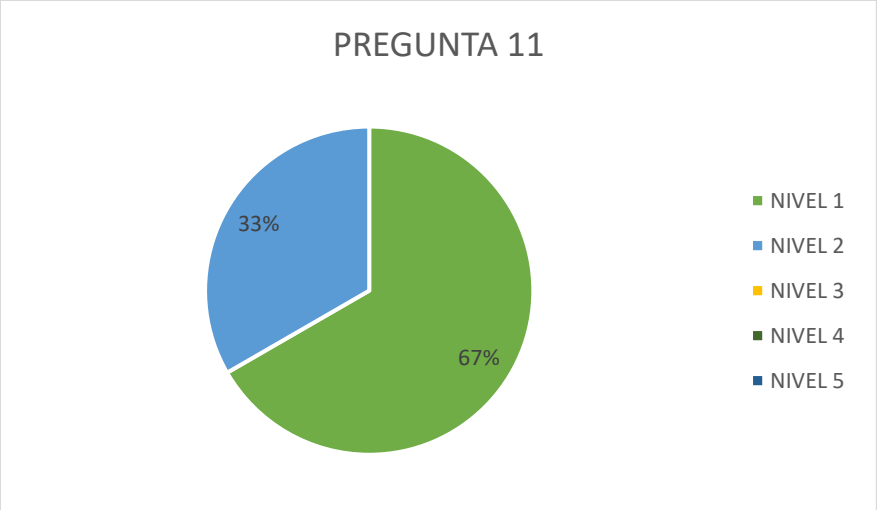

Figura 8. *Encuesta Estructurada, Parte III: Técnicas para la Protección de Datos y Seguridad de la Información, Pregunta 11.*

Fuente. *Elaboración propia (2022).*

De acuerdo a lo expuesto en la gráfica 8, correspondiente a la pregunta 11, los encuestados respondieron de acuerdo a la relevancia que le da la Alta dirección de la Universidad de Margarita a la Seguridad de la Información, en la que el 67% expreso que la relevancia en ámbito de seguridad

de la información se encuentra en el nivel más bajo o nivel 1 dentro de la escala, mientras que el 33% se muestra en el segundo nivel más bajo.

Preguntas	Si	No	Parcialmente	No lo se
12. ¿Se cuenta con Gestión de dispositivos móviles y el teletrabajo?	(0)	(3)	(1)	(0)
13. ¿Existe un Inventario de los Activos de la Información y están clasificados como Público, Privado y Confidencial?	(0)	(1)	(0)	(3)
14. ¿Se realiza control y administración de riesgos en cuanto a la seguridad de la información?	(0)	(3)	(0)	(1)
15. ¿Existe tecnología para el etiquetado de la Información (Pública, Privada o Confidencial)?	(0)	(4)	(0)	(0)

Tabla 6. *Encuesta Estructurada, Parte III: Técnicas para la Protección de Datos y Seguridad de la Información, Pregunta 12, 13, 14 y 15.*

Fuente. *Elaboración propia (2022).*

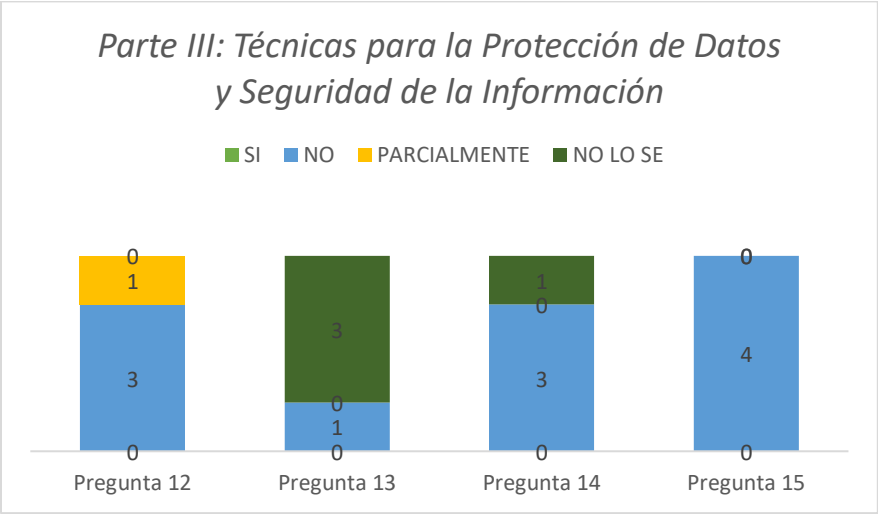

Figura 9. *Encuesta Estructurada, Parte III: Técnicas para la Protección de Datos y Seguridad de la Información, Pregunta 12, 13, 14 y 15.*

Fuente. *Elaboración propia (2022).*

Según lo expuesto en la tabla 2, en las cuatro (4) preguntas (12, 13, 14 y 15) realizadas a la muestra de la población total (4 personas de la Comisión de Sistemas y Tecnología de la Universidad de Margarita), se obtuvieron las siguientes respuestas:

Pegunta 12: de los encuestados, 3 negaron que en la Universidad de Margarita se cuente con Gestión de dispositivos móviles y el teletrabajo, mientras que 1 de los encuestados expresó que solo se gestiona parcialmente.

Pregunta 13: de los encuestados, 3 desconocen si existe un Inventario de los Activos de la Información y están clasificados como Público, Privado y Confidencial y 1 niega que exista dicho inventario en la Universidad de Margarita.

Pregunta 14: de los encuestados, 3 negaron que se realice control y administración de riesgos en cuanto a la seguridad de la información, mientras que 1 desconoce si se realizan los controles en la Universidad de Margarita.

Pregunta 15: la totalidad de los encuestados respondió que no existe tecnología para el etiquetado de la Información (Pública, Privada o Confidencial) en la Universidad de Margarita.

Preguntas	**Si**	**No**	**Parcialmente**	**No lo se**
16. ¿Se cuenta con Tecnología de Cifrado y Criptografía?	(0)	(4)	(0)	(0)
17. ¿Se cuenta con Tecnología para evitar y responder ante amenazas cibernéticas?	(0)	(3)	(1)	(0)
18. ¿Se realizan tareas de monitoreo a los sistemas de información y de comunicación?	(0)	(0)	(2)	(2)
19. ¿Han realizado simulacros frente a la caída de los sistemas de información y de comunicación?	(1)	(3)	(0)	(0)

Tabla 7. *Encuesta Estructurada, Parte III: Técnicas para la Protección de Datos y Seguridad de la Información, Pregunta 16, 17, 18 y 19.*

Fuente. *Elaboración propia (2022).*

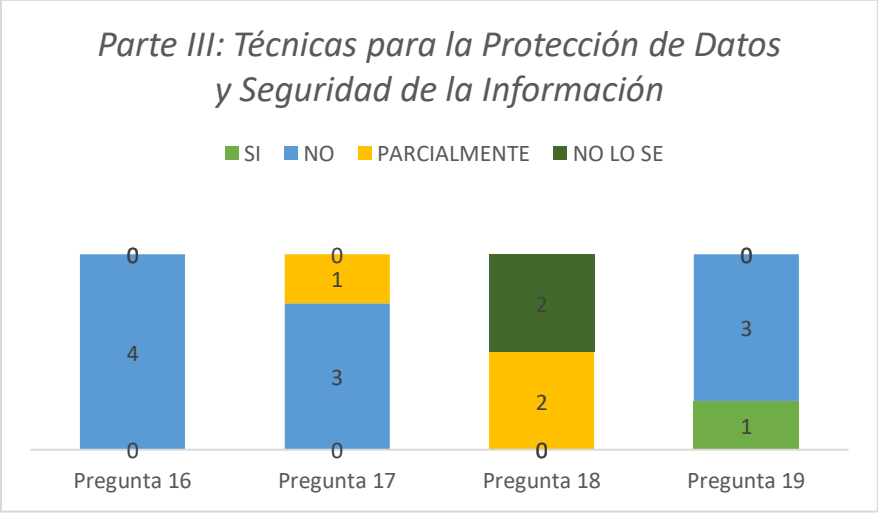

Figura 10. *Encuesta Estructurada, Parte III: Técnicas para la Protección de Datos y Seguridad de la Información, Pregunta 16, 17, 18 y 19.*

Fuente. *Elaboración propia (2022).*

En la gráfica 10, se muestran las respuestas obtenidas a las preguntas 16, 17, 18 y 19, en las que los encuestados facilitaron los siguientes resultados:

Pegunta 16: la totalidad de los encuestados expresaron que la Universidad de Margarita no cuenta con Tecnología de Cifrado y Criptografía.

Pregunta 17: de los encuestados, 1 declaro en su respuesta que solo parcialmente se cuenta con tecnología para evitar y responder ante amenazas cibernéticas, más los 3 encuestados restantes negaron que la Universidad de Margarita cuente con este tipo de tecnología.

Pregunta 18: en esta pregunta, la distribución de respuesta es equitativa, es decir, 2 encuestados respondieron que parcialmente se realizan tareas de monitoreo a los sistemas de información y de comunicación, mientras que los otros 2 respondieron que desconocen si se realizan monitores al sistema de información.

Pregunta 19: 3 de los encuestados negaron que se hayan realizado simulacros con respecto a la caída de los sistemas de información y comunicación, mientras que 1 aseguro que si se han realizado.

20. ¿Se cuenta con Tecnología para el respaldo y Recuperación de la Información? **(Software de Respaldo + Disco) (Software de Respaldo + Nube) (No) (No lo sé) (Otro: especifique)**

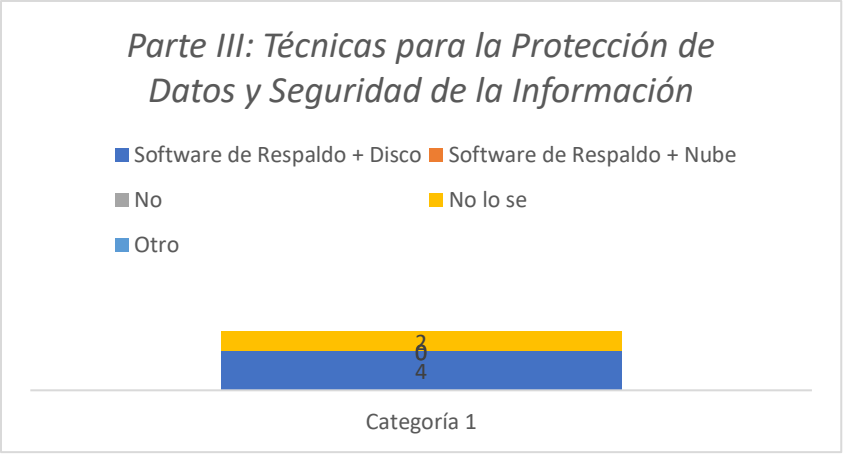

Figura 11. *Encuesta Estructurada, Parte III: Técnicas para la Protección de Datos y Seguridad de la Información, Pregunta 20.*

Fuente. *Elaboración propia (2022).*

En la gráfica 11 correspondiente a la pregunta 20, se muestran respuestas de opción múltiple, de las cuales los encuestados respondieron en su totalidad que se cuenta con Software de respaldo y disco como tecnología de respaldo y recuperación de la información en la Universidad de Margarita, más al menos 2 de los encuestados también respondieron que desconocen acerca de si la Universidad de Margarita cuenta con esta tecnología.

21. ¿Se cuenta con Tecnología para la seguridad de las Comunicaciones TIC?

(Firewalls) (Seguridad Perimetral) (Sistemas de alimentación ininterrumpida (SAI)) (Data Lost Prevention (DLP)) (Módulos de Seguridad de Hardware) (No) (No lo sé)

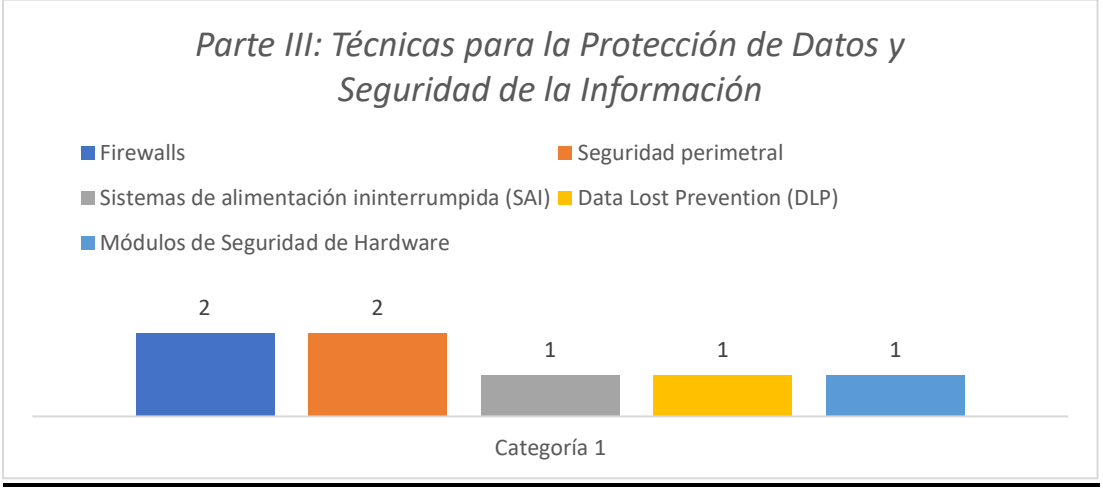

Figura 12. *Encuesta Estructurada, Parte III: Técnicas para la Protección de Datos y Seguridad de la Información, Pregunta 21.*

Fuente. *Elaboración propia (2022).*

En la gráfica 12, se muestran los resultados de la pregunta 21 de opción múltiple, en la cual los encuestados respondieron al menos 2 que en la Universidad de Margarita se cuenta con Tecnología para la seguridad de las Comunicaciones TIC, 2 respondieron que posee seguridad perimetral y al menos 1 respondió que hay sistemas de alimentación ininterrumpida, 1 de Data Lost Prevention (DLP) y 1 de Módulos de Seguridad de Hardware.

FRECUENCIA	
Improbable	Sucede una vez por año
Posible	Sucede una vez por semestre
Ocasional	Sucede una vez por trimestre
Probable	Sucede una vez por mes
Frecuente	Sucede varias veces en un mes

Tabla 8. *Matriz de Riesgo, Tabla de Frecuencia*

Fuente. *Elaboración propia (2022).*

En la tabla 4, se muestran las cinco (5) escalas de frecuencia a evaluar en la matriz de riesgo; improbable, es la probabilidad de que ocurra un riesgo o que se materialice, siendo esta demasiado baja o casi nula; Posible, en este valor la probabilidad de que ocurra es baja, aunque puede presentarse un evento; en el valor Ocasional, el riesgo puede materializarse en cualquier momento; Probable, la materialización del riesgo es alta, es decir, que suele presentarse; y por último, Frecuente, en donde la probabilidad de ocurrencia del riesgo es muy alta. En tal sentido, la frecuencia se entiende como la probabilidad de que ocurra un riesgo.

IMPACTO	
Insignificante	Generaría pérdidas de 20 dólares o menos
Menor	Generaría pérdidas de 21 y 100 dólares
Moderado	Generaría pérdidas de 101 y 10000 dólares
Mayor	Generaría pérdidas de 1001 y 5000 dólares
Catastrófico	Generaría pérdidas de 5000 dólares

Tabla 9. *Matriz de Riesgo, Tabla de Impacto*

Fuente. *Elaboración propia (2022).*

En la tabla 5, se presentan los niveles de impacto de la Matriz de Riesgo, es decir, el conjunto de consecuencias que origina la materialización de un riesgo, los cuales pueden significar un impacto a nivel económico, legal o incluso reputacional. Dicha tabla de impacto está definida por cinco (5) valores de la siguiente manera: Insignificante, en donde el impacto no representa un problema para la organización; Menor, el impacto que causa la materialización del riesgo en los objetivos de la empresa es mínimo; en el nivel Moderado la materialización del riesgo puede causar una pérdida momentánea; el nivel Mayor genera retrasos importantes que afectan el cumplimiento de los objetivos de la organización, en este caso de estudio, de la Universidad de Margarita; por último, el nivel Catastrófico puede detener la operación de la empresa, incluso, tener consecuencias como el cierre definitivo. En la tabla 5, se muestra que los cinco niveles establecidos para el impacto del riesgo representan pérdidas económicas para la organización.

NOMBRE DEL DEPARTAMENTO
Comisión de Sistemas y Tecnología
Control de Estudios
Dirección de Administración
Todos

Tabla 10. *Matriz de Riesgo, Tabla de Departamentos*

Fuente. *Elaboración propia (2022).*

En la tabla 6 se presentan los tres (3) departamentos de la población de la presente investigación, de acuerdo a la totalidad de la misma, es decir, la Comisión de Sistemas y Tecnología, la cual está integrada por 4 personas que representan la muestra de tipo intencional del estudio; el departamento de Control de Estudios, con 5 personas; y la Dirección de Administración con 8 personas en el departamento. La tabla de departamentos define la asociación de los departamentos con los riesgos y la frecuencia-impacto de los mismos.

ID	NOMBRE DEL RIESGO	DEPARTAMENTO AL QUE ESTA ASOCIADO
R1	Error humano	Todos
R2	Desastres naturales	Todos
R3	Correos Maliciosos	Todos
R4	No realizar copias de seguridad	Comisión de Sistemas y Tecnología
R5	Contraseñas de alto nivel	Todos
R6	Uso de aplicaciones de almacenamiento online	Todos
R7	Hurto de equipo	Todos
R8	Falla eléctrica	Todos
R9	Falla de Internet	Todos
R10	Caída del Sistema	Comisión de Sistemas y Tecnología
R11	Caída de la base de datos	Comisión de Sistemas y Tecnología

Tabla 11. *Matriz de Riesgo, Tabla de riesgos asociados a los departamentos*

Fuente. *Elaboración propia (2022).*

En la tabla 7, se representan los riesgos de acuerdo a los identificadores de la Matriz de Riesgo (la sigla R seguida del número correspondiente al riesgo), empleados en la ISO/IEC 27001 principalmente. Así pues, los identificadores de los riesgos asociados a departamentos van representados como y luego un número a partir del tres (3) hasta el trece (13). En la tabla se describen los nombres del riesgo, luego el departamento al que está asociado y cada cuanto podría suceder, es decir, la frecuencia del riesgo. De modo que sea posible visualizar la asociación con las tablas 4 y 6.

ID	PROBABILIDAD	IMPACTO	PROBABILIDAD	IMPACTO	PUNTAJE	NIVEL DE RIESGO
R1	Sucede varias veces en un mes	Generaría pérdidas de 21 y 100 dólares	5	2	5:2	Alto
R2	Sucede una vez por año	Generaría pérdidas de 1001 y 5000 dólares	1	4	1:4	Medio
R3	Sucede una vez por semestre	Generaría pérdidas de 101 y 10000 dólares	2	3	2:3	Medio
R4	Sucede varias veces en un mes	Generaría pérdidas de 5000 dólares	5	5	5:5	Muy Alto
R5	Sucede una vez por mes	Generaría pérdidas de 101 y 10000 dólares	4	3	4:3	Medio
R6	Sucede una vez por mes	Generaría pérdidas de 20 dólares o menos	4	1	4:1	Medio
R7	Sucede una vez por año	Generaría pérdidas de 5000 dólares	1	5	1:5	Alto
R8	Sucede varias veces en un mes	Generaría pérdidas de 1001 y 5000 dólares	5	4	5:4	Muy Alto
R9	Sucede varias veces en un mes	Generaría pérdidas de 101 y 10000 dólares	5	4	5:4	Muy Alto
R10	Sucede varias veces en un mes	Generaría pérdidas de 5000 dólares	5	5	5:5	Muy Alto
R11	Sucede una vez por mes	Generaría pérdidas de 5000 dólares	4	5	4:5	Muy Alto

Tabla 12. *Matriz de Riesgo, Tabla de coordenadas de acuerdo a la Probabilidad-Impacto.*

Fuente. *Elaboración propia (2022).*

En la tabla 8, se utilizan los identificadores para hacer un llamado a los riesgos, de modo que se muestran los dos aspectos de la tabla, Probabilidad-Impacto. También se presenta el valor del nivel de probabilidad-impacto, para poder calificar el nivel de riesgo de la matriz. Consecuentemente, la tabla 8 permite obtener las coordenadas de la calificación del riesgo para definir el nivel del mismo en cuatro (4) colores: verde como el nivel más bajo, amarillo como un nivel intermedio-bajo, naranja como un nivel intermedio-alto y rojo como el nivel más alto de riesgo. Se evidencia que al menos 5 riesgos presentan un nivel muy alto en la tabla de Probabilidad-Impacto, 2 se encuentran en un nivel Alto y 4 se encuentran en el nivel medio, por lo que no existe ningún riesgo dentro del rango bajo.

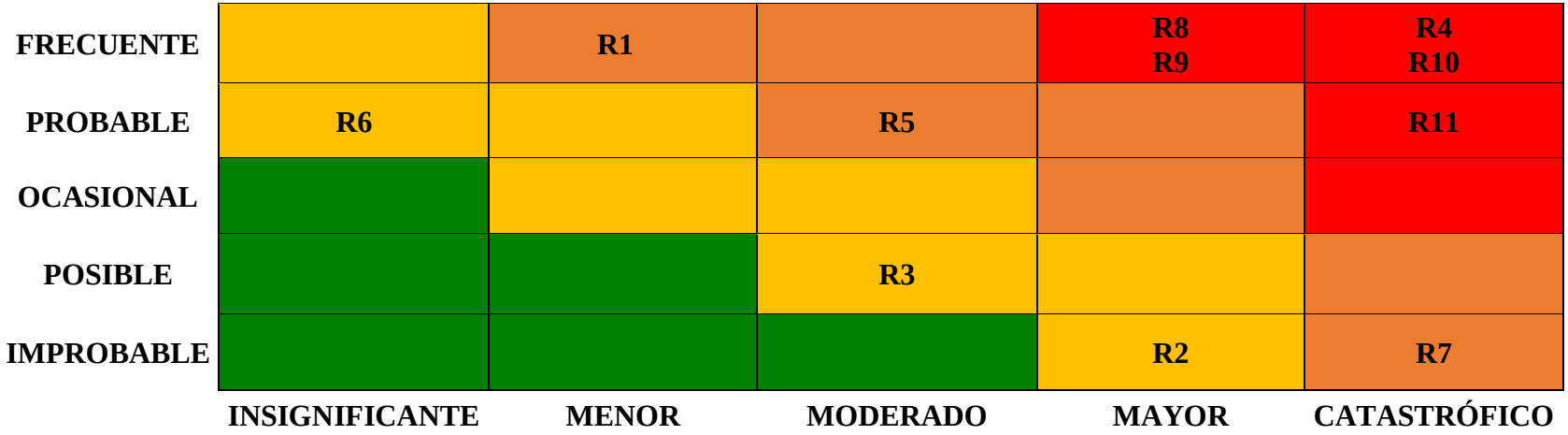

Figura 13. *Matriz de Riesgo*

Fuente. *Elaboración propia (2022).*

La figura 13 muestra la matriz con los riesgos (representados por las siglas R, seguido del número identificador) asociados a seguridad informática en la Universidad de Margarita (UNIMAR), en la cual se evidencian los niveles de riesgo desde varios niveles; bajo, medio, alto y muy alto. De acuerdo a la calificación del riesgo, es posible representar en la matriz los riesgos asociados de acuerdo a la probabilidad y el impacto de estos en la UNIMAR, de acuerdo a los dominios y controles presentados anteriormente en las tablas 11 y 12 respectivamente.

Se evidencia que, en promedio, la distribución de la matriz de riesgos presenta que, de los 11 riesgos asociados a la seguridad informática, 8 de esos riesgos se encuentran en los niveles alto (3 riesgos; R1, R5 y R7) y muy alto (5 riesgos; R4, R8, R9, R10 y R11) definidos en la tabla 12. Por lo tanto, el nivel de amenaza, en base a la matriz de riesgo, se encuentra en un nivel crítico de seguridad informática en el que la implantación se la normativa ISO se podrán mitigar estos riesgos de acuerdo a las acciones recomendadas en esta investigación

La implementación de la matriz de riesgos en la institución, permite planear y resumir, en base a los datos obtenidos, y bajo los lineamientos de la normativa, los indicadores a tomar en cuenta en materia de riesgos para proponer acciones concretas y poder disminuir o mitigar los riesgos y estimar el impacto que estas acciones tendrán sobre el nivel de riesgo de los trabajadores. En tal sentido, es posible observar el nivel de exposición al riesgo, gracias a la representación de los niveles de riesgo mediante la escala de colores, de acuerdo a la Frecuencia-Impacto de los riesgos presentes la UNIMAR.

4.3 Elaborar políticas y normas basadas en la ISO 27001 para gestionar, monitorear, supervisar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información (SGSI) dentro de los departamentos de la Universidad de Margarita.

Las normas ISO son un conjunto de estándares de reconocimiento internacional, basándose en el mejoramiento de los procesos, funciones y reconocimiento de las organizaciones, por lo tanto, son un referente de calidad a nivel mundial, dado que permiten establecer niveles de homogeneidad en relación a la gestión, prestación y desarrollo de servicios. Asimismo, buscan orientar, coordinar, simplificar y unificar los usos para conseguir menores costes y efectividad. No solo se beneficia la organización que las implementa, sino también sus clientes. Es por esto que, en la Universidad de margarita, el implementar las normas ISO, específicamente la ISO/IEC 27001:2013, las personas involucradas con esta organización se ven favorecidas por un mejor servicio, en este caso, de seguridad informática, dado que la universidad hace uso de sistemas de información y, por tanto, con la implementación de la norma se asegura que los bienes y servicios cumplen con los requisitos obligatorios relacionados con la calidad, la seguridad, el medio ambiente, y otros aspectos.

La Universidad de Margarita gestiona información vital que se debe gestionar de forma jerárquica de acuerdo a los criterios de seguridad de la información, respetando la triada de seguridad (confidencialidad, integridad y disponibilidad). Por tanto, la aplicación de normas y políticas de seguridad en los departamentos contribuye al mejoramiento continua a corto, medio y

largo plazo de las capacidades de los empleados y los departamentos a los que pertenecen. Las políticas de tecnología de la información (TI) para la gestión de seguridad informática están establecidas por los procesos que se desenvuelven en los distintos departamentos, brindándole a los usuarios la atención y servicios necesarios.

Política	Descripción	Contenido
Usuarios	Políticas para los usuarios (cuentas) que integran la organización y emplean el sistema informático de la misma, de modo que se asegure la autenticación (administración y acceso a los recursos).	• Creación y vigencia de usuarios de red. • Acciones ante la desvinculación o eliminación de cuentas de usuarios. • Creación y caducidad de contraseñas. • Responsabilidad de uso de contraseñas. • Acciones durante el "hiatus" de los usuarios. • Usuarios/participantes externos o invitados.
Software	Políticas para establecer las guías para la administración de los programas que integran las herramientas tecnológicas de la organización.	• Responsables de la instalación y requerimientos esenciales de software. • Aprobaciones de adquisiciones. desarrollo o implementación de software. • Responsables de nuevas soluciones de software. • Requerimientos de automatizar o mejorar procesos de la empresa. • Soporte de desarrollo o implementación de software.
Hardware	Políticas para asegurar un correcto uso de los equipos electrónicos, así como de los periféricos y accesorios disponibles en las distintas áreas (departamentos), para el desarrollo laboral de los empleados y el tratamiento de la información.	• Adquisición, asignación y configuración de hardware y software. • Actividades permitidas en el uso de hardware y software. • Responsabilidades de los equipos entregados a los empleados. • Autorización de salida de equipo fuera de la compañía. • Tiempo establecido para el cambio de equipo. • Seguridad implementada para los equipos. • Privilegios establecidos según el rol de usuario. • Responsabilidades de compra de hardware, periféricos y accesorios. • Actividades permitidas en los equipos de cómputo.

Política	Descripción	Contenido
Datos y Respaldo	Políticas dispuestas para la protección de los activos de información almacenada en los distintos dispositivos o servidores, siendo almacenada en conocimiento y propiedad de la organización.	• Selección de la herramienta para realizar el respaldo de información. • Contenidos permitidos y prohibidos de almacenar. • Responsables de realizar el respaldo de información. • Descripción de los esquemas de respaldo • Tiempo estimado de conservar el respaldo. • Copia de seguridad de los servidores.
Impresoras	Políticas para controlar y gestionar el servicio de impresión, copiado y escaneado de la organización, evitando el plagio de activos de la información.	• Descripción de equipos de impresión. • Control de cupos de impresión o copiado. • Prohibiciones de impresión de documentos. • Soporte técnico de los equipos de impresión. • Responsables de movimiento de equipos de impresión.
Correo electrónico	Políticas para asegurar el correcto uso de las herramientas de comunicación por medios electrónicos, así como de la información compartida por el mismo.	• Información prohibida para transmitir mediante el servicio de correo. • Actividades prohibidas en la creación de los mensajes. • Controles de correo SPAM. • Tamaño máximo de mensajes de entrada y salida. • Tipos de archivos no permitidos de enviar o recibir. • Descripción del filtrado de correo electrónico.
Internet e Intranet	Políticas establecidas para controlar el acceso al servicio de internet e intranet por parte de los usuarios de la organización.	• Descripción de los perfiles de navegación. • Actividades prohibidas. • Filtrado de contenido en páginas web.

Política	Descripción	Contenido
Prevención contra intrusos	Políticas dispuestas para el análisis de vulnerabilidades en el sistema, así como en los equipos electrónicos empleados en los departamentos y por los empleados de la organización, de acuerdo a la planificación del plan den base a la norma ISO/IEC 27001:2013.	• Análisis de vulnerabilidades. • Software antivirus. • Capacitaciones a usuarios.
Telefonía	Políticas dispuestas para el servicio de telefonía (recepción y emisión de llamadas) desde los distintos dispositivos dispuestos por la organización (análogos, digitales o IP).	• Descripción de perfiles de telefonía según el área (departamento). • Responsabilidades de asignación de líneas. • Restricciones del servicio de telefonía (fija, VoIP, móvil, entre otros)
Soporte técnico	Políticas dispuestas para dar a conocer la prestación de servicio de soporte técnico para la organización en sus distintos departamentos.	• Descripción de los servicios de TI. • Responsables de mantenimiento de los equipos de tecnología.

Tabla 13. *Políticas de Tecnología de la Información (TI)*

Fuente. *Elaboración propia (2022).*

PARTE V

LA PROPUESTA

5.1 Importancia de la propuesta

La seguridad informática dispone de muchos beneficios y oportunidades para las organizaciones de cualquier índole, dado que su importancia radia en la prevención, garantizando un acceso y uso seguro de la información registrada en equipos informáticos, así como de sistemas de información, protegiéndolos de posibles ataques y amenazas. Las mejores prácticas en materia de seguridad informática y de la información, significan la distinción de las organizaciones en el mercado al que pertenecen.

La normativa ISO, en su norma 27001, para las buenas prácticas en materia de seguridad informática y de la información, implementa controles y protocolos, que sirven como criterios de evaluación para las organizaciones en cuanto a los activos y recursos que estas disponen. Partiendo de las fases de implantación de la norma, se evidencia que, al reconocer los riesgos, es posible actuar sobre los mismos, mediante las normativas y regulaciones pertinentes, es decir que brinda más de un beneficio en gestión de información, también en el proceso de desarrollo y crecimiento de las organizaciones que manejan información.

El precisar de normas y políticas basadas en las normas ISO, para el diseño de un plan de seguridad informática, se agilizarán los procesos para la solución de problemas en materia de seguridad informática, así como permitir a la organización que las implementa mejorar su desempeño laboral, en sus distintas áreas y departamentos, pero principalmente, reduciendo los riesgos y amenazas que implicarían una pérdida de tiempo y dinero, beneficiando a la institución en gran medida si es aplicada.

5.2 Viabilidad de aplicación de la propuesta

A continuación, se presenta la viabilidad para la Universidad de Margarita (UNIMAR), en la cual se podrá analizar si la propuesta brindara los beneficios esperados para el plan de seguridad informática basado en la ISO/IEC 27001:2013, lo que da lugar conocer las posibles pérdidas o posibles beneficios para la UNIMAR en cuestión de tiempo y dinero. Consecuentemente, es necesario valorar la madurez de seguridad, midiéndola a través de la capacidad de la organización

para utilizar eficazmente las herramientas disponibles y dispuestas por la misma, de forma que se cree un nivel correcto y adecuado de seguridad, siendo sostenible a lo largo del tiempo.

Primeramente, es necesario establecer el punto de inicio de la madurez de la seguridad, de modo que pueda usarse para definir todas las áreas en las que se centra la seguridad y sus herramientas para con la organización. Así pues, es necesario evaluar en qué punto se encuentra y determinar el lugar que debería ocupar en vista de los riesgos a los que se enfrentan. Por consiguiente, la madurez de la seguridad, como una medida de las prácticas de una organización con respecto a las mejores prácticas para la seguridad sostenible, posee los siguientes niveles:

- Nivel 0, el "sentido común".
- Nivel 1, el cumplimiento de la legislación obligatoria
- Nivel 2, evaluación del proceso de Gestión de Seguridad.
- Nivel 3, analizar el riesgo y la gestión de su resolución.
- Nivel 4, adquisición de productos para integrarlos en los Sistemas de Gestión.
- Nivel 5, integración de los componentes certificados en sistemas compuestos y su certificación.

Para alinear el nivel de madurez y estrategia de seguridad asociada a la organización, se define la madurez como; Básica, en la que existen algunas medidas eficaces de seguridad, utilizadas como primera barrera en respuesta de operaciones e incidentes; Estándar, con capas múltiples de defensa, implementadas para respaldar una estrategia definida; Optimizada, siendo la protección más efectiva, con garantía de la utilización del mantenimiento de las mejores prácticas recomendadas. En este caso, la leyenda de la siguiente tabla está definida por: Verde, cumple las mejores prácticas, Amarillo, necesita mejorar y Rojo, Carencias severas.

Infraestructura	X	**Operaciones**	X
Defensa del perímetro	X	**Entorno**	X
Reglas y filtros de firewall	X	Host de gestión	X
Antivirus	X	**Directiva de seguridad**	X
Acceso remoto	X	Clasificación y Eliminación de los datos	X
Segmentación	X	Protocolos y servicios	X
Sistema de detección de intrusiones	X	Gestión de cuentas de usuario	X
Inalámbrico	X	Regulación	X

Autenticación	X	Directiva de seguridad	X
Usuarios administrativos	X	**Gestión de actualizaciones y revisiones**	X
Usuarios internos	X	Documentación de la red	X
Usuarios de acceso remoto	X	Flujo de datos de la aplicación	X
Directivas de contraseñas	X	Gestión de actualizaciones	X
Cuentas inactivas	X	Gestión de cambios y configuración	X
Gestión y control	X	**Copias de seguridad y recuperación**	X
Informes sobre incidentes y respuesta	X	Archivos de registro	X
Creación segura	X	Planificación de recuperación ante desastres	X
Seguridad física	X	Copias de seguridad	X
Aplicaciones	X	Dispositivos de copia de seguridad y restauración	X
Implementación y uso	X	**Personal**	X
Equilibrio de carga	X	**Requisitos y evaluaciones**	X
Clústeres	X	Requisitos de seguridad	X
Aplicación y recuperación de datos	X	Evaluaciones de seguridad	X
Almacenamiento y comunicación de datos	X	**Formación y conocimiento**	X
Cifrado	X	Conocimiento de seguridad	X
Cifrado - Algoritmo	X	Formación sobre seguridad	X

Tabla 14. *Tarjeta de puntuación de la evaluación de riesgos, Herramienta MSAT.*

Fuente. *Elaboración propia (2022).*

De acuerdo a la tabla de puntuación, se puede evidenciar que en los apartados de gestión la valoración es muy baja, representado en rojo, de los aspectos y criterios evaluados, en los que se resaltan el respaldo de datos, así como el almacenamiento y comunicación de los mismos, siendo estos factores significativos en cuanto a las buenas prácticas de seguridad informática y el cumplimiento de los principios de seguridad en la organización.

En tal sentido, la implantación de la norma ISO/IEC 27001:2013 en el diseño de un plan de seguridad informática para la Universidad de Margarita (UNIMAR), es viable dada la capacidad de la organización de mejorar su madurez de seguridad, así como promover el crecimiento y desarrollo de la institución mediante el mejoramiento de los aspectos y criterios de seguridad, es

decir, la confiabilidad basada en la triada de principios confidencialidad, integridad y disponibilidad.

5.2.1 Factibilidad técnica

Para el diseño de un plan de seguridad informática basado en la ISO/IEC 27001, en su edición del año 2013, para la Universidad de Margarita (UNIMAR), ubicada en El Valle del Espíritu Santo, Isla de Margarita, Nueva Esparta, Venezuela. Se cuenta con la siguiente documentación:

- ISO/IEC 27001:2013.
- Guía de implantación ISO 27001:2013 (NQA)
- ISO 27002 (Buenas prácticas)

COMPONENTE	DESCRIPCIÓN
Procesador	Intel Pentium Inside
Memoria RAM	4 GB
Disco Duro	128 GB
Sistema Operativo	Windows 7 Professional
Arquitectura	64 bits
Antivirus	360 Total Security
Fuente de Poder	500 W

Tabla 15. *Componentes técnicos de los equipos de la UNIMAR.*

Fuente. *Elaboración propia (2022).*

En la tabla 15, se muestran los componentes técnicos de los equipos de la Universidad de Margarita (UNIMAR), en los que se evidencian los principales componentes internos como: Procesador, Memoria RAM, Disco Duro, Sistema Operativo (S.O), Arquitectura, Antivirus y Fuente de poder, siendo estos los componentes internos sin incluir los periféricos de los equipos (monitor, teclado, mouse o ratón, entre otros). En cuanto al software de los equipos, se tiene que con Windows 7 Professional (x64) y un Intel Pentium Inside, 4GB de RAM y 128 de almacenamiento en disco, es viable implementar un plan de seguridad basado en la normativa de acuerdo a los equipos que dispone la institución. La operatividad de este SO es funcional, incluso cuando la empresa desarrolladora de software Microsoft ha terminado con el desarrollo de actualizaciones de Windows para esta versión, Windows 7 presenta un porcentaje menor en errores que con sus versiones más actuales de Windows 10.

5.2.2 Factibilidad operativa

Con la finalidad de alcanzar los objetivos planteados, se implantará la norma ISO/IEC 27001:2013 sobre seguridad informática, para el diseño de plan de seguridad que permita mejorar la gestión de los activos de información, así como de los recursos informáticos de la Universidad de Margarita (UNIMAR). En la presente investigación se describirán los pasos y fases a llevar a cabo, construyendo una metodología que garantice el cumplimiento de la norma de seguridad informática ISO/IEC 27001:2013, bajo normas y políticas aptas para la UNIMAR, los departamentos que la integran y los distintos procesos y subprocesos que se llevan a cabo en la organización.

Director de Seguridad de la Información

Es un cargo, también se le denomina CISO (Chief Information Security Officer), el cual está desempeñado (o debería estarlo) por un alto ejecutivo dentro del organigrama de la entidad, dadas las funciones y responsabilidades que entraña. Por lo tanto, debe cumplir con los siguientes requerimientos para cumplir con el papel:

- Tener conocimientos de seguridad, de acuerdo a los recursos y activos que gestiona la institución.
- Ser responsable con las iniciativas de seguridad.
- Mantenerse al día con los avances tecnológicos en materia de seguridad.
- Ser analítico, lógico y efectivo al momento de solucionar problemas.
- Mantener buena comunicación con los usuarios e integrantes de la institución que gestionen equipos informáticos.
- Tener habilidades comunicativas con respecto a aspectos técnicos de informática.
- Mantener registros sobre los eventos e incidencias bajo su cargo.
- Administrar el tiempo de forma eficiente, priorizar tareas y trabajar bajo la presión de cumplir plazos determinados.
- Velar por el cumplimiento de las normas y políticas en las distintas áreas de la organización que gestionen activos y recursos informáticos.

Gerente de riesgos (Risk Manager)

La gerencia de riesgos es la técnica de gestión de riesgos que tiende a salvaguardar el patrimonio (activos) de la misma frente a las pérdidas que puedan afectar su actividad. La gestión de riesgos tiene que estar totalmente integrada en la cultura de la empresa y estar presente en todos los niveles

organizativos, empezando por la Alta Dirección de la institución. En tal sentido, el puesto de gerente de riesgos debe cumplir con lo siguiente:

- Tener conocimientos sobre riesgos asociados a la institución, así como posibles eventos o de los antecedentes de la organización.
- En sus responsabilidades esta: el identificar y analizar distintos tipos de riesgo, desarrollar controles de gestión y planes de contingencia, y comunicar recomendaciones a la dirección.
- Tener experiencia en procedimientos de auditoria y denuncia.
- Tener conocimiento de los estándares y reglamentos en materia de cumplimiento de seguridad.
- Sólidos conocimientos informáticos y capacidad de investigación.
- Mente analítica y capacidad para solucionar problemas
- Excelentes habilidades de comunicación y presentación

En este sentido, ambos cargos pueden ser desempeñados por personas capaces en materia de seguridad y gestión, dispuestos por la Universidad de Margarita. Sin embargo, no es obligatorio que una sola persona posea todos los requerimientos necesarios, solo es importante el nivel de conocimiento, de ser múltiples personas, deben trabajar en equipo para mejorar la seguridad informática, así como las buenas prácticas en esta área, teniendo como objetivo el mejorar el resguardo de los activos que gestionan en las distintas áreas de la organización.

5.2.3 Factibilidad económica

El proyecto es factible a nivel económico, debido a que se implantará la norma ISO/IEC 27001:2013 de acuerdo a la documentación que esta dispone sobre seguridad informática, permitiendo desarrollar un plan que abarque los activos y recursos informáticos de la Universidad de Margarita (UNIMAR), de acuerdo a los departamentos que mantienen procesos proactivos en cuanto a información vital como lo son la Comisión de Sistemas y Tecnología, Control de Estudios y Dirección de Administración.

La factibilidad económica está dispuesta por el nivel de acción que tome la Alta Dirección de la UNIMAR en materia de seguridad informática, debido a que, en el presente proyecto, la implantación de la norma se lleva a cabo con la aplicación de las normas y políticas, con respecto a los sistemas de información, resaltando que la implementación de un plan de seguridad informática implica un ahorro de dinero, dado que previene de eventos e incidencias que se puedan convertir en riesgos o amenazas a nivel económico. Asimismo, se tiene en cuenta que, de existir

un compromiso de inversión, implicara la gestión del tiempo de los empleados o usuarios involucrados en la capacitación de personal. De igual forma, con respecto a la adquisición de recursos en materia de seguridad informática, dependerá de las acciones que se tomen por parte de la Alta Dirección, así como de la certificación de la Universidad de Margarita (UNIMAR) en la ISO/IEC 27001:2013 para la seguridad informática.

- **5.3 Objetivos de la propuesta**

5.3.1 Objetivo General

Diseñar un plan de seguridad informática basado en la norma ISO/IEC 27001:2013 para la Universidad de Margarita (UNIMAR), ubicada en El Valle del Espíritu Santo, Isla de Margarita, Nueva Esparta, Venezuela.

5.3.2 Objetivos específicos

- Preparar normas y políticas de seguridad basadas en la norma ISO/IEC 27001:2013 para la Universidad de Margarita (UNIMAR) en sus distintos departamentos.
- Evaluar los riesgos asociados a la seguridad informática en la Universidad de Margarita (UNIMAR)
- Elaborar el plan de seguridad informática para activos e información de la Universidad de Margarita (UNIMAR).

5.3.3. Descripción técnica de la propuesta

La presenta propuesta está orientada al diseño de un plan de seguridad informática que permita mejorar y asegurar la confidencialidad, integridad y disponibilidad de la información, basada en los parámetros y criterios que dispone la norma ISO/IEC 27001, en su edición 2013, para la Universidad de Margarita (UNIMAR), ubicada en El Valle del Espíritu Santo, Isla de Margarita, Nueva Esparta, Venezuela.

La información como recurso es un activo primordial en las organizaciones, con un valor significativo por el tipo de data que se gestiona. Por consiguiente, debe ser debidamente resguardada, con el objetivo de proteger su integridad, mantener una alta confidencialidad de la información, y brindar disponibilidad inmediata de acceso a los usuarios o sistemas autorizados a la misma. El estándar ISO 27001:2013 está preparado para proporcionar un modelo que permita establecer, implementar, operar, monitorear, revisar, mantener y mejorar los Sistemas de Gestión de Seguridad de la Información (SGSI). De modo que, bajo esta norma, se garantiza la continuidad

de los sistemas de información, minimizando los riesgos de daño y contribuyendo a una mejor gestión de activos e información en la UNIMAR.

Así pues, para que los principios de seguridad se cumplan, es necesario la implementación de normas y políticas de seguridad de la información de modo que formen parte de la cultura organizativa de la UNIMAR, lo que implica contar con el apoyo y compromiso de los empleados involucrados con la institución con respecto a la Tecnología de la Información (TI), para contribuir con la difusión, consolidación y cumplimiento de esta normativa, así como promover sus buenas prácticas en las distintas áreas de la institución.

Entre los parámetros de la ISO/IEC 27001:2013, están los controles de seguridad factibles a implementar por la institución, así como el dominio de la normativa y los objetivos de control de la misma. Estos aspectos están plasmados en un documento denominado Declaración de Aplicabilidad (SoA, por las siglas en ingles de Statement of Aplicability), el cual sirve para mantener registro y control de las medidas de seguridad que son aplicadas, así como la justificación de las mismas. En este apartado se detalla y verifica la aplicabilidad a la situación actual de la Universidad de Margarita (UNIMAR), en base a la normativa ISO, en términos de controles. El proceso consiste en enumerar los controles de seguridad que son factibles a implementar en la institución, por lo que la SoA incluye:

- El dominio de la norma ISO/IEC 27001:2013.
- Los objetivos de control que se implementan.
- Los objetivos de control que son seleccionados y su justificación de acuerdo a los parámetros de la norma.
- Los objetivos de control que se han excluido y la justificación para tomar tal decisión.

1. Políticas de seguridad de la información **Objetivo: Mantener el control acerca de cómo deben ser escritas y revisadas las políticas de seguridad de la información.**					
Sección	**Controles ISO 27001**	**Aplicabilidad**		**Justificación de aplicabilidad**	**Justificación de exclusión**
		Si	**No**		
1.1	Directrices de gestión de la seguridad de la información				
1.1.1	Políticas para la seguridad de la información	X		Es esencial el diseño de una política de seguridad de TI aprobada por la Alta Dirección que marque las directrices del plan de seguridad.	
1.1.2	Revisión de las políticas para la seguridad de la información	X		Es imprescindible realizar revisiones periódicas de las políticas, para garantizar el cumplimiento y evitar que queden obsoletas	
2. Aspectos organizativos de la seguridad de la información **Objetivo:** Controlar la asignación de las responsabilidades; además de la revisión de los controles para los dispositivos móviles y el teletrabajo.					
2.1	Organización interna				
2.1.1	Roles y responsabilidades en seguridad de la información	X		Es esencial definir y documentar las diferentes responsabilidades con respecto a la seguridad de la información.	

2.1.2	Segregación de tareas	X		Es necesario separa roles del personal, de acuerdo a sus capacidades en la seguridad de la información.	
2.1.3	Contacto con las autoridades	X		Las actividades llevadas a cabo deben mantener una coordinación	
2.1.4	Contacto con grupos de interés especial	X		Debe existir un monitoreo de interés especial, para identificar nuevos riesgos potenciales.	
2.1.5	Seguridad de la información en la gestión de proyectos	X		Es necesario agregar la seguridad como parte de la gestión de proyectos.	
2.2	Dispositivos para movilidad y teletrabajo				
2.2.1	Política de uso de dispositivos para movilidad	X		Es necesario establecer medidas y políticas de seguridad que regulen, el uso de dispositivos para la movilidad, así como también en el caso de ser necesario trabajar desde lugares diferentes a la oficina.	
2.2.2	Teletrabajo	X			
3. Seguridad de los recursos humanos **Objetivo:** Asegurar que el personal de la empresa sea el indicado; comprenda sus funciones dentro de la empresa antes, durante y después de emplear.					
3.1	Antes de la contratación				

3.1.1	Investigación de antecedentes	X		Debe ser un requisito necesario para para contratación de personal, verificar los antecedentes en concordancia con la ética y leyes relevantes.	
3.1.2	Términos y condiciones de contratación	X		Es necesario al momento de la contratación especificar las políticas y reglamentos en el cual el personal deba regirse.	
3.2	Durante la contratación				
3.2.1	Responsabilidades de gestión	X		Se debe asegurar que los empleados cumplan con las políticas de seguridad de la organización.	
3.2.2	Concienciación, educación y capacitación en seguridad de la información	X		Es necesario la formación continua bajo capacitaciones que formen una cultura de seguridad.	
3.2.3	Proceso disciplinario			Definir procesos formales para el tratamiento de empleados que falten a la seguridad.	
3.3	Cese o cambio de puesto de trabajo				
3.3.1	Cese o cambio de puesto	X		Es importante mantener políticas, que sean aclaradas durante la firma del contrato y al	

				momento del cese de trabajo no conlleve consecuencias.	
4. Gestión de activos **Objetivo:** Controlar todo lo relacionado con el inventario de activos, su uso aceptable, clasificación de la información y además la gestión de los medios de almacenamiento.					
4.1	Responsabilidad sobre los activos				
4.1.1	Inventario de activos	X		Es fundamental conocer y mantener actualizado el listado de activos de información de la empresa.	
4.1.2	Propiedad de los activos	X		Es necesario tener conocimiento del encargado de monitorear y llevar un control de activos.	
4.1.3	Uso aceptable de los activos	X		Indispensable establecer controles que promuevan la utilización adecuada de los activos.	
4.1.4	Devolución de activos	X		Debe existir un proceso formal para la devolución de los activos de información.	
4.2	Clasificación de la información				
4.2.1	Clasificación de la información	X		Es necesario especificar un plan para la clasificación de la información, basándose en la confidencialidad, integridad y disponibilidad	

4.2.2	Etiquetado de la información	X		Debe establecerse un proceso de etiquetado de información.	
4.2.3	Manipulación de la información	X		Se debe establecer medidas de control que verifiquen que solo el personal autorizado pueda manipular la información.	
4.3	Manejo de los soportes				
4.3.1	Gestión de soportes extraíbles	X		Se debe definir procedimientos para la utilización y el manejo de soportes extraíbles.	
4.3.2	Eliminación de soportes	X		Es necesario definir procedimientos para la eliminación de soportes de información.	
4.3.3	Soportes físicos en tránsito	X		Es necesario cumplir con controles de seguridad que se establezcan para soportes físicos que necesitan ser trasladados.	
5. Control de accesos **Objetivo:** Establecer y controlar las políticas de control de acceso, gestión de acceso para usuarios, control de acceso para el sistema, aplicaciones, y responsabilidades del usuario.					
5.1	Requisitos para controlar los accesos				
5.1.1	Política de control de accesos	X		Es importante mantener políticas en donde se indiquen los accesos creados, a quienes y, a que sistemas en la organización.	

5.1.2	Acceso a las redes y a los servicios de red	X		Los accesos deben ser autorizados y controlados, en sistemas y aplicaciones.	
5.2	Gestión de acceso de usuarios				
5.2.1	Registro y eliminación de usuarios	X		Debe existir un procedimiento adecuado de control de la base de datos de los usuarios	
5.2.2	Provisión de acceso de usuarios	X		Hay que disponer de una gestión centralizada de permisos para los usuarios.	
5.2.3	Gestión de privilegios de acceso	X		En requerida una monitorización periódica de quien tiene privilegios de administrador	
5.2.4	Gestión de información confidencial de autenticación de usuarios	X		Se debe controlar para mantener la confidencialidad de información y evitar su filtración.	
5.2.5	Revisión de los derechos de acceso de usuarios	X		Es necesario revisar los derechos de acceso periódicamente para detectar permisos erróneos.	
5.3	Responsabilidades del usuario				
5.3.1	Uso de información confidencial para la autenticación	X		Es necesario para mantener segura la información sensible como contraseñas.	
5.4	Control de acceso a sistemas y aplicaciones				
5.4.1	Restricción del acceso a la información	X		Se debe restringir los accesos indeseados o para usuarios ajenas a la organización.	

5.4.2	Procedimientos seguros de inicio de sesión	X		Es importante para todo sistema y equipos sensibles que requieran autenticación, garantizando inicios de sesión seguros.	
5.4.3	Sistema de gestión de contraseñas	X		Es necesario para controlar el acceso con contraseñas de calidad para todo sistema y equipo.	
5.4.4	Uso de utilidades con privilegios del sistema	X		Se debe revisar y proporcionar acceso específicamente para personas autorizadas.	
6. Criptografía **Objetivo:** Establecer controles relacionados con la gestión de cifrado y claves, para la compartición de información.					
6.1	Controles criptográficos				
6.1.1	Política de uso de controles criptográficos	X		Es necesario desarrollar e implantar una política de uso de controles criptográficos para la protección de la información.	
6.1.2	Gestión de claves	X		Es necesario para tener en cuenta el ciclo de vida completo (generación, uso y protección, distribución, renovación o destrucción), además para determinar fechas de activación y desactivación de claves.	
7. Seguridad física y ambiental					

Objetivo: Definir controles para las áreas físicas; estableciendo controles de entrada, protección contra amenazas, y seguridad de los equipos.					
7.1	Áreas seguras				
7.1.1	Perímetro de seguridad física	X		Necesario para proteger los equipos y activos de información.	
7.1.2	Controles físicos de entrada	X		Es necesario para establecer controles físicos de entrada a sitios en donde se encuentren los equipos y activos de información.	
7.1.3	Seguridad de oficinas, despachos y recursos	X		Es indispensable para controlar la seguridad de los lugares en donde se encuentre información sensible.	
7.1.4	Protección contra las amenazas externas y ambientales	X		Es necesario para establecer un plan ante amenazas ambientales o desastres naturales, para la protección de equipos.	
7.1.5	Trabajo en áreas seguras	X		Es indispensable para la protección física en áreas seguras y establecer prohibiciones.	
7.1.6	Áreas de acceso público, carga y descarga	X		Es necesario para establecer puntos sensibles para la seguridad física y los respectivos controles en las áreas de acceso público.	
7.2	Seguridad de los equipos				

7.2.1	Emplazamiento y protección de equipos	X		Es necesario para establecer zonas estratégicas que permitan disminuir el riesgo de amenazas y daños ambientales que afecten el estado físico de los equipos.	
7.2.2	Instalaciones de suministro	X		Es necesario mantener monitoreado periódicamente el sistema UPS que proporcione potencia adecuada, confiable y de calidad.	
7.2.3	Seguridad del cableado	X		Esencial para la protección y separación entre cableado de comunicaciones con el de suministro eléctrico, y evitar daños e interferencias.	
7.2.4	Mantenimiento de los equipos	X		Importante para realizar programaciones periódicas, para efectuar mantenimientos de los equipos.	
7.2.5	Salida de activos fuera de las dependencias de la empresa	X		Es necesario controlar los equipos fuera de las instalaciones, así también mantener un registro de los usuarios que lo puedan realizar.	
7.2.6	Seguridad de los equipos y activos fuera de las instalaciones	X		Es necesario establecer el uso aceptable y compromiso del empleado en la seguridad de los equipos fuera de las instalaciones.	

7.2.7	Reutilización o eliminación segura de equipos	X		Indispensable controlar la reasignación o eliminación de equipos, y el respaldo o borrado seguro de la información.	
7.2.8	Equipo informático de usuario desatendido	X		Requerido para aplicar a todos los equipos y evitar la suplantación de identidad.	
7.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla	X		Aplicable para todos los usuarios y los respectivos equipos que eviten la suplantación y robo de información.	
8. Seguridad operativa **Objetivo:** Revisar los controles relacionados con la gestión de la operatividad en las TI.					
8.1	Procedimientos y responsabilidades operacionales				
8.1.1	Documentación de procedimientos de operación	X		Debe existir en los procesos operativos la documentación con estricta gestión y seguridad, para ponerlos a disposición de los demás.	
8.1.2	Gestión de cambios	X		Debe existir un plan de control para gestionar los cambios en sistemas operacionales.	
8.1.3	Gestión de capacidades	X		Necesario para realizar monitoreos continuos del uso de los recursos, evitando interrupciones de servicio.	

8.1.4	Separación de entornos de desarrollo, prueba y operatividad	X		Es requerido para mantener la seguridad de la información separando datos para sistemas de pruebas o de lanzamiento.	
8.2	Protección contra código malicioso (malware)				
8.2.1	Controles contra el código malicioso	X		Es necesario garantizar la protección de la información, y establecer una programación para realizar controles antimalware.	
8.3	Copias de seguridad				
8.3.1	Copias de seguridad de la información	X		Es importante que se establezcan periodos adecuados, para que se realicen copias de seguridad garantizando que la información este respaldada y disponible.	
8.4	Registro de actividad y supervisión				
8.4.1	Registro y gestión de eventos de actividad	X		Es necesario realizar un monitoreo y registro de las eventualidades que se presenta dentro de la red corporativa.	
8.4.2	Protección de los registros de información	X		Los servicios y la información de registro de la actividad deben estar protegidos contra acciones forzadas o accesos no autorizados.	

8.4.3	Registros de administración y operación	X		Las actividades del administrador y operador del sistema deben registrarse.	
8.4.4	Sincronización de relojes	X		Los relojes de todos los sistemas de procesamiento de información dentro del dominio corporativo deben estar sincronizados con una fuente de tiempo acordada y precisa.	
8.5	Control de software				
8.5.1	Instalación de software	X		Se debe implementar procedimientos para controlar la instalación de software en sistemas operativos.	
8.6	Gestión de la vulnerabilidad				
8.6.1	Gestión de las vulnerabilidades técnicas	X		Se debe monitorear la red, mantener actualizado los sistemas y obtener información sobre las vulnerabilidades técnicas de los sistemas de información utilizados.	
8.6.2	Restricciones en la instalación de software	X		Es indispensable para controlar que solo los administradores instalen software en los equipos.	
8.7	Consideraciones de las auditorías de los sistemas de información				

8.7.1	Controles de auditoría de los sistemas de información	X		Es necesario para garantizar, el correcto respaldo y confidencialidad de la información en los sistemas evitando interrupciones.	
9. Seguridad de las comunicaciones **Objetivo:** Controlar las acciones relacionadas con la seguridad de redes en el intercambio de información					
9.1	Gestión de la seguridad de redes				
9.1.1	Controles de red	X		La red debe estar controlada adecuadamente para protegerla de las amenazas y mantener la seguridad en los sistemas y aplicaciones.	
9.1.2	Seguridad de los servicios de red	X		Deben identificar e incluir, en cualquier acuerdo sobre los servicios de red, las características de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios.	
9.1.3	Segregación de redes	X		Necesaria para controlar la segregación de red según los grupos de servicios, usuarios y sistemas de información.	
9.2	Intercambio de información con partes externas				

9.2.1	Políticas y procedimientos de intercambio de información	X		Se debe implementar políticas, procedimientos y controles de intercambio de información sean por canales seguros.	
9.2.2	Acuerdos de intercambio	X		Es necesario para establecer acuerdos que deben abordar el intercambio seguro de información entre la organización y partes externas.	
9.2.3	Mensajería electrónica	X		La información que se administra mediante la mensajería electrónica debe estar protegida.	
9.2.4	Acuerdos de confidencialidad	X		Es necesario para establecer acuerdos documentados para regular la confidencialidad y "no divulgación" de información.	
10. Adquisición, desarrollo y mantenimiento de los sistemas de información **Objetivo:** Administrar los controles que definen los requerimientos de seguridad en los procesos de desarrollo y soporte de los sistemas de información					
10.1	Requisitos de seguridad en los sistemas de información				
10.1.1	Análisis y especificaciones de los requisitos de seguridad	X		La seguridad de la información debe incluirse en los requisitos para nuevos sistemas o mejoras a los sistemas de información existentes.	

10.1.2	Asegurar los servicios de aplicaciones en redes públicas	X		Es necesario para resguardar la información en cuanto a las redes públicas, evitando accesos o irrupciones indeseadas.	
10.1.3	Protección de la transmisión de información en los servicios de aplicaciones	X		Es necesario para garantizar la protección de la transmisión entre aplicaciones y garantizar las comunicaciones extremo a extremo.	
10.2	Seguridad en los procesos de desarrollo y soporte				
10.2.1	Política de desarrollo seguro de software	X		La empresa debe establecer políticas que fomenten el desarrollo seguro de software, para seguridad de la información.	
10.2.2	Procedimientos de control de cambios en los sistemas	X		Debe existir documentación que identifique los procedimientos de cambio en los sistemas.	
10.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	X		Las aplicaciones de negocio deben ser revisadas y probadas posterior al cambio, para garantizar que no se hayan generado impactos adversos en las operaciones o la seguridad de información.	
10.2.4	Restricciones a los cambios en los paquetes de software	X		Se deben controlar los cambios en los paquetes de software, limitándose a los cambios que son realmente necesarios.	

10.2.5	Uso de principios de ingeniería en protección de sistemas	X		Los sistemas deben estar establecidos, documentados y revisado la seguridad en todo el diseño de software	
10.2.6	Seguridad en entornos de desarrollo	X		Se deben establecer una protección adecuada de los entornos de desarrollo e integración de sistemas, que abarque todo el ciclo de vida del desarrollo del sistema.	
10.2.7	Externalización del desarrollo de software	X		La organización debe supervisar y monitorear las actividades de desarrollo del sistema que se han subcontratado.	
10.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas	X		Las pruebas de funcionalidad deben realizarse en aspectos de seguridad durante las etapas de desarrollo.	
10.2.9	Pruebas de aceptación	X		Se debe establecer procesos de prueba y criterios para la aceptación de sistemas de información nuevos, y/o nuevas versiones.	
10.3	Datos de prueba				
10.3.1	Protección de los datos utilizados en pruebas	X		Se deben seleccionar cuidadosamente los datos de prueba, los mismos que deben ser monitoreados.	
11. Relación con proveedores **Objetivo: A**nalizar los controles que existentes o que deben incluirse en los contratos con proveedores					

11.1	Seguridad en las relaciones con proveedores				
11.1.1	Política de seguridad de la información en las relaciones con los proveedores	X		La organización debe documentar las condiciones seguridad de la información en los activos, para mitigar los riesgos que se asocien al acceso por parte de los proveedores.	
11.1.2	Requisitos de seguridad en contratos con terceros	X		Los acuerdos con terceros que impliquen acceso, procesamiento, comunicación o gestión de la información de la empresa deben cubrir todos los requisitos de seguridad relevantes.	
11.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	X		Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información relacionados con la cadena de suministro de productos.	
11.2	Gestión de la prestación del servicio por proveedores				
11.2.1	Supervisión y revisión de los servicios prestados por terceros	X		La organización debe monitorear, revisar y auditar la presentación de los servicios del proveedor regularmente.	
11.2.2	Gestión de cambios en los servicios prestados por terceros	X		Los cambios en servicios prestados por terceros deben mantenerse o mejorar las	

				condiciones de las políticas de seguridad de la información.	
12. Gestión para incidentes en la seguridad de la información **Objetivo:** Establecer controles que permitan encontrar y archivar debilidades					
12.1	Gestión de incidentes de seguridad de la información y mejoras				
12.1.1	Responsabilidades y procedimientos	X		Se deben establecer responsabilidades y procedimientos de gestión para garantizar una respuesta inmediata, eficaz y ordenada a los incidentes de seguridad de la información.	
12.1.2	Notificación de los eventos de seguridad de la información	X		Los eventos de seguridad de la información deben ser comunicados lo más pronto posible, al personal o administrador apropiado.	
12.1.3	Notificación de puntos débiles de la seguridad	X		Se debe informar sobre cualquier debilidad sospechosa en la seguridad de la información en los sistemas o servicios.	
12.1.4	Valoración de eventos de seguridad de la información y toma de decisiones	X		Los eventos de seguridad de la información deben ser evaluados antes de la toma de una decisión.	

12.1.5	Respuesta a los incidentes de seguridad	X		Se debe contar con un plan de contingencia documentado los procedimientos realizados que solventen los incidentes.	
12.1.6	Aprendizaje de los incidentes de seguridad de la información	X		Se debe basar en el conocimiento obtenido del análisis y resolución de incidentes, para reducir la probabilidad de impacto en incidentes futuros.	
12.1.7	Recopilación de evidencias	X		Se debe definir y aplicar procedimientos necesarios ante cada evento negativo, crear un registro de incidentes	
13. Aspectos para la seguridad de la información y gestión de la continuidad de la organización **Objetivo:** Establecer controles que permitan la planificación para la continuidad de la organización					
13.1	Continuidad de la seguridad de la información				
13.1.1	Planificación de la continuidad con respecto a la seguridad de la información	X		Es necesario determinar requisitos necesarios para la seguridad de la información y su administración en situaciones adversas.	
13.1.2	Implantación de la continuidad de la seguridad de la información	X		Es indispensable para que pueda ser puesto en marcha el plan de continuidad de seguridad de la información.	

13.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	X		Se debe realizar periódicamente una revisión y evaluación de la continuidad para la seguridad de la información.	
13.2	Redundancias				
13.2.1	Disponibilidad de instalaciones para el procesamiento de la información	X		Se debe implementar una redundancia suficiente en las instalaciones de procesamiento de información y en correspondencia con los requisitos de disponibilidad.	
14. Cumplimiento **Objetivo:** Verificar el cumplimiento tanto de los controles, políticas y normas establecidas; así como las normativas contractuales con el fin de garantizar una adecuada gestión de la seguridad de la información.					
14.1	**Cumplimiento de los requisitos legales y contractuales**				
14.1.1	Identificación de la legislación aplicable	X		Se deben identificar todos los requisitos legales reglamentarios y contractuales	
14.1.2	Derechos de propiedad intelectual (DPI)	X		Se debe implementar para garantizar el cumplimiento de requisitos legales, relacionados con los derechos de propiedad intelectual y el uso de software original.	

14.1.3	Protección de los registros de la organización	X		Es importante establecer protección de los registros importantes de la empresa, evitando perdida, destrucción, falsificación o publicación no autorizada.	
14.1.4	Protección de datos y privacidad de la información personal	X		Es necesario determinar normativas para mantener un control y privacidad de los datos personales, tanto de los usuarios como de la empresa.	
14.1.5	Regulación de los controles criptográficos	X		Al aplicar mecanismos de cifrado es necesario tener en cuenta las normativas de uso de controles criptográficos vigentes, como la firma electrónica.	
14.2	**Revisiones de la seguridad de la información**				
14.2.1	Revisión independiente de la seguridad de la información	X		El enfoque de la organización para la implementación y administración de la seguridad de la información debe evaluarse en base a revisiones de manera independiente, en intervalos planificados o cuando se producen cambios específicos en la organización.	

14.2.2	Cumplimiento de las políticas y normas de seguridad	X		Se debe revisar y evaluar periódicamente al personal con respecto al cumplimiento de las políticas de seguridad de la información.	
14.2.3	Comprobación del cumplimiento técnico	X		Es necesario revisar regularmente el cumplimiento y que realmente funcionen.	

Tabla 16. *Declaración de aplicabilidad*

Fuente: *Elaboración propia (2022)*

En base a la declaración de aplicabilidad realizada, se evidencia que la Universidad de Margarita (UNIMAR), posee un nivel de aplicabilidad alto con respecto a los protocolos de la norma ISO/IEC 27001:2013, es decir, con respecto al Control de Anexos de la normativa en cada uno de sus apartados. Lo que permite que las normas y políticas sean definidas bajo dichos criterios, analizando los controles y delimitando el alcance de las mismas. Para la implementación de los controles se evaluó la estructuración individual con respecto a la seguridad en la institución. De tal forma, la ejecución bajo esta normativa permite que los procesos de seguridad estén equilibrados y exista una alta coordinación entre sí, por lo que las metodologías contribuyen a la mitigación de riesgos y a incrementar el nivel de seguridad en la información existente en la UNIMAR.

En relación a lo anterior, la ISO 27001 es la norma internacional para los Sistemas de Gestión de Seguridad de la Información (SGSI), la cual proporciona y dispone de un marco robusto y significativo para proteger la información, como activo, de la organización. De acuerdo a esto, la normativa se basa en un ciclo de mejora continua, también denominado Ciclo Deming o Ciclo PHVA, el cual es aplicable no solo al sistema de gestión, sino también a cada elemento individual para proporcionar un enfoque en la mejora continua, por lo que se define de la siguiente manera:

- Planificar: establecer objetivos, recursos, requisitos de la organización, política organizativa e identificar riesgos y oportunidades.
- Hacer: implantar lo planificado.
- Verificar: controlar y medir los procesos para establecer el rendimiento de la política, objetivos, requisitos y actividades planificadas e informar de los resultados.
- Actuar: tomar acciones para mejorar el rendimiento, en la medida de lo necesario.

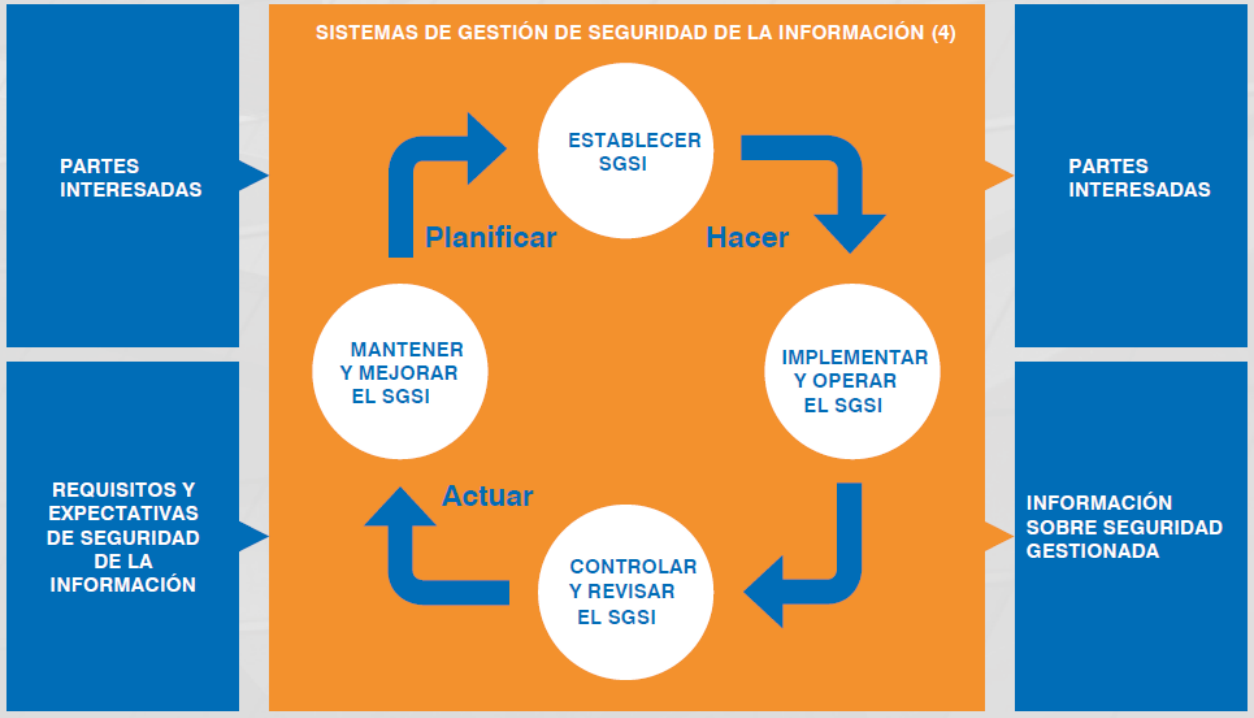

Figura 14. *Modelo PHVA para ISO 27001.*

Fuente: *NQA. ISO 27001:2013. Guía de Implantación para la Seguridad de la Información* https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

Para los lineamientos que dispone el ciclo PHVA, se tiene en consideración de que no existe un final al momento de obtener los resultados, debido a que el ciclo se reinicia de manera periódica y por lo que se le atribuye como un proceso de mejora continua. Por lo tanto, al evaluar y analizar los criterios de la norma ISO/IEC 27001, dispuestos en sus controles presentados en la tabla 16, el ciclo de mejora continua en conjunto con los controles de la normativa, permite establecer un modelo comparable a lo largo del tiempo, de modo que se puede medir el grado de mejora alcanzado al definir el plan de seguridad informática.

Presentación del plan de seguridad informática

De acuerdo a la evaluación y análisis mediante los controles de la norma ISO/IEC 27001:2013, bajo la metodología del Ciclo Deming, en la Universidad de Margarita (UNIMAR) con respecto a las actividades y procesos que se llevan a cabo en la misma, se ha podido determinar que la probabilidad de ocurrencia de incidentes con la seguridad de la información es alta. Por lo tanto, es necesario establecer políticas se seguridad lógicas, coherentes y enmarcadas dentro de los límites

de la UNIMAR, cuyo propósito será apoyar, promover y proporcionar la guía normativa para la gestión y buenas prácticas de la seguridad de la información.

A continuación, se definen las normas y políticas, las cuales cubren las necesidades en materia de seguridad; organizacional, lógica, física y legal de la UNIMAR, de acuerdo a los principios de seguridad; confidencialidad, integridad y disponibilidad, y bajo los lineamientos y controles de la norma ISO/IEC 27001:2013. Asimismo, se puntualizan los aspectos de seguridad de acuerdo a las necesidades, de la siguiente forma:

Seguridad Organizacional (Gestión de Activos – Recursos Humanos)

En esta sección se establece un marco formal con respecto a los aspectos de gestión de activos, recursos humanos, así como físicos, también las responsabilidades y actividades y acciones complementarias ante eventualidades e incidentes relacionados a la seguridad de la información en la organización, de tal forma que sirva como base para las políticas, partiendo desde el desarrollo de la UNIMAR, y el cumplimiento de las normas y protocolos de seguridad.

Seguridad Lógica (Control de Acceso – Gestión de las Operaciones y Comunicaciones)

En este apartado se muestran los lineamientos y regulaciones para la gestión de control de acceso por parte de los usuarios tanto al sistema de información como a equipos de la entidad, de modo que se prevengan y eviten alteraciones en la configuración de los mismos. Además, se definen normativas para el control de vulnerabilidades por causa de software malicioso (Malware) en los equipos.

Seguridad Física

Se establecen límites en cuanto a la definición de perímetros de seguridad, teniendo en cuenta los factores existentes en la organización, de igual forma, se implementarán controles relacionados con el manejo, mantenimiento y soporte técnico de los equipos como activos de la Universidad de Margarita (UNIMAR) empleados en los distintos procesos internos de la misma, por los usuarios (estudiantes, empleados o visitantes autorizados).

Seguridad Legal (Cumplimiento)

Se deben integrar las políticas y normativas de seguridad establecidas bajo la normativa ISO, de modo que su operatividad permita verificar el cumplimiento de las mismas y, a partir de ello, definir sanciones al personal de la organización ante faltas cometidas y que vulneren la seguridad de la información, con el propósito de promover una cultura organizacional con respecto a las normas y regulaciones en la UNIMAR en materia de seguridad informática.

POLÍTICAS QUE REGULAN ACTIVIDADES RELACIONADAS AL USO DE TECNOLOGÍAS DE LA INFORMACIÓN

Finalidad

Las políticas de Tecnología de la Información (TI), tienen como finalidad el proteger y resguardar la información, a la organización y buscar un aumento en la seguridad y aprovechamiento de la tecnología, lo que contribuye de manera determinante a aumentar la eficiencia en el trabajo y garantizar la continuidad de las operaciones de la entidad, con el objetivo de cumplir los principios de seguridad en las distintas áreas de la misma y en la gestión de sus activos.

Ámbito

Las políticas de las TI serán aplicadas de manera obligatoria por los empleados, servidores y trabajadores que integran la Universidad de Margarita (UNIMAR), ubicada en El Valle del Espíritu Santo, Isla de Margarita, Nueva Esparta, Venezuela, que utilicen el hardware, software y tecnologías de comunicación, para el cumplimiento de sus actividades y operaciones diarias.

Responsable o Encargado

La Universidad de Margarita (UNIMAR) será la delegada a seleccionar encargados capacitados en la administración y ejecución de estas políticas a través de procedimientos, asimismo las políticas deben cumplirse a nivel organizacional, en todos sus departamentos, por las dependencias que tienen a su cargo el uso de recursos tecnológicos.

Recursos Tecnológicos

Las políticas de Tecnología de la Información regularán y estandarizarán el uso de los recursos informáticos (activos) que la Universidad de Margarita (UNIMAR) proporciona a todo el personal para desarrollar sus actividades y cumplir con la misión de la institución.

Términos

En las políticas de Tecnología de la Información se definen los siguientes términos:

- Tecnologías de Información y Comunicación (TIC): equipos informáticos, software y dispositivos de impresión personalizados y centralizados que se utilizarán para almacenar, procesar, convertir, proteger, transferir y recuperar información, datos, voz, imágenes y video.
- Hardware: componente físico de un computador y dispositivos externos.
- Información: conjunto de datos procesados y organizados.

- Usuarios: personas o individuos que utilizan la estructura tecnológica y de comunicaciones que manejan la información, bien sea de forma habitual u ocasional.
- Seguridad informática: es el área de tecnología de la información que se centra en la protección de la infraestructura informática y todo lo relacionado con ella, especialmente, la información contenida o circulante.
- Integridad: se refiere a la corrección y complementación de los datos en una base de datos.
- Confidencialidad: la información solo debe ser accesible únicamente para personal autorizado.
- Disponibilidad: debe estar disponible cuando se necesita, es decir, accesible.
- Amenaza: evento que puede desencadenar en un incidente en la empresa, que cause daños materiales o pérdidas inmateriales en sus activos.
- Impacto: medir la consecuencia al materializarse una amenaza.
- Vulnerabilidad: posibilidad de que ocurra mediante una exploración, se viole la seguridad del sistema.
- Ataque: evento exitoso o no, que atenta sobre el buen funcionamiento de un sistema.
- Backup: respaldo de la información.
- Passwords: Clave que se asigna a los usuarios.
- Retención: tiempo de vigencia de un respaldo.
- Dirección MAC: identificador de 48 bits (6 bloques hexadecimales) que corresponde de manera única a una tarjeta o dispositivo de red.
- Dirección IP: es un número que identifica, lógica y jerárquicamente, una interfaz de red (elemento de comunicación / conexión) de un dispositivo (computadora, tableta, computadora portátil, teléfono inteligente) que utiliza el protocolo IP (Protocolo de Internet), que corresponde al modelo de red de nivel TCP/IP.
- URL: dirección web.
- TI: Tecnologías de la Información.

POLÍTICA PARA EL USO ADECUADO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMNICACIÓN

Responsables

La Universidad de Margarita (UNIMAR) será la delegada a seleccionar encargados capacitados en la administración y ejecución de estas políticas a través de procedimientos, asimismo las

políticas deben cumplirse a nivel organizacional, en todos sus departamentos, por las dependencias que tienen a su cargo el uso de recursos tecnológicos.

Generales

Para el uso adecuado por parte de los usuarios de los recursos tecnológicos de la Universidad de Margarita (UNIMAR), se tomarán en cuenta las siguientes indicaciones:

1. Para el hardware (equipos, impresoras, escáner, servidores y demás recursos tecnológicos) propiedad de la UNIMAR, la institución y sus integrantes designados por la Alta Dirección, son los únicos autorizados para realizar las actividades de soporte técnico, mantenimiento y cambios de configuración en el equipo de cómputo. En el caso de trabajos de mantenimiento efectuadas por terceros, éstas serán previamente autorizadas y supervisadas por la administración de la entidad.
2. En caso de equipos tecnológicos en estado de arrendamiento, la empresa proveedora es la única autorizada a realizar los trabajos de mantenimiento y cambio de hardware o en su caso autorizar dichas labores, previa coordinación con la Alta Dirección de la UNIMAR.
3. El acceso al área de infraestructura informática es restringido y únicamente ingresará personal autorizado.
4. Se restringirá el acceso a los equipos tecnológicos, a aquellos usuarios que no cuenten con una autorización previa de su gerencia para laborar fuera de horario.
5. Las/os usuarios autorizados de los sistemas informáticos de la UNIMAR, no harán uso indebido de suministro, información administrativa, datos en general y datos considerados como confidenciales.
6. Los recursos almacenados deben mantenerse en un sitio designado por la Alta Dirección de la UNIMAR, o los encargos que esta designe para la tarea, de existir activos separados o no compatibles con la infraestructura tecnológica se implementarán proyectos de integración y/o migración de aplicativos y base de datos.

Hardware

El hardware de propiedad de la Universidad de Margarita (UNIMAR) o arrendado, se utilizará únicamente para actividades relacionadas con los objetivos de la entidad, para lo cual se observará lo siguiente:

1. Para el correcto funcionamiento del hardware se realizará mantenimiento preventivo, de acuerdo a un plan de mantenimiento preventivo del equipo de cómputo anual, elaborado por los técnicos de soporte del departamento de Tecnología de la Información.
2. Cuando exista algún incidente (robo, extravío, daño físico, etc.) que afecte de manera directa al hardware de la UNIMAR, se notificará de inmediato a las autoridades competentes de la entidad.
3. Solamente el personal de la UNIMAR autorizado por la Alta Dirección, está capacitado para abrir los gabinetes de las computadoras personales o de cualquier otro equipo de cómputo propiedad de la empresa, que NO cuenten con la garantía técnica vigente.
4. Para los equipos cuya garantía técnica aún se encuentre vigente, lo efectuará únicamente el personal técnico calificado de la empresa proveedora.
5. Para los equipos de cómputo de arrendamiento, la empresa arrendadora es la única autorizada para abrir los gabinetes de dichos equipos o en su caso autorizará la apertura de ellos, previa coordinación con la Alta Dirección de la UNIMAR, o de los encargados que esta designe.

Almacenamiento de data

La Universidad de Margarita (UNIMAR) designará la ubicación de la información sensible y demás activos de acuerdo a su segmentación, así como los equipos de comunicaciones necesarios para la operación de las actividades informáticas de la institución y se observará los siguiente:

1. El acceso a las localizaciones o centros de datos, designados por la UNIMAR, son de acceso restringido y sólo personal autorizado por la Alta Dirección pueden tener acceso a él.
2. El acceso a los servidores de los centros de datos o los equipos designados para el almacenamiento de data, ya sea usando la consola de administración local o una consola de administración remota es restringido al personal autorizado por la Alta Dirección de la UNIMAR.

Propiedad de la información

Los usuarios de cualquier equipo de cómputo de la Universidad de Margarita (UNIMAR), deben estar informados y conocer que los datos que estos crean y manipulan en los sistemas, aplicaciones y cualquier medio de procesamiento electrónico, durante sus actividades laborales, son de propiedad y responsabilidad de la UNIMAR, para lo cual se respetará lo siguiente:

1. Los derechos patrimoniales de un programa de computación, hojas de cálculo, archivos de Word, macros, etc., y su documentación, creados por uno o varios empleados en el ejercicio de sus actividades laborales corresponden a la UNIMAR.
2. Los respaldos que contengan información de la UNIMAR y que fueron realizados o solicitados, se tendrán exclusivamente bajo resguardo, debiendo ser entregaos al superior inmediato al finalizar su relación laboral con la entidad.

Usos inadecuados

En la Universidad de Margarita (UNIMAR), las siguientes actividades están prohibidas:

1. Violar los derechos de cualquier persona u organización protegidos por derechos de autor, patentes o cualquier otra forma de propiedad intelectual.
2. Difundir información identificada como confidencial a través de medios que involucren el uso de equipos tecnológicos.
3. Introducir software malicioso en la red o en los servidores (virus, troyanos, ráfagas de correo electrónico no solicitado, etc.).
4. Utilizar la infraestructura de tecnología de información de la UNIMAR para conseguir o transmitir material con fines de lucro.
5. Utilizar el sistema de comunicaciones de la UNIMAR con el fin de realizar algún tipo de acoso, difamación, calumnia o cualquier actividad hostil.
6. Hacer propuestas fraudulentas de productos o servicios cuyo origen sean los recursos o servicios propios de la UNIMAR.
7. Realizar actividades que incumplan la seguridad de los sistemas o que generen interrupciones de la red o de los servicios.
8. Monitorear puertos o realizar análisis del tráfico de la red con el propósito de evaluar vulnerabilidades de seguridad. Solo el personal capacitado, designado por la Alta Dirección, encargado de la Seguridad Informática puede realizar estas actividades siempre y cuando cuente con la aprobación por parte del jefe de área.
9. Eludir mecanismos de seguridad, autenticación, autorización o de auditoría de cualquier servicio de red, aplicación, servidor o cuenta de usuario.
10. Usar comandos o programas para el envío de mensajes de cualquier tipo con el propósito de interferir o deshabilitar una sesión de usuario a través de cualquier medio, local o remoto (Internet, Intranet).

11. Instalar cualquier tipo de software en los equipos de cómputo de la UNIMAR sin la previa autorización de los encargados en el área de seguridad informática designados por la Alta Dirección de la entidad.
12. Modificar la configuración del software antivirus, firewall personales o políticas de seguridad en general implementadas en los equipos de cómputo de la UNIMAR sin consultar o estar autorizados por los encargados en el área de seguridad informática designados por la Alta Dirección de la entidad.

Excepciones

Para propósitos de mantenimiento de la red y de seguridad, por excepción el personal debidamente autorizado, podrá estar exento de seguir algunas de las restricciones anteriores, debido a las responsabilidades bajo su cargo o de eventos programados. Estos privilegios de accesos deberán ser solicitados a los encargados en el área de seguridad informática designados por la Alta Dirección de la Universidad de Margarita (UNIMAR), anexando la justificación respectiva, vía correo electrónico y/o de manera escrita.

POLÍTICAS DE CONTRASEÑAS

Responsables

La Universidad de Margarita (UNIMAR) será la delegada a seleccionar encargados capacitados en la administración y gestión de contraseñas.

Generales

El cumplimiento de la política de contraseñas por parte de los usuarios internos de la UNIMAR, es vital debido a que se establecen como la primera línea de defensa para garantizar que el acceso a los aplicativos y sistemas de información sólo sea realizado por personal autorizado.

Administración

En la Universidad de Margarita (UNIMAR), se acatará lo siguiente:

1. Todos los usuarios internos de la UNIMAR requieren de un nombre de usuario y una contraseña para utilizar el equipo de cómputo que se le haya asignado y servicios de red como correo electrónico, impresión, archivos compartidos, Intranet, Internet etc.
2. Todas las contraseñas son personales e intransferibles. Se prohíbe a los usuarios de la UNIMAR dar a conocer a terceras personas su contraseña, quien así lo hiciere debe considerar que sigue siendo el único responsable de las actividades que se realicen con su usuario y contraseña.

3. Todas las contraseñas del sistema (cuentas de administrador, cuentas de aplicaciones, entre otras.) se cambiarán con una periodicidad de al menos cada 30 días, en su defecto 60 días.
4. Todas las contraseñas del usuario (cuentas de usuario, cuentas de servicios web, etc.) se cambiarán al menos cada 30 días, en su defecto 60 días.
5. En caso de que el usuario detecte que su contraseña ha sido comprometida deberá cambiar su contraseña o solicitarlo a los encargados en el área de seguridad informática designados por la Alta Dirección de la UNIMAR.
6. En caso de olvido o bloqueo de su contraseña, el usuario debe coordinar el restablecimiento de la misma con los encargados en el área de seguridad informática designados por la Alta Dirección de la UNIMAR.
7. Las contraseñas de los usuarios deben cumplir con ciertos requerimientos de seguridad los cuales definirán los encargados en el área de seguridad informática designados por la Alta Dirección de la UNIMAR, con el objeto de evitar que los usuarios elijan contraseñas débiles. No se utilizarán contraseñas que resulten obvias, fáciles de descubrir, o predecibles para un atacante o intruso: (el mismo nombre de usuario, palabras de diccionario, fechas o nombres de personas cercanas, secuencias de números repetidos o consecutivos).
8. Las contraseñas para acceso al equipo informático deberán ser modificadas por el usuario la primera vez que acceda a su cuenta.
9. Todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI deben ser identificables de manera única.
10. Los usuarios internos de la UNIMAR, deberán negar la opción de recordar contraseñas que se presentan en los navegadores, con el fin de evitar la autenticación automática de acceso a los sistemas informáticos que operan en la intranet como en el Internet.
11. Cuando un usuario se desvincule de la entidad o se le asigne un rol diferente, el jefe o encargado del área o departamento inmediato deberá notificar a los encargados en el área de seguridad informática designados por la Alta Dirección de la UNIMAR, para suspender los usuarios de la red corporativa, sistemas especializados, etc.
12. Los empleados, deberán suscribir un compromiso de responsabilidad en seguridad y uso de usuario y claves de acceso a la información de recursos tecnológicos administrados por los encargados en el área de seguridad informática designados por la Alta Dirección de la UNIMAR.

Prohibiciones

Las actividades que se detallan a continuación están prohibidas:

1. Revelar o compartir su contraseña de cualquier manera.
2. Escribir la contraseña o almacenarla en archivos, comunicarla en el texto de correo electrónico, o en cualquier otro medio de comunicación electrónica.
3. Comunicar las contraseñas en conversaciones telefónicas.

POLÍTICA DE USO DEL CORREO ELECTRONICO

Responsables

La Universidad de Margarita (UNIMAR) será la delegada a seleccionar encargados capacitados esta área y apartado.

Generales

El correo electrónico institucional es un recurso que la Universidad de Margarita (UNIMAR) pone a disposición de sus empleados, como una herramienta de comunicación, colaboración e intercambio de información, se observará lo siguiente:

1. El acceso a estos recursos, estará limitado a la aceptación de la presente Política de Uso.
2. Las comunicaciones de la UNIMAR efectuadas por correo electrónico, solo podrán ser realizadas por las cuentas institucionales creadas en la entidad.
3. Las cuentas de correo asignadas a los empleados de cada área, deberán ser utilizadas sólo para actividades laborales que estén relacionadas con los propósitos y funciones de la UNIMAR.
4. Los buzones de correo electrónico, creados para los empleados de la UNIMAR, y toda la información contenida en los mismos, son propiedad exclusiva de la institución.

Tipos de Cuentas

1. Cuentas personales: el personal de la UNIMAR, contará con una cuenta de correo electrónico institucional con capacidad de bandeja asignada.
2. Cuentas departamentales: estas cuentas serán creadas, con el objetivo de comunicación a todos los miembros de una determinada área o lista de usuarios específica.

Responsabilidades

1. Los usuarios son los únicos responsables de todas las actividades realizadas, desde sus cuentas de acceso y buzones.

2. La información transmitida mediante el servicio de correo electrónico institucional, es responsabilidad única y exclusiva de cada usuario.
3. La cuenta de correo institucional es intransferible, por lo que la información que corresponde al inicio de sesión (usuario y contraseña) no se debe proporcionar a otras personas.
4. La información que se recibe de manera personal y confidencial por correo electrónico institucional, no se puede reenviar a otra persona, sin la autorización del remitente.

Uso inaceptable

En la Universidad de Margarita (UNIMAR) se considera mal uso del correo electrónico las siguientes actividades:

1. Utilizar el correo electrónico institucional para actividades comerciales diferentes a las de la UNIMAR.
2. Enviar o reenviar mensajes con contenido ofensivo, difamatorio, racista u obsceno.
3. Enviar mensajes anónimos, así como aquellos que consignen cargos o funciones no oficiales.
4. Utilizar mecanismos y sistemas, que traten de ocultar o suplantar la identidad del emisor del correo electrónico.
5. La saturación y falta de mantenimiento del buzón de correo por parte del usuario.
6. Apropiarse de cuenta(s) de correo diferente a la asignada a su persona.
7. Enviar de forma masiva publicidad o cualquier otro tipo de correo no solicitado, considerado como "spam".

POLÍTICA DE USO DE SEGURIDAD INFORMÁTICA Y DE LA INFORMACIÓN

Responsables

La Universidad de Margarita (UNIMAR) será la delegada a seleccionar encargados capacitados esta área y apartado.

Generales

Los usuarios internos de la UNIMAR cumplirán las siguientes recomendaciones:

1. Si no va a estar cerca de su sitio de trabajo, bloquee el equipo. Se recomienda activar el bloqueo automático de la pantalla del computador para que cuando detecte inactividad no pueda ser utilizado sin ingresar una contraseña.

2. No modificar las configuraciones del equipo como fondo de pantalla y protector de pantalla, así como la configuración de software y hardware. Si en su equipo se han realizado modificaciones, se debe notificar inmediatamente para que se realice la reconfiguración del mismo.
3. Está prohibido instalar aplicaciones o programas que no sean aprobados o que difieran del software designado por la UNIMAR, que no tengan licencias o que para su uso se deba corromper la seguridad de licenciamiento del mismo.
4. Para evitar pérdida de información, el usuario es responsable de respaldar su información importante periódicamente y verificar que los respaldos generados se encuentren disponibles, e íntegros para su uso cuando sea requerido.
5. No pueden moverse los equipos o reubicarlos sin permiso. En caso de que necesite movilizar un equipo propiedad de la UNIMAR se requiere autorización del jefe inmediato en coordinación con los encargados en el área de seguridad informática designados por la Alta Dirección.
6. Está prohibido desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otros usuarios y/o alterar o dañar los recursos informáticos.
7. Todo el personal que accede a los sistemas de información de la UNIMAR debe utilizar únicamente las versiones de software instaladas y siguiendo sus normas de uso.

Compromiso de Confidencialidad

Los empleados de la Universidad de Margarita (UNIMAR) deberán firmar compromisos de confidencialidad y de no-divulgación de información de conformidad con lo dispuesto de acuerdo a las necesidades de protección de información de la universidad.

1. Se deberá controlar y coordinar que los compromisos de confidencialidad de la información, documento físico o electrónico, sean firmados por todo el personal de la UNIMAR sin excepción, custodia de los compromisos firmados, adjuntar con el contrato de cada empleado, y controlar que la firma de los compromisos de confidencialidad sea parte de los procedimientos de incorporación de nuevos integrantes a la institución.
2. El personal de entidades externas; deberá de igual manera suscribir el compromiso de confidencialidad previo su acceso a la información.

Responsables de la seguridad

Los responsables de la seguridad informática de los activos serán designados por la Universidad de Margarita (UNIMAR).

Clasificación de la Información

Los responsables directos de la información designados por la Universidad de Margarita (UNIMAR) deberán clasificar adecuadamente la información que manejan y asegurarse de que se respete el acceso a la misma por parte del personal que está a su cargo. Así pues, los activos de información de la UNIMAR, así como la información, serán rotulados claramente con la clasificación que le sea otorgada, la misma que debe ser clara y visible. Toda la información generada en la UNIMAR y que no se le dé una clasificación específica, mantendrá el nivel de PRIVADA y deberá ser considerada como tal.

1. Criterios de Clasificación:
    a) Valor: el principal criterio de clasificación, se basa en el valor del activo desde el punto de vista del negocio (valor propio del activo o producto del mismo).
    b) Edad: la clasificación de cierta información puede variar si el valor de la información se reduce con el tiempo.
    c) Vida útil: la información se vuelve obsoleta en base a nueva información generada, por cambios organizacionales u otros motivos.
2. Niveles de clasificación de la información:
    a) Pública: información que, por su naturaleza, puede ser visible o divulgada por el personal general de la UNIMAR, usuarios o el público en general, sin riesgo de que su contenido pueda afectar en ningún sentido la integridad de la entidad.
    b) Privada: para uso interno, destinada al uso exclusivo por parte de los empleados de la UNIMAR en el desarrollo diario de los procesos de la institución.
    c) Restringida: información destinada solo para uso exclusivo de la UNIMAR. Esta información debe ser accedida y visualizada solo por el personal de la institución que cuente con la autorización por parte de la UNIMAR.
    d) Confidencial: información considerada como sensible y está destinada a uso solamente interno y por parte del personal específico que debe tener permisos y autorización para su visualización y/o manejo.

3. Acceso a recursos y privilegios: los usuarios deberán tener el nivel necesario de privilegios para acceso a las aplicaciones, o acceso a recursos para cumplir con las actividades de su cargo.
4. Gestión de incidentes de seguridad: se debe realizar considerando los siguientes objetivos básicos:
    - Respuesta rápida y eficiente.
    - Solución del daño causado por los incidentes.
    - Prevención de daños futuros.
5. Prevención y entrenamiento continuo: las políticas, reglamentos y normas referentes a la Seguridad de la Información deberán ser conocidos por todos los miembros de la organización y para el efecto, la UNIMAR proveerá recursos necesarios para realizar capacitaciones a los distintos usuarios de aplicaciones, personal técnico y demás personal de la institución en general.

Almacenamiento

La información obtenida de cualquier servicio y que sea almacenada localmente en el equipo de cómputo del usuario y sea propiedad de la Universidad de Margarita (UNIMAR), no podrá ser distribuida o transmitida por ningún medio de comunicación sin la autorización del inmediato superior.

Transmisión de datos

A fin de garantizar los principios de seguridad, desde la integridad, confidencialidad y disponibilidad de la información obtenida de los sistemas y aplicativos informáticos de la UNIMAR y en razón de que los dispositivos móviles, magnéticos y los soportes extraíbles generan vulnerabilidades como divulgación no autorizada, robo, datos dañados o comprometidos, por la facilidad de uso, los encargados del área de seguridad informática delegados por la Alta Dirección de la UNIMAR, de forma programada y bajo pedido, procederán a salvaguardar la información cuando se requiera que sea transferida.

Respaldo de la información tecnológica

La Universidad de Margarita (UNIMAR), y las diferentes áreas propietarias de la información, determinarán el procedimiento de resguardo y contención de la información obtenida de los sistemas y/o aplicativos informáticos, considerando al menos los siguientes puntos:

1. Se debe establecer un cronograma donde se detallen los períodos de tiempo en los cuales se realizarán los respaldos de la información.
2. Etiquetado de las copias de respaldo, tipo de contenido, periodicidad y retención.
3. Extensión y frecuencia en que se realicen los respaldos.
4. Guardado de los respaldos en un sitio seguro, evitar cualquier daño debido a desastres en la UNIMAR.
5. Grado apropiado para la protección física y ambiental.
6. Eventos regulares para verificar y restaurar los respaldos, garantizando que sean confiables para su uso en alguna emergencia.

Recursos compartidos

El uso de carpetas compartidas en los equipos informáticos de propiedad de la Universidad de Margarita, es una práctica que tiene algunos riesgos que pueden afectar los principios de confidencialidad, integridad y disponibilidad de la información, por lo tanto, su uso para la aplicación debe ser controlado. Por lo cual la organización define los siguientes puntos para su uso seguro:

1. Se debe evitar el uso de carpetas compartidas sin autorización del propietario de la información en equipos de cómputo.
2. Los administradores de red establecen e implementan, en las solicitudes aprobadas la configuración de acceso a la carpeta compartida, previo requerimiento formal de la misma a través de la mesa de ayuda.
3. El usuario que autorice y tiene a su disposición el recurso compartido es principal responsable de las acciones y los accesos sobre la información de dicha carpeta.
4. Se debe definir el tipo de acceso y los roles que sean estrictamente necesarios sobre la carpeta compartida (lectura, lectura y escritura).
5. Se debe definir el límite de tiempo durante el cual estará disponible la información.
6. El acceso a las carpetas compartidas debe delimitarse a los usuarios que las necesitan y estar protegidas con contraseñas.
7. No se debe permitir el acceso a dichas carpetas a usuarios que no cuenten con antivirus actualizado.

Registro de eventos

En la Universidad de Margarita (UNIMAR), el registro de eventos permitirá un control en las operaciones realizadas en los sistemas de información y sistemas operativos, para monitorear los servicios informáticos.

1. Todos los sistemas de información, aplicaciones, sistemas operativos, bases de datos, dispositivos de seguridad, dispositivos de comunicación y servidores deben tener registros o registros de auditoría que verifiquen las actividades del usuario, excepciones, fallas y eventos de seguridad.
2. Los registros sobre actividades de los usuarios, excepciones, fallas y eventos de seguridad de la información se deben preparar, mantener y revisar periódicamente.
3. Es responsabilidad de los propietarios de la información, solicitar y saber qué eventos han ocurrido en los sistemas de tratamiento de su información.
4. Se debe garantizar que no se pierda, ni se sobrescriba los respaldos de archivos logs de los sistemas de información.

POLÍTICAS DE LA ORGANIZACIÓN EN LA SEGURIDAD DE LA INFORMACIÓN

Responsables

La Universidad de Margarita (UNIMAR) será la encargada de seleccionar a las personas aptas para esta área o apartado.

Generales

Las siguientes políticas tienen la finalidad de controlar la asignación de las responsabilidades y del correcto uso de los dispositivos móviles y el teletrabajo, se tomarán en cuenta los siguientes lineamientos.

Uso equipos portátiles, dispositivos móviles y teletrabajo

Los colaboradores, contratistas y terceros se comprometen hacer uso adecuado de los dispositivos móviles para el acceso a los servicios corporativos de movilidad proporcionados por la UNIMAR, tales como escritorios y aplicaciones virtuales, correo electrónico, redes virtuales privadas (VPN), entre otros, atendiendo las siguientes directrices:

1. La asignación de los equipos se debe realizar mediante un procedimiento documentado, en el cual se registre las características, modelo, serie, estado en el que se encuentra el dispositivo, de esta manera mantener un inventario activo.
2. Al tratarse de dispositivos sensibles, es necesario implementar un software de localización.

3. Los equipos deben estar configurados para bloqueo automático por un tiempo de inactividad a través de medios disponibles de configuración tales como: contraseña, patrón huella dactilar, reconocimiento de voz, entre otras.
4. Uso de aplicación de antivirus en los equipos.
5. Las conexiones a redes ajenas a la UNIMAR, no se deben configurar como visibles a otros dispositivos de la red.

Prohibiciones

En la Universidad de Margarita (UNIMAR), están prohibidas las siguientes actividades:

1. Instalar software que ocasiones modificaciones de configuración de los equipos sin de los encargados en el área de seguridad informática designados por la UNIMAR.
2. Modificar configuraciones del sistema BIOS por parte del usuario.
3. Exponer los equipos a altas temperaturas que ocasionen daños a los equipos.
4. Usar los equipos para fines personales distintos a los de la UNIMAR.

POLÍTICA PARA EL USO Y ADMINISTRACIÓN DE REDES

Responsables

La Universidad de Margarita (UNIMAR) será la delegada a seleccionar encargados capacitados en materia de administración y uso de redes y servidores, en conjunto con los encargados seleccionados por la Alta Dirección para el cumplimiento de la presente política.

Generales

Las normas con respecto al acceso de red de la institución establecidas en el siguiente apartado están dirigidas al uso y administración de redes por parte de los administradores o responsables que seleccione la Universidad de Margarita (UNIMAR).

Acceso a la Red

1. La unidad, equipo o usuario que requiera conectarse a la red de la UNIMAR, deberá solicitar un estudio por parte del área o responsables designados por la institución para la determinación de requerimientos, necesidades y características técnicas para la conexión, así como del presupuesto de ser necesario.
2. Para enlaces externos, ninguna unidad podrá contratar enlaces (proveedores) sin solicitar y coordinar previamente con la Alta Dirección de la institución o los encargados designados por la misma.

3. La comunicación para Internet se hará única y exclusivamente a través del enlace o proveedor contratado por la UNIMAR y su alta Dirección, y es responsabilidad de la misma el mantener un enlace adecuado para cubrir las necesidades de la organización.
4. Los encargados delegados por la Alta Dirección de la UNIMAR, para el área de redes, tendrán entre sus labores el asesorar a los usuarios que lo requieran, con respecto a la configuración y reemplazo de componentes existentes o nuevos, del mismo modo, realizarán las mediciones del rendimiento de red, para determinar el uso de la misma.
5. En el esquema de direccionamiento de la red, así como de los protocolos de comunicaciones serán determinados por los responsables designados por la Alta Dirección de la UNIMAR.
6. Las redes de los laboratorios, departamentos y demás áreas, no deberán contener ninguna otra máquina que no sea destina única y exclusivamente para el uso especifico de las tareas o acciones designadas de su área, ya sea el uso de los estudiantes, empleados o usuarios autorizados.

Seguridad

1. El acceso a la red de la UNIMAR deberá ser a través de su cuenta institucional (usuario y contraseña) provista por la institución, respetando y cumpliendo con lo establecido en la presente política.
2. La implementación de cualquier nueva tecnología o recurso, deberá ser configurada adecuadamente, asegurando la seguridad de información y del acceso a la red.

Varias

1. Cada unidad o equipo deberá contar con un administrados local, y deberá notificar a los responsables designados por la Alta Dirección de la UNIMAR.
2. Solo los responsables designados por la Alta Dirección de la UNIMAR serán los encargados de medir las tendencias de uso de los recursos de comunicaciones, así como del mapeado de las redes.

POLÍTICA PARA EL USO E IMPLEMENTACIÓN DE SERVIDORES

Responsables

La Universidad de Margarita (UNIMAR) será la delegada a seleccionar encargados capacitados para el uso e implementación de servidores, en conjunto con los encargados seleccionados por la Alta Dirección para el cumplimiento de la presente política.

Generales

1. Mantener actualizados los servidores, ya sea en infraestructura computacional del área o en la información gestionada por los mismo, así como por los encargados designados por la Alta Dirección de la UNIMAR para la gestión de los servidores.
2. Es prioridad de los encargados designados por la Alta Dirección de la UNIMAR, el mantener en correcto funcionamiento las unidades destinadas al área de servidores, así como todos los activos allí presentes.

Para la implementación

1. De un servidor local, el cual se puede administrar desde la propia línea de comandos y ser alojado en los equipos de nivel administrativo por parte de los encargados designados por la Alta Dirección de la UNIMAR para la gestión de los servidores.
2. De un servidor virtual (VPS), el cual consiste en particiones virtuales de un servidor físico, lo que permite una mayor flexibilidad para ejecutar múltiples sistemas operativos (SO) o un conjunto de programas en servidores individuales al mismo tiempo.

Se deben tener lo siguiente en consideración:

   a. El control de seguridad por parte de los encargados y personal autorizado con respecto al acceso al servidor, así como a las instalaciones del mismo.
   b. El control de datos, como activos de la UNIMAR, por lo que la gestión debe ser total sobre la ubicación y estado de las copias de seguridad.
   c. La centralización de incidencias, su registro o récord que sirva como históricos para eventos futuros.

Respaldo y recuperación de la información

1. Para los backups de sistema, los cuales deben retenerse por un tiempo límite estimado por los encargados del área designados por la Alta Dirección de la UNIMAR. Después de cumplido el tiempo de retención, los backups pueden eliminarse.
2. La destrucción o reutilización de los medios de almacenamiento debe realizarse de manera segura, mediante procedimientos seguros y formales, así como la reutilización segura de los medios que contengan información confidencial. Los procedimientos de eliminación en el servidor, deben ser proporcionales a la sensibilidad de la información, definidos por los encargados del área designados por la Alta Dirección de la UNIMAR.

3. El acceso a las instalaciones designadas para los servidores y medios de almacenamiento de los backups debe ser restringido, considerándose como áreas seguras dentro de la institución. Por ningún motivo debe ingresar personal no autorizado. Asimismo, los medios donde se almacenan los backups o gestionan los servidores deben ser manipulados por personal sin la debida autorización.
4. Antes de realizar algún cambio sobre algún sistema de información, debe realizarse un backup y proceder a verificar la información en el servidor. Esto debe estar incluido en el proceso de gestión de cambios de la UNIMAR.

Seguridad y protección

1. El acceso de usuarios que sirven de colaboradores a las instalaciones designadas para los servidores debe ser controlado mediante la exigencia del uso a toda hora de un carnet visible para la distinción de invitado.
2. Debe existir un registro de eventos e incidencias presentados en los servidores que sean propiedad de la UNIMAR, de modo que se puedan gestionar y mitigar dentro del ciclo de mejora continua basado en la seguridad de los activos de la organización.
3. Los encargados del área designados por la Alta Dirección de la UNIMAR, deberán seleccionar aquellas medidas que mejoren la seguridad de los servidores, ya sean llaves SSH, Detección de Intrusos (IDS), Red Privada Virtual (VPN) o cualquier otra medida a considerar.
4. Promover el endurecimiento (hardening) en los servidores propiedad de la UNIMAR, para impedir que salga root como usuario en el proceso de autentificación o limitar el acceso a determinados usuarios.

POLÍTICA DE USO DE SOFTWARE

Responsables

La Universidad de Margarita (UNIMAR) será la encargada de seleccionar a las personas aptas para esta área o apartado**.**

Administración

Dentro de las responsabilidades de la administración e instalación de software se detallan las siguientes:

1. Mantener el resguardo de las licencias de uso de software de la UNIMAR.
2. Revisar periódicamente la vigencia de uso de las licencias que se hayan adquirido.

3. Establecer los procedimientos para el uso de software.
4. Realizar el análisis de las necesidades y los requerimientos de la UNIMAR, con la finalidad de planificar la adquisición o desarrollo de software.

Uso e instalación de software

Para el uso e instalación de software en la Universidad de Margarita (UNIMAR) se regirá a lo siguiente:

1. Solo las personas designadas por la UNIMAR están autorizadas, así como son responsables de realizar la instalación de software y proporcionar soporte técnico del mismo en los equipos de cómputo de la institución.
2. El software utilizado por la UNIMAR, deberá ajustarse a las especificaciones técnicas y arquitectura tecnológica disponible.
3. El software que se adquiera debe cumplir con los procesos formales de recepción, validación técnica y pruebas, previos a la aceptación del producto.

Restricciones

En la Universidad de Margarita (UNIMAR), se prohíbe la instalación y/o uso del software en los siguientes casos:

1. Copias ilegales de cualquier sistema informático, programa o software.
2. Software que haya sido descargado de internet.
3. Instalaciones no autorizadas o que no hayan sido solicitadas formalmente a la UNIMAR.
4. Software adquirido para uso personal del usuario (sin fines empresariales).
5. Software de entretenimiento o que no tenga relación con las actividades de la UNIMAR.
6. Software sin licencia.

POLÍTICA DE DESARROLLO DE SOFTWARE

Responsables

La Universidad de Margarita (UNIMAR) será la encargada de seleccionar a las personas aptas para esta área o apartado**.**

Generales

Para el desarrollo de software en la Universidad de Margarita (UNIMAR) se requiere:

1. Toda solicitud de desarrollo, evaluación o modificación de sistemas informáticos deberá empezar con el pedido formal para su análisis y aprobación.

2. El área solicitante deberá validar que el software cumpla con las funcionalidades y requerimientos solicitados, previo a la liberación en ambiente de producción.
3. Todo software desarrollado debe garantizar el registro de rastros de auditoría, donde se evidencien los eventos realizados por los usuarios dentro de la aplicación.

Actualizaciones de parches de seguridad en los sistemas de información

1. Vigilar el estado de actualización de todos los dispositivos y aplicaciones en la UNIMAR.
2. Elegir la opción de actualizaciones automáticas siempre que esté disponible para los equipos en la UNIMAR.
3. Instalar las actualizaciones de seguridad tan pronto como se publiquen, especialmente las de los sistemas operativos, navegadores, antivirus y sistemas utilizados en la UNIMAR.
4. Ser cuidadosos con las aplicaciones que se instalan, huyendo de fuentes no confiables y vigilando los privilegios que se les concede.
5. Evitar hacer uso de aplicaciones y sistemas operativos antiguos que ya no dispongan de actualizaciones de seguridad.

POLÍTICA DE USO DE INTERNET E INTRANET

Generales

Los servicios de Internet e Intranet son recursos que la Universidad de Margarita (UNIMAR) pone a disposición de sus empleados, como una herramienta para consulta de información, investigación y acceso a los sistemas de la UNIMAR, facilitando la realización de las labores diarias, se debe tomar en cuenta lo siguiente:

1. El uso y acceso a los servicios de Internet e Intranet está limitado a la aceptación de las presentes políticas.
2. El uso del servicio de Internet e Intranet está condicionado a la realización de actividades laborales que estén relacionadas con los propósitos y funciones propuestos por la UNIMAR.
3. En el caso de que un usuario externo a la UNIMAR, requiera el acceso al servicio de Internet, se le asignará un perfil de acceso limitado, navegación básica y a través de una conexión de red que no ponga en riesgo la seguridad de los equipos internos de la UNIMAR.
4. El intercambio de información entre las distintas áreas de la UNIMAR se realizará a través de red local, Intranet o una conexión privada virtual.

Prohibiciones

En la Universidad de Margarita (UNIMAR), se prohíbe lo siguiente:

1. Utilizar el servicio de internet como un medio para realizar cualquier actividad comercial o lucrativa individual o la participación y distribución de actividades o materiales que vayan en contra de la UNIMAR y sus objetivos.
2. Utilizar el servicio de internet con propósitos que puedan influir negativamente en la imagen de la UNIMAR, de sus autoridades o empleados.
3. Realizar actividades que puedan comprometer la seguridad de los servidores y recursos informáticos de la UNIMAR.
4. Accesos a sitios web que puedan ser declarados como obscenos, que distribuyan o promocionen material pornográfico, ofensivo o con humor inapropiado; que vaya en contra de la moral y buenas costumbres.
5. Transmitir amenazas, material indecente o de hostigamiento. Así como intimidar, difamar, insultar, acosar, ofender a otras personas o interferir en las labores de otros usuarios.
6. Distribuir por internet material que ocasione daños, específicamente la distribución de software malicioso.
7. Congestionar, interferir o paralizar el uso del servicio de internet e intranet.
8. Descargar música, fotos, videos, u otro material que no esté relacionado con las actividades o propósitos laborales de la UNIMAR.

POLÍTICA DE CRIPTOGRAFÍA

Responsables

La Universidad de Margarita (UNIMAR) será la encargada de seleccionar a las personas aptas para esta área o apartado.

Generales

Definir métodos criptográficos de protección de la información crítica o sensible, para reducir los riesgos de confidencialidad, disponibilidad o integridad de la información mediante la ayuda de técnicas criptográficas, para lo cual se debe tomar en cuenta lo siguiente:

1. Las normativas de desarrollo de esta política deben indicar la aplicación de criptografía en cada caso y escenario concretos:
    - Firma electrónica
    - Autenticación electrónica

- Cifrado

2. Las claves criptográficas deben estar disponibles operativamente tanto en tiempo como lo requiera el servicio criptográfico correspondiente.
3. Una clave se utilizará durante un plazo concreto, o período criptográfico.
4. Para la protección de claves criptográficas, en caso de requerirse encriptación, se proporcionará una protección adecuada al equipamiento utilizado para generar, almacenar y archivar sus claves privadas, considerándolo crítico o de alto riesgo.
5. Protección y uso de firmas digitales avanzadas, los certificados digitales avanzados se deberán almacenar en equipamiento especializado del tipo HSM (Hardware Security Module).

Excepciones

Frente a casos especiales, los responsables delegados por la Universidad de Margarita (UNIMAR), podrán establecer condiciones puntuales de excepción en el cumplimiento de las directrices de esta Política, siempre que no infrinja la legislación vigente ni afecte directrices de otras políticas. Toda excepción debe ser documentada y se le debe efectuar seguimiento, generando un proceso de revisión de la misma, para determinar si amerita una nueva directriz particular o un cambio en otra ya existente.

SANCIONES

Responsables

La Universidad de Margarita (UNIMAR), en conjunto con los encargados del área de seguridad informática, serán los designados para evaluar o efectuar las sanciones.

Incumplimiento de las Políticas

Ante el incumplimiento de las obligaciones establecidas en este instrumento que compete a la Universidad de Margarita (UNIMAR), dependiendo de la gravedad de la infracción cometida, se iniciarán las respectivas acciones y procedimientos administrativos, de conformidad a las normas que las regulan, con el fin de que se determine la responsabilidad administrativa y penal. Así pues, la entidad en conjunto con las personas calificadas y designadas por la Alta Dirección en materia de seguridad informática, y en conocimiento de este instrumento, calificarán la falta e impondrán las siguientes acciones:

1. Ante un incumplimiento leve de las Políticas, se notificará por escrito recordándole la vigencia de las Políticas al usuario responsable de la falta, así como se pondrá en conocimiento del jefe del área a la que pertenezca el usuario para su seguimiento y control.
2. En el evento de presentarse un incumplimiento moderado en las Políticas, o una reincidencia en un incumplimiento leve, se notificará por escrito al jefe del área a la que pertenezca el usuario y, de considerarlo necesario, se podrá disponer la suspensión temporal del servicio al usuario responsable hasta que el jefe del área apruebe por escrito la restauración del servicio.
3. En caso de presentarse un incumplimiento grave de las Políticas, causará el retiro de los equipos, bienes, servicios y herramientas informáticas, como la desvinculación total de la UNIMAR por parte de los usuarios implicados, siendo evaluado por la entidad y Alta Dirección.

5.4 Representación Gráfica y Estructura de la Propuesta.

Haciendo uso de figuras, se explica la estructura de la propuesta, representandose de manera mas efectiva y directa, sobre las fases y funciones del plan de seguridad basada en la normativa ISO/IEC 27001, en su edición del 2013, de acuerdo a la documentación implementada en esta investigación. Asimismo, se presentará el diagrama definido por la normativa:

5.4.1 Implantación de la norma

Figura 15. *Proceso de implantación la ISO 27001:2013*

Fuente: *Stratominds Capacitación S.A. de C.V. (2022).*

https://www.stratominds.com/ISO_27001.php

El propósito central de un Sistema de Gestión de Seguridad de la Información (SGSI) es proporcionar protección a la información sensible o de valor para la entidad. La información sensible incluye información sobre los empleados, estudiantes o usuarios. La información de valor incluye propiedad intelectual, datos financieros, registros legales, datos comerciales y datos operativos. En la figura, se observa la estructura de la implantación de la norma, iniciando en la identificación de los recursos (activos) de la organización, luego realizando la evaluación de riesgos de acuerdo a los recursos activos en la institución, entiendo por activos la información, recursos lógicos y físicos de la misma. Al obtener los resultados de la evaluación de riesgos, se puede ejecutar un análisis de impacto en el que se evidencien los procesos operativos, jerarquizando el análisis en base a los riesgos y amenazas asociadas.

En este orden de ideas, con el análisis de impacto, se procede a seleccionar e implementar los controles de acuerdo a la normativa ISO/IEC 27001, en su edición del 2013, de acuerdo a los anexos y protocolos que esta dispone, para proceder a la fase final de la implementación, en la que se hace tratamiento de los riesgos, asumiéndolos, reduciéndolos, eliminándolos y transfiriéndolos sea el caso. Por lo que, al cumplir con las fases de implementación, se pueden definir las normas y políticas pertinentes para el diseño del plan en la Universidad de Margarita (UNIMAR), de acuerdo a los activos que esta gestiona.

5.4.2 Diagramación de la normativa

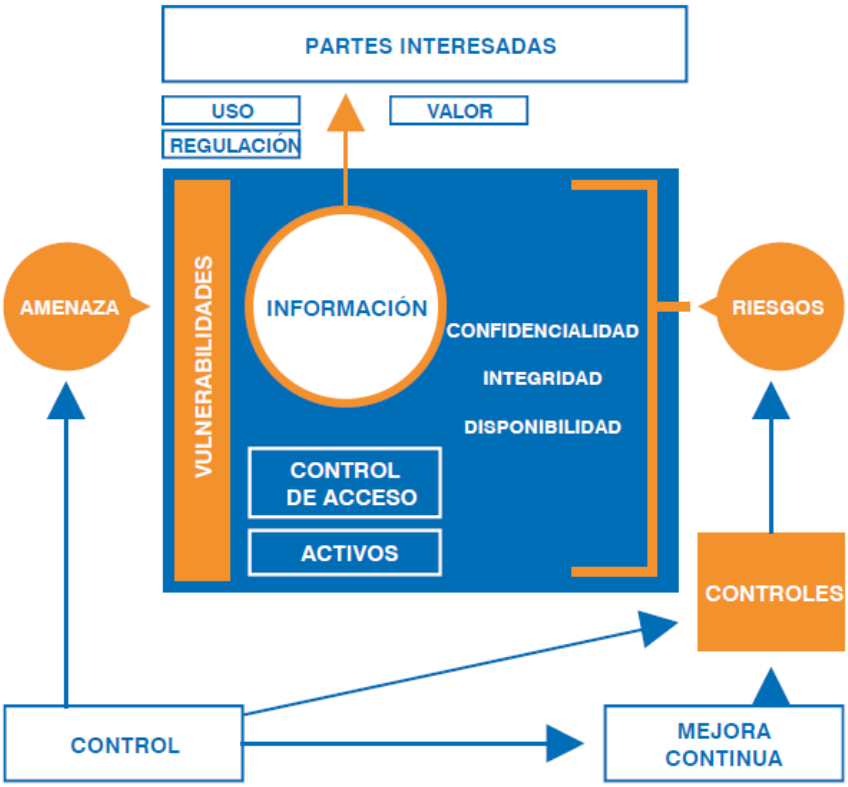

Figura 16. *Diagramación de la ISO 27001:2013*

Fuente: *NQA. ISO 27001:2013. Guía de Implantación para la Seguridad de la Información.*

La figura anterior ejemplifica las partes involucradas en el plan de seguridad basado en la normativa ISO/IEC 27001:2013. Se evidencia la relación de los principios de seguridad informática, o la triada CID, Confidencialidad, Integridad y Disponibilidad, con respecto a la información como activos dentro de la institución, asimismo, se observa la correlación con las vulnerabilidades, que pueden volverse amenazas para la organización y los riesgos que puede correr para con la CID. Los controles dispuestos por la norma ISO (anexos, criterios y protocolos) en conjunto con el ciclo de mejora continua, permiten mitigar los riesgos y las amenazas, y salvaguardar la información y todos los activos que las partes interesadas dispone y requiere, mediante la valoración de los mismos, su uso y la regulación bajo las normas y políticas definidas.

CONCLUSIONES

La Universidad de Margarita (UNIMAR) como institución de educación superior, es un referente en la Isla de Margarita, debido a la cantidad y calidad de egresados de la misma en las distintas carreras que ofrece. Por lo tanto, gestiona una gran cantidad de información vital, de carácter sensible, que debe ser gestionada y administrada de la mejor forma posible para brindarle un mejor servicio a los estudiantes, o usuarios involucrados activamente, promoviendo la confiabilidad en la institución. La creación y definición de normas y políticas en materia de seguridad informática le va a permitir asegurar la información, mejorar los procesos activos en la institución, promover la cultura en materia de seguridad informática.

En la actualidad, las amenazas están latentes y todo sistema de información es vulnerable, por lo que la probabilidad de riesgo es inminente, sin embargo, al aplicar metodologías, controles y protocolos bajo normas estandarizadas, como la ISO/IEC 27001, en su edición 2013, orientada al tratamiento de seguridad de la información mediante la gestión riesgos, se obtiene una mejora significativa en la seguridad de los activos de información de la organización. Así pues, la implantación de la norma ISO/IEC 27001:2013, en conjunto con la ISO 27002, comprenden las mejores prácticas para establecer un ciclo de mejora continua basado en la gestión de seguridad informática y de la información.

Asimismo, en Venezuela se evidencia una ausencia en la legislación referente a seguridad informática en cuanto al resguardo de datos personales, información sensible o de carácter vital, lo que se traduce en riesgos de confidencialidad, integridad y disponibilidades de la información para las personas y organizaciones. El diseño de un plan de seguridad informática basado en la norma ISO/IEC 27001:2013 para la Universidad de Margarita (UNIMAR) le diferenciará del resto de las organizaciones en materia de seguridad informática, al reconocer los riesgos a los que se encuentra expuesta, evaluándolos y, mediante los controles, mitigándolos para obtener beneficios comerciales y operacionales, así como también mantener una ventaja competitiva, mejorando su imagen y brindándole confianza a los usuarios.

RECOMENDACIONES

- ✓ Implantar la normativa ISO/IEC 27001:2013, en base a los objetivos y lineamientos de la institución, para así evaluar de forma correcta los riesgos de seguridad asociados a los activos y recursos.
- ✓ Implementar las normas y políticas definidas en este trabajo para mejorar las prácticas de seguridad informática en la Universidad de Margarita (UNIMAR).
- ✓ Mantener actualizada la normativa, los controles y protocolos de acuerdo a los objetivos y lineamientos de la Universidad de Margarita (UNIMAR).
- ✓ La implementación del plan de seguridad basado en la norma ISO/IEC 27001:2013 para la Universidad de Margarita (UNIMAR), debe ser supervisado por un experto que garantice el éxito de su implementación.
- ✓ Se recomienda definir las tareas y funciones de un Oficial de Seguridad de la Información, además de disponer de personal dedicado exclusivamente a cumplir dicho rol.

REFERENCIAS

Aguinaga, H (2013), *Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO / IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo*.

Asociación de Auditoría y Control de Sistemas de Información (ISACA), Ciberseguridad. Recuperado el 19 de junio de 2022:

https://mozcalti.com/ciberseguridad.html#:~:text=Según%20los%20profesionales%20en%20seguridad,la%20información%20que%20es%20procesada%2C

Baca, V. (2016). DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA LA UNIDAD DE GESTIÓN EDUCATIVA LOCAL-CHICLAYO.

https://revistas.uss.edu.pe/index.php/ING/article/view/357/346

Bradanovic, T. (2006, pág. 12), principios de seguridad informática, 21 de junio de 2022

http://repositorio.utc.edu.ec/bitstream/27000/536/1/T-UTC-1052%281%29.pdf

Business News CR (2022). Seguridad. Recuperado el 18 de junio 2022:

https://www.businessnewscr.com/index.php/tecnologia/seguridad/755-se-estima-que-el-costo-global-anual-de-la-ciberdelincuencia-sera-de-10-5-billones-para-2025#:~:text=Ese%20comportamiento%20de%20disparo%20se,a%20inicios%20de%20este%20año.

Constitución de la República Bolivariana de Venezuela. Gaceta Oficial Extraordinaria N°36.860. 30 de diciembre de 1999**.**

Corda et al. (2017). Riesgo informático. Recuperado el 21 de junio de 2022

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjflqibzuf6AhXGkWoFHUDlBjIQFnoECA0QAw&url=https%3A%2F%2Fwww.palabraclave.fahce.unlp.edu.ar%2Farticle%2Fdownload%2FPCe032%2F8822%2F18825%23%3A~%3Atext%3DEl%2520riesgo%2520inform%25C3%25A1tico%2520refiere%2520a%2Cesperados%2520de%2520un%2520sistema%2520inform%25C3%25A1tico.&usg=AOvVaw0lGcVGzlSHPh2GPHzOwJ5Y

Criptonoticias (2017) se registra primer caso de universidad venezolana bajo ataque de ransomware. Recuperado el 20 de junio de 2022:

https://www.criptonoticias.com/seguridad-bitcoin/registra-primer-caso-universidad-venezolana-ataque-ransomware/

Escuela Europea de Excelencia (2019) Norma ISO 27001, Recuperado el 21 de junio de 2022:

https://www.escuelaeuropeaexcelencia.com/2019/11/como-funciona-la-seguridad-de-la-informacion-en-iso-27001/

Espinoza, H. (2013). ANÁLISIS Y DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001:2005 PARA UNA EMPRESA DE PRODUCCIÓN Y COMERCIALIZACIÓN DE PRODUCTOS DE CONSUMO MASIVO.

https://tesis.pucp.edu.pe/repositorio/bitstream/handle/20.500.12404/4957/ESPINOZA_HANS_ANALISIS_SISTEMA_GESTION_SEGURIDAD_INFORMACION_ISO_IEC%2027001_2005_COMERCIALIZACION_PRODUCTOS_CONSUMO_MASIVO.pdf;jsessionid=4333A84A8EA04AF983868578724CBAEF?sequence=1

FONDONORMA (2022), Norma ISO/IEC 27001. Recuperado el 19 de junio de 2022:

https://www.fondonorma.org.ve/index.php/es/certificacion-footer/26

Fournier, s (1985), diferencia entre amenaza y riesgo, 21 de junio de 2022

https://www.desenredando.org/public/libros/1993/ldnsn/html/cap3.htm

Gómez, A (2006), Enciclopedia de la Seguridad Informática. Recuperado el19 de junio de 2022:

https://www.ceupe.com/blog/seguridad-informatica-y-proteccion-de-datos.html

Grupo de Informática y Comunicaciones Avanzadas (ICA) (2020), vulnerabilidades que afectan a tus sistemas informáticos, Recuperado el 20 de junio de 2022:

https://www.grupoica.com/blog/-/blogs/conoce-las-vulnerabilidades-que-afectan-a-tus-sistemas-informaticos#:~:text=En%20Ciberseguridad%2C%20cuando%20hablamos%20de,la%20información%20y%20servicios%20soportados

Guamán, J. (2017). DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL DEPARTAMENTO DE INFORMÁTICA DE LA DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DEL COMANDO CONJUNTO DE LAS FF.AA, UTILIZANDO LA NORMA ISO 27001:2013.

http://www.dspace.espol.edu.ec/xmlui/bitstream/handle/123456789/42609/D-106352.pdf?sequence=-1&isAllowed=y

ISO/IEC 27001 (2013) Sistema de Gestión de seguridad de la información (SGSI). Recuperado el 21 de junio de 2022:

https://www.iso27000.es/sgsi.html

ISOTools Excellence (2015), Normas ISO. Recuperado el 19 de junio de 2022:

https://www.isotools.org/2015/03/19/que-son-las-normas-iso-y-cual-es-su-finalidad/

ISOTools Excelence (2015), Riesgos y Seguridad. Recuperado el 19 de junio de 2022: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

ISOTools Exccellence (2013:pa.6). Norma ISO/IEC 27001. Emitida en octubre de 2005. Actualizada en 2013. Recuperado el 21 de junio de 2022: https://www.isotools.pe/iso-27001-origen-y-evolucion/

ISO/IEC 27001 (2013) Sistema de Gestión de seguridad de la información (SGSI), 21 de junio de 2022 https://www.iso27000.es/sgsi.html

López, R. (2017). Sistema de gestión de la seguridad informática. Recuperado el 20 de junio de 2022: https://core.ac.uk/download/pdf/326424017.pdf

Maxitana, J y Naranjo, B (2005, pág. 3). Administración de riesgos, 21 de junio de 2022 https://www.dspace.espol.edu.ec/bitstream/123456789/15896/3/Resumen%20Cicyt.-%20Administración%20de%20Riesgos%20de%20TI%20de%20una%20empresa%20del%20sector%20Informático.pdf

Mintzberg, H. (1984). Estructuras organizativas, 20 de junio de 2022 https://www3.uji.es/~agrandio/Aedem94.htm#:~:text=LAS%20ESTRUCTURAS%20ORGANIZATIVAS%20DE%20MINTZBERG.&text=Las%20estructuras%20organizativas%20son%20consideradas,1984%20p.

Organización Internacional de Estandarización (ISO) (1947), Normas ISO. Recuperado el 21 de junio de 2022: https://www.eafit.edu.co/escuelas/administracion/publicaciones/panorama-contable/actualidad/Documents/Boletin-1-NORMAS-ISO-Y-SU-COBERTURA.pdf

Orozco, M (2013). Activos Informáticos. Recuperado el 21 de junio de 2022: https://es.slideshare.net/meztli9/16-activos-inf

PMG-SSI (2015) ISO 27001: Los activos de información, 20 de junio de 2022 https://www.pmg-ssi.com/2015/03/iso-27001-los-activos-de-informacion/#:~:text=Los%20activos%20son%20los%20recursos,ha%20propuesto%20la%20alta%20dirección.&text=Un%20proyecto%20de%20Seguridad%20tiene,dominio%20en%20estudio%20del%20proyecto.

Ríos, J. (2015). Seguridad informática. Recuperado el 21 de junio de 2022 https://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica

Sevillano, F. (2021), plan de gestión de seguridad informática, 21 de junio de 2022

https://willistowerswatsonupdate.es/ciberseguridad/ciber-riesgo-plan-seguridad-informatica/#:~:text=Hablamos%2C%20en%20este%20caso%2C%20de,fin%20de%20resguardar%20la%20información

TECON (2018), seguridad de la información, 21 de junio de 2022

https://www.tecon.es/la-seguridad-de-la-informacion/#:~:text=Por%20seguridad%20de%20la%20información,se%20utilizan%20en%20una%20organización.