EVALUACIÓN DE LA SEGURIDAD EN LOS ACTIVOS DE INFORMACIÓN DEL DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES EN LA ORGANIZACIÓN EAR CONSTRUCCIONES

JHON DAWINSON MORENO PEREA
JHON FERNANDO RINCÓN TORRES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2023

EVALUACIÓN DE LA SEGURIDAD EN LOS ACTIVOS DE INFORMACIÓN DEL DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES EN LA ORGANIZACIÓN EAR CONSTRUCCIONES

JHON DAWINSON MORENO PEREA
JHON FERNANDO RINCÓN TORRES

Proyecto de Grado - Proyecto aplicado presentado para optar por el título de ESPECIALISTA EN SEGURIDAD INFORMATICA

Director del Curso
ALEXANDER LARRAHONDO NUÑEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2023

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

DEDICATORIA

Con amor dedico este trabajo a mi hijo, que con su carisma y comprensión me acompañó en cada etapa vivida, colaborándome de manera indirecta, minimizando mis preocupaciones de padre, también lo dedico a mi mamá que con su apoyo, consagración y paciencia disminuyo mis tareas en el hogar permitiéndome una entrega más tranquila en el estudio y trabajo.

AGRADECIMIENTOS

Agradezco a las directivas de la Universidad Nacional Abierta y a Distancia UNAD, quienes con su trabajo continuo nos brindan la oportunidad de estudiar y laborar, por otro lado, a cada uno de los tutores y asesores que me acompañaron en el proceso les reconozco que sin su apoyo y colaboración éste logro no hubiera sido posible.

CONTENIDO

pág.

LISTA DE CUADRO

Pág.

LISTA DE ILUSTRACIONES

Pág.

GLOSARIO

ACTIVOS DE INFORMACIÓN: Son toda la información vital o recursos relacionados para su creación, almacenamiento y tratamiento de datos de una empresa u organización.

AMENAZA INFORMÁTICA: Son incidentes o alteraciones que se presentan o se detectan de potencial destructivo y que puede afectar negativamente los sistemas informáticos de una organización.

ANÁLISIS DE RIESGO: Son los riesgos que se evalúan por posibles amenazas y eventos no deseados, con la elaboración de estos análisis pueden ayudar para la toma de decisiones por la Alta Gerencia.

ATAQUE INFORMÁTICO: Son intentos de acceder de manera externo o interna, por medio de equipos informáticos especializados, utilizando técnicas avanzadas de ataques como la inyección de códigos maliciosos, virus, malware, con la finalidad de alterar el normal funcionamiento para posteriormente sustraer, dañar, borrar o secuestrar información sensible de una organización.

BACKUP O COPIA DE RESPALDO: Copias de seguridad que se realiza a la información considerada como clasificada o sensible con el objetivo de salvaguardar estos datos de manera segura para su posterior utilización o restauración ante una eventual pérdida, o falla de datos, lo que garantiza la continuidad del negocio.

BASE DE DATOS: Es un conjunto de datos relacionados perteneciente a una misma temática, que se almacenan y se ordenan de forma sistemática, para ser analizada, consultada, recuperada entre otras funcionalidades, son indispensables para recolectar cantidades enormes de información de los diferentes sistemas de información y/o aplicaciones.

DATA CENTER: O centro de datos es un espacio con acceso restringido donde se alojan los equipos pertenecientes a la infraestructura tecnológica que son de vital importancia para cualquier organización para su procesamiento y almacenamiento algunos de estos equipos son; Servidores, Switches, Routers, UPS, Racks, Sistema de cableado de red, Aire de Precisión, entre otros.

CIBERSEGURIDAD: Son un conjunto de buenas prácticas que se encargan de brindar protección ante un eventual ataque digital o ciberataque a la infraestructura tecnológica y los sistemas de información que lo conforman, estas acciones preventivas tienen como objetivo repeler el acceso no autorizado proveniente de afuera como desde dentro de la organización.

CONFIDENCIALIDAD: Es la propiedad mediante la cual los activos de la información no están disponible a cualquier persona u organización no autorizada.

INTEGRIDAD: Es el uso por el cual la información se mantiene inalterada, es decir que no se podrá modificar dicha información sin previa autorización.

DISPONIBILIDAD: Es el mecanismo, mediante el cual los usuarios autorizados pueden acceder a la información cuando lo requiera.

ESTÁNDAR: Son acuerdo plasmados en un documento que contienen especificaciones técnicas, con criterios precisos establecidos, son considerados como guías, reglas, definiciones, entre otros, que ayudan a cumplir un propósito común.

IMPACTO: Son las modificaciones que sufre una organización cuando una amenaza o ataque informático es materializado.

ISO 27001:2013: Normal internación que facilita un marco de trabajo para el SGSI o sistemas de gestión de seguridad de la información, con el objetivo de garantizar la confidencialidad, integridad y disponibilidad de la información.

ISO 27002:2013: Es la normal más importante de la serie y proporciona los requisitos para establecer, implementar y mantener una mejora continua en el sistema de gestión de la seguridad de la información (SGSI).

KALI LINUX: Es un sistema operativo orientado o diseñado específicamente para realizar auditoria y seguridad en los sistemas de información, esta distribución de Debian GNU/Linux trae embebida una serie de herramientas, como: Escaneo de puertos de red, supervisión y captura de paquetes de datos, explotación y post-explotación, entre otras funcionalidades.

MAGERIT: Es la metodología que permite conocer y gestionar los riesgos relacionados con la seguridad de la información de una empresa y/o organización.

MALWARE: Son códigos maliciosos diseñados por ciberdelincuentes con el objetivo de infectar la red y ordenadores y demás dispositivos que la integran afectando el normal funcionamiento, una vez se logra tomar el control este puede substraer borrar, modificar, secuestrar los datos (ransomware), de manera ilícita.

NESSUS: Es una herramienta de código abierto y de pago, que permite escanear vulnerabilidades de los sistemas operativos más comunes como (Windows, Linux, MAC, entre otros) con el objetivo de encontrar o identificar fallos o bugs que ponen en amenaza la seguridad de un sistema, para detectar los huecos de seguridad utiliza una base de datos muy nutrida con vulnerabilidades que se actualiza constantemente, los reportes se pueden visualizar en varios formatos como pdf, CSV, txt, XML, HTML, entre otros.

NORMA: Son todos los elementos de gestión de calidad que se reglamenta para que los productos y servicios por una organización sean óptimo en el contexto de la calidad.

RIESGOS INFORMÁTICOS: Son amenazas y vulnerabilidades latentes, que al ser materializada pueden afectar gravemente los sistemas de información de una organización.

SEGURIDAD INFORMATICA: Se dedica a la protección de los sistemas informáticos ante una eventual riesgo o amenazas (ataques informáticos, virus, robos de información, ransomware, etc.) provenientes de manera interna o externa de la organización.

SERVIDORES DE ALMACENAMIENTO: Son dispositivos de alojamiento de datos conectados a la red, puede ser utilizado para compartir archivos y carpetas de manera controlada y segura, su principal funcionalidad es realizar respaldos o copias de seguridad de los archivos generados por los sistemas de información de una organización.

VULNERABILIDAD: Son los huecos o puntos débiles de una infraestructura tecnológica, estas falencias pueden comprometer gravemente la confidencialidad, integridad y disponibilidad de la información de la organización.

RESUMEN

E.A.R Construcciones es una Empresa que nace de la perseverancia de un grupo de profesionales visionarios, unidos por un firme compromiso, el contribuir a través del conocimiento a hacer realidad los sueños, proyectos e ideales de los clientes, cuya formación está fundamentada en los principios morales y éticos que toda empresa debe tener, es lo que conforma hoy E.A.R construcciones S.A.S; con su esfuerzo y pujanza se encamina hacia la creación, fortalecimiento y formación de bases sólidas en el mercado, que con el tiempo sustentarán lo que hoy en día representa la misión; el cual durante el tiempo ha demostrado su capacidad para superar los desafíos surgidos y ha podido llenar las expectativas de los clientes .

Cualquier empresa hoy en día su activo más valioso es la información, actualmente la empresa EAR Construcciones no tiene un modelo de seguridad para la protección de su información y activos, sabiendo esto, es el motivo por el cual se ve, la necesidad de evaluar la seguridad de los activos de información de toda la organización ,una vez realizado esto se hará el diseño de una propuesta de política y controles de seguridad y privacidad de la información basado en la norma ISO/IEC 27002:2013, dicho esto, la empresa hoy en día puede recibir ataques de secuestro de información (ransomware) que al indagar con el gerente de la organización se logró identificar que hace unos 8 años recibieron un ataque de éstos donde en ese tiempo como no se conocía sobre ataque cibernéticos los ingenieros de la empresa concluyeron que fue daño del disco duro, lo que ha generado un alto riesgo asociado al desconocimiento sobre la seguridad de la información al no contar con los recursos tecnológicos y tampoco con directrices claras en cuanto a la mitigación de los riesgos .

La empresa deposita su información en este trabajo de grado para lograr articular cada uno de sus procesos internos y poder avanzar en cuanto a la gestión de los riesgos que actualmente presenta por las falencias que tienen, vamos a realizar

como producto final una serie de documentos que les llamaremos guías, procedimientos y formatos los cuales les servirán como buenas prácticas en su diario trabajo para el fortalecimiento de su seguridad interna.

PALABRAS CLAVE:

- Activos de información
- MAGERIT
- Políticas de seguridad
- ISO 27001:2013
- Gestión de Riesgos

ABSTRACT

E.A.R Construcciones is a Company that is born from the perseverance of a group of visionary professionals, united by a firm commitment, contributing through knowledge to realize the dreams, projects and ideals of customers, whose formation is based on the moral and ethical principles that every company must have, is what makes up today E.A.R Construcciones S.A.S; with its effort and strength is directed towards the creation, strengthening and formation of solid bases in the market, that over time will support what today represents the mission; which over time has demonstrated its ability to overcome the challenges that have arisen and has been able to meet the expectations of customers.

Any company today its most valuable asset is information, currently the company EAR Constructions does not have a security model for the protection of your information and assets, knowing this, is the reason why it looks, the need to assess the security of information assets across the organisation, once this is done, the design of a proposed information security and privacy policy and controls based on ISO/IEC 27002:2013 will be done, That said, the company today can receive information hijacking attacks (ransomware) that when inquiring with the manager of the organization was able to identify that about 8 years ago they received an attack of these where at that time as it was not known about cyber attack the engineers of the company concluded that it was damage of the hard disk, which has generated a high risk associated with a lack of knowledge about information security due to the lack of technological resources and clear guidelines on risk mitigation.

The company deposits its information in this degree work to achieve articulate each of its internal processes and to be able to move forward in the management of the risks that currently presents by the shortcomings that have, We are going to make as a final product a series of documents that we will call guidelines, procedures and

formats which will serve as good practices in your daily work to strengthen your internal security.

KEY WORDS:

• Information Assets
• MAGERIT
• Security Policies
• ISO 27001:2013
• Risk Management

INTRODUCCIÓN

Este es un proyecto aplicado él cual se va a realizar para apoyar la empresa EAR construcciones en la toma de medidas de seguridad, se espera poder mejorar los procesos de la organización y así mitigar los riesgos a los cuales hoy en día cualquier empresa se encuentra vulnerable sin haber implementado políticas de seguridad de la información.

Dicho esto, surge la necesidad se entregar los lineamientos asociados a los riesgos con el propósito de mitigar y salvaguardar la información debido a esto se tomó como opción para realizar un proyecto aplicado a la organización antes mencionada y porque años atrás sufrió de un ataque de ransomware lo que tuvo como resultado la pérdida de toda la información de vital importancia para la operación que se alojaba en un fileserver con una capacidad de 300 Gb.

Durante el trascurso de este proyecto observarán cómo se van desarrollando cada uno de los objetivos de tal forma que el lector pueda evidenciar el proceso que se le está realizando en la organización y de donde salen los datos a tener en cuenta para poder tomar cada activo de información y hacerle su valoración con la metodología de magerit la cual nos da un valor de probabilidad del riesgo para poder empezar con la mitigación de estos hallazgos, de igual manera se va a realizar una encuesta de forma anónima al personal administrativo de la organización EAR Construcciones para poder conocer más a fondo que perspectivas tienen de la organización y así poder tener un punto de vista amplio de la opinión de los colaboradores de la empresa.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

La empresa EAR Construcciones actualmente no cuenta con ningún protocolo de seguridad para el manejo de sus activos de información, tampoco tienen una política de seguridad de la información, que permita gestionar el riesgo de estos.

En este mismo sentido, los equipos de la empresa no cuentan con licenciamiento de Windows, no hay homogeneidad de software en los equipos, se han encontrado diversidad de S.O. por ejemplo: Winxp, Win7 y Win10. Algunos de los equipos tienen más de 5 años de uso, lo cual dificulta la actualización de estos sistemas operativos, por esta razón dichos equipos tienen vulnerabilidades al tener un sistema operativo obsoleto, sin actualizaciones ni soporte por el fabricante.

Presentan una vulnerabilidad en cuanto manejo y gestión de contraseñas, dado que cualquier persona ajena a la empresa puede sentarse en un equipo de trabajo y poder hacer uso de este, por lo que es un error fatal ya que cualquier persona podría sustraer información, modificarla o eliminarla.

Durante los últimos años la organización ha venido incrementando sus clientes de manera exponencial, pero los servidores y su sistema de seguridad perimetral no cuenta con la configuración adecuada para poder mitigar las vulnerabilidades, porque no se les realiza un mantenimiento preventivo desde hace más de 4 años, no cuentan con soporte y garantía. Dicho esto, se puede decir que desde el tiempo en que los equipos perdieron esta representación con fábrica (Soporte) no se han actualizado las políticas de seguridad, firmware y actualizaciones del sistema lo que conlleva a un riesgo mucho mayor, porque al no contar con las últimas actualizaciones o parches de seguridad liberadas por el fabricante como es debido las brechas de seguridad serán más propensos a ataques informáticos.

El no contar con una solución tecnológica que permita apalancar la operación de la infraestructura actual pone en muy alto riesgo a la organización, así como imposibilitar la continuidad de los servicios que actualmente ofrece a la comunidad en general.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo la adopción de políticas y controles de seguridad y privacidad de la información aplicada a la organización EAR Construcciones y nos permite garantizar y preservar la integridad, confidencialidad y disponibilidad de la información?

2 JUSTIFICACIÓN

En virtud de lo anterior, surge el planteamiento de este proyecto el cual es importante para que la organización se beneficie, al conocer sus falencias tecnológicas y puedan comenzar a realizar un tratamiento de la información para remediar las vulnerabilidades encontradas.

Es importante para la organización EAR Construcciones la implementación de estos protocolos de seguridad ya que hace 7 años atrás sufrieron un ataque de ransomware y así perdieron mucha información de los clientes, planos, cotizaciones, registro fotográfico entre otros.

La implementación y el uso de un sistema de seguridad de la información (SSI) deberá estar acompañado con el diseño y creación de políticas de seguridad con sus respectivos procedimientos, lo cual permitirá detectar y mitigar las vulnerabilidades existentes dentro de cualquier organización, es por esto que se hace indispensable tener una política de seguridad y privacidad de la información que le permita a la organización EAR Construcciones, llegar a proteger su infraestructura tecnológica la cual se encuentra soportada por diferentes soluciones y que se divide principalmente en los siguientes elementos: equipos de Procesamiento (servidores) de mediana capacidad, equipo de almacenamiento masivo de datos (Storage), equipos de comunicaciones (switches). Estos elementos en conjunto procesan y almacenan información de vital importancia para la organización, los cuales requieren ser preservados para garantizar la integridad, confidencialidad y disponibilidad de la información que garanticen la prestación de los diferentes servicios ofrecidos.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Evaluar la seguridad de los activos de información de la organización EAR Construcciones, para el diseño de una propuesta de políticas y controles de seguridad y privacidad de la información basado en las normas ISO/IEC 27001 y 27002:2013.

3.2 OBJETIVOS ESPECÍFICOS

- Analizar la seguridad de los activos de información de la organización EAR Construcciones mediante una metodología de gestión de riesgo con el fin de tener identificado el estado actual de las vulnerabilidades, amenazas y riesgos.

- Proponer Controles de seguridad basados en la guía de buenas prácticas ISO/IEC 27002:2013, para la mitigación del riesgo asociado a los activos de información para la organización EAR Construcciones.

- Diseñar políticas de seguridad, basado en el análisis de riesgo con el fin de alinearse a las necesidades de la organización EAR Construcciones.

- Proponer una estrategia de socialización de los niveles de riesgos de los activos de información de la empresa EAR Construcciones y sus políticas de seguridad con el fin crear conciencia en los usuarios de la organización.

4 MARCO REFERENCIAL

Abarca los aspectos que fundamentan la investigación, por ejemplo: marco teórico, marco conceptual, marco legal, entre otros.

4.1 MARCO TEÓRICO

4.1.1 La importancia de implementar un SGSI en la organización. En la actualidad el avance tecnológico que se está presentando trae consigo desafíos que generan preocupaciones a los altos directivos organizacionales, debido a esto surge **la importancia de implementar un SGSI en la organización** para garantizar un máximo nivel de disponibilidad, integridad y confidencialidad de la información manejada diariamente en las organizaciones es un aspecto de gran importancia que se procura tener en cuenta dentro de las labores empresariales hoy en día.

Por lo anterior, es de gran utilidad para las organizaciones la implementación de un SGSI (Sistema de Gestión de Seguridad de la Información) el cual está fundamentado sobre la norma ISO/IEC 27001:2013 y establece un proceso sistemático para la protección ante cualquier amenaza que podría llegar afectar la confidencialidad, integridad o disponibilidad de la información. Este sistema ofrece las mejores prácticas y procedimientos que siendo aplicados correctamente en el ámbito empresarial, proporcionan una mejora continua y apropiada para evaluar los riegos a los que enfrentarían diariamente, establecer controles para una mejor protección y defender así el activo más importante para la organización[1].

[1] SAFESOCIETY; [Sitio web]; Safesociety; La importancia de implementar un SGSI en nuestra organización; [Consulta: 21 de octubre 2021]; Disponible en: https://www.safesociety.co/blogitem/4/la-importancia-de-implementar-un-sgsi-en-nuestra-organizacion

4.1.2 Beneficios de implementar ISO 27001:2013 Los principales beneficios que la aplicación de la norma ISO 27001:2013 tiene para la empresa son :

- Cumplimiento de la normativa vigente: cada día se aprueban nuevas normas relativas a la seguridad de la información y cumpliendo la ISO 27001:2013 garantizamos el cumplimiento de la práctica totalidad de esa normativa .

- Ventaja comercial: si la empresa está certificada en el cumplimiento de esta norma tendrá una ventaja respecto a otras empresas no certificadas ya que los clientes tendrán más confianza de que sus datos personales están protegidos .

- Reducción de costes: ISO 27001:2013 pretende evitar que la empresa sufra una brecha de seguridad y estas tienen un importante coste económico, aunque sean pequeñas. Es mayor el ahorro obtenido por la empresa que la inversión en ISO 27001:2013 .

- Mejorar la organización: muchas veces las empresas no tienen tiempo para fijar sus procedimientos y los empleados desconocen qué deben hacer y cuándo. Al aplicar ISO 27001:2013 se solucionan estas situaciones al inducir a las empresas a redactar sus principales procesos [2].

[2] CIBERSEGURIDAD; [Sitio web]; Ciberseguridad; ISO 27001; [Consulta: 21 de octubre 2021]; Disponible en: https://ciberseguridad.com/normativa/espana/sgsi/iso-27001/#Beneficios_para_la_empresa

4.1.3 Importancia de implementar procesos en una empresa al realizar la implementación de procesos en cualquier organización se obtendrá el máximo rendimiento de todos sus componentes y sus resultados se verán altamente beneficiados. Piensa por un momento ¿cómo funciona tu empresa?, ¿está dividida en departamentos que trabajan cada uno por su lado, independientes de los demás? Esta es la manera tradicional en la que una empresa funciona, y a la vez es poco efectiva porque dificulta la relación entre cada departamento, separándolos cuando deberían funcionar en conjunto. Si cada dependencia de la empresa permanece aislada del resto los objetivos en común no podrán cumplirse. Al contrario, con la implementación de procesos, la empresa es vista como un conjunto de procesos que se relacionan entre sí, que están conectados, favoreciendo la participación de varias personas de distintas dependencias dentro de un mismo proceso, así todas las partes de la empresa se ven beneficiadas y empiezan a funcionar en conjunto[3].

4.1.4 La implementación de la ISO/IEC 27001:2013 al interior de las organizaciones las ventajas que nos proporcionan por la certificación ISO/IEC 27001:2013 son representativas para las empresas, sobre todo porque son reconocidas mundialmente, conozca algunos beneficios asociados a la aplicación de la norma :

- Mejor concienciación sobre la seguridad de la información
- Mayor control de activos e información sensible
- Ofrece un enfoque para la implementación de políticas de control
- Oportunidad de identificar y corregir puntos débiles
- Reducción del riesgo de responsabilidad por la no implementación de un

[3] PRACTISIS; [Sitio web]; Practisis; La importancia de implementar procesos operativos en tu empresa; [Consulta: 21 de octubre 2021]. Disponible en: https://www.practisis.com/post-one/la-importancia-de-implementar-procesos-operativos-en-tu-empresa

SGSI o determinación de políticas y procedimientos

- Se convierte en un diferencial competitivo para la conquista de clientes que valoran la certificación
- Mejor organización con procesos y mecanismos bien diseñados y gestionados
- Promueve reducción de costos con la prevención de incidentes de seguridad de la información
- Conformidad con la legislación y otras reglamentaciones .

4.2 MARCO CONCEPTUAL

4.2.1 Amenaza Tecnológicas: Cuando se está frente a una amenaza ante un agente interno y/o externo que pone en peligro al ser humano en todas sus dimensiones de la vida como son: Sus obras y el entorno que lo rodea, donde frente a esto existe la posibilidad de que se creen accidentes tecnológicos. Por lo tanto, teniendo en cuenta esta definición se destaca que la evaluación de las amenazas tecnológicas tiene como origen diversos factores o variables las cuales pueden ser: Historial de eventos en la zona o en la fuente de riesgo, condiciones de seguridad en que funciona el sistema que posee la amenaza, grado de interacción de la amenaza con los sistemas amenazados. La amenaza en sí no está determinada por el desarrollo tecnológico o el uso de sustancias químicas, sino más bien por la forma en que el hombre interactúa con los diferentes agentes de amenaza [4].

4.2.2. Pilares de la Seguridad de la Información[5]. A continuación, se presentan los pilares de la seguridad de la información:

[4] DERECHO DE AUTOR; [Sitio web]; Colombia: Derechos de autor; Sobre derechos de autor; [Consulta: 25 de septiembre 2021]; Disponible en: http://derechodeautor.gov.co:8080/documents/10181/182597/23.pdf/a97b8750-8451-4529-ab87-bb82160dd226

[5] TELCEL.COM; [Sitio web]; Pilares de seguridad de la información; [Consulta: 02 de mayo 2023]; Disponible en: https://www.telcel.com/empresas/tendencias/notas/pilares-seguridad-de-informacion#:~:text=Los%20tres%20pilares%20principales%20de,de%20seguridad%20de%20la%20informaci%C3%B3n

Confidencialidad: Es la propiedad mediante la cual los activos de la información no están disponibles a cualquier persona o entidad no autorizada.

Integridad: Es el uso por el cual la información se mantiene inalterada, es decir que no se podrá modificar dicha información sin previa autorización.

Disponibilidad: Es el mecanismo, mediante el cual los usuarios autorizados pueden acceder a la información cuando lo requieran. acceso y utilización de la información y los sistemas de tratamiento de esta por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

4.2.3 Análisis de riesgo informático[6]: Es el proceso que realiza la identificación de los activos de información, vulnerabilidades y amenazas a los que se pueden encontrar expuestos, de igual manera que tan repetitiva y que tanto impacta a las partes. Dicho esto, se deben implementar controles adecuados para aceptar, disminuir, transferir, o evitar la ocurrencia del este riesgo .

Las amenazas son agentes (elementos o acciones), capaces de atentar contra la seguridad de la información y, como consecuencia de ello, causar pérdidas o daños a los activos de una empresa.

Estas amenazas surgen a partir de la existencia de vulnerabilidades, es decir que una amenaza sólo puede existir si existe una vulnerabilidad que pueda ser aprovechada, e independientemente de que se comprometa o no la seguridad de un sistema de información.

---

[6] GESTIÓN PENSEMOS; [Sitio web]; Gestión pensemos; Análisis de riesgo informático: 4 pasos para implementarlo; [Consulta: 02 de mayo 2023]; Disponible en: https://gestion.pensemos.com/analisis-de-riesgo-informatico-4-pasos-para-implementarlo

Es importante analizar tanto las amenazas intencionales como no intencionales.

4.2.4. Vulnerabilidad: Se puede definir como un error en el código o una debilidad de un sistema y/o dispositivo que cuando se explota, puede llegar a comprometer la disponibilidad, confidencialidad e integridad del sistema que ha sido vulnerado o explotado.

En seguridad cibernética, una vulnerabilidad es una debilidad que puede ser explotada por un ataque cibernético para obtener acceso no autorizado o realizar acciones no autorizadas en un sistema informático. Las vulnerabilidades pueden permitir a los atacantes ejecutar código, acceder a la memoria de un sistema, instalar malware y robar, destruir o modificar datos confidenciales.

Para aprovechar una vulnerabilidad, un atacante debe poder conectarse al sistema informático. Las vulnerabilidades pueden explotarse mediante una variedad de métodos que incluyen inyección SQL, desbordamientos de búfer, scripting entre sitios (XSS) y kits de explotación de código abierto que buscan vulnerabilidades conocidas y debilidades de seguridad en aplicaciones web [7].

4.2.5. Activos de información: Los activos de información son los recursos que utiliza un Sistema de Gestión de Seguridad de la Información para que las organizaciones funcionen y consigan los objetivos que se han propuesto por la alta dirección.

Los activos se encuentran asociados, de forma directa o indirectamente, con las demás entidades. Puede ser que le interese leer este artículo ISO 27001: ¿Cómo analizar y gestionar los riesgos en un SGSI? Un proyecto de seguridad tiene el

[7] HOSTDIME; [Sitio web], Hostdime; ¿Qué es una vulnerabilidad en seguridad informática?; [Consulta: 25 de septiembre 2021]; Disponible en: https://www.hostdime.com.pe/blog/que-es-una-vulnerabilidad-en-seguridad-informatica-ejemplos/

objetivo de controlar la seguridad de los activos de información que generan el dominio en el estudio de proyectos.

El límite del conjunto de activos del dominio no imposibilita la consideración de las relaciones en materia de seguridad de dichos activos de información con el entorno. Uno de los primeros pasos que debe seguir la entidad para adaptarse a la norma ISO 27001 es llevar a cabo un inventario de activos de información. Tendrán los activos de información que representan algún valor para la empresa y que quedan dentro del alcance del SGSI.

En principio puede parecer un poco abrumador para un principiante, por la gran cantidad de activos que se van ocurriendo. Por este motivo se decide comenzar por clasificarlos de alguna forma. Entre las muchas formas que se encuentran podemos elegir la definida por los expertos. Parece la manera más completa. Muestra ejemplo de cada tipo y es válido para entidades de muy diferente naturaleza [8].

4.2.6. Políticas de seguridad[9]: Las políticas de seguridad informática consisten en una serie de normas y directrices que permiten garantizar la confidencialidad, integridad y disponibilidad de la información y minimizar los riesgos que le afectan.

Una política de seguridad se define a alto nivel, esto es, qué se debe proteger y cómo, es decir, el conjunto de controles que se deben implementar. Esta se desarrolla en una serie de procedimientos e instrucciones técnicas que recogen las medidas técnicas y organizativas que se establecen para dar cumplimiento a dicha

[8] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES; [Sitio web]; Colombia: MINTIC; Registro de activos de información; [Consulta: 25 de septiembre 2021]; Disponible en: https://mintic.gov.co/portal/inicio/Atencion-y-Servicio-a-la-Ciudadania/Transparencia/135888:Registro-de-Activos-de-Informacion

[9] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES; [Sitio web]; Colombia: MINTIC; Articulo Elaboración de la política general de seguridad y privacidad de la información; pág. 7,13; [Consulta: 02 de mayo 2023]; Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

política.

La definición de una política de seguridad debe estar basada en una identificación y análisis previo de los riesgos a los que está expuesta la información y debe incluir todos los procesos, sistemas y personal de la organización. Además, tiene que haber sido aprobada por la dirección de la organización y comunicada a todo el personal.

Entrando más en detalle, el cuerpo normativo de seguridad de la información de una organización consta principalmente de las siguientes políticas y procedimientos:

4.2.7. Buenas prácticas S.I. El documento de buenas prácticas de Seguridad de la Información puede ser un documento específico, cláusulas anexas a los contratos de los empleados, etc, debería recoger, entre otras cosas, el uso aceptable de los sistemas y la información por parte del personal, las directrices para mantener el puesto de trabajo despejado, el bloqueo de equipo desatendido, la protección de contraseñas [10].

4.2.8. Fuga de información: Se denomina fuga de información al incidente que pone en poder de una persona ajena a la organización, información confidencial y que sólo debería estar disponible para integrantes de esta (tanto todos como un grupo reducido).

Se trata de un incidente que puede ser tanto interno como externo, y a la vez intencional o no. Algunos ejemplos de fuga de información pueden ser desde un empleado vendiendo información confidencial a la competencia (incidente interno e intencional), una secretaria que pierde un documento en un lugar público (incidente interno y no intencional) o en la misma línea la pérdida de una laptop o un pendrive,

[10] UNIR; [Sitio web]; Unir; Políticas de seguridad informática; [Consulta: 25 de septiembre 2021]; Disponible en: https://www.unir.net/ingenieria/revista/politicas-seguridad-informatica/

así como también el acceso externo a una base de datos en la organización o un equipo infectado con un Spyware que envíe información a un delincuente[11].

4.3 MARCO HISTÓRICO:

El ciber ataque hacia las organizaciones ha venido en un notable crecimiento y más por el tema del teletrabajo, su mayor dificultad es cuando se comprometen los datos privados, daños a la infraestructura, bases de datos, etc., afectando las operaciones de cualquier organización. Según un reporte realizado por Symantec, que realizó un estudio entre 157 países, revelo que Colombia fue la sexta nación de Latinoamérica con los mayores ataques en el 2017. Por todos estos casos la ciberseguridad se ha vuelto un agente primordial para la seguridad de la infraestructura computacional y completa relación de esta, fundamentalmente los datos que circulan en la web[12].

Por otro lado, en Colombia los casos de cibercrimen han aumentado cerca del 28% cada año de acuerdo con reportes del centro Cibernético Policial, donde afecta en gran parte la seguridad y privacidad de los usuarios. [13]

Si bien el teletrabajo no era algo nuevo en Colombia, pues se había ido implementando de a poco en diversas empresas, la llegada del covid-19 y las restricciones de movilidad impulsaron esta modalidad logrando que, en 2020, 209.173 empleados se convirtieran en teletrabajadores, fomentando un incremento de 71 % con respecto a 2018, cuando solo había 122.278 .

---

[11] WELIVESECURITY; [Sitio web]; Welivesecurity; ¿Qué es la fuga de información?; [Consulta: 25 de septiembre 2021]; Disponible en: https://www.welivesecurity.com/la-es/2010/04/13/que-es-la-fuga-de-informacion/

[12] UNIVERSIDAD PILOTO DE COLOMBIA; [Sitio web]; Unipiloto; Ciberseguridad en Colombia. Universidad Piloto de Colombia; pag 1-12; [Consulta: 25 de septiembre 2021]; Disponible en: http://repository.unipiloto.edu.co/handle/20.500.12277/2579/browse?type=author&value=Valoyes+Mosquera%2C+AmancioMosquera Amancio, V. (2017). Ciberseguridad en Colombia. Universidad Piloto de Colombia, 1-12.

[13] EL TIEMPO; [Sitio web]; Colombia: Periódico el Tiempo; Cibercrimen le cuesta a Colombia más de $190 mil millones de pesos al año; [Consulta: 25 de septiembre 2021]; Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/cibercrimen-le-cuesta-a-colombia-190-000-millones-de-pesosal-ano-380830

Así lo reveló el quinto estudio de Penetración y Percepción del Teletrabajo presentado este miércoles por el viceministro de Transformación Digital del Ministerio de las TIC, Iván Durán [14].

4.4 ANTECEDENTES:

Entre los antecedentes se tienen los siguientes trabajos que han permitido tenerlos como referente para la fundamentación del trabajo a desarrollar, donde se toma de la página de la policía nacional los índices de Hurtos, violación a los datos, acceso no autorizado o abusivo a los sistemas de información. Esto con el fin de poder tomar puntos de referencia a las organizaciones que en la actualidad no han implementado controles ante esta amenaza inminente y generar conciencia de lo que ocurre a su alrededor.

Según el reporte de Tendencias Cibercrimen Colombia 2019-2020 ha presentado **DELITOS INFORMATICOS MÁS COMUNES EN COLOMBIA**[15]**,** donde por fuentes oficiales de la Policía Nacional, fiscalía general de la Nación, muestra el siguiente reporte de los delitos informáticos que más se cometieron en Colombia fueron:

- Hurtos por medios informáticos - 31.058 casos
- Violación a los datos Personal - 8.037 casos
- Acceso abusivo a sistema informático - 7.994 casos
- Transferencia no consentida de activos - 3.425 casos
- Software Malicioso - 2.387 casos

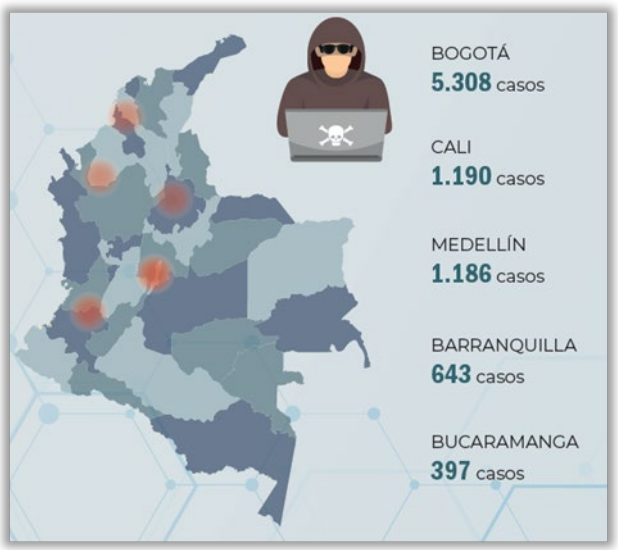
[14]MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES; [Sitio web]; Colombia: MINTIC; Colombia superó los 209.000 teletrabajadores en 2020; [Consulta: 21 de octubre 2021]; Disponible en: https://mintic.gov.co/portal/inicio/Sala-de-prensa/179742:Colombia-supero-los-209-000-teletrabajadores-en-2020-Ministerio-de-las-TIC

[15]CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES; [Sitio web]; Colombia: Ccit; Tendencias Cibercrimen Colombia 2019-2020, pág. 7,8; [Consulta: 21 de octubre 2021]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Delitos informáticos por ciudades:

En la siguiente grafica se puede observar las ciudades en Colombia con mayor número de ataques informáticos según el documento emitidos por el Csirt denominado Tendencias Cibercrimen 2020 - Compressed-3.

Ilustración 1 - Tendencias Cibercrimen 2020 - Compressed-3



Fuente 1 - CCIT.ORG.CO; [Sitio web]; CCIT Colombia, Informe tendencias cibercrimen, pág. 8; [Consulta: 10 de marzo de 2022]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

LA TENDENCIA PARA EL 2020 - 2021[16]**:**

La tendencia de ciberataques en los próximos años será:

- Inteligencia Artificial y Malware
- Uso de perles falsos en redes sociales para difusión de Malware
- BEC basado en Deepfake
- Uso de Botnet para difusión de correos extorsivos
- Uso de mercados ilegales en DarkNet

[16] CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES; [Sitio web]; Colombia: Ccit; Tendencias Cibercrimen Colombia 2019-2020, pág. 29; [Consulta: 21 de octubre 2021]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Según lo manifiesta el documento Tendencias Cibercrimen 2020 - Compressed-3.

- En ese mismo orden de ideas, en el trabajo da los lineamientos para diseñar los controles de seguridad que salvaguarden los activos de información, describiendo las nociones relacionadas con el tema de seguridad de la información en las organizaciones, tratando un enfoque global mostrando los modelos, técnicas e instrumentos que suministran las guías necesarias para disminuir el nivel de fragilidad que tienen los activos ante una amenaza. Dichos lineamientos se hacen siguiendo la metodología MAGERIT alineado con la norma ISO/IEC 27001 para una empresa de transporte de pasajeros. Se define la situación actual de la empresa, se identifican los activos con sus pertinentes amenazas, se realiza la comprobación de riesgos efectivos y se sugieren las protecciones necesarias que podría formar parte del plan de implantación [17].

- **DISEÑO DEL SISTEMA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA QWERTY S.A.**

En este proyecto se toma como marco referencial porque realizan el diseño de un SGSI hacía una entidad que tiene inconvenientes de como asegurar sus activos de información y es por esto que se toma como referente para evidenciar su metodología al momento de realizar la mitigación del riesgo existente, dicho esto el trabajo consistió en la ejecución de un proyecto aplicado, donde se realizó el diseño de un sistema de gestión de seguridad de la información, el cual permitió mejorar y dinamizar la administración de los activos de información de la empresa QWERTY S.A., asegurando el control del cumplimiento de su misión basados en la normatividad vigente. La empresa QWERTY S.A. actualmente se especializa en el desarrollo tecnológico en comunidades colombianas a través del uso de tecnologías

[17]UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Márquez Buitrago, Yon Ivan, Diseño de controles de seguridad para los activos informáticos en la empresa Transportes Tierra Grata y Compañía Ltda; [Consulta: 21 de septiembre 2021]. Disponible en: https://repository.unad.edu.co/handle/10596/21345

de información, donde cuenta con 120 colaboradores entre directivos, administrativos y operativos, quienes usan de forma regular los medios de información para la consulta de datos, pero la empresa presenta algunas fallas de seguridad en sus sistemas y manejo de recursos tecnológicos, lo cual hace que sea vulnerable ante cualquier incidente que se presente y ponga en riesgo la integridad de la empresa. Por lo anterior, la empresa QWERTY S.A., preocupada por la seguridad de sus activos de información, acudió a la universidad UNAD, en donde solicitó la asignación de un director de proyecto para que diseñara un sistema de gestión de seguridad de la información. Para dar respuesta a dicha solicitud se creó un sistema gestión de seguridad de la información, de acuerdo con la norma ISO 27001, a partir de los procesos, activos de información y falencias que presentaba la entidad [18].

- **ANÁLISIS Y EVALUACIÓN DE RIESGOS, DE LOS ACTIVOS DE INFORMACIÓN DE LA DIRECCIÓN EJECUTIVA SECCIONAL DE ADMINISTRACIÓN JUDICIAL DE TUNJA - DESAJT, ADOPTANDO UNA METODOLOGÍA DE GESTIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN.**

El presente trabajo se toma como referencia ya que incorporan metodologías de la gestión del riesgo de MAGERIT y es así como tomamos esta referencia para la ejecución de nuestro proyecto donde se destacan por proporcionar las actividades que le permiten a una organización conocer los riesgos que pueden generarse con el uso de los sistemas tecnológicos, de comunicaciones y el entorno asociado a su nivel de operación. Con los resultados de este estudio, de forma aplicada se ha tomado una organización con activos y sistemas de información específicos, con el objeto proponer la metodología de gestión de riesgos, que se ajusta a los requerimientos en materia de seguridad de la organización y determinar los riesgos

[18] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Edwin Anderson, Diseño del Sistema Gestión de Seguridad de la Información para la Empresa QWERTY S.A.; [Consulta: 22 de septiembre 2021]. Disponible en: https://repository.unad.edu.co/handle/10596/39069

a los que se encuentran sometidos sus activos a través del análisis y evaluación de los riesgos. Con fundamento en lo anterior, esta monografía desarrolla los siguientes temas: en el primer capítulo se describe la estructura organizacional de la Dirección Ejecutiva Seccional de Administración Judicial de Tunja – DESAJT (organización tomada como caso de estudio), y la estructura de procesos de su Sistema Integrado de Gestión y Control de la Calidad y el Medio Ambiente – SIGCMA, obteniendo a través de sus procesos de apoyo el inventario de los activos de información más relevantes, mediante los cuales se soporta el funcionamiento operativo y la prestación de servicios de la organización. En el segundo capítulo se estudian los aspectos más importantes de las metodologías de gestión de riesgos para sistemas de la información: MAGERIT versión 3 y NIST SP800-30 revisión 1, donde se exponen las actividades y procedimientos de cada metodología respecto del proceso de análisis y evaluación de riesgos [19].

- **DISEÑAR UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) A LA EMPRESA UNITRANSA S.A. UBICADA EN LA CIUDAD DE BUCARAMANGA.**

DESCRIPCIÓN DEL CONTENIDO:

Este proyecto es tomado como referencia porque abarca la metodología Magerit la cual es útil para cualquier empresa sin importar su tamaño (Grande, mediano o pequeña), esta herramienta utilizada para la gestión de seguridad de la información, enfocándose en la criticidad de los riesgos relacionados con los sistemas de información, El trabajo inicia con la Introducción, que plantea la importancia de incorporar en las organizaciones mecanismos tecnológicos que agilicen sus procesos y permitan almacenar cantidades considerables de información en dispositivos muy pequeños, así como la incorporación de redes de datos que logran un ahorro importante de recursos con una mayor organización y eficiencia a la hora

[19] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Jiménez Fonseca, Teresa Herminia, Análisis y evaluación de riesgos, de los activos de información de la Dirección Ejecutiva Seccional de Administración Judicial de Tunja - DESAJT, adoptando una metodología de gestión de riesgos de los sistemas de información; [Consulta: 22 de septiembre 2021]. Disponible en: https://repository.unad.edu.co/handle/10596/21575

de tomar las decisiones. Se aborda la metodología MAGERIT versión 3 para realizar el análisis y evaluación de los riesgos y las vulnerabilidades a las que están expuestos los activos de información de UNITRANSA S.A., una empresa de transporte urbano de pasajeros en la ciudad de Bucaramanga y su área metropolitana. El estándar internacional ISO/IEC 27001 establece los requisitos para establecer, monitorear y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI). Este documento está hecho bajo las ordenanzas de esta norma. Mantener la seguridad de la información y sus activos requiere como primera medida la adopción de una Política de Seguridad de la Información (PSI) robusta, documentada, conocida por todos, aprobada por la administración y revisada periódicamente, sin desconocer la aplicación de la legislación penal colombiana en materia de Seguridad Informática. Este manuscrito contiene de manera clara y sucinta las reglas de uso aceptado de los Activos de Información y la Información misma, al igual que las leyes colombianas aprobadas por el congreso para combatir los delitos informáticos. La gestión de Activos de Información requiere la adopción de un mecanismo de control adecuado que permita algunas acciones como: control de acceso, uso, controles, importancia para los procesos de la empresa, criticidad de la información que manejan, entre otros [20].

- **DISEÑO DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA UNIDAD DE TECNOLOGÍA DE LA CÁMARA DE COMERCIO DE CÚCUTA.**

DESCRIPCIÓN DEL CONTENIDO:

El presente proyecto presenta el diseño de las Políticas de Seguridad de la Información para la Dirección de Tecnología de la Cámara de Comercio de Cúcuta, como respuesta a la necesidad de disminuir el impacto de las amenazas sobre los activos de información. Para llegar a estas políticas se hace inicialmente una evaluación del nivel de madurez de la Cámara de Comercio de Cúcuta con respecto

[20]UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; García Ramírez, Germán, Castro Angarita, Jaime Alfonso, Diseñar un Sistema de Gestión de la Seguridad de la Información (SGSI) a la empresa Unitransa S.A. ubicada en la ciudad de Bucaramanga; [Consulta: 22 de septiembre 2021]. Disponible en: https://repository.unad.edu.co/handle/10596/11914

a los controles de seguridad definidos por la ISO 27001:2013. Posteriormente se plantean una serie de fases de acuerdo con la metodología de análisis de riesgos seleccionada como la más adecuada de acuerdo con las características de la organización. Se realiza la identificación de los activos de información, se valoran en sus dimensiones de seguridad y se identifican los riesgos a los que están expuestos aplicando los criterios de valoración por probabilidad de impacto. Se definen las Políticas de Seguridad teniendo en cuenta el análisis previo realizado a la organización que contribuyan a minimizar las probabilidades de materialización de riesgos de seguridad de la información [21].

- **REALIZAR EL ANÁLISIS PARA GESTIÓN DE RIESGOS EN LOS SISTEMAS DE INFORMACIÓN DE LA IPS SOLIDARIOS SALUD DEL MUNICIPIO DE CUASPUD CARLOSAMA A PARTIR DE LA NORMA ISO 27001 APLICANDO LA METODOLOGÍA MAGERIT.**

DESCRIPCIÓN DEL CONTENIDO:

Se toma como referencia este trabajo por la aplicabilidad que tiene la metodología Magerit que no ayuda a identificar los activos de información, la valoración, amenazas e impacto o consecuencia que asumiría la entidad en caso de materializarse cualquiera de estos riesgos asociados a los sistemas de información, este proyecto de investigación tratará aspectos relativos a la IPS Solidarios Salud del municipio de Cuaspud Carlosama, como es, la reseña histórica, el tipo de entidad dentro del sector salud y la formalización de la plataforma estratégica, además, se tratará los conceptos referentes de la Metodología MAGERIT v 3.0, como es la identificación de activos, su valoración, determinación de vulnerabilidades, amenazas y el impacto que causarían en los activos si llegaran a materializar el riesgo. También, se efectuará el análisis e identificación de los riesgos como aporte central del presente proyecto, determinando el plan de

[21] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Duarte Martínez, María Carolina, Diseño de políticas de Seguridad de la Información para la Unidad de Tecnología de la Cámara de Comercio de Cúcuta; [Consulta: 22 de septiembre 2021]. Disponible en: https://repository.unad.edu.co/handle/10596/30304

tratamiento de riesgos, la evaluación de los controles de la norma ISO 27001 y 27002, y se culminará el trabajo con la Gestión de Riesgos [22].

- **PROPUESTA DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA PROTEGER LOS ACTIVOS DE INFORMACIÓN EN LAS ORGANIZACIONES.**

Se escoge este trabajo como referente debido a que utilizan la metodología de magerit y nos da un amplio conocimiento para poder implementar los recursos en nuestro proyecto ya que ellos dentro del diseño se define un aspecto fundamental en seguridad informática en donde se evalúan las herramientas tecnológicas para asegurar, aplicar, monitorear algunos componentes establecidos en la política de seguridad para evitar ataques a los sistemas de información y que sea de uso obligatorio de los usuarios en las organizaciones. La política de seguridad se debe sensibilizar con todas las partes interesadas iniciando con la alta dirección quienes avalan para luego socializar con empleados, terceros, ya que se debe estructurar, identificar, detectar, relacionar, proporcionar todas las vulnerabilidades para realizar una evaluación de riesgos y aplicar controles necesarios para reducir el impacto vs la consecuencia dejando los riesgos a un nivel residual bajo. La política debe ser fácil de comprender, concisa para los usuarios, deben enmarcar las guías y las actividades de una organización, se deben aplicar según las directrices en donde se especifica el estándar y/o norma a utilizar como la ISO 27001:2013 protegiendo la información de cualquier amenaza. Se debe tener Comprensión y entendimiento de los requerimientos de seguridad y la Identificación de aspectos legales, comerciales y regulatorios relacionados con seguridad de la información. Palabras claves: Sistema de gestión de seguridad de la información, políticas, Riesgos, Activos de Información, Confidencialidad, Integridad, disponibilidad [23].

---

[22] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Arellano Montenegro, Fabio Adalberto, Realizar el análisis para gestión de riesgos en los sistemas de información de la IPS Solidarios Salud del municipio de Cuaspud Carlosama a partir de la norma ISO 27001 aplicando la metodología Magerit; [Consulta: 21 de septiembre 2021]. Disponible en: https://repository.unad.edu.co/handle/10596/21476

[23] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Oñate Arboleda, Adriana, Propuesta de Políticas de Seguridad de la Información para proteger los activos de información en las organizaciones; [Consulta: 22 de septiembre 2021]. Disponible en: https://repository.unad.edu.co/handle/10596/41984

- **DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD PARA LA RED DATOS BAJO LA NORMA ISO 27001:2013 EN EL CENTRO DE ESTUDIOS EMSSANAR CETEM DE LA CIUDAD DE PASTO.**

Se toma como referencia este trabajo para la verificación e implementación de las metodologías utilizadas que dan un aporte positivo a nuestro proyecto.

En la actualidad las redes de datos como parte de una plataforma tecnológica permiten agilizar gran cantidad de tareas dentro de un centro de formación para el trabajo y desarrollo humano. Como es el caso del Centro De Estudios EMSSANAR CETEM, la red de datos es fundamental para el desarrollo de labores administrativas y académicas ya que permite la comunicación interna y externa de funcionarios, docentes y estudiantes. Lastimosamente esta red es de uso público y no cuenta con las medidas de seguridad y de control físico y lógicos adecuados. Por lo antes expuesto, el presente proyecto, tiene como propósito mostrar el proceso de diseño de un sistema de gestión de seguridad para la red datos bajo la norma ISO27001:2013 en el centro de estudios EMSSANAR CETEM de la ciudad de pasto a través de unas fases estructuradas, partiendo del análisis de riesgos sobre los activos de información relacionados con la investigación a través de la metodología MAGERIT, siguiendo con la identificación de controles implementados teniendo como referencia la ISO/IEC 27002:2013 y la escala de madurez del COBIT 4.1 y terminando con la definición de las políticas de seguridad acordes con los objetivos del negocio y valoración de los activos de información [24].

- **ETAPA DE PLANIFICACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL ÁREA DE TECNOLOGÍA DE LA IPS GARPER MÉDICA SAS BASADO EN LA NORMA ISO/IEC 27001:2013.**

[24] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Coral Ojeda, Jesús Armando, Adriana, Diseño de un sistema de gestión de seguridad para la red datos bajo la norma ISO 27001:2013 en el Centro de Estudios Emssanar Cetem de la ciudad de Pasto; [Consulta: 22 de septiembre 2021]. Disponible en: https://repository.unad.edu.co/handle/10596/11875

Este proyecto aplicado para la etapa de planificación de un sistema de Gestión de seguridad de la información a través de un proceso integral para el área de Tecnología de la IPS Garper Médica SAS, como Institución prestadora de servicios de salud privada, se realiza con el fin de planificar un SGSI, establecer las políticas y lineamientos de seguridad de la información, en beneficio de proteger la información teniendo en cuenta los pilares fundamentales como son la confidencialidad, integridad y disponibilidad, lo anterior, efectuando con el compromiso constitucional de salvaguardar la información de la entidad y así garantizar la continuidad en su prestación de servicios.

Para el desarrollo del SGSI (Sistema de gestión de seguridad de la información) se enmarca la norma ISO/IEC 27001:2013, donde se establecen los requisitos para la planeación, implementación, mantenimiento y mejora continua de un sistema de gestión, definiendo el alcance del SGSI, se someterá a evaluación o auditoría los sistemas de seguridad informática e infraestructura TI de la entidad, este diagnóstico indicará en qué estado se encuentran estos sistemas y las medidas correctivas para el mejoramiento, a su vez, se reunirá toda la documentación deseada que alimentará una base de conocimiento, agrupando por tareas lógicas y actividades que será ajustable según el tamaño de la empresa. Igualmente, se organizará dicha documentación por fases de ejecución y organización del proyecto mediante el uso del diagrama Gantt. Se definirá un tratamiento de los riesgos detectados y decidiendo la aplicación o controles a implementar, se presentará los resultados de la medición de la eficacia de los controles, dando un panorama completo de los alcances de la norma. Por último, se hace el despliegue y puesta[25].

- **PLAN DE IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA UNIDAD ADMINISTRATIVA PARQUES**

[25] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Criollo Betancourt, Irmaena, Etapa de planificación de un sistema de gestión de seguridad de la información para el área de tecnología de la IPS Garper Médica SAS basado en la norma ISO/IEC 27001:2013.; [Consulta: 02 de mayo 2022]. Disponible en: https://repository.unad.edu.co/handle/10596/48702

NACIONALES NATURALES DE COLOMBIA, SEGÚN NORMA ISO 27001: 2013:

Tipo de investigación aplicada se analizó la situación inicial de la entidad, se aplicaron las técnicas necesarias para recolectar y analizar datos con el fin de describir, generar e implementar normas y/o procedimientos acordes con las necesidades de la Entidad. Se hizo una comparación entre procedimientos y políticas existentes, para realizar un análisis diferencial de las medidas y normas en relación con la seguridad de la información que tenía la organización, mediante la metodología Magerit v.3. tomando como referencia la norma ISO / IEC27001: 2013 y el código de buenas prácticas detallado en la ISO / IEC27002: 2013, contemplando los controles y objetivos de los dominios[26].

- **DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL ÁREA TI DE LA ESE HOSPITAL UNIVERSITARIO ERASMO MEOZ DE CÚCUTA BASADO EN LA NORMA ISO 27001:2013:**

Se realizó un estudio descriptivo de la seguridad informática en la ESE Hospital Universitario Erasmo Meoz, recolectando información para realizar el análisis de riesgos de los activos informáticos usando la metodología MAGERIT. Finalmente, con la información obtenida de las actividades anteriores se realiza el Diseño de la propuesta de solución planificada y de mejora continua bajo la norma ISO 27001[27] .

- **DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LA IPS AASSALUD DE COROZAL SUCRE, MEDIANTE LA IMPLEMENTACIÓN DE LA METODOLOGÍA MAGERIT (V3.0) Y LA NORMA ISO 27001:2013:**

---

[26] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; González Tabares, Eduin Gildardo, Plan de implementación de un sistema de gestión de seguridad de la información para la Unidad Administrativa Parques Nacionales Naturales de Colombia, según Norma ISO 27001: 2013.; [Consulta: 02 de mayo 2022]. Disponible en: https://repository.unad.edu.co/handle/10596/23186

[27] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Tarazona Anteliz, Javier Ricardo Leal Sandoval, Cherly Liliana, Diseño de un sistema de gestión de seguridad de la información para el área TI de la ESE Hospital Universitario Erasmo Meoz de Cúcuta basado en la norma ISO 27001:2013; [Consulta: 02 de mayo 2022]. Disponible en: https://repository.unad.edu.co/handle/10596/17414

El proyecto Diseño de un Sistema de Gestión de la Seguridad de la Información en la IPS Assalud de Corozal Sucre, mediante la Implementación de la Metodología Margerit (v3.0) y la Norma ISO 27001:2013, es una monografía donde se analizaran las vulnerabilidades, amenazas y riesgos en los activos informáticos de esta entidad con el propósito de garantizar la protección de estos activos en cada una de sus dimensiones garantizando así un buen funcionamiento del Sistema de Información de la IPS Assalud[28] .

- **DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN BAJO LA NORMA ISO 27001:2013 EN LA E.P.S ASMET SALUD:**

Trabajo de grado para la obtención el título de especialista en seguridad informática, proyecto aplicado, se inicia con una visión sobre una herramienta que brinda la posibilidad de medir la confidencialidad, integridad y disponibilidad entre los diferentes activos de información, que intuye la etapa para poder diseñar un Sistema de Gestión de la Seguridad de la Información basado en la norma ISO 27001:2013 y no de su implementación al interior de la E.P.S Asmet Salud en el municipio de Timana Huila[29] .

- **DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL ÁREA DE SISTEMA DE LA EMPRESA RYMCO S.A BAJO LA NORMA ISO IEC/27001:2013:**

Hoy en día nos encontramos que en algunas empresas en Colombia sus profesionales del área de informática, aún se encuentran llenos de tabúes, en cuanto a la protección de la información. Considerando que con el solo hecho de tener software y antivirus licenciados y de realizar periódicamente backup es

[28] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Díaz Ricardo, Luis Carlos, Diseño de un Sistema de Gestión de la Seguridad de la Información en la IPS Aassalud de Corozal Sucre, mediante la implementación de la metodología Magerit (v3.0) y la Norma ISO 27001:2013; [Consulta: 02 de mayo 2022]. Disponible en: https://repository.unad.edu.co/handle/10596/14386

[29] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Reyes Artunduaga, Jonathan Fernando, Diseño de un sistema de gestión de seguridad de información bajo la Norma ISO 27001:2013 en la E.P.S Asmet Salud; [Consulta: 02 de mayo 2022]. Disponible en: https://repository.unad.edu.co/handle/10596/27057

suficiente para estar protegidos ante posibles ataques informáticos. Es decir, aun no admiten la necesidad de implementar los Sistemas de Gestión de la Seguridad de la Información SGSI. Este proyecto es un diseño metodológico para implementación de un SGSI en el área de sistema de la empresa RYMCO S.A bajo la norma ISO IEC/27001:2013[30] .

- **DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL COLEGIO GERMÁN ARCINIEGAS I.E.D., BAJO LA NORMA TÉCNICA COLOMBIANA NTC ISO/IEC 27001:2013:**

Se realiza el diseño de un sistema de gestión de la seguridad de la información, para el Colegio Germán Arciniegas I.E.D., bajo la norma técnica colombiana NTC-ISO-IEC 27001:2013, que permita el aseguramiento de la información mediante el reconocimiento de la institución, sus necesidades, expectativas, la identificación de las partes interesadas, determinación del alcance del sistema dentro de la organización, la definición de la política de seguridad, de los roles y de las responsabilidades frente al sistema. Por otra parte, se identifican y analizan los riesgos a los que se encuentran expuestos los sistemas informáticos de la institución y la información en general; adicionalmente, se realizan los planes de acción para tratar los riesgos y se definen los controles, objetivos e indicadores para cumplir con el sistema de seguridad de la información. Finalmente, el sistema proveerá de medidas preventivas, procesos y controles para la seguridad de la información que garantice la disponibilidad, confiabilidad, e integridad de la información en el colegio Germán Arciniegas. Esto se llevará a cabo mediante la recolección de la información en cada una de las áreas de la IED, la realización del inventario de los activos informáticos de la Institución, el análisis de riesgos y la definición de procesos de seguridad de la información en la IED, acorde con las directrices dadas en la NTC-

[30] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Samper Ibañez, Pedro Antonioo, Diseño de un sistema de gestión de seguridad de la información en el área de sistema de la empresa Rymco S.A bajo la norma ISO IEC/27001:2013; [Consulta: 03 de mayo 2022]. Disponible en: https://repository.unad.edu.co/handle/10596/3987

ISO-IEC 27001:2013 y la definición de los procesos de seguridad de la información generada en la IED[31] .

- **DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA INTRANET DEL POLICLÍNICO DEL SUR OLAYA BOGOTÁ, BAJO LA NORMA ISO 27001:**

El presente documento tuvo como objetivo fundamental, el análisis y gestión de riesgos de la organización, el estudio de la metodología Magerit, y la norma ISO 27001. La seguridad de la información a nivel cotidiano tiene un papel importante en las organizaciones por esta razón se busca a través de un análisis y gestión de riesgos realizar la identificación llevando a cabo las diferentes acciones que se desarrollan dentro de la metodología Magerit, como lo son el análisis de activos, amenazas, el impacto y riesgo que estos presentan dentro de la Institución, para con estos datos luego llegar a la obtención de la matriz de riesgos con la finalidad de escoger los controles y objetivos más adecuados de la norma ISO 27001[32].

- **DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL ÁREA DE RECURSOS INFORMÁTICOS DE LA CONTRALORÍA DEPARTAMENTAL DEL META, SEGÚN LA NORMA ISO 27001:**

La oficina de Gestión de Recursos Informáticos, es la dependencia que se encarga de prestar el servicio de soporte TI, copias de seguridad, gestión de la navegación de internet, administración de los sistemas de información entre otros en la Contraloría Departamental del Meta, los cuales ayudan al normal funcionamiento de

---

[31] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Figueroa Cubillos, Carolina, Diseño de un sistema de gestión de seguridad de la información para el Colegio Germán Arciniegas I.E.D., bajo la norma técnica colombiana NTC ISO/IEC 27001:2013; [Consulta: 06 de mayo 2022]. Disponible en: https://repository.unad.edu.co/handle/10596/25633

[32] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Bolívar Leon, Yeinny Andrea, Diseño de un sistema de gestión de seguridad de la información en la intranet del policlínico del sur Olaya Bogotá, bajo la norma ISO 27001; [Consulta: 06 de mayo 2022]. Disponible en: https://repository.unad.edu.co/handle/10596/5513

los procesos misionales, así mismo es el área que se encarga de velar por los activos informáticos y la seguridad de la información de la entidad. De esta manera al diseñar el SGSI, se pretende dejar fija bases para una futura implementación del SGSI en la dependencia, mediante el uso de las mejores prácticas de seguridad como la norma ISO/IEC 27001:2013 apoyado en la metodología de gestión de riesgos MAGERIT y de esta manera establecer un plan para la continuidad de los servicios[33].

- **DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BAJO LA NORMA ISO/IEC 27001:2013, EN LA COOPERATIVA MULTIACTIVA DEL PERSONAL DEL SENA, EN BOGOTÁ:**

Este proyecto de titulación, presenta una descripción detallada de los objetivos, el alcance, los componentes, el funcionamiento, las ventajas y la metodología relacionada a la planificación para diseñar un modelo de Sistema de Gestión de Seguridad de la Información (SGSI), bajo la norma ISO/IEC 27001:2013 para la institución COOPSENA; comenzando con el estudio de la situación actual de la entidad desde la perspectiva de sus procesos críticos, normativas jurídicas, análisis y gestión de riesgos, tratamiento de riesgos; y finalizando con la gestión de la continuidad del negocio, todo con el fin de fomentar la seguridad de la información en dicha organización[34].

- **DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001 PARA LA DIRECCIÓN DE SISTEMAS DE LA GOBERNACIÓN DE BOYACÁ:**

---

[33] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Cazaran Buitrago, Olger Yonatan, Diseño de un sistema de gestión de seguridad de la Información en el área de recursos informáticos de la Contraloría Departamental del Meta, según la norma ISO 27001, bajo la norma ISO 27001; [Consulta: 06 de mayo 2022]. Disponible en: https://repository.unad.edu.co/handle/10596/17423

[34] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Ruiz Peña, José Higinio, Diseño de un sistema de gestión de seguridad de la información (SGSI) bajo la norma ISO/IEC 27001:2013, en la Cooperativa Multiactiva del personal del Sena, en Bogotá, bajo la norma ISO 27001; [Consulta: 06 de mayo 2022]. Disponible en: https://repository.unad.edu.co/handle/10596/17300

Este documento inicia con una introducción acerca de la importancia que tiene un diseño de sgsi basado en la norma ISO/IEC 27001, pretende minimizar riesgos a los que se encuentra expuesto la dirección de sistemas de la gobernación de Boyacá, utilizando la metodología Magerit donde permite realizar un análisis de los riesgos, análisis de los activos, valoración cuantitativa de los activos, identificación de amenazas, definición de los salvaguardas, aplicabilidad de los controles que conforma el SGSI, con el fin de realizar una evaluación de riesgos. La evaluación de riegos determinara que activos de la dirección de sistemas están en riesgo, para tomar las medidas adecuadas y mitigarlos, teniendo como objetivo principal garantizar la confidencialidad, disponibilidad, e integridad de la información de la dirección de sistemas de la gobernación de Boyacá[35].

- **POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA INSTITUCIÓN EDUCATIVA LUIS CARLOS GALÁN SARMIENTO, BASADOS EN LA NORMA ISO/IEC 27001:2013:**

Este trabajo de grado tiene como propósito verificar la situación actual de la institución Educativa Luis Carlos Galán Sarmiento, donde se evidencie los activos de la información mediante la metodología de MAGERIT Libro 2, identificando amenazas y vulnerabilidades a los activos y de allí definir controles acordes a la situación presentada, de acuerdo al anexo A de la norma ISO 27001:2013; dando políticas de seguridad a los controles que se definieron. En el primer capítulo se realiza un diagnóstico al colegio Luis Carlos Galán Sarmiento con el propósito de identificar los tipos de activos más relevantes, según metodología Magerit Libro 2 y de acuerdo a ello se clasifica según su tipo de Información para valorar las dimensiones de seguridad informática a estos activos. En el segundo capítulo se identifica las amenazas: internas/externas que pueden tener los activos de la

[35] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Contreras Esguerra, Lidia Constanza, Diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001 para la dirección de sistemas de la gobernación de Boyacá; [Consulta: 06 de mayo 2022]. Disponible en: https://repository.unad.edu.co/handle/10596/11895

institución y el riesgo que puede ocasionar a éstos. En el tercer capítulo se define los controles acordes para la institución educativa Luis Carlos Galán Sarmiento, de acuerdo al anexo A de la norma ISO 27001:2013. Por último, se propone políticas de seguridad de la información para la Institución Educativa Luis Carlos Galán Sarmiento teniendo en cuenta los controles aplicados de la norma ISO 27001:2013[36].

- **DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO/IEC 27001-27002 PARA EL ÁREA ADMINISTRATIVA Y DE HISTORIAS CLÍNICAS DEL HOSPITAL SAN FRANCISCO DE GACHETÁ:**

El documento presenta el diseño de un sistema de gestión de seguridad informática basado en la norma ISO/IEC 27001- 27002 versión 2013 para el área administrativa y de historias clínicas del Hospital San Francisco de Gachetá, el cual fue elaborado con la metodología MAGERIT, el documento muestra un análisis inicial de vulnerabilidades y amenazas a las que se ve expuesta la información de la entidad y de acuerdo a esta se diseña un SGSI para las áreas mencionadas en el proyecto cuyo fin es mitigar el riesgo y mejorar la seguridad de la información de acuerdo a los pilares establecidos por MAGERIT[37].

- **PLANTEAMIENTO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN APLICANDO LA NORMA NTC ISO/IEC 27001 - 27002 DEL 2013 EN EL PROCESO DE LA REVISIÓN TÉCNICO - MECÁNICA DEL CDA CORPOTRANS:**

---

[36] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Garrido Sánchez, Ana Lucia Bravo Lara, Pascual, Políticas de seguridad de la información para la Institución Educativa Luis Carlos Galán Sarmiento, basados en la norma ISO/IEC 27001:2013; [Consulta: 06 de mayo 2022]. Disponible en: https://repository.unad.edu.co/handle/10596/18515

[37] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Bojacá Garavito, Edgar Alonso, Diseño de un Sistema de Gestión de Seguridad Informática basado en la norma ISO/IEC 27001- 27002 para el área administrativa y de historias clínicas del Hospital San Francisco de Gachetá; [Consulta: 06 de mayo 2022]. Disponible en: https://repository.unad.edu.co/handle/10596/12685

El proyecto tiene como propósito implementar controles, procesos y procedimientos que le permitan conocer al administrador del sistema de gestión y la alta dirección la seguridad a nivel físico, lógico, y recurso humano, el objetivo fue, Plantear un sistema de gestión de seguridad de información que permita establecer políticas, controles y procesos en el Centro de Diagnóstico Automotor basados en la norma NTC ISO/IEC 27001 - 27002 del 2013 para proponer una mejora continua y preservar la confidencialidad, integridad y disponibilidad en los procesos de la revisión técnico - mecánica. La metodología utilizada se basó en el enfoque cuantitativo que permitió verificar el estado del CDA frente a los requisitos de las normas que establecen el cumplimiento para la seguridad informática y de información basándose en la NTC - ISO/IEC 27001, las conclusiones dieron cuenta de la identificación y estado actual tanto de hardware, como del software, aplicaciones web, la transferencia de información en línea y el personal en todo el proceso de revisión técnico - mecánica, es de vital importancia para conocer cuáles son los requisitos de cumplimiento en la prestación de sus servicios y las necesidades de mejora que cada uno de los mismos requiere[38].

- **DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA UNIDAD DE INFORMÁTICA, INGENIERÍA DE SISTEMAS Y TELEMÁTICA DE LA UNIVERSIDAD DE NARIÑO SOPORTADA EN LOS ESTÁNDARES MAGERIT E ISO/IEC 27001 Y 27002-2013:**

Cada día las instituciones de educación superior reconocen la importancia de la información como uno de los activos más importantes que debe ser manejado eficientemente, para garantizar ventajas dentro del campo administrativo y académico competidos en la actualidad, por lo que las instituciones incrementan su inversión en el uso de diferentes tecnologías tales como páginas web informativas, tecnologías de identificación por lector de huellas dactilares, llaves de hardware que

[38] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Giraldo Reina, Edna Rocío, Planteamiento del sistema de gestión de seguridad de información aplicando la Norma NTC ISO/IEC 27001 - 27002 del 2013 en el proceso de la revisión técnico - mecánica del CDA Corpotrans; [Consulta: 06 de mayo 2022]. Disponible en: https://repository.unad.edu.co/handle/10596/27058

permiten verificar identidades y otras herramientas como sistemas de alertas, cifrado de datos, etc. Una de estas tecnologías para el manejo de la información son los sistemas de información web, tales como portales web y sitios web que facilitan la interacción entre los usuarios y los servicios que pueden prestarse a través de ellos. Es claro que, en este contexto, el objetivo es el de proteger la información contra ataques internos y externos ya sean sabotajes informáticos para causar daños al hardware o al software del sistema. Este tipo de amenazas y vulnerabilidades pueden causar daños en la infraestructura física o en la información de varias formas, que van desde las más simples como desconectar el computador de la electricidad mientras se está trabajando, hasta las más complejas como el uso de programas lógicos destructivos, o el uso de los virus informáticos. Hoy en día ninguna organización está exenta de esta clase de vulnerabilidades, amenazas o ataques, que deben ser detectados a tiempo para así diseñar una serie de controles que las contrarresten, para lograrlo se han creado diferentes normas, entre las cuales existe la norma ISO/IEC 27000 que proporcionan un marco de gestión de la seguridad de la información que puede adaptarse por cualquier organización pública o privada[39].

- **DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (S.G.S.I) PARA EL CENTRO DE DATOS DE LA PERSONERÍA DE BOGOTÁ D.C. BAJO LAS NORMAS NTC-ISO-IEC 27001:2013 Y GTC-ISO-IEC 27002:2013:**

La gestión de la seguridad debe ser un proceso de mejora continua y de constante adaptación a los cambios en la organización, en cuanto a procesos de negocio y a la tecnología implicada. La seguridad de la información se desarrolla atendiendo a tres dimensiones principales, las cuales son, confidencialidad entendida como la garantía del acceso a la información únicamente de los usuarios autorizados,

[39] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Guerrero Angulo, Yezid Camilo, Diseño del sistema de gestión de seguridad de la información para la Unidad de Informática, Ingeniería de Sistemas y Telemática de la Universidad de Nariño soportada en los estándares Magerit e ISO/IEC 27001 y 27002-2013; [Consulta: 06 de mayo 2022]. Disponible en: https://repository.unad.edu.co/handle/10596/31718

integridad como la preservación de la información de forma completa y exacta y disponibilidad como la garantía del acceso a la información en el instante en que el usuario la necesita; la dedicación para una adecuada formulación de un SGSI debe ser establecida teniendo en cuenta la naturaleza de la entidad. El proyecto tiene como propósito formular un diseño del Sistema de Seguridad de la Información -SGSI- para el Centro de Datos de la Personería de Bogotá D. C. y así contribuir y garantizar la adecuada gestión de la seguridad en la entidad. En el centro de datos de la Personería de Bogotá se concentran los servidores, aplicativos y dispositivos críticos que soportan el eje funcional de la entidad; la no disponibilidad de los mismos, puede causar consecuencias graves para la imagen institucional y el cumplimiento de su misión. En el desarrollo de la presente propuesta, se aprecian los resultados producto del desglose de las etapas de Planificación, Ejecución, Seguimiento y Mantenimiento y se formulan varias oportunidades de mejora, dentro de las cuales se destacan como estrategias de continuidad del proyecto el autodiagnóstico del cumplimiento de compromisos, simulacros de materialización de riesgos y contratación de consultorías para realizar mediciones objetivas de la ejecución del sistema, tomando como metodología para el análisis de riesgos Magerit y para el desarrollo[40].

- **DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN LA NORMA ISO 27001: 2013 PARA LA RED INALÁMBRICA DE LA EMPRESA INNOVACIÓN GLOBAL S.A, UBICADA EN EL MUNICIPIO DE SIBUNDOY PUTUMAYO:**

El texto inicia con el respectivo resumen y palabras claves, continúa con la identificación de sus autores; posteriormente se presenta la introducción, planteamiento del problema justificación y objetivos respecto a la investigación que aborda la seguridad de la red inalámbrica como de los activos de información de la

[40] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Acosta Ubaque, Nubia Esperanza León Patiño, Tania Kruskaya, Diseño del Sistema de Gestión de Seguridad de la Información (S.G.S.I) para el centro de datos de la personería de Bogotá D.C. bajo las normas NTC-ISO-IEC 27001:2013 y GTC-ISO-IEC 27002:2013; [Consulta: 06 de mayo 2022]. Disponible en: https://repository.unad.edu.co/handle/10596/11940

empresa de Innovación Global S.A. En un segundo segmento se indica la referencia teórica que se tuvo en cuenta y que da soporte a la investigación, para continuar posteriormente con la descripción de la metodología y finalmente el desarrollo de la misma la cual enmarca los pasos para el diseño de un sistema de gestión de la seguridad de informática (SGSI), basada en la norma ISO/IEC 27001:2013 y el anexo A ISO/IEC 27002:2013, con el fin de solventar la situación de la red inalámbrica de la empresa en estudio, que permita determinar los controles y políticas de seguridad que mitiguen el riesgo al que se expone[41].

- **ANÁLISIS Y EVALUACIÓN DE RIESGOS DE SEGURIDAD INFORMÁTICA PARA LA CÁMARA DE COMERCIO DE LA DORADA, PUERTO BOYACÁ, PUERTO SALGAR Y MUNICIPIOS DE ORIENTE DE CALDAS:**

Debido a su crecimiento y la normatividad contemplada en la Ley 1581 de 2012 y su Decreto Reglamentario 1377 de 2013, Decreto 2042 de 2014 y al Código de Comercio, la Cámara de Comercio de La Dorada, Puerto Boyacá, Puerto Salgar y Oriente de Caldas, debe implementar sus Políticas de Seguridad Informática, y actualmente se carece de estas, se tienen un documento con algunas políticas, pero estas se quedan cortas ya que solo consideran aspectos muy básicos relativos a la seguridad de la información, el único inventario con que se cuenta es el que manejan en el área contable, el cual nada tiene que ver un inventario de activos de información. Ante este panorama se hace necesario realizar un análisis y evaluación de riesgos, para lo cual se realiza un inventario de activos de información, se determinan las amenazas y vulnerabilidades a que está expuesta la organización, aplicando Magerit V3, luego se realiza el análisis y evaluación de los riesgos, se verifica también la existencia de controles de acuerdo a las normas ISO 27001:2013

[41] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Jojoa Paz, Doris Esther Córdoba Cuaycal, Karol Martín, Diseño de un sistema de gestión de seguridad de la información (SGSI) basado en la norma ISO 27001: 2013 para la red inalámbrica de la empresa innovación global S.A, ubicada en el municipio de Sibundoy Putumayo; [Consulta: 06 de mayo 2022]. Disponible en: https://repository.unad.edu.co/handle/10596/6146

e ISO 27002:2013 y de acuerdo a los resultados obtenidos se realiza el documento entregable con los hallazgos y controles a implementar[42].

4.5 MARCO LEGAL:

- **NORMAS Y POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN:**

Establece reglas y lineamientos técnicos para la práctica paulatina de activos de los datos que minimice el peligro de daño de datos, accesos no autorizados, publicidad no controlada, duplicación y obstáculo premeditado de los datos dentro de la empresa[43].

- **MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN:**

Establecer las políticas que regulan la protección de los datos en el territorio organizacional de la mesa directiva del Gobierno DAPRE y mostrar en representación intermedia y razonable los elementos que conforman la administración de protección que deben saber, acatar y efectuar todos los funcionarios, contratistas, particulares en encargo administrativa, visitantes y terceros que presten sus servicios o tengan alguien que esté relacionado con el DAPRE, a cargo del liderazgo del Área de Tecnologías[44].

---

[42] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Cardona Castañeda, José Nayid Salcedo Ruiz, Willis Alberto, Análisis y evaluación de riesgos de seguridad informática para la Cámara de Comercio de la Dorada, puerto Boyacá, Puerto Salgar y municipios de oriente de Caldas; [Consulta: 07 de mayo 2022]. Disponible en: https://repository.unad.edu.co/handle/10596/14418

[43] LOS PATIOS NORTE DE SANTANDER; [Sitio web]; Colombia: Los patios norte de Santander; Oficina TIC Los Patios. Manual de Normas y Políticas de Seguridad de la Información. Ocaña, pág. 30; [Consulta: 21 de octubre 2021]. Disponible en: https://www.lospatios-nortedesantander.gov.co/Conectividad/InformesGEL/GT-D-05%20POLITICAS%20DE%20SEGURIDAD%20DE%20LA%20INFORMACION.pdf

[44] DEPARTAMENTO ADMINISTRATIVO DE LA PRESIDENCIA DE LA REPUBLICA; [Sitio web]; Colombia: DAPRE; Manual de Políticas de Seguridad de La Información, Política de seguridad del DAPRE, pág. 14; [Consulta: 21 de octubre 2021]. Disponible en: https://dapre.presidencia.gov.co/dapre/DocumentosSIGEPRE/M-TI-01-Manual-Politicas-Seguridad-Informacion.pdf

- **SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN:**

Conduce a la conservación de la confidencialidad, lealtad, acceso a los recursos de los datos, permitiendo certificar la privacidad de los datos, mediante la diligencia de una causa de encargo de las debilidades, brindando seguridad a las partes interesadas acerca del adecuado encargo de los riesgos para su solución[45].

- **LEY 1273 DE 2009: "DE LA PROTECCIÓN DE LA INFORMACIÓN Y DE LOS DATOS"** [46]

Esta ley hay que destacar los siguientes artículos, los cuales son los más relevante:

Artículo 269A: El que sin autorización viole o acceda a un sistema informático protegido en contra de la voluntad de quien tenga el legítimo derecho. Tendrá una pena de prisión de cuatro (4) a ocho (8) años y una sanción de 100 a 1000 salarios mínimos legales mensuales vigentes .

ARTÍCULO 269B: El que sin tener la potestad obstaculice el acceso o normal funcionamiento a los datos de un sistema informático o red de telecomunicaciones; tendrá la pena de cuatro (4) a ocho (8) años y una sanción de 100 a 1000 salarios mínimos legales mensuales vigentes; esto siempre y cuando la conducta no constituya delito sancionado con una pena mayor .

ARTÍCULO 269C: El que sin contar con orden emitida por un ente legal intercepte datos informáticos de origen a destino o en el interior de un sistema informático; tendrá la pena de tres (3) a seis (6) años .

---

[45] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES; [Sitio web]; Colombia: MINTIC; Modelo de Seguridad y Privacidad de la Información, Modelo de seguridad y privacidad de la información, pág. 20; [Consulta: 21 de octubre 2021]; Disponible en: https://mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

[46] EN TIC CONFIO; [Sitio web]; En Tic confió; LEY 1273 DE 2009, De la protección de la información y de los datos; [Consulta: 20 de noviembre 2021]. Disponible en: https://www.enticconfio.gov.co/images/stories/normatividad/Ley_1273_de_2009%20.pdf

ARTÍCULO 269E: El que, sin autorización, produzca, trafique, adquiera, distribuya, venda, envíe, ingrese o extraiga del territorio nacional software malicioso; tendrá una pena de prisión de cuatro (4) a ocho (8) años y una sanción de 100 a 1000 salarios mínimos legales mensuales vigentes .

● **LEY 1581 DE 2012: "LEY ESTATUTARIA"[47]:**

Esta ley fue creada con el fin de garantizar la protección almacenamiento y buen uso de los datos personales, si su empresa cuenta con una afiliación a la Cámara de Comercio de Colombia y cumple con alguna de las siguientes afirmaciones :

- Si recolecta datos personales de diversos titulares llámese clientes, proveedores, contratistas, entre otros
- Almacena, usa o circula datos persones bien sea en archivos físicos o electrónicos.
- No cuenta con una manual de políticas y procedimiento de protección de datos personales.

La empresa deberá hacer uso de lo establecido en la ley de protección de datos personales.

[47] DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA; [Sitio web]; Función pública; Ley 1581 de 2012, Ley Estatutaria; [Consulta: 21 de noviembre 2021]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

5 DISEÑO METODOLÓGICO

5.1 METODOLOGÍA DESCRIPTIVA Y EXPERIMENTAL

Para la realización del proyecto aplicado se escoge la metodología descriptiva y experimental la cual tiene como fin describir y evaluar ciertas características de una situación particular en uno o varios puntos del tiempo. Además, se realiza un análisis de datos recolectados para descubrir las variables que tienen relación entre sí.

En esta metodología los resultados se pueden interpretar desde distintos ángulos, dicho esto, se asevera que utilizan métodos cualitativos.

Este tipo de metodología se sitúa en el presente, recoge y tabula la información para luego ser analizados e interpretados de forma imparcial[48].

5.2 POBLACIÓN Y MUESTRA

Se consideraron todos y cada uno de los funcionarios de la organización EAR construcciones, que laboran en la oficina de tecnologías de la información y las comunicaciones, como muestra poblacional para el ejercicio se contemplan 13 empleados para una muestra del 100% de la población. La distribución del personal muestreo se distribuyen de la siguiente manera donde hay entre 2 funcionarios por cada cargo.

[48] MONOGRAFIAS; [Sitio web]; Monografías; Método descriptivo y experimental; [Consulta: 11 de diciembre 2021]. Disponible en: https://www.monografias.com/docs/metodo-descriptivo-y-experimental-FKLDMCGPJ8G2Yhttps://www.monografias.com/docs/metodo-descriptivo-y-experimental-FKLDMCGPJ8G2Y

Administrados de servidores, desarrolladores web, administrador de redes, administrador de directorio activo, 2 ingenieros de mesa de servicio, administrador de firewall y administrador de licenciamientos.

5.3 TÉCNICAS PARA RECOLECCION DE INFORMACIÓN

Para recolectar la información como elaboración para el desarrollo del proyecto se aplica la técnica de observación, sumado a la experticia del profesional que elaborará el inventario de los activos de información, insumo que conlleva a la identificación de vulnerabilidades presentes sobre cada activo de información, se realizaron a través de las entrevistas, la estimación de los activos de información conforme lo requiera la metodología MAGERIT.

5.4 METODOLOGIA DE DESARROLLO:

Para el desarrollo de este proyecto se utilizó la metodología MAGERIT para la identificación y gestión del riesgo, vulnerabilidades y amenazas asociadas a los activos de información identificados en el área de la oficina de tecnologías de la información y las comunicaciones, con el objetivo de concluir de forma exitosa el proyecto y poder establecer los controles para proteger los activos de información.

Dentro de la metodología se desplegarán unas actividades que se describirán a continuación:

5.4.1 Identificación de los activos de información presentes en la dependencia de la oficina de tecnologías de la información y las comunicaciones de la empresa EAR construcciones.

Actividad. Clasificar e identificar los activos de información: Se realizará la identificación de los activos de información para realizar el registro dentro de la matriz de MAGERIT.

5.4.2. Establecer riesgos, vulnerabilidades. Amenazas y riesgos en los activos de información ya identificados.

Actividad. Una vez identificadas las vulnerabilidades, amenazas y riesgos se procederá a dar una valoración a cada uno de los activos de acuerdo con la metodología MAGERIT.

5.4.2 Diseñar de un plan de tratamiento del riesgo a partir del análisis de las vulnerabilidades detectadas para cada activo de información.

Actividad. Se debe realizará el plan de tratamiento del riesgo a partir de la detección de vulnerabilidades para cada activo de información, se establecerán salvaguardas y controles necesarios para minimizar y en lo posible la mitigación del riesgo.

6 ANALIZAR LA SEGURIDAD DE LOS ACTIVOS DE INFORMACIÓN DE LA ORGANIZACIÓN EAR CONSTRUCCIONES MEDIANTE UNA METODOLOGÍA DE GESTIÓN DE RIESGO CON EL FIN DE TENER IDENTIFICADO EL ESTADO ACTUAL DE LAS VULNERABILIDADES, AMENAZAS Y RIESGOS.

6.1 ACTIVIDADES OBJETIVO 1:

- Identificación y clasificación de los activos de información de la organización EAR Construcciones.

- Diseñar a la empresa procedimientos y/o formatos para la realización de solicitudes acordes a los lineamientos de la empresa.

Desarrollo del Objetivo 1:

ITEM 1: Identificación y clasificación de los activos de información de la organización EAR Construcciones.

Identificación y clasificación de los activos de información obtenidos de la empresa EAR Construcciones y se utiliza dando cumplimiento a la metodología de MAGERIT como primer paso ya que utiliza una metodología sistemática para analizar los riesgos derivados del uso de las tecnologías de la información y las comunicaciones para implementar medidas y controles adecuados para la mitigación del riesgo.

Dentro de los procesos de gestión del riesgo es la identificación de los activos de información a los cuales posteriormente se les realizará la valoración y con esto determinar los riesgos y amenazas asociados al activo y así realizar la mitigación del mismo.

6.1.1 Situación real de EAR Construcciones:

- **Componentes de diagnóstico:** Fundamentados por los lineamientos de la norma ISO 27001:2013 en el numeral 16 con el cual se realiza el diseño de preguntas para ser aplicados a la organización EAR construcciones, que ofrece servicios de obras civiles a grandes, medianas y pequeñas empresas o particulares en todo el territorio nacional.

Con la herramienta de uso aplicativo se presentaron los siguientes datos (encuesta), donde se observa el nivel de madurez para poder determinar los riesgos de acuerdo al manejo que le dan a los incidentes de ciberseguridad, para poder tener un mejor panorama y así mitigar estas brechas que la organización hoy en día tiene, por motivos de teletrabajo al interior de la empresa se realizó una encuesta a los empleados de las áreas de sistemas, la parte administrativa y documental donde ocupaban cargos asistenciales, técnicos, profesionales y especializados. Dicha encuesta está conformada por 11 preguntas claves, estas encuestas se realizaron a través de la herramienta de Google forms y la distribución de la misma se realizó mediante correo corporativo o se compartió la url a través del WhatsApp de los empleados de la organización.

Cuadro 1 - Activos de información

DATOS DEL ACTIVO DE INFORMACION			
	NOMBRE DEL ACTIVO DE INFORMACIÓN	PROCESO PROPIETARIO DEL ACTIVO	TIPO DE ACTIVO
1	Windows Server R8 2008	Oficina TIC	SOFTWARE
2	Server NAS (10 TB) / Soft. Admin	Oficina TIC	HARDWARE
3	DRIVE (10 TB)	Oficina TIC	SERVICIOS
4	Antivirus	Oficina TIC	SOFTWARE
5	Equipos de comunicaciones/LAN/WAN	Oficina TIC	HARDWARE
6	Equipos de seguridad perimetral Firewall	Oficina TIC	HARDWARE
7	VPN	Oficina TIC	SERVICIOS
8	Suite Office	Oficina TIC	SOFTWARE

9	Buzón de correo electrónico (Outlook)	Oficina TIC	SERVICIOS
10	Software Contable (Financiera)	Oficina TIC	SOFTWARE
11	Equipos de escritorio (30), equipos portátiles (6)	Oficina TIC	HARDWARE
12	Pool de licencias Windows (XP,7,10)	Oficina TIC	SERVICIOS
13	Personal que labora en esta área	Oficina TIC	PERSONAL
14	Suite de AutoCAD - Dibujantes	Creativos	SOFTWARE
15	Server Directorio Activo	Oficina TIC	HARDWARE
16	Server Impresión	Oficina TIC	HARDWARE
17	SST (Salud y seguridad en el trabajo)	Talento Humano	PERSONAL
18	Archivos (Documentos Físicos)	Administrativa	PERSONAL
19	Almacén (Bodega Insumos)	Administrativa	PERSONAL
20	Software Nomina	Talento Humano	SOFTWARE
21	Router	Oficina TIC	SOFTWARE
22	Hub	Oficina TIC	SOFTWARE
23	Archivador documental	Administrativa	DATOS

Fuente 2 - Elaboración propia

En el cuadro anterior se puede evidenciar los nombres de los activos de información, quien es el propietario de dicho activo de información una vez realizada la identificación y el tipo de activo al cual pertenece.

Ilustración 2 - Valoración de los activos de información

DIMENSION					ATRIBUTOS									UBICACIÓN	
Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	¿Es activo de información de terceros o de clientes que debe protegerse?	¿Activo de información que debe ser restringido a un número limitado de empleados?	Activo de información que debe ser restringido a personas externas	Activo de información que puede ser alterado o comprometido para fraudes ó corrupción	Activo de información que es muy crítico para las operaciones internas	Activo de información que es muy crítico para el servicio hacia terceros	Activo de información que en caso de ser conocido, utilizado o modificado por alguna persona o sistema sin la debida autorización, impactaría negativamente a los sistemas y/o procesos de la empresa, de manera:			Físico	Electrónico
											Leve	Importante	Grave		
A	A	A	A	A	NO	SI	SI	SI	SI	SI		X		X	
M	A	A	M	M	NO	SI	SI	SI	SI	SI			X	X	
B	B	B	B	MA	SI	SI	SI	SI	SI	SI		X			X
M	M	M	A	A	SI	SI	SI	NO	NO	NO	X				X
A	A	A	A	A	NO	SI	SI	SI	SI	SI		X		X	
A	A	A	A	A	NO	SI	SI	SI	SI	SI			X	X	
A	A	A	A	A	NO	SI	SI	SI	SI	SI		X			X
MB	M	MB	MB	M	SI	SI	SI	NO	NO	NO	X				X
M	MB	M	M	MB	SI	SI	SI	SI	SI	SI		X			X
A	A	A	A	A	SI	SI	SI	SI	SI	SI			X		X
M	M	A	A	A	NO	SI	SI	SI	NO	NO	X			X	
A	A	M	M	M	NO	SI	SI	NO	NO	NO	X				X
A	A	A	A	A	NO	SI	SI	SI	SI	SI		X		X	
M	M	B	M	B	SI	SI	SI	SI	SI	SI		X			X
A	A	A	A	A	NO	SI	SI	SI	SI	SI		X		X	
B	B	B	B	MB	NO	SI	SI	NO	NO	NO	X			X	
A	A	A	A	A	NO	SI	SI	NO	NO	NO	X			X	
A	A	A	A	A	NO	SI	SI	SI	NO	NO	X			X	
A	A	A	A	A	NO	SI	SI	SI	SI	SI		X		X	
A	A	A	A	A	SI	SI	SI	SI	SI	SI		X			X

Fuente 3 - Elaboración propia

En la ilustración anterior se puede apreciar la valoración que se le dio a cada uno de los activos de información mediante la matriz de Magerit[49].

Ilustración 3 - Resultado de la valoración del riesgo

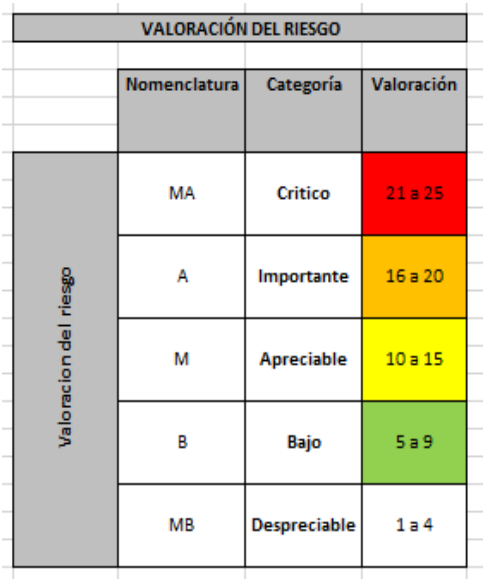
	NOMBRE	RIESGO	AUTENTICIDAD	TRAZABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR
1	Windows Server R8 2008	IMPORTANTE	20	20	20	20	20	20
2	Server NAS (10 TB) / Soft. Admin	IMPORTANTE	15	20	20	15	15	17
3	DRIVE (10 TB)	APRECIABLE	9	9	9	9	25	12
4	Antivirus	IMPORTANTE	15	15	15	20	20	17
5	Equipos de comunicaciones/LAN/WAN	IMPORTANTE	20	20	20	20	20	20
6	Equipos de seguridad perimetral Firewall	IMPORTANTE	20	20	20	20	20	20
7	VPN	IMPORTANTE	20	20	20	20	20	20
8	Suite Office	BAJO	4	15	4	4	15	8
9	Buzón de correo electrónico (Outlook)	APRECIABLE	15	4	15	15	4	11
10	Software Contable (Financiera)	IMPORTANTE	20	20	20	20	20	20
11	Equipos de escritorio (30), equipos portátiles (6)	IMPORTANTE	15	15	20	20	20	18
12	Pool de licencias Windows (XP,7,10)	IMPORTANTE	20	20	15	15	15	17
13	Personal que labora en esta área	IMPORTANTE	20	20	20	20	20	20
14	Dibujantes - Suite de AutoCAD	APRECIABLE	15	15	9	15	9	13
15	Server Directorio Activo	IMPORTANTE	20	20	20	20	20	20
16	Server Impresión	BAJO	9	9	9	9	4	8
17	SST (Salud y seguridad en el trabajo)	IMPORTANTE	20	20	20	20	20	20
18	Archivos (Documentos Fisicos)	IMPORTANTE	20	20	20	20	20	20
19	Almacen (Bodega Insumos)	IMPORTANTE	20	20	20	20	20	20
20	Software Nomina (Talento Humano)	IMPORTANTE	20	20	20	20	20	20
21	Router	IMPORTANTE	15	20	20	15	20	18
22	Hub	APRECIABLE	9	9	9	15	15	11
23	Archivador documental	IMPORTANTE	15	15	20	20	20	18

Fuente 4 - Elaboración propia

[49] SEMILLEROCEROSYUNO.COM; [Sitio web]; Matriz de Riesgos Magerit - Luis Fernando Zambrano; [Consulta: 28 de septiembre de 2021]. Disponible en: semillerocerosyuno.com/wp-cont.../Matriz-Version-5.3-29.04.2021-1.xls

En la ilustración anterior se puede observar el nivel de riesgo que tiene cada activo de información una vez se le asignó un valor teniendo como resultado la valoración del riesgo.

Ilustración 4 - Muestra para valoración del riesgo



VALORACIÓN DEL RIESGO			
	Nomenclatura	Categoría	Valoración
Valoracion del riesgo	MA	Critico	21 a 25
	A	Importante	16 a 20
	M	Apreciable	10 a 15
	B	Bajo	5 a 9
	MB	Despreciable	1 a 4

Fuente 5 - Elaboración propia

En la ilustración anterior se puede observar la forma en la que se mide el riesgo y como se le asigna un valor a cada activo de información mediante los rangos que nos da la metodología de magerit.

Ilustración 5 - Clasificación general de los activos

Clasificación general y Número de activos	
Tipo de activo	**Cantidad**
Tipo Dato	1
Tipo Claves Criptograficas	0
Tipo Servicio	4
Tipo Software	6
Tipo Hardware	6
Tipo Comunicaciones	2
Tipo Soporte de Información	0
Tipo Equipamento Auxiliar	0
Tipo Instalaciones	0
Tipo Personal	4
Total de Activos	**23**

Fuente 6 - Elaboración propia

En la ilustración anterior se puede tener un inventario de la clasificación del riesgo según los activos de información que posee la empresa EAR Construcciones.

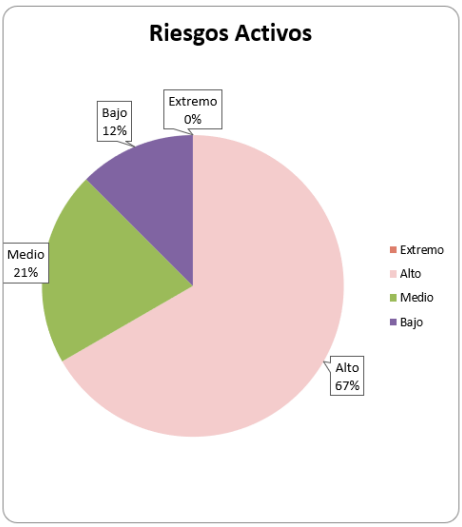
Ilustración 6 - Clasificación según valor

Clasificación de activos según su valor	
Número de activos de clientes o terceros que deben protegerse	10
Activos de información que deben ser restringidos a un número limitado de empleados	23
Número de activos de información que deben ser restringidos a personas externas	23
Activos de información que pueden ser alterados o comprometidos para fraudes o corrupción	18
Número de activos de información que son muy críticos para las operaciones internas	16
Número de activos de información que son muy críticos para el servicio hacia terceros	16

Fuente 7 - Elaboración propia

En la ilustración anterior se puede ver la clasificación de los activos de información según el valor que se le dio al momento de su evaluación.

Ilustración 7 - Estadísticas de riesgos de los activos



Fuente 8 - Elaboración propia

En la ilustración anterior se puede observar una estadística tipo torta donde se ve de forma porcentual los riesgos de los activos.

Ilustración 8 - Resumen del nivel de riesgo de los activos

Resumen de nivel de riesgo en los activos	
Extremo	0
Alto	16
Medio	5
Bajo	3

Fuente 9 - Elaboración propia

En la ilustración anterior se puede evidenciar un resumen de nivel de riesgo de los activos de información.

Ilustración 9 - Resumen valoración de los activos

Resumen de Valoración de los activos en escala C.C Eficiente					
Nombre	**Riesgo**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Valor**
Windows Server R8 2008	ALTO	6	6	6	6
Server NAS (10 TB) / Soft. Admin	MEDIO	6	5	5	5
DRIVE (10 TB)	MEDIO	3	3	9	5
Antivirus	MEDIO	5	5	5	5
Equipos de comunicaciones/LAN/WAN	ALTO	6	6	6	6
Equipos de seguridad perimetral Firewall	ALTO	6	6	6	6
VPN	MEDIO	5	5	5	5
Suite Office	ALTO	6	6	6	6
Buzón de correo electrónico (Outlook)	ALTO	6	6	6	6
Software Contable (Financiera)	MEDIO	5	5	5	5
Equipos de escritorio (30), equipos portátiles (6)	ALTO	6	6	6	6
Pool de licencias Windows (XP,7,10)	BAJO	3	5	3	4
Personal que labora en esta área	ALTO	6	6	6	6
Dibujantes - Suite de AutoCAD	BAJO	3	3	3	3
Server Directorio Activo	ALTO	6	6	6	6
Server Impresión	ALTO	6	6	6	6
SST (Salud y seguridad en el trabajo)	ALTO	6	6	6	6
Archivos (Documentos Fisicos)	ALTO	6	6	6	6
Almacen (Bodega Insumos)	ALTO	6	6	6	6
Software Nomina (Talento Humano)	BAJO	3	3	3	3
Router	ALTO	6	6	6	6
Hub	ALTO	6	6	6	6
Archivador documental	ALTO	6	6	6	6

Fuente 10 - Elaboración propia

6.1.1.1 Análisis de resultados:

Como se observó en la encuesta anteriormente presentada al gerente de la organización, de los cargos asistenciales, técnicos, profesionales y especializados de la organización EAR Construcciones estuvo conformado por 11 preguntas para lo cual se enfocaron en la identificación de cómo se gestionan los incidentes de ciber seguridad dentro de la organización.

Esta encuesta nos permite observar que la empresa tiene varias fallas mostrando las debilidades que se están presentando dentro de la misma, dicho esto se sugiere crear un plan de gestión para la mitigación de incidentes en ciberseguridad.

Con base a lo anterior es de anotar que actualmente la organización no cuenta con un modelo de gestión, procesos, procedimientos y guías para resolver incidentes en ciberseguridad, esto es una debilidad grande para la empresa ya que gracias a esto han sufrido distintos ataques de ransomware y aún no saben cómo mitigar estas falencias y así poder salvaguardar sus activos de información y toda la plataforma tecnológica de TI.

Hablando con el ingeniero encargado de seguridad de la información nos hace mención que no cuentan con un formato o protocolo a seguir para poder reportar estos incidentes, no se sabe cómo medir el riesgo que causa esto al momento de realizar una actividad o culminar con un proyecto y poder prestar el servicio de almacenado seguro de la información. El no poseer estos controles es una gran amenaza para la información que EAR Construcciones maneja ya que pueden seguir sufriendo distintos ataques de ciberseguridad y así poner en peligro toda la información que ellos manejan lo cual pondría en peligro a sus clientes y el Core de tu trabajo.

ITEM 2: Diseñar a la empresa procedimientos y/o formatos para la realización de solicitudes acordes a los lineamientos de la empresa.

Para el desarrollo de este objetivo se realizó el acompañamiento a cada una de las áreas de la Organización E.A.R Construcciones evidenciando cada uno de los procesos realizados en su cotidianidad, esta información recolectada y suministrada por cada una de las dependencias, es la base principal para la elaboración de los formatos, guías, procedimiento entre otros.

Ilustración 10 - Actividades: Creación de documentos ITEM 2, Objetivo 1

Fuente 11 - Elaboración propia

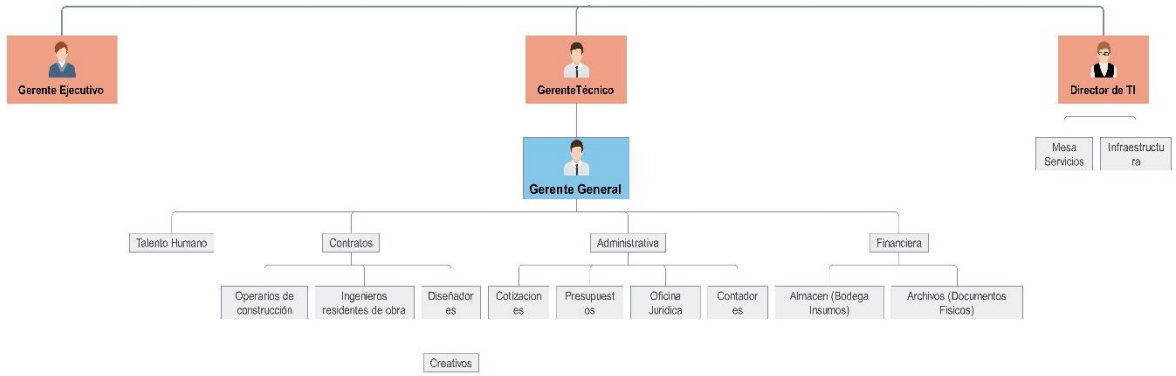
7 PROPONER CONTROLES DE SEGURIDAD BASADOS EN LA GUÍA DE BUENAS PRÁCTICAS ISO/IEC 27002:2013, PARA LA MITIGACIÓN DEL RIESGO ASOCIADO A LOS ACTIVOS DE INFORMACIÓN PARA LA ORGANIZACIÓN EAR CONSTRUCCIONES.

Una vez identificada las vulnerabilidades se proponen los controles de seguridad que permitan mitigar las amenazas y riesgos de acuerdo a la Norma ISO/IEC 27002:2013 teniendo en cuenta la valoración de todos los activos de información desarrollados en la metodología MAGERIT. Dicho esto, algunos de los controles a proponer dentro de la organización son el cambio seguro y periódico de contraseñas, manejar un control de acceso para los distintos puntos físicos de la organización, cifrado de la información que se almacena dentro de los servidores de la empresa, realizar un aseguramiento adecuado a los equipos de telecomunicaciones de la empresa, procesos y/o procedimientos para realizar el

buen manejo y tratamiento de la información, hacer uso de la política de protección de datos para salvaguardar la información de la empresa y terceros de acuerdo con la Ley de protección de datos personales (1581 de 2012), entre otros.

7.1.1 PRINCIPALES RIESGOS Y VULNERABILIDADES:

Ilustración 11 - Estructura Organizacional EAR Construcciones



Fuente 12 - Elaboración propia

Como se observa en la estructura organizacional de EAR Construcciones donde se puede identificar cada una de las dependencias por la cual está constituida la empresa y sus niveles de jerarquía dentro de ella.

7.1.2 Inventario de organización EAR Construcciones:

Para poder realizar un levantamiento e identificación de los riesgos y vulnerabilidades que tiene la organización, se debe hacer un levantamiento de la información (inventario), para conocer la infraestructura actual de la empresa, clasificación y tipo con la que cuenta para así poder catalogar cada uno de ellos respecto a los procesos misionales que apoyan.

Para poder dar un dictamen a los activos de información utilizaremos un nivel de criticidad para darle importancia a cada uno de estos y poder determinar la protección y nivel de seguridad que deben tener al interior del área de trabajo.

EAR Construcciones actualmente tiene a su disposición una variedad de computadores, portátiles, diversidad en sus sistemas operativos, activos de información para lo cual son utilizados para generar la diversidad de informes a los clientes, cotizaciones o simplemente llevar el presupuesto de cada proyecto que ellos realizan donde evidencian los gatos de cada insumo que necesitan.

7.1.3 NIVELES DE RIESGOS DE LA EMPRESA:

Después de realiza el análisis de como llevan a cabo sus actividades diarias en los equipos de la organización se puede observar que la información trabajada día a día no está siento alojada en el file server de la organización, afrontando un riesgo inminente de pérdida de la información al poderse dañar un sistema operativo o ingreso de ataque ransomware.

No poseen una política de bloqueo de sesiones de equipos, contraseñas seguras entre otras, se evidencia una falta seguridad en la navegación web de cada equipo ya que, al tener un firewall, pero mal parametrizado, los usuarios tienen acceso a distintos sitios web no seguros y así poner en riesgo toda la información de la organización.

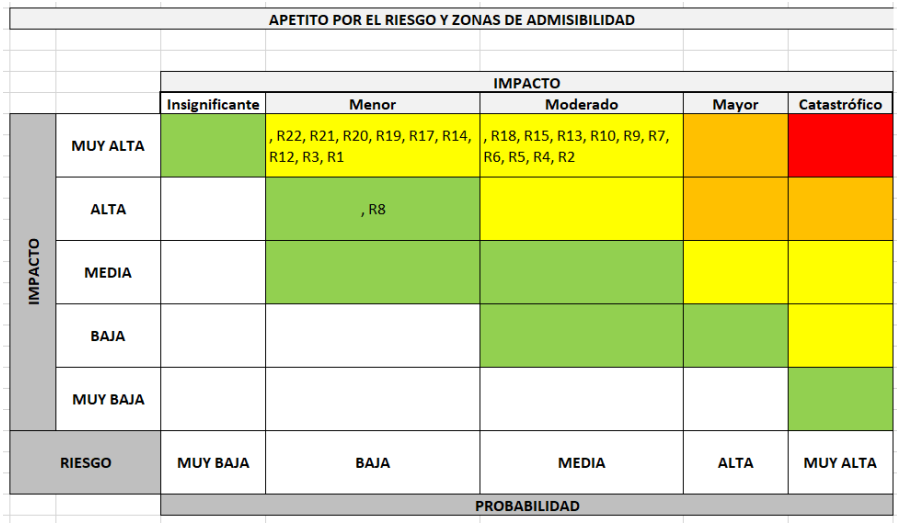
Primeramente se determinan cuáles son las actividades que la organización realiza con frecuencia para poder saber si estas actividades son sí o no rutinarias, una vez obtenida esta información se procede a la clasificación del riesgo según los valores asignados ya sean por probabilidad o severidad de acuerdo a la ocurrencia de un evento, riesgo o amenaza y se finalizaría con una valoración del riesgo para obtener el nivel bajo, medio o alto para con esta información la organización acepta el riesgo y vive con él o se realiza proceso de mitigación.

Para determinar los niveles del riesgo: se basa en lo estipulado por lo establecido en la ISO 73:2009, el cual mide el nivel de riesgo según el impacto que tenga por la probabilidad de que exista el suceso o el evento.

7.1.4 MATRIZ DE RIESGOS:

Mediante el mapa que se presenta a continuación se puede observar un inventario de los activos de información que tienen menor riesgos, riesgos medios, riesgos asumibles y altos. Esto se realiza con el propósito de tomar acciones para mitigar los riesgos y alcanzar un alto grado de madurez de los activos de información.

Ilustración 12 - Mapa de riesgos



Fuente 13 - Elaboración propia

Una vez realizada la valoración del riesgo a cada uno de los activos de información encontramos que algunos activos se encuentran con riesgo menor y otros moderados, como en la valoración solo se observan la nomenclatura con el R seguido del número de activo de información les presentamos una tabla con la estructura de dichos activos.

Finalizada la valoración se puede observar que la organización EAR Construcciones no actualmente no tiene activos de información con riesgo mayor y/o catastrófico.

Cuadro 2 - Inventario Matriz de Riesgos

INVENTARIO MATRIZ DE RIESGO			
NOMENCLATURA	**TIPO ACTIVO**	**NOMBRE ACTIVO**	**IMPACTO / RIESGO**
R22	Datos	Archivador documental	Muy alto / Menor
R21	Hardware	Hub	Muy alto / Menor
R20	Hardware	Router	Muy alto / Menor
R19	Personal	Almacén (Bodega Insumos)	Muy alto / Menor
R17	Personal	SST (Salud y seguridad en el trabajo)	Muy alto / Menor
R14	Software	Dibujantes - Suite de AutoCAD	Muy alto / Menor
R12	Servicios	Pool de licencias Windows (XP,7,10)	Muy alto / Menor
R3	Servicios	Server NAS (10 TB) / Soft. Admin	Muy alto / Menor
R1	Software	Windows Server R8 2008	Muy alto / Menor
R18	Software	Software Nomina (Talento Humano)	Muy alto / Moderado
R15	Hardware	Server Directorio Activo	Muy alto / Moderado
R13	Personal	Personal que labora en esta área	Muy alto / Moderado
R10	Software	Software Contable (Financiera)	Muy alto / Moderado
R09	Servicios	Buzón de correo electrónico (Outlook)	Muy alto / Moderado
R7	Servicios	VPN	Muy alto / Moderado
R6	Hardware	Equipos de seguridad perimetral Firewall	Muy alto / Moderado
R5	Hardware	Equipos de comunicaciones/LAN/WAN	Muy alto / Moderado
R4	Servicios	Antivirus	Muy alto / Moderado
R2	Auxiliar	Server NAS (10 TB) / Soft. Admin	Muy alto / Moderado
R8	Software	Suite Office	Alto / Menor

Fuente 14 - Elaboración propia

Una vez analizada la información obtenida por la metodología de Magerit se pueden observar varios de los activos de información en un riesgo alto, es por esto que se le recomienda a la organización comenzar a trabajar en la elaboración de procedimientos, guías las cuales deberán estar alineadas para mitigar dichos riesgos.

Estos procedimientos van desde la creación de usuarios, cambio de contraseñas, escritorio seguro, autobloqueo de estaciones de trabajo, cambio de contraseña periódicamente administrado desde el directorio activo entre otros, una vez analizada la información obtenida por la metodología de Magerit se pueden observar varios de los activos de información en un riesgo alto, es por esto que se le recomienda a la organización comenzar a trabajar en la elaboración de procedimientos, guías las cuales deberán estar alineadas para mitigar dichos riesgos.

Estos procedimientos van desde la creación de usuarios, cambio de contraseñas, escritorio seguro, autobloqueo de estaciones de trabajo, cambio de contraseña periódicamente administrado desde el directorio activo entre otros.

Dicho esto, y una vez implementados los controles para mitigar los riesgos la empresa EAR Construcciones deberá realizar como mínimo una vez al año una auditoría interna para verificar que se estén cumpliendo.

8 DISEÑAR POLÍTICAS DE SEGURIDAD, BASADO EN EL ANÁLISIS DE RIESGO CON EL FIN DE ALINEARSE A LAS NECESIDADES DE LA ORGANIZACIÓN EAR CONSTRUCCIONES.

Se va a realizar un escrito donde se describe las políticas de seguridad de la información definidos por la Alta Gerencia de la empresa EAR Construcciones tomando como base la Norma ISO/IEC 27011 y las diferentes recomendaciones definidas en el estándar ISO/IEC 27002.

Lo primordial para la organización es poder establecer y dar a conocer las medidas organizacionales, técnicas, físicas y legales, necesarias para la protección de la confidencialidad, integridad y disponibilidad de los activos de información frente a los posibles Con base en lo anterior, la Seguridad de la Información es una prioridad para la entidad EAR Construcciones y por lo tanto es responsabilidad de todos sus funcionarios, contratistas, proveedores y aliados velar por el cumplimiento de cada una de las políticas y controles establecidos en el presente escrito.

Su objetivo riesgos que se encuentran expuestos, disponiendo de los recursos necesarios que garanticen el progreso del Sistema de Gestión de Seguridad de la Información en la organización EAR Construcciones.

8.1.1 ALCANCE DE LAS POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

De manera genérica a continuación se entrega un texto guía para la elaboración de la política general de seguridad de la información, este puede ser base del desarrollo

de dicho documento ya que contempla los principios básicos a tener en cuenta en su elaboración dentro de la planeación del sistema de gestión de seguridad de la información en una entidad.

Por el presente escrito de Seguridad de la Información se adoptan políticas internas alineadas a lo descrito en la política general de seguridad y privacidad de la información de acuerdo al (articles-5482_G2_Politica_General) de MINTIC[50]., así:

1. EAR-AC-001 - Acuerdo Confidencialidad VPN
2. EAR-PO-001 - Política Escritorio y Pantalla Limpia
3. EAR-PO-002 - Política de Protección de Datos Personales
4. EAR-PR-001 - Procedimiento de Gestión del Cambio
5. EAR-FT-001 - Formato Instalación y Desinstalación de Software
6. EAR-FT-002 - Actualización Elementos Informáticos
7. EAR-FT-003 - Formato Instalación Teletrabajo (Visita 1)
8. EAR-FT-004 - Formato Instalación Teletrabajo (Visita 2)
9. EAR-FT-005 - Formato Acta Instalación e Implementación Teletrabajo
10. EAR-FT-006 - Formato Actualización Elementos Informáticos
11. EAR-GS-001 - Guía Para La Realización de Copias de Respaldo
12. EAR-GS-002 - Guía Para La Creación de Usuarios de Red y Correo D.A
13. EAR GS-003 - Guía de Gestión de Incidentes de Seguridad
14. EAR GS-004 - Guía Cifrado de Archivos Confidenciales
15. EAR GS-005 - Guía Para La Realización de Mantenimientos Preventivo
16. EAR GS-006 - Guía de Control de Acceso (Validar)
17. EAR GS-007 - Guía Mantenimiento Infraestructura Tecnológica
18. EAR GS-008 - Guía de Borrado Seguro.
19. Seguro Gestión de Incidentes De Ciber Seguridad Pre - Post

[50]MINTIC.GOV.CO; [Sitio web]; Articulo 5482 G2 Política general de seguridad y privacidad de la información; [Consulta: 11 de mayo de 2022]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

La organización EAR Construcciones, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para EAR Construcciones, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de
- seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de EAR Construcciones
- Garantizar la continuidad del negocio frente a incidentes.

- EAR Construcciones ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

Finalmente es de gran ayuda incluir la descripción general de otras políticas relevantes para el cumplimiento de los Objetivos planteados dentro del proyecto del SGSI ya que éstas son el apoyo sobre el cual se desarrolla; éstas deben ser descritas de forma sencilla, puntual y muy efectiva.

Dentro de las temáticas que se tocan en este punto se encuentran por ejemplo la gestión de activos, seguridad física y ambiental, control de accesos, etc. Para abordar este punto es necesario remitirse a la “Guía de políticas específicas de seguridad y privacidad de la información” y mencionar aquellas que la Entidad haya establecido como necesarias y primordiales. De esta forma se presenta el siguiente ejemplo:

A continuación, se establecen 12 principios de seguridad que soportan el SGSI de EAR Construcciones:

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.

- EAR Construcciones protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.

- EAR Construcciones protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

- EAR Construcciones protegerá su información de las amenazas originadas por parte del personal.

- EAR Construcciones protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

- EAR Construcciones controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

- EAR Construcciones implementará control de acceso a la información, sistemas y recursos de red.

- EAR Construcciones garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

- EAR Construcciones garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

- EAR Construcciones garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

- EAR Construcciones garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración de EAR Construcciones con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros. la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

EAR Construcciones, para asegurar la dirección estratégica de la Entidad, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- · Minimizar el riesgo de los procesos misionales de la entidad.
- · Cumplir con los principios de seguridad de la información.
- · Cumplir con los principios de la función administrativa.
- · Mantener la confianza de los funcionarios, contratistas y terceros.
- · Apoyar la innovación tecnológica.
- · Implementar el sistema de gestión de seguridad de la información.
- · Proteger los activos de información.

Alcance/Aplicabilidad:

- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.

- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes del EAR Construcciones.

- Garantizar la continuidad del negocio frente a incidentes.

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

A continuación, se establecen las 12 políticas de seguridad que soportan el SGSI de EAR Construcciones:

- EAR Construcciones ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.

- EAR Construcciones protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.

- EAR Construcciones protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

- EAR Construcciones protegerá su información de las amenazas originadas por parte del personal.

- EAR Construcciones protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

- EAR Construcciones controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

- EAR Construcciones implementará control de acceso a la información, sistemas y recursos de red.

- EAR Construcciones garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

- EAR Construcciones garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

- EAR Construcciones garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basado en el impacto que pueden generar los eventos.

- EAR Construcciones garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

Para realizar una correcta implementación de políticas de seguridad de la información, es necesario cumplir con una serie de fases que se sugieren en este documento, las cuales tienen como objetivo que la entidad desarrolle, apruebe, implemente y socialice e interiorice las políticas para un uso efectivo por parte de todos los funcionarios, contratistas y/o terceros de la entidad.

IMPORTANCIA DE LAS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN:

Para las entidades es importante contar con políticas de seguridad ya que son ellas quienes guiaran el comportamiento personal y profesional de los funcionarios, contratistas o terceros sobre la información obtenida, generada o procesada por la entidad, así mismo las políticas permitirán que la entidad trabaje bajo las mejores prácticas de seguridad y cumpla con los requisitos legales a los cuales esté obligada a cumplir la entidad.

9 PROPONER UNA ESTRATEGIA DE SOCIALIZACIÓN DE LOS NIVELES DE RIESGOS DE LOS ACTIVOS DE INFORMACIÓN DE LA EMPRESA EAR CONSTRUCCIONES Y SUS POLÍTICAS DE SEGURIDAD CON EL FIN CREAR CONCIENCIA EN LOS USUARIOS DE LA ORGANIZACIÓN.

Realizar transferencia de conocimiento mediante reuniones en cada una de las dependencias de EAR Construcciones, tomando como ejemplo las actividades que se realizan a diario.

La transferencia de conocimiento se deberá informar a los funcionarios, contratistas, proveedores y aliados y a las demás partes interesadas a través de los canales y mecanismos institucionales dispuestos para estos fines. Además, deberán ser incluidas en las iniciativas de generación de cultura en seguridad de la información de la organización EAR Construcciones dando charlas y/o capacitaciones a todo el personal de la organización, mediante el uso videos al inicio de sesión de los equipos de la empresa, cambio de pantalla que contengan tics o campañas de seguridad de la información, Pop-ads con recordatorios del uso de buenas practica de seguridad en puesto de trabajo y realizar como mínimo una auditoría interna anual para analizar que tanto están realizando los controles sugeridos.

Estas capacitaciones serán otorgadas por el personal idóneo de lo oficina TIC de la empresa teniendo en cuenta los estándares de la norma ISO 27001:2013 y los controles de seguridad asociados a la norma ISO 27002:2013.

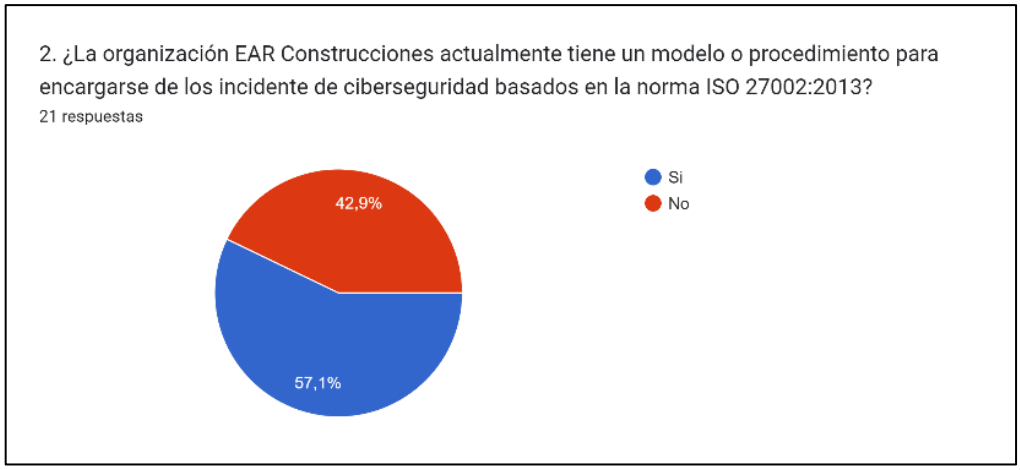
9.1 ENCUESTA AL PERSONAL DE EAR CONSTRUCCIONES:

Se le realizo la encuesta a 21 personas de las diferentes dependencias de la entidad donde se obtuvo como resultado las siguientes respuestas:

Ilustración 13 - Pregunta 1 - Encuesta al personal de EAR Construcciones

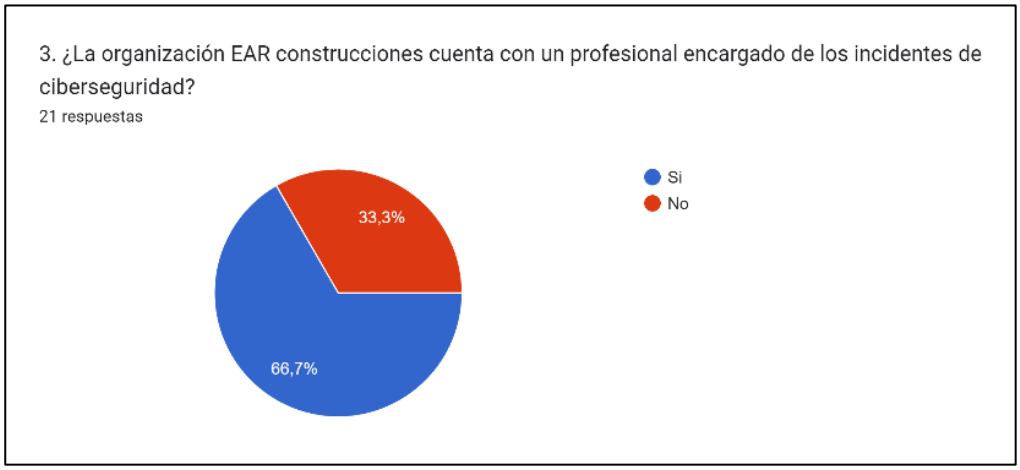
Fuente 17 - Elaboración propia

Ilustración 15 - Pregunta 2 - Encuesta al personal de EAR Construcciones



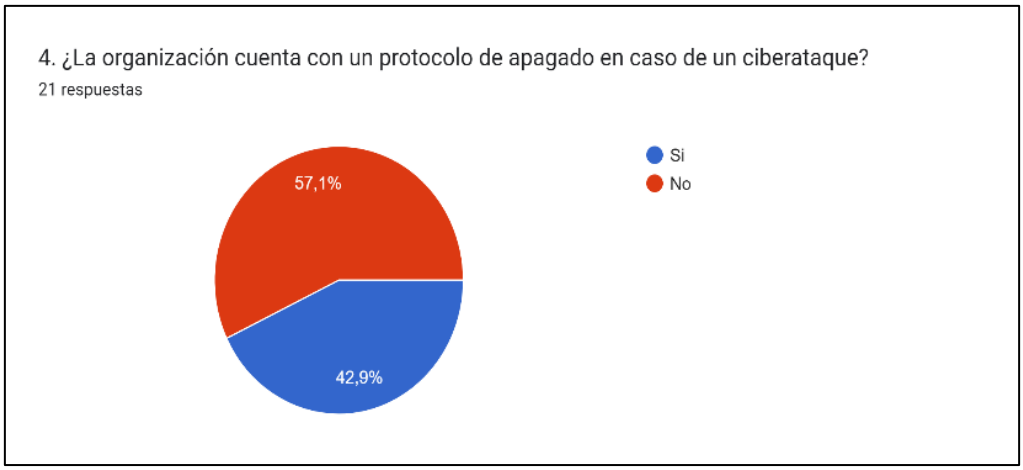
Fuente 16 - Elaboración propia

Ilustración 14 - Pregunta 3 - Encuesta al personal de EAR Construcciones



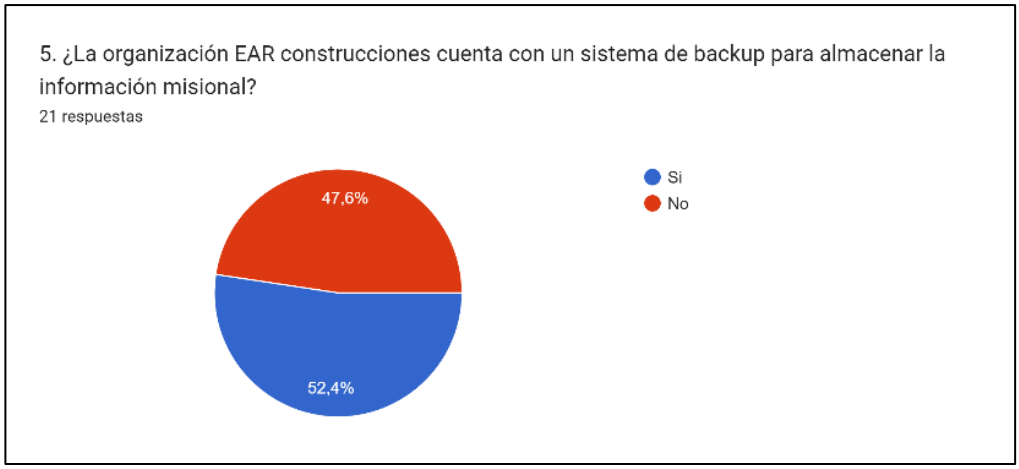
Fuente 15 - Elaboración propia

Ilustración 18 - Pregunta 4 - Encuesta al personal de EAR Construcciones



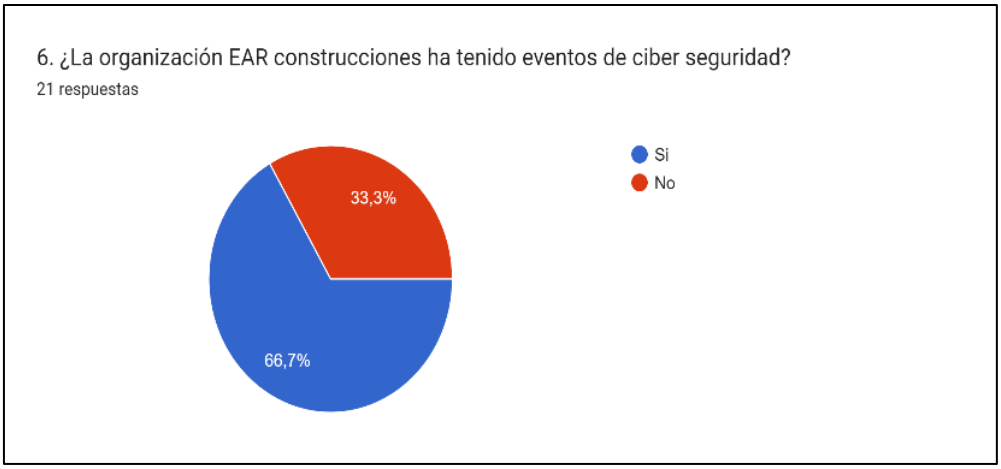
Fuente 20 - Elaboración propia

Ilustración 17 - Pregunta 5 - Encuesta al personal de EAR Construcciones



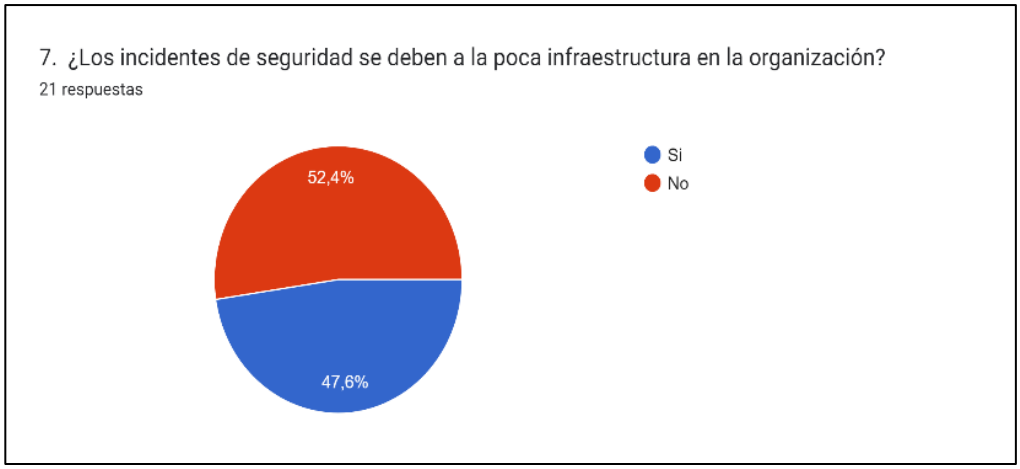
Fuente 19 - Elaboración propia

Ilustración 16 - Pregunta 6 - Encuesta al personal de EAR Construcciones



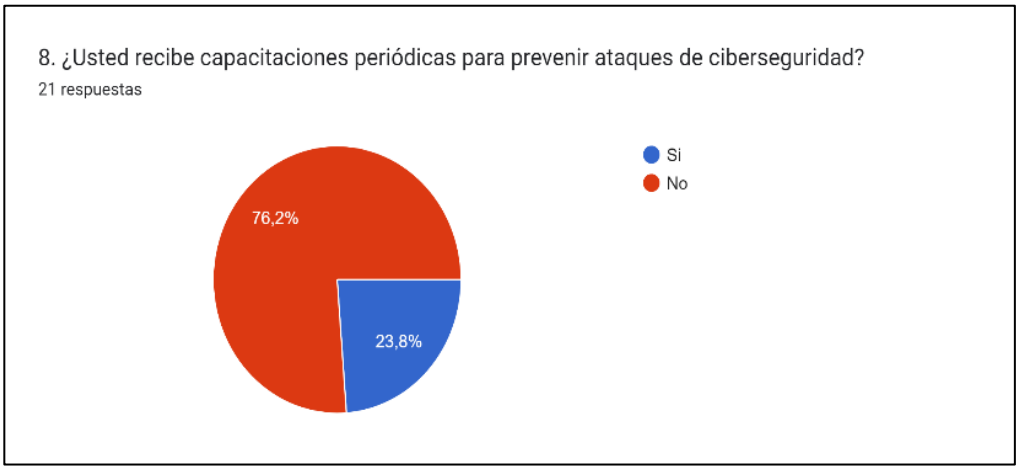
Fuente 18 - Elaboración propia

Ilustración 21 - Pregunta 7 - Encuesta al personal de EAR Construcciones



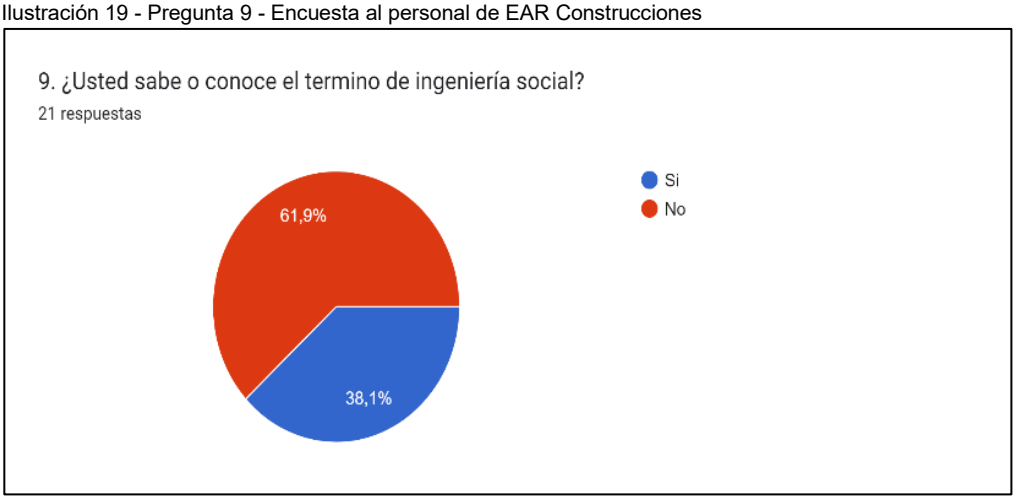
Fuente 23 - Elaboración propia

Ilustración 20 - Pregunta 8 - Encuesta al personal de EAR Construcciones



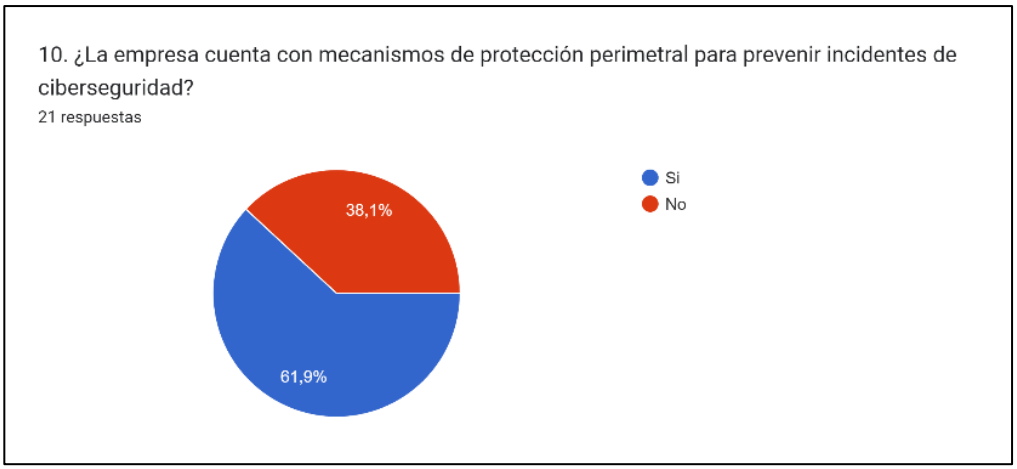
Fuente 22 - Elaboración propia

Ilustración 19 - Pregunta 9 - Encuesta al personal de EAR Construcciones



Fuente 21 - Elaboración propia

Ilustración 22 - Pregunta 10 - Encuesta al personal de EAR Construcciones



Fuente 24 - Elaboración propia

9.1.1 METODOLOGÍA DE GESTIÓN DEL RIESGO

Para el análisis y gestión del riesgo de la infraestructura tecnológica y los activos de información perteneciente a la organización EAR construcciones se tiene contemplado utilizar la metodología de MAGERIT la cual presenta las siguientes ventajas.

- Alcance en el análisis y gestión del riesgo
- Documentación suficiente con relación a recursos de información, amenazas y tipos de activos.
- Es de uso libre y no requiere adquirir licenciamiento para su uso.
- Divide los activos y con esto se puede realizar una mejor valoración a cada activo

El objetivo es poder realizar el inventario de activos, un análisis de riesgos para determinar las amenazas y/o vulnerabilidades a las que están expuestos los activos de información con los que cuenta la oficina de tecnologías de la información y las comunicaciones de la empresa EAR construcciones y con esto determinar las salvaguardas para los activos de información.

Ilustración 23 - Pasos para aplicar la metodología MAGERIT

Fuente 25 - Elaboración propia

En la figura anterior se puede observar los pasos que se deben seguir dependiendo del objetivo y propuesta la aplicación dentro de una organización la metodología MAGERIT.

9.2 ALCANCE DEL ANÁLISIS:

El alcance para el manejo de la aplicación con metodología MAGERIT dentro del proyecto que involucra a todas las dependencias de la empresa, iniciará con la identificación de los riesgos a los que están expuestos los activos de información y la infraestructura tecnológica de la organización EAR construcciones, luego de definirá un plan del tratamiento del riesgo, que nos apruebe la aceptación de medidas de seguridad. Interesados a minimizar o controlar las vulnerabilidades y amenazas que puedan llegar a afectar dichos activos, favoreciendo con esto la continuidad de la operación de la organización y garantizar la aplicabilidad de controles que aseguren la información, hardware y software que manejan.

10 CONCLUSIONES

Se realizó un análisis profundo de todos los activos de información de la empresa EAR Construcciones teniendo en cuenta como base la metodología MAGERIT y el uso de buenas prácticas indicado en las normas ISO/IEC 27001:2013 y 27002:2013, como resultado de este análisis la empresa puede tomar decisiones y gestionar si es el caso la mitigación de los riesgos encontrados a través de políticas de seguridad de la información diseñadas para la organización.

Una vez realizada la implementación de la metodología de MAGERIT se logró la identificación de los activos de información de la empresa y al implementar el tratamiento de datos mediante el buen uso de la herramienta se les pudo otorgar un valor el cual podemos evaluar y manifestar que tan críticos es cada uno de los activos de información para la organización EAR Construcciones dicho esto, se procede con el tratamiento necesario para su mitigación y minimización del riesgo.

Al realizar la implementación de los controles requeridos para la mitigación del riesgo asociado a la compañía EAR Construcciones nos ayudó a minimizar varias amenazas latentes que en el día a día la empresa debe afrontar, esto no quiere decir que con dichos controles la entidad no se vea abocada en la materialización de un ciberataque, pero sí el campo de ataque será mínimo gracias a los controles establecidos porque se mitigaron con la implementación realizada.

Con la realización del diseño de políticas de seguridad para la organización EAR construcciones se realizan guías con el paso a paso de las mejores prácticas que se deben seguir y alinear para tener el aseguramiento de la información física y digital de la empresa y así preservar sus activos de información mitigando posibles amenazas.

Al involucrar a toda la compañía en la socialización y aplicación de nuevos controles para la mitigación de los riesgos asociados a la ciberseguridad, estamos creando cada vez más conciencia en todas las personas que están involucradas en este

proyecto y así prevenir ataques de ingeniería social, prevención de ransomware entre otros para la organización EAR construcciones.

Es importante para la organización realizar auditorías internas con el fin de controlar que cada uno de los procesos se estén ejecutando de forma correcta.

11 RECOMENDACIONES

De acuerdo con el inventario realizado a la compañía EAR Construcciones se recomienda mantener al actualizados los inventarios de sus activos de información como mínimo una vez al mes según la demanda de la organización.

Realizar auditorías periódicas para verificar que los controles establecidos se estén ejecutando de forma exitosa e identificar que los activos de información que posee la empresa son los que se van auditar sin excluir ninguno.

Realizar de forma periódica simulacros de pérdida de información para verificar que hacer al momento de una contingencia y accionar el plan de recuperación y sostenibilidad de la operación de la compañía.

Mantener al día los números y/o contactos de los organismos de emergencia en caso de materializarse un ciber ataque y saber qué hacer y que protocolos seguir.

Ejecutar de forma periódica las restauraciones del plan de backup establecido en la organización EAR Construcciones y subir esta información en un ambiente de pruebas para verificar si con estos respaldos la organización puede trabajar en caso de tener un posible ataque de Ransomware, virus, pérdida de información, avería del file server y/o desastre natural.

BIBLIOGRAFÍA

CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES; [Sitio web]; Colombia: Ccit; Tendencias Cibercrimen Colombia 2019-2020, pág. 7,8; [Consulta: 21 de octubre 2021]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES; [Sitio web]; Colombia: Ccit; Tendencias Cibercrimen Colombia 2019-2020, pág. 29; [Consulta: 21 de octubre 2021]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

CIBERSEGURIDAD; [Sitio web]; Ciberseguridad; ISO 27001; [Consulta: 21 de octubre 2021]; Disponible en: https://ciberseguridad.com/normativa/espana/sgsi/iso-27001/#Beneficios_para_la_empresa

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA; [Sitio web]; Función pública; Ley 1581 de 2012, Ley Estatutaria; [Consulta: 21 de noviembre 2021]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

DEPARTAMENTO ADMINISTRATIVO DE LA PRESIDENCIA DE LA REPUBLICA; [Sitio web]; Colombia: DAPRE; Manual de Políticas de Seguridad de La Información, Política de seguridad del DAPRE, pág. 14; [Consulta: 21 de octubre 2021]. Disponible en: https://dapre.presidencia.gov.co/dapre/DocumentosSIGEPRE/M-TI-01-Manual-Politicas-Seguridad-Informacion.pdf

DERECHO DE AUTOR; [Sitio web]; Colombia: Derechos de autor; Sobre derechos de autor; [Consulta: 25 de septiembre 2021]; Disponible en:

http://derechodeautor.gov.co:8080/documents/10181/182597/23.pdf/a97b8750-8451-4529-ab87-bb82160dd226

EL TIEMPO; [Sitio web]; Colombia: Periódico el Tiempo; Cibercrimen le cuesta a Colombia más de $190 mil millones de pesos al año; [Consulta: 25 de septiembre 2021]; Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/cibercrimen-le-cuesta-a-colombia-190-000-millones-de-pesosal-ano-380830

EN TIC CONFIO; [Sitio web]; En Tic confió; LEY 1273 DE 2009, De la protección de la información y de los datos; [Consulta: 20 de noviembre 2021]. Disponible en: https://www.enticconfio.gov.co/images/stories/normatividad/Ley_1273_de_2009%20.pdf

GESTIÓN PENSEMOS; [Sitio web]; Gestión pensemos; Análisis de riesgo informático: 4 pasos para implementarlo; [Consulta: 25 de septiembre 2021]; Disponible en: https://gestion.pensemos.com/analisis-de-riesgo-informatico-4-pasos-para-implementarlo

HOSTDIME; [Sitio web], Hostdime; ¿Qué es una vulnerabilidad en seguridad informática?; [Consulta: 25 de septiembre 2021]; Disponible en: https://www.hostdime.com.pe/blog/que-es-una-vulnerabilidad-en-seguridad-informatica-ejemplos/

INCIBE.ES; [Sitio web]; España: Temáticas Gestión de incidentes de seguridad; [Consulta: 19 de octubre 2023]. Disponible en: https://www.incibe.es/empresas/tematicas/gestion-incidentes-seguridad

ISO27000.ES; [Sitio web]; España: Glosario, definición Activo; [Consulta: 20 de octubre 2023]. Disponible en: http://www.iso27000.es/glosario.html

ISO27000.ES; [Sitio web]; España: Glosario, definición Amenaza; [Consulta: 20 de octubre 2023]. Disponible en: http://www.iso27000.es/glosario.html

ISO27000.ES; [Sitio web]; España: Glosario, definición Análisis de Riesgos; [Consulta: 20 de octubre 2023]. Disponible en: http://www.iso27000.es/glosario.html

ISO27000.ES; [Sitio web]; España: Glosario, definición de Control; [Consulta: 20 de octubre 2023]. Disponible en: http://www.iso27000.es/glosario.html

ISO27000.ES; [Sitio web]; España: Glosario, definición de Gestión de incidentes de seguridad de la información; [Consulta: 20 de octubre 2023]. Disponible en: http://www.iso27000.es/glosario.html

ISO27000.ES; [Sitio web]; España: Glosario, definición de Gestión de riesgos; [Consulta: 20 de octubre 2023]. Disponible en: http://www.iso27000.es/glosario.html

ISO27000.ES; [Sitio web]; España: Glosario, definición de Impacto; [Consulta: 20 de octubre 2023]. Disponible en: http://www.iso27000.es/glosario.html

ISO27000.ES; [Sitio web]; España: Glosario, definición de Riesgo; [Consulta: 20 de octubre 2023]. Disponible en: http://www.iso27000.es/glosario.html

ISO27000.ES; [Sitio web]; España: Glosario, definición de Vulnerabilidad; [Consulta: 20 de octubre 2023]. Disponible en: http://www.iso27000.es/glosario.html

LOS PATIOS NORTE DE SANTANDER; [Sitio web]; Colombia: Los patios norte de Santander; Oficina TIC Los Patios. Manual de Normas y Políticas de Seguridad de la Información. Ocaña, pág. 30; [Consulta: 21 de octubre 2021]. Disponible en: https://www.lospatios-nortedesantander.gov.co/Conectividad/InformesGEL/GT-D-05%20POLITICAS%20DE%20SEGURIDAD%20DE%20LA%20INFORMACION.pdf

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES; [Sitio web]; Colombia: MINTIC; Registro de activos de información; [Consulta: 25 de septiembre 2021]; Disponible en: https://mintic.gov.co/portal/inicio/Atencion-y-Servicio-a-la-Ciudadania/Transparencia/135888:Registro-de-Activos-de-Informacion

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES; [Sitio web]; Colombia: MINTIC; Colombia superó los 209.000 teletrabajadores en

2020; [Consulta: 21 de octubre 2021]; Disponible en: https://mintic.gov.co/portal/inicio/Sala-de-prensa/179742:Colombia-supero-los-209-000-teletrabajadores-en-2020-Ministerio-de-las-TIC

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES; [Sitio web]; Colombia: MINTIC; Modelo de Seguridad y Privacidad de la Información, Modelo de seguridad y privacidad de la información, pág. 20; [Consulta: 21 de octubre 2021]; Disponible en: https://mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

MINTIC.GOV.CO; [Sitio web]; Colombia: Confidencialidad; pag.: 8 [Consulta: 20 de octubre 2023]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

MINTIC.GOV.CO; [Sitio web]; Colombia: Glosario, definición de Antivirus; [Consulta: 20 de octubre 2023]. Disponible en: https://www.mintic.gov.co/portal/inicio/Glosario/

MINTIC.GOV.CO; [Sitio web]; Colombia: Glosario, definición de Centro de datos; [Consulta: 20 de octubre 2023]. Disponible en: https://www.mintic.gov.co/portal/inicio/Glosario/

MINTIC.GOV.CO; [Sitio web]; Colombia: Glosario, definición de CSIRT; [Consulta: 20 de octubre 2023]. Disponible en: https://www.mintic.gov.co/portal/inicio/Glosario/

MINTIC.GOV.CO; [Sitio web]; Colombia: Guía de gestión de riesgos: Probabilidad; pag.: 32 [Consulta: 20 de octubre 2023]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

MINTIC.GOV.CO; [Sitio web]; Colombia: Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información; [Consulta: 19 de octubre 2023]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

MONOGRAFIAS; [Sitio web]; Monografías; Método descriptivo y experimental; [Consulta: 11 de diciembre 2021]. Disponible en:

https://www.monografias.com/docs/metodo-descriptivo-y-experimental-FKLDMCGPJ8G2Y

PRACTISIS; [Sitio web]; Practisis; La importancia de implementar procesos operativos en tu empresa; [Consulta: 21 de octubre 2021]. Disponible en: https://www.practisis.com/post-one/la-importancia-de-implementar-procesos-operativos-en-tu-empresa

SAFESOCIETY; [Sitio web]; Safesociety; La importancia de implementar un SGSI en nuestra organización; [Consulta: 21 de octubre 2021]; Disponible en: https://www.safesociety.co/blogitem/4/la-importancia-de-implementar-un-sgsi-en-nuestra-organizacion

SEMILLEROCEROSYUNO.COM; [Sitio web]; Matriz de Riesgos Magerit - Luis Fernando Zambrano; [Consulta: 28 de septiembre de 2021]. Disponible en: semillerocerosyuno.com/wp-cont.../Matriz-Version-5.3-29.04.2021-1.xls

UNIR; [Sitio web]; Unir; Políticas de seguridad informática; [Consulta: 25 de septiembre 2021]; Disponible en: https://www.unir.net/ingenieria/revista/politicas-seguridad-informatica/

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Márquez Buitrago, Yon Ivan, Diseño de controles de seguridad para los activos informáticos en la empresa Transportes Tierra Grata y Compañía Ltda; [Consulta: 21 de septiembre 2021]. Disponible en: https://repository.unad.edu.co/handle/10596/21345

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Edwin Anderson, Diseño del Sistema Gestión de Seguridad de la Información para la Empresa QWERTY S.A.; [Consulta: 22 de septiembre 2021]. Disponible en: https://repository.unad.edu.co/handle/10596/39069

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Jiménez Fonseca, Teresa Herminia, Análisis y evaluación de riesgos, de los activos de información de la Dirección Ejecutiva Seccional de Administración Judicial de Tunja - DESAJT, adoptando una metodología de gestión de riesgos de los sistemas de información; [Consulta: 22 de septiembre 2021]. Disponible en: https://repository.unad.edu.co/handle/10596/21575

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; García Ramírez, Germán, Castro Angarita, Jaime Alfonso, Diseñar un Sistema de Gestión de la Seguridad de la Información (SGSI) a la empresa Unitransa S.A. ubicada en la ciudad de Bucaramanga; [Consulta: 22 de septiembre 2021]. Disponible en: https://repository.unad.edu.co/handle/10596/11914

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Duarte Martínez, María Carolina, Diseño de políticas de Seguridad de la Información para la Unidad de Tecnología de la Cámara de Comercio de Cúcuta; [Consulta: 22 de septiembre 2021]. Disponible en: https://repository.unad.edu.co/handle/10596/30304

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Arellano Montenegro, Fabio Adalberto, Realizar el análisis para gestión de riesgos en los sistemas de información de la IPS Solidarios Salud del municipio de Cuaspud Carlosama a partir de la norma ISO 27001 aplicando la metodología Magerit; [Consulta: 21 de septiembre 2021]. Disponible en: https://repository.unad.edu.co/handle/10596/21476

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Oñate Arboleda, Adriana, Propuesta de Políticas de Seguridad de la Información para proteger los activos de información en las organizaciones;

[Consulta: 22 de septiembre 2021]. Disponible en: https://repository.unad.edu.co/handle/10596/41984

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Coral Ojeda, Jesús Armando, Adriana, Diseño de un sistema de gestión de seguridad para la red datos bajo la norma ISO 27001:2013 en el Centro de Estudios Emssanar Cetem de la ciudad de Pasto; [Consulta: 22 de septiembre 2021]. Disponible en: https://repository.unad.edu.co/handle/10596/11875

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Criollo Betancourt, Irmaena, Etapa de planificación de un sistema de gestión de seguridad de la información para el área de tecnología de la IPS Garper Médica SAS basado en la norma ISO/IEC 27001:2013.; [Consulta: 02 de mayo 2022]. Disponible en: https://repository.unad.edu.co/handle/10596/48702

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; González Tabares, Eduin Gildardo, Plan de implementación de un sistema de gestión de seguridad de la información para la Unidad Administrativa Parques Nacionales Naturales de Colombia, según Norma ISO 27001: 2013.; [Consulta: 02 de mayo 2022]. Disponible en: https://repository.unad.edu.co/handle/10596/23186

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Tarazona Anteliz, Javier Ricardo Leal Sandoval, Cherly Liliana, Diseño de un sistema de gestión de seguridad de la información para el área TI de la ESE Hospital Universitario Erasmo Meoz de Cúcuta basado en la norma ISO 27001:2013; [Consulta: 02 de mayo 2022]. Disponible en: https://repository.unad.edu.co/handle/10596/17414

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Díaz Ricardo, Luis Carlos, Diseño de un Sistema de Gestión de la Seguridad

de la Información en la IPS Aassalud de Corozal Sucre, mediante la implementación de la metodología Magerit (v3.0) y la Norma ISO 27001:2013; [Consulta: 02 de mayo 2022]. Disponible en: https://repository.unad.edu.co/handle/10596/14386

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Reyes Artunduaga, Jonathan Fernando, Diseño de un sistema de gestión de seguridad de información bajo la Norma ISO 27001:2013 en la E.P.S Asmet Salud; [Consulta: 02 de mayo 2022]. Disponible en: https://repository.unad.edu.co/handle/10596/27057

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Samper Ibañez, Pedro Antonioo, Diseño de un sistema de gestión de seguridad de la información en el área de sistema de la empresa Rymco S.A bajo la norma ISO IEC/27001:2013; [Consulta: 03 de mayo 2022]. Disponible en: https://repository.unad.edu.co/handle/10596/3987

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Figueroa Cubillos, Carolina, Diseño de un sistema de gestión de seguridad de la información para el Colegio Germán Arciniegas I.E.D., bajo la norma técnica colombiana NTC ISO/IEC 27001:2013; [Consulta: 06 de mayo 2022]. Disponible en: https://repository.unad.edu.co/handle/10596/25633

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Bolívar Leon, Yeinny Andrea, Diseño de un sistema de gestión de seguridad de la información en la intranet del policlínico del sur Olaya Bogotá, bajo la norma ISO 27001; [Consulta: 06 de mayo 2022]. Disponible en: https://repository.unad.edu.co/handle/10596/5513

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Cazaran Buitrago, Olger Yonatan, Diseño de un sistema de gestión de

seguridad de la Información en el área de recursos informáticos de la Contraloría Departamental del Meta, según la norma ISO 27001, bajo la norma ISO 27001; [Consulta: 06 de mayo 2022]. Disponible en: https://repository.unad.edu.co/handle/10596/17423

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Ruiz Peña, José Higinio, Diseño de un sistema de gestión de seguridad de la información (SGSI) bajo la norma ISO/IEC 27001:2013, en la Cooperativa Multiactiva del personal del Sena, en Bogotá, bajo la norma ISO 27001; [Consulta: 06 de mayo 2022]. Disponible en: https://repository.unad.edu.co/handle/10596/17300

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Contreras Esguerra, Lidia Constanza, Diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001 para la dirección de sistemas de la gobernación de Boyacá; [Consulta: 06 de mayo 2022]. Disponible en: https://repository.unad.edu.co/handle/10596/11895

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Garrido Sánchez, Ana Lucia Bravo Lara, Pascual, Políticas de seguridad de la información para la Institución Educativa Luis Carlos Galán Sarmiento, basados en la norma ISO/IEC 27001:2013; [Consulta: 06 de mayo 2022]. Disponible en: https://repository.unad.edu.co/handle/10596/18515

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Bojacá Garavito, Edgar Alonso, Diseño de un Sistema de Gestión de Seguridad Informática basado en la norma ISO/IEC 27001- 27002 para el área administrativa y de historias clínicas del Hospital San Francisco de Gachetá; [Consulta: 06 de mayo 2022]. Disponible en: https://repository.unad.edu.co/handle/10596/12685

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Giraldo Reina, Edna Rocío, Planteamiento del sistema de gestión de seguridad de información aplicando la Norma NTC ISO/IEC 27001 - 27002 del 2013 en el proceso de la revisión técnico - mecánica del CDA Corpotrans; [Consulta: 06 de mayo 2022]. Disponible en: https://repository.unad.edu.co/handle/10596/27058

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Guerrero Angulo, Yezid Camilo, Diseño del sistema de gestión de seguridad de la información para la Unidad de Informática, Ingeniería de Sistemas y Telemática de la Universidad de Nariño soportada en los estándares Magerit e ISO/IEC 27001 y 27002-2013; [Consulta: 06 de mayo 2022]. Disponible en: https://repository.unad.edu.co/handle/10596/31718

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Acosta Ubaque, Nubia Esperanza León Patiño, Tania Kruskaya, Diseño del Sistema de Gestión de Seguridad de la Información (S.G.S.I) para el centro de datos de la personería de Bogotá D.C. bajo las normas NTC-ISO-IEC 27001:2013 y GTC-ISO-IEC 27002:2013; [Consulta: 06 de mayo 2022]. Disponible en: https://repository.unad.edu.co/handle/10596/11940

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Jojoa Paz, Doris Esther Córdoba Cuaycal, Karol Martín, Diseño de un sistema de gestión de seguridad de la información (SGSI) basado en la norma ISO 27001: 2013 para la red inalámbrica de la empresa innovación global S.A, ubicada en el municipio de Sibundoy Putumayo; [Consulta: 06 de mayo 2022]. Disponible en: https://repository.unad.edu.co/handle/10596/6146

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA; [Sitio web]; Colombia: UNAD; Cardona Castañeda, José Nayid Salcedo Ruiz, Willis Alberto, Análisis y evaluación de riesgos de seguridad informática para la Cámara de Comercio de la

Dorada, puerto Boyacá, Puerto Salgar y municipios de oriente de Caldas; [Consulta: 07 de mayo 2022]. Disponible en: https://repository.unad.edu.co/handle/10596/14418

UNIVERSIDAD PILOTO DE COLOMBIA; [Sitio web]; Unipiloto; Ciberseguridad en Colombia. Universidad Piloto de Colombia; pag 1-12; [Consulta: 25 de septiembre 2021]; Disponible en: http://repository.unipiloto.edu.co/handle/20.500.12277/2579/browse?type=author&value=Valoyes+Mosquera%2C+Amancio

WELIVESECURITY; [Sitio web]; Welivesecurity; ¿Qué es la fuga de información?; [Consulta: 25 de septiembre 2021]; Disponible en: https://www.welivesecurity.com/la-es/2010/04/13/que-es-la-fuga-de-informacion/