DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL ÁREA ADMINISTRATIVA DEL PARTIDO DE LA U BASADO EN ISO 27001:2022

JULIANA REYES ESCOBAR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CIUDAD BOGOTÁ
AÑO 2023

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL ÁREA ADMINISTRATIVA DEL PARTIDO DE LA U BASADO EN ISO 27001:2022

JULIANA REYES ESCOBAR

Proyecto de Grado – Aplicado presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

Nombre
Tutor de Curso
EDUARD MANTILLA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CIUDAD BOGOTÁ
AÑO 2023

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

DEDICATORIA

Con cariño para mi madre quien siempre me acompaña incondicionalmente en mis procesos y me alienta a continuar, a mi hermano por ser mi polo a tierra siempre y a mis dos ángeles en el cielo mi padre y mi abuela que día a día guían mis pasos desde el cielo.

AGRADECIMIENTOS

Quiero manifestar mi gratitud a la UNAD por darme la oportunidad de mejorar mi perfil profesional. También quiero reconocer la orientación y apoyo brindado por los maestros que me asesoraron en el proceso, ya que sin ellos no hubiera sido posible lograr este objetivo. Además, agradezco al Partido de la U por confiar en mí para realizar este proyecto.

CONTENIDO

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

ACTIVOS TI: Recursos de tecnología de la información, como hardware, software, redes y datos, que son valiosos para la organización.

AMENAZAS: Evento o acción que pueda dañar los activos de la compañía, tomando en cuenta posibles amenazas como ataques informáticos, fenómenos naturales impredecibles, fallos humanos. y fallas técnicas.

CONFIDENCIALIDAD: proteger información sensible de la compañía para evitar la divulgación no autorizada o el acceso a ella.

DISPONIBILIDAD: Capacidad de los activos de TI de estar disponibles y accesibles para su uso cuando se necesiten.

INFORMACIÓN: Dato o conocimiento que tenga valor para la organización, en cualquier medio de soporte.

INTEGRIDAD: Exactitud y completitud de la información y a su protección contra la modificación no autorizada**.**

POLÍTICA: lineamientos y directrices que rigen las acciones de la organización, incluyendo políticas de seguridad que establecen los requisitos para la salvaguardar la información sensible.

RIESGOS: Probabilidad de que ocurran amenazas y las consecuencias asociadas si lo hacen.

SGSI: Se trata de un conjunto de medidas, tanto políticas como de procedimientos y controles, que tienen como objetivo salvaguardar la información de una entidad organizacional

VULNERABILIDADES: debilidades o fallos en los activos TI que pueden ser explotados por amenazas para comprometer la seguridad.

RESUMEN

En la actualidad toda organización debe enfocar esfuerzos para proteger sus activos de información para garantizar una gestión óptima y evitar la materialización de riesgos, estableciendo políticas y controles efectivos. El Partido de la U cuenta con reconocimiento en el País, representa intereses de un sector de la población, propende formar a sus militantes en temas ideológicos para fortificar la democracia y la intervención ciudadana[1]. A través del diseño de un SGSI se pretende asegurar la protección de su activo más importante la información dado que no se evidencian los controles y procedimientos necesarios para hacerlo, existen antecedentes de intentos de ataques a otros partidos políticos[2] y organismos electorales como CNE[3] dada la información sensible y de relevancia que manejan en el ámbito electoral y político del país y los intereses que existen de por medio. Por lo descrito anteriormente mediante este proyecto se pretende diseñar para el área administrativa del Partido de la U un SGSI que permita mejorar procesos y proteger activos, velando por proteger la información sensible del partido y contando con el respaldo de los directivos para mantenerlo y mejorarlo continuamente, se evaluará la situación actual de seguridad, se identificarán activos críticos y riesgos asociados y se establecerán políticas y controles de seguridad basado en ISO 27001:2022 norma que establece requisitos para un SGSI efectivo y eficiente evitando estar expuestos.

La fase de diagnóstico y análisis actual se hará a través de recaudación de información y entrevistas, igual para el levantamiento de activos, se realizará un análisis cualitativo y cuantitativo para evaluación de riesgos y amenazas y un análisis descriptivo para ordenar resultados, se empleará MAGERIT para complementar lo referente a riesgos y análisis de aplicabilidad y resultado de riesgos para formulación de políticas. Se espera que el proyecto permita al Partido ser pionero junto con alianza Verde en velar por la ciberseguridad en su sector y establecer una cultura organizacional de seguridad, así como contar procesos y activos asociados a la información seguros y reducir el riesgo de ataques cibernéticos.

Palabras Claves: Controles, Gestión de Riesgos, ISO 27001:2022, MAGERIT Políticas de seguridad, SGSI

[1] Partido de la U. Partido de La Unión por la Gente. [Sitio Web]. [Consultado: 12 de marzo de 2023]. Disponible en: https://partidodelau.com/.

[2] Fuerza Alternativa Revolucionaria del Común (FARC). Ataque informático al sitio web de FARC. [Sitio Web]. [Consultado: 12 marzo de 2023]. Disponible en: https://www.farc-ep.co/noticias/ataque-informatico-al-sitio-web-de-farc.html.

[3] Consejo Nacional Electoral (CNE). Comunicado de prensa: CNE informa sobre intentos de ataques informáticos en la jornada electoral. [Sitio Web]. [Consultado: 12 de marzo de 2023]. Disponible en: https://cne.gov.co/portal/informacion-para-periodistas/comunicados-de-prensa/1822-cne-informa-sobre-intentos-de-ataques-informaticos-en-la-jornada-electoral

ABSTRACT

Currently, the entire organization must focus efforts to protect its information assets to guarantee optimal management and avoid the materialization of risks, propose effective policies and controls. The Partido de la U is recognized in the country, represents the interests of a sector of the population, tends to train its militants in ideological issues to strengthen democracy and citizen intervention. Through the design of an ISMS, it is intended to ensure the protection of its most important asset, the information, since the controls and procedures necessary to do so are not evident, there is a history of attempted attacks on other political parties and electoral organizations such as the CNE given the sensitive and relevant information they handle in the electoral and political sphere of the country and the interests that exist in between.

As described above, the objective of this project is to design an ISMS for the administrative area of Partido de la U that allows improving processes and protecting assets, guaranteeing the protection of sensitive information that is handled in the organization and, most importantly, having the support managers to maintain and improve it continuously, the current security situation will be evaluated, critical assets and associated risks will be identified, and security policies and controls will be established based on the ISO 27001:2022 standard, which establishes requirements for an effective and efficient ISMS, promoting be exposed

The diagnosis phase of the current situation will be done through information collection and interviews, the same for the survey of assets, a qualitative and quantitative analysis will be carried out for the evaluation of risks and threats and a descriptive analysis to order results, MAGERIT will be used To complement the reference to risks and for the design of the ISMS.

The project is expected to allow the Party to be a pioneer in ensuring cybersecurity in its sector and establish an organizational culture of security, as well as having processes and assets associated with secure information and reducing the risk of cyber attacks.

Keywords: Controls, Risk Management, ISO 27001:2022, MAGERIT Security Policies, SGSI.

INTRODUCCIÓN

En un entorno de crecientes amenazas cibernéticas, es fundamental que las organizaciones implementen acciones para resguardar sus bienes de información. El Partido de la U, reconocido en el país y representante de intereses de un segmento de la población, Carece de los elementos necesarios para resguardar su información sensible. Ante la existencia de antecedentes de intentos de ataques a otros partidos políticos y organismos electorales, se hace necesario diseñar un SGSI que permita mejorar procesos y proteger la información. Este proyecto contempla la evaluación de la situación actual de seguridad, identificar activos críticos y riesgos asociados, y el establecimiento de políticas y controles de seguridad basados en la norma ISO 27001:2022 con el objetivo de instituir una cultura organizacional de seguridad y reducir el riesgo de ataques cibernéticos. Este proyecto busca que el Partido de la U sea pionero junto con Alianza Verde en velar por la ciberseguridad en su sector y garantizar procesos y activos asociados a la información seguros.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

La información es el activo más significativo en cualquier organización, toda organización se encuentra expuesta a ataques, fugas de información, virus, spam, espionaje o sabotaje, y la organización debe aunar esfuerzos para la protección de la misma. En la actualidad el área administrativa del Partido de la U no cuenta con un sistema integral de controles de seguridad que garantice que la información sea confidencial, integra y que esté siempre disponible, lo que incrementa los riesgos asociados a pérdida, daño o acceso de personal no autorizado a la información, este ítem es relevante dado que maneja información sensible de militantes, simpatizantes, estrategias políticas y detalles confidenciales que pueden ser vulnerados y explotados para su perjuicio o el de sus adeptos. No se han evidenciado registros de auditorías de sistemas, se han realizado auditorías generales de revisoría fiscal y han sido superficiales y de temas básicos, existen unas políticas de seguridad que hace más de 6 años no son actualizadas y no se evidencia un análisis previo de riesgos asociadas a las mismas, dichas políticas deben ser ajustadas e implementadas para garantizar su cumplimiento y no se queden sólo en el papel asegurando estar alineadas a las nuevas necesidades y requerimientos dados los cambios de sede y tecnológicos que ha sufrido la infraestructura, no cuenta con un equipo de gestión de seguridad que revise y actualice constantemente dichas políticas y su cumplimiento, no cuenta con roles y responsabilidades establecidos. No se han presentado propuestas para fortalecer la ciberseguridad de la organización y que las mismas estén respaldadas por la alta dirección, no cuenta con planes que permitan asegurar el normal funcionamiento ante incidentes y la gestión eficiente de los mismos.

Los ataques cibernéticos a partidos políticos en Colombia han sido un tema preocupante en los años recientes, especialmente durante elecciones, estos ataques pueden incluir pishing para engañar empleados y votantes, propagación de noticias falsas, exposición de información confidencial a través de violación de bases de datos y explotación alguna de vulnerabilidad de sus activos, procesos de gestión asociados y recurso humano interno.

En las elecciones presidenciales 2018 en Colombia, el Consejo Nacional Electoral (CNE,2018) denunció que se habían registrado al menos 68 intentos de ataques cibernéticos en su sistema durante la jornada electoral, además el partido político FARC (FARC,2018) también informó que su sitio web había sido atacado durante la campaña electoral, otro caso relevante fue el del Partido Liberal Colombiano que presentó una filtración donde se expusieron los datos de más de 1.7 millones

de afiliados, lo que generó una alerta que implica dirigir esfuerzos para reforzar la seguridad que proteja la información en los partidos políticos (Rojas, 2020)[4].

Tal como se expone en los últimos años Colombia ha sido víctima de varios ciberataques dirigidos a partidos políticos y entes electorales, y se debe establecer como salvaguardar datos sensibles de estas organizaciones para evitar afectar su imagen y proteger sus datos.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo mejorar la protección de la información sensible del Partido de la U, incluyendo datos de los afiliados, estrategias políticas, planes de campaña y otros activos importantes en un entorno de crecientes amenazas cibernéticas, mediante la implementación de un SGSI?

[4] ROJAS, Adriana. Filtración de datos del Partido Liberal afecta a más de 1,7 millones de afiliados. El Espectador. [Sitio Web]. [Consultado: 9 de abril de 2023]. Disponible en: https://www.elespectador.com/tecnologia/filtracion-de-datos-del-partido-liberal-afecta-a-mas-de-17-millones-de-afiliados-articulo-921898/

2. JUSTIFICACIÓN

Ante el incremento de los ciberataques es necesario fortalecer la seguridad en el Partido de la U, diseñar un SGSI basado en ISO 27001:2022 es vital dado que es necesario y primordial proteger la información confidencial y sensible de riesgos y amenazas, estos datos y activos confidenciales pueden ser explotados por terceros para perjudicar al partido, sus miembros y procesos electorales en curso.

Implementar un SGSI permite proteger los datos de las partes interesadas garantizando el cumplimiento del Habeas Data, mejorar la confianza y reputación del partido entre sus seguidores y la sociedad, a la par de permitir consolidar al partido como pionero entre sus similares junto con alianza verde al ser los primeros partidos políticos que cuentan con un SGSI y este se encuentra respaldado por la alta dirección. Dentro de la organización este proyecto contribuirá a establecer una cultura de seguridad, sensibilizando a colaboradores sobre la importancia de proteger la información y fomentando medidas adecuadas para la administración de los datos, desde lo académico este proyecto permite aplicar conocimientos teóricos adquiridos en la formación como especialista en seguridad informática al llevar a la práctica conceptos y herramientas relacionadas con el manejo de riesgos, ejecución de controles y políticas de seguridad, y finalmente en lo personal este proyecto representa un reto y una oportunidad de aprendizaje en un área en constante evolución y creciente importancia en el mundo actual, además me permite fortalecer el liderazgo, capacidad de comunicación y trabajo en grupo al interactuar con los diferentes responsables de la organización.

3. OBJETIVOS

3.1 OBJETIVOS GENERAL

Diseñar un Sistema de Gestión de Seguridad de la Información para el área administrativa del partido de la U basado en ISO 27001:2022 que garantice la confidencialidad, integridad y disponibilidad de la información, minimizando el riesgo de pérdida, daño o acceso no autorizado a la información.

3.2 OBJETIVOS ESPECÍFICOS

Analizar el estado actual de la seguridad de la información basado en controles ISO 27001:2022 contemplando procedimientos, procesos y políticas en el área administrativa del Partido de la U.

Examinar la infraestructura TI del área administrativa del partido de la U a partir de la identificación y clasificación sus activos de información.

Evaluar amenazas y vulnerabilidades de seguridad a las cuales está expuesta el área administrativa del Partido de la U mediante la metodología de gestión de riesgos MAGERIT.

Proponer políticas y controles de seguridad de la información a partir del análisis realizado en el área administrativa del Partido de la U.

4. MARCO REFERENCIAL

4.1 MARCO TEÓRICO

El Partido de la U cuenta con 19 años de reconocimiento en el País, representa intereses y opiniones de un sector de la población, propende formar a sus militantes y simpatizantes en temas políticos e ideológicos y programáticos para fortificar la democracia y la participación activa de ciudadanos, ejerce control político sobre el gobierno y órganos del estado para asegurar su transparencia, responsabilidad y velar por la rendición de cuentas claras. También participa en la elaboración de proyectos que beneficien a los colombianos y vele por sus derechos. Su sede principal está localizada en Bogotá y en las últimas elecciones de Congreso 2022 según la Registraduría Nacional contó con 1.506.000 votos[5] y cuenta con más de 40.000 militantes.

Al abordar los desafíos de seguridad que enfrenta y garantizar la entereza de sus operaciones y sistemas, demostrará su compromiso con el amparo de los datos y la seguridad cibernética, lo que puede ayudar a aumentar la confianza pública en el partido y sus procesos democráticos. El partido de la U será pionero junto con alianza Verde en cuanto a partidos políticos que cuenta con un SGSI dado que ningún otro posee uno, existen algunas entidades públicas que han hecho una implementación efectiva para garantizar la salvaguarda de su información y activos, entre las entidades gubernamentales que han implementado un SGSI se encuentran el Partido Alianza Verde[6] , Ministerio de TICS (MinTIC)[7], la Agencia Nacional de Tierras (ANT)[8] , la Agencia de Seguridad Vial (ANSV)[9] , la Aeronáutica Civil (UAEAC)[10], Personería de Bogotá[11] que han mostrado interés en la ciberseguridad de su infraestructura TI y procesos.

[5] Registraduría Nacional del Estado Civil. Registraduría Nacional del Estado Civil Home. [Sitio Web]. [Consultado: 15 marzo de 2023]. Disponible en: https://www.registraduria.gov.co

[6] Partido Alianza. Home. [Sitio Web]. [Consultado: 08 de abril de 2023]. Disponible en: Verde https://www.alianzaverde.org.co/

[7] Ministerio de Tecnologías de la Información y las Comunicaciones. Inicio. [Sitio Web]. [Consultado: 15 de marzo de 2023]. Disponible en: https://www.mintic.gov.co/portal/inicio/

[8] Agencia Nacional de Tierras. Agencia Nacional de Tierras. [Sitio Web]. [Consultado: 15 de marzo 2023]. Disponible en: https://www.ant.gov.co/

[9] Agencia Nacional de Seguridad Vial. Agencia Nacional de Seguridad Vial. [Sitio Web]. [Consultado: 15 de marzo 2023]. Disponible en: https://ansv.gov.co/

[10] Unidad Administrativa Especial de Aeronáutica Civil. Aeronáutica Civil. [Sitio Web]. [Consultado: 12 de marzo de 2023]. https://www.aerocivil.gov.co

[11] Personería de Bogotá. Sistema de Seguridad y Gestión de la información. [Sitio Web]. [Consultado: 12 de marzo de 2023]. https://www.personeriabogota.gov.co/sistemas-de-gestion/sistema-de-seguridad-y-gestion-de-la-informacion-sgsi

4.1.1 Antecedentes Partidos Políticos en Latinoamérica que han implementado un SGSI.

Existen varios partidos políticos en Latinoamérica que cuentan con un sistema de gestión de seguridad de la información, aunque no es posible conocer exhaustivamente la lista completa de ellos.

Entre los partidos políticos que se sabe que han implementado SGSI, podemos mencionar.

Movimiento Ciudadano (México)

El Movimiento Ciudadano es un partido político en México que se define como una organización progresista, humanista y ciudadana, con un programa orientado a promover los derechos humanos, la equidad social, la transparencia y la responsabilidad pública[12]. En cuanto a su SGSI, el Movimiento Ciudadano ha implementado un SGSI para proteger la información confidencial de sus militantes y afiliados, así como para garantizar la integridad de sus procesos internos y su participación en el ámbito político. La implementación del SGSI tiene como objetivo principal Salvaguardar los datos delicados de la población y mantener su privacidad, así como garantizar la seguridad y los procesos relacionados con la participación ciudadana en el partido. Además, el Movimiento Ciudadano ha destacado la importancia de la transparencia y la obligación de informar en su política de seguridad, lo que les ha permitido generar confianza y credibilidad entre sus seguidores y la sociedad en general.

Alianza Verde (Colombia)

El Partido Alianza Verde es una agrupación política de Se concentra en preservar el entorno natural, promover los derechos humanos, erradicar la corrupción y fomentar la equidad y la justicia social. Fue fundado en el año 2005 y se ha posicionado en una de las fuerzas políticas más significativas del país[13].

En cuanto a su SGSI, se trata de una herramienta que permite proteger y salvaguardar la información que maneja el partido, tanto interna como externa. El SGSI está diseñado para identificar y controlar las amenazas a la seguridad, instituir lineamientos y prácticas de seguridad, y garantizar la continuidad y disponibilidad de la información.

[12]Movimiento Ciudadano. Home, [Sitio Web]. [Consultado: 08 de abril de 2023]. Disponible en: https://movimientociudadano.mx/

[13] Partido Alianza. Home. [Sitio Web]. [Consultado: 08 de abril de 2023]. Disponible en: Verdehttps://www.alianzaverde.org.co/

El SGSI del Partido Alianza Verde se basa en la norma ISO/IEC 27001, que establece los parámetros para un SGSI, de esta manera el partido puede asegurar que su información está protegida de manera efectiva, y que se toman medidas para minimizar los riesgos y garantizar que la información se mantenga confidencial, íntegra y disponible.

El Partido Socialista de Chile

Es una agrupación política de centroizquierda que se fundó en 1933. Se enfoca en la promoción de políticas en pro de fomentar la igualdad social, económica y cultural en el país.[14]

En cuanto a su SGSI, el Partido Socialista de Chile tiene implementado una serie de lineamientos, métodos y prácticas para preservar la información que maneja el partido. Su SGSI se basa en la norma ISO/IEC 27001, referente internacional.

El SGSI del Partido Socialista de Chile tiene como objetivo garantizar que los datos sean confidenciales, íntegros y disponibles en cuanto a información que maneja el partido, minimizando los riesgos de seguridad y asegurando la normal operación del negocio en caso de incidentes de seguridad.

Entre las medidas que el partido ha implementado para proteger su información se encuentran la implementación de contraseñas robustas y la encriptación de información confidencial. y la implementación de cortafuegos y software de detección de amenazas.

Partido Nacional PAN de México

Es un partido de México fundado en 1939. Es un partido de centroderecha que promueve la democracia, la economía capitalista y la libertad individual. El PAN ha gobernado México en dos ocasiones, de 2000 a 2012, con los presidentes Vicente Fox y Felipe Calderón[15].

En cuanto a su SGSI, ha tomado medidas preventivas para resguardar la información que está bajo su responsabilidad. En 2012, el partido fue certificado por el Instituto Nacional de Transparencia (INAI) por su SGSI, apoyado en la norma ISO/IEC 27001.

[14] Partido Socialista de Chile. Home: [Sitio Web]. [Consultado: 9 de abril de 2023]. Disponible en: https://www.pschile.cl/

[15]Partido Nacional PAN. Home: [Sitio Web]. [Consultado: 9 de abril de 2023]. Disponible en: https://www.pan.org.mx/

La implementación de un SGSI ha permitido al PAN garantizar que su información sea confidencial, integra y esté disponible, minimizando los riesgos de seguridad y garantizando la continuidad de las operaciones en situaciones de incidentes de seguridad

4.1.2 SGSI

Un SGSI busca implantar un marco y una serie de políticas, métodos y controles para certificar la protección de la información de una compañía. Su principal objetivo es asegurar que la información sea confidencial, integra y esté disponible, así como garantizar su cumplimiento legal y regulatorio.

Un SGSI es definido como "el conjunto de políticas, procedimientos y estructuras organizaciones y recursos necesarios para establecer, implementar, revisar, monitorear y mejorar la seguridad de la información" (ISO/IEC, 2018, P.2)[16]. Permite a las organizaciones gestionar y proteger sus activos críticos, y ayuda a minimizar los riesgos y asegurar la confianza en la organización. Un SGSI efectivo puede mejorar la confianza y la notoriedad de la organización entre sus clientes y partes interesadas en general.

Importancia de implementar un SGSI: ayuda a proteger información de la organización contra posibles amenazas, riesgos y ataques, cumplimiento legal y normativo aplicables en lo referente a privacidad y protección de datos, así como con los estándares y normas internacionales de seguridad, contribuye a garantizar la continuidad del negocio ya que la información es clave para la operación de la organización, ayuda a fortalecer la imagen y prestigio de la organización ya que manifiesta el compromiso de dicha organización con la protección de la información y finalmente ayuda a reducir costos asociados a incidentes de seguridad.

Un SGSI busca identificar los riesgos y amenazas a la seguridad, evaluar su impacto y probabilidad, y establecer medidas de seguridad para mitigarlos. Al establecer controles de seguridad adecuados, un SGSI busca minimizar la posibilidad de interrupciones en el negocio o pérdidas financieras causadas por la pérdida o compromiso de información valiosa. Un marco teórico para un SGSI incluye los siguientes elementos:

Normas y estándares: Los estándares internacionales, como la norma ISO 27001, proporcionan un marco para la ejecución de un SGSI.

[16] ISO/IEC. Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requisitos (ISO/IEC 27001:2013). [Sitio Web]. [Consultado: 04 de abril de 2023]. Disponible en: https://www.iso.org/standard/54534.

Política de seguridad de la información: describe la postura de una organización en cuanto a la protección de la información.

Evaluación de riesgos: ayuda a identificar las posibles amenazas a la información y a determinar la probabilidad y el impacto de dichas amenazas.

Controles de seguridad: son acciones tomadas para atenuar los riesgos identificados durante la evaluación de riesgos.

Planificación de la continuidad del negocio: contribuye a garantizar la continuidad de las operaciones de la organización en situaciones críticas.

Monitoreo y revisión: ayuda a garantizar que se estén cumpliendo los objetivos de seguridad y a detectar cualquier problema o área que requiera mejoras.

Capacitación y concientización: La capacitación y concientización del personal sobre la seguridad, es esencial para asegurar que todos los miembros del personal entiendan la relevancia de proteger la información y puedan tomar medidas adecuadas para hacerlo.

Figura 1 Elementos SGSI

Fuente: el Autor. (2023)

4.1.3 Seguridad Informática.

Es de gran importancia actualmente dado que los sistemas y redes de comunicaciones son elementos fundamentales para el funcionamiento de las organizaciones y para la vida diaria de las personas.
Se define como "la protección de la información y los sistemas informáticos contra el acceso no autorizado, la divulgación, alteración, destrucción o interrupción" (NIST, 2019)[17].

Figura 2 Procesos Seguridad Informática.

Fuente: el Autor (2023).

4.1.4 ISO 27000

Conjunto de estándares internacionales que implanta las exigencias y adecuadas prácticas para la administración de la seguridad en las compañías. Establece un marco de trabajo, comprende varias normas y guías que cubren diferentes aspectos de seguridad, incluyendo la gestión de riesgos, la administración de la continuidad de operaciones tecnológicas, la administración de incidentes de seguridad, entre otros. proporciona una metodología sistemática para instituir, realizar, conservar y mejorar un SGSI en una organización[18], de manera que se pueda proteger la información de la organización y cumpliendo con regulaciones aplicables en materia de ciberseguridad. La norma ISO 27000 ha sido adoptada por muchas organizaciones en todo el mundo, y su implementación les permite mejorar su postura en cuanto a ciberseguridad, incrementar la confianza de los clientes y disminuir los riesgos de sufrir posibles incidentes de seguridad.

[17] NIST. (2019). Computer Security.[Sitio Web]. [Consultado: 4 de abril de 2023]. Disponible en: https://www.nist.gov/topics/computer-security
[18] International Organization for Standardization ISO 27001:2013 Information technology - Security techniques - Information security management systems – Requirement.[En línea]. [Consultado:9 de abril de 2023]. Disponible en: https://www.iso.org/standard/54534.html

4.1.5 ISO 27001

Establece los criterios necesarios para llevar a cabo un SGSI en una organización. Suministra un marco para gestionar la seguridad efectivamente basados en las necesidades de la organización y las regulaciones aplicables. Establece los requisitos de un SGSI, permite identificar activos críticos respecto a información, los riesgos asociados, la adopción de medidas de resguardo para mitigar dichos riesgos, permite desarrollar normativas y pautas de seguridad, y gestionar la seguridad basado en la mejora continua

Es parte de la serie ISO 27000, que define los criterios y las prácticas más adecuadas para el gobierno de la seguridad de información.

4.1.6 Ciclo PHVA

Este modelo implica planificar lo que se quiere hacer, realizar la tarea planificada, verificar los resultados obtenidos y, finalmente, tomar medidas para mejorar el proceso, se utiliza para gestionar efectivamente la calidad y en otros ámbitos de la gestión organizacional, incluyendo la seguridad de los datos e información[19]. Este Ciclo se basa en la premisa de que cualquier proceso puede ser mejorado continuamente Mediante la identificación de aspectos que pueden mejorarse o perfeccionarse y la implementación de acciones correctivas. Se compone de cuatro fases:

1. Planear: instituyen los objetivos y metas del proceso, se identifican los riesgos y oportunidades de mejora, se establecen los enfoques y los programas necesarios para alcanzar las metas establecidas. y se establecen los indicadores que se utilizarán para medir y establecer el éxito del proceso.

2. Hacer: Se llevan a cabo las estrategias y los planes definidos en la fase de planear.

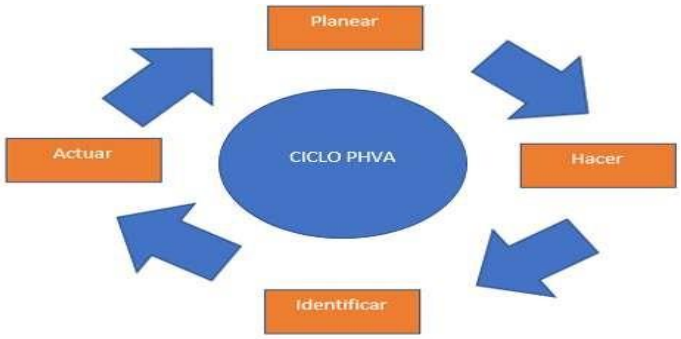
3. Verificar: En esta fase se monitorea y se verifica el cumplimiento del proceso utilizando los indicadores de desempeño definidos en la fase de planear.

4. Actuar: Ese realiza análisis de resultados derivados de la fase de verificación y se toman acciones correctivas para mejorar el proceso.

[19] International Organization for Standardization ISO 27001:2013 Information technology - Security techniques - Information security management systems – Requirement.[En línea]. [Consultado:9 de abril de 2023]. Disponible en: https://www.iso.org/standard/54534.html

La implementación del ciclo PHVA permite a las compañías mejorar continuamente su desempeño y sus procesos incluyendo la seguridad de su información.

Figura 3 Ciclo PHVA



Fuente: el Autor (2023).

4.1.7 MAGERIT

Es un enfoque para manejar los riesgos vinculados a la seguridad. Desarrollada por el Centro Criptológico Nacional de España[20]. Esta metodología se enfoca en la identificación, análisis y abordaje de los riesgos y peligros de seguridad en las organizaciones. MAGERIT permite analizar tanto cualitativa como cuantitativamente los riesgos y amenazas de seguridad. La metodología utiliza una matriz de riesgos que combina la posible ocurrencia de un evento y su posible efecto para evaluar la gravedad del riesgo. Esta evaluación se realiza mediante una combinación de análisis cualitativos y cuantitativos. No se limita a un enfoque exclusivamente cualitativo o cuantitativo, sino que utiliza ambos enfoques para una gestión más completa y positiva de las amenazas de seguridad asociados a la información Esto permite a las organizaciones tomar decisiones informadas sobre cómo abordar los riesgos y amenazas identificados en su entorno.

4.1.8 Análisis Cualitativo

De acuerdo con Braun y Clarke (2019) es una técnica de investigativa basada en la recolección y estudio de datos no numéricos, obtenidos de entrevistas, documentos o procesos de observación. El análisis cualitativo busca identificar los significados y las interpretaciones subyacentes de los datos, a menudo a través de

[20] Centro Criptológico Nacional. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT versión 3). [Sitio Web]. [Consultado: 04 de abril de 2023]. Archivo Pdf. Disponible en: https://www.ccn-cert.cni.es/pdf/magerit-v3-1-manual-completo.pdf

la identificación de patrones y temas emergentes[21]. Es una herramienta importante en la investigación social y permite basado en los datos obtenidos tomar decisiones. Hay varios enfoques para el análisis cualitativo, puede realizarse un análisis de temas, contenido o discurso. Cada enfoque tiene sus propias técnicas y procedimientos para obtener y examinar información de manera sistemática., pero todos comparten el objetivo de comprender los significados e interpretaciones subyacentes de los datos.

4.1.9 Análisis Cuantitativo

Según Hair, Black, Babin y Anderson (2018) El análisis cuantitativo es una técnica de investigación utilizada en diversas disciplinas para recolectar y analizar datos numéricos, generalmente mediante el uso de estadísticas y modelos matemáticos[22]. El análisis cuantitativo se enfoca en la obtención de datos numéricos que pueden ser medidos y analizados para encontrar patrones y tendencias, cuenta con unos pasos que incluyen definir el problema que se investiga, la elección de la muestra, la recolección de datos, la validación de datos, el analiza datos e interpretar resultados obtenidos. La delimitación de la problemática a investigar es crucial para realizar el análisis cuantitativo, ya que debe establecerse claramente qué se quiere medir y cómo se medirá. Luego, se selecciona una muestra de individuos o elementos que representen la población que se quiere estudiar. La recolección de datos en el análisis cuantitativo generalmente implica la utilización de encuestas, cuestionarios, pruebas o mediciones físicas. Una vez que se han recolectado los datos, se validan y se procesan para realizar el análisis.

4.1.10 Análisis Descriptivo

Según Laureano-Cruces y Romero (2019), el análisis descriptivo es una técnica estadística empleada para resumir y describir datos numéricos o variables[23] Esta técnica se utiliza para obtener una comprensión general de las características de un conjunto de datos, como su distribución, tendencia central y variabilidad. El análisis descriptivo contempla una serie de pasos que incluyen la captación de datos, la clasificación de los datos, el cálculo de medidas estadísticas, la capacidad de ver y entender los resultados obtenidos.

---

[21] BRAUN, Virginia. y CLARKE, Victoria. Reflecting on reflexive thematic analysis. Qualitative Research in Sport, Exercise and Health. 11(4), 589-597. [En Línea]. [Consultado: 9 abril de 2023].

[22] HAIR, Joseph.; BLACK, William, BABIN, Barry y Anderson, Rolph. (2018). Análisis multivariante (7ma ed.). Cengage Learning.

[23] LAUREANO, Ana, y ROMERO, Juan. Descriptive analysis: A method for identifying, summarizing and comparing data. Research in Psychotherapy: Psychopathology, Process and Outcome, 22(3), 391-399. [En línea]. [Consultado:9 de abril de 2023]. Disponible en: https://doi.org/10.4081/ripppo.2019.391.

4.2 MARCO CONCEPTUAL

4.2.1 Información

Basado en lo expuesto por Beekman, G., & Quinn, M. J. (2018) es un conjunto de datos procesados y organizados de manera significativa, que permiten a los usuarios tomar decisiones y realizar tareas específicas[24]. En este sentido, la información es un recurso para tomar determinaciones y ejecutar procedimientos en distintos ámbitos

4.2.2 Amenaza

Hace mención a una acción o evento que puede causar deterioro o pérdida de datos o activos de la organización, pueden ser intencionales o involuntarias y pueden proceder de diversas fuentes.

Las amenazas pueden ser internas o externas y pueden tener distintas formas, como malware, phishing, ingeniería social, ataques de denegación de servicio.

4.2.3 Riesgo

Hace mención a la probabilidad de que una amenaza se cristalice y cause daño, puede implicar pérdida o daños en activos. Ha mención a la posibilidad de que ocurran eventos no deseados que afecten seguridad datos y sistemas del área informática de una organización. Estos riesgos pueden ser causados por amenazas internas o externas, vulnerabilidades en la infraestructura tecnológica o fallas en los procesos de seguridad.

4.2.4 Activo de información

Según Whitman & Mattord, 2020 es cualquier información o recurso de tecnología que tenga valor para una organización y que requiera protección contra amenazas[25] Los activos de información pueden ser datos almacenados en un sistema informático, aplicaciones, hardware, software, redes y sistemas de comunicaciones, y cualquier otro elemento que contenga información valiosa para la organización. Es importante identificar y catalogar los activos para establecer medidas de seguridad adecuadas y protegerlos de manera efectiva.

[24] BEEKMAN, George y QUINN, Michael J. Introducción a la informática. (2018). Pearson Educación.

[25] WHITMAN, Michael. y MATTFORD, Herbert .Principles of Information Security. (2020). (6th ed.). Cengage Learning.

4.2.5 Políticas de seguridad

Según Whitman & Mattord, 2020, Una política de información es una serie de directrices y procedimientos que precisan como una organización gestiona, protege y comparte su información. Estas políticas se utilizan para establecer las reglas y normas que rigen el uso, conservación, envío y posibilidad de obtener información y garantizar la seguridad de la misma. Las políticas también pueden incluir medidas de seguridad técnicas y organizativas, así como roles y responsabilidades claras para los empleados de la organización.

4.2.6 Controles

Según Whitman & Mattord, 2020, Los controles son soluciones técnicas y organizativas que se emplean para resguardar los sistemas y datos de una organización frente amenazas internas y externas. Estos controles incluyen políticas, procedimientos, herramientas y tecnologías de seguridad que se utilizan con el objetivo de reducir al mínimo las posibilidades de riesgo y preservar los recursos de información de la organización. Existen diferentes tipos de controles en seguridad informática, como controles preventivos, detectivos y correctivos, que se utilizan para mejorar la seguridad de sistemas y datos.

4.2.7 Confidencialidad

Preservación de la información sensible o valiosa de una entidad para evitar que sea revelada o divulgada a personas no autorizadas. La confidencialidad se asegura a través de la utilización de métodos de resguardo que limitan el acceso a los datos para que puedan ser accedidos sólo por aquellos que tienen una necesidad legítima de conocerlos. El resguardo de la confidencialidad es especialmente transcendental para preservar la salvaguarda de la información privada y la propiedad intelectual de la Compañía.

4..2.8 Disponibilidad

Disposición de los sistemas y recursos de TI para ser usados por los usuarios autorizados cuando se requieran Esto implica certificar que los sistemas informáticos, aplicaciones, datos y otros recursos estén disponibles y funcionen correctamente para apoyar las operaciones de la organización en todo momento. La disponibilidad es importante para garantizar que los usuarios que ha sido autorizados logren acceder a la información y los servicios que precisan para realizar sus labores y cumplir con las metas de la organización.

4.2.9 Integridad

Proteger la información de cambios realizados sin permiso o de manera accidental. La integridad se mantiene cuando los datos permanecen exactos, completos e inalterados durante su creación, transmisión, almacenamiento y procesamiento. Para garantizar la integridad, se deben tomar medidas que aseguren que la información no sea alterada de manera no autorizada o accidental. Esto incluye establecer políticas y procedimientos de control de cambios, la autenticación de usuarios y la implementación de medidas técnicas de seguridad, como firmas digitales, cifrado y sistemas de detección de cambios.

4.1.10 Vulnerabilidad

Debilidad en un sistema, aplicación, proceso o procedimiento que puede ser aprovechado por un atacante para vulnerar la seguridad. Las vulnerabilidades pueden deberse a errores de diseño, configuración, implementación o mantenimiento de los sistemas informáticos y pueden permitir que los atacantes accedan a información confidencial, modifiquen o dañen datos o interrumpan los servicios críticos de la empresa.

4.2.11 Incidente de seguridad

Evento que pueda poner en peligro la información de una compañía. Estos incidentes pueden incluir ataques cibernéticos, intrusiones, robo o pérdida de datos, fallas en los sistemas o desastres naturales. Cuando se produce un evento de seguridad, la organización debe responder rápidamente para atenuar el impacto del incidente y proteger la información. Esto puede incluir la investigación del incidente para determinar la causa, la notificación a las partes afectadas, la recuperación de información y la ejecución de medidas de seguridad adicionales que permitan evitar incidentes parecidos en el futuro.

4.3 MARCO HISTÓRICO

En el marco histórico del proyecto de diseño de un SGSI para el partido de la U en Colombia existen factores políticos, sociales y tecnológicos que deben ser considerados para asegurar la información del partido en un entorno complejo y cambiante.

Conflicto armado: Colombia ha sufrido durante décadas un conflicto armado interno que ha tenido un impacto significativo en la seguridad y la estabilidad del país. La presencia de grupos armados y organizaciones delictivas ha generado un ambiente de inseguridad en el que la protección de la información y la ciberseguridad se han transformado en aspectos críticos. Además, el proceso de paz iniciado en 2016 ha sido un factor clave en la estabilidad política del país y deberá ser contemplado en el diseño del SGSI.

Políticas y leyes: En Colombia, el Gobierno ha implementado políticas y leyes para mejorar la seguridad de la información. La Ley 1581 de Protección de Datos Personales establece los requisitos para el tratamiento de información personal y es importante contemplarla en el diseño del SGSI para asegurar su cumplimiento. Asimismo, el Gobierno ha promovido la creación de entidades especializadas en ciberseguridad, como la Agencia Nacional de Seguridad Cibernética (ANSPEC)[26], para fortalecer la protección de la información en el país.

Digitalización: El crecimiento de la tecnología y la digitalización ha llevado a un mayor riesgo de ciberataques y violaciones de seguridad informática. Colombia ha avanzado en la adopción de tecnologías digitales en diversos sectores, lo que ha aumentado la exposición de la información a riesgos cibernéticos. En este sentido, el SGSI deberá contemplar las acciones requeridas para proteger la información del partido de la U y garantizar su integridad y confidencialidad.

Participación política de la U: La participación política del partido de la U ha tenido altibajos a lo largo de la historia del país, con periodos de fuerte influencia y otros de menor presencia en el escenario político. Es importante considerar la posición actual del partido y su proyección futura al diseñar el SGSI, así como las necesidades específicas de protección de la información que pueda tener el partido en su actividad política.

[26] Ministerio de Defensa. Agencia Nacional de Seguridad Cibernética. [Sitio Web]. [Consultado: 9 de abril 2023]. Disponible en: https://www.mindefensa.gov.co/irj/go/km/docs/Mindefensa/Documentos/descargas/Seguridad/AgenciaNacionaldeSeguridadCibernetica.pdf

4.4 MARCO CONTEXTUAL

El Partido de la U es una agrupación política colombiana fundada en 2005, cuyo nombre completo es Partido de la Unión por la Gente. Esta organización tiene como objetivo trabajar por una sociedad más justa, solidaria e igualitaria, y estimular la participación ciudadana en las decisiones políticas tomadas.

El partido cuenta con representantes en los distintos órganos de gobierno del país, incluyendo el Congreso de la República, las gobernaciones, alcaldías y concejos municipales. Su ideología se basa en la lucha por el Estado de derecho social, la garantía de los derechos humanos y fomentar la democracia participativa.

El Partido de la U se enfoca en la elaboración de estrategias gubernamentales que promuevan la igualdad social y la inclusión, especialmente en temas como la educación, la salud, la vivienda y el trabajo. Además, impulsa la colaboración internacional y la integración regional para avanzar hacia un desarrollo sostenible del país.

En su estructura interna, el partido cuenta con diferentes instancias de participación y toma de decisiones, como la Mesa Directiva Nacional y las mesas directivas departamentales y municipales., y los comités de base. Estas instancias tienen como objetivo garantizar la participación activa la ciudadanía tiene un papel importante en la vida política del país y cuenta con una sede administrativa principal.

Compañía que cuenta con más de 80 empleados, una sede física de dos pisos domicilio Bogotá, que cuenta con 19 años de trayectoria en el sector.

4.4.1 Misión

El Partido de la U es una entidad política que se rige por principios democráticos y populares de centro, con el objetivo de satisfacer la entidad busca satisfacer las demandas de los ciudadanos y fomentar los principios del Estado Social y Democrático de Derecho. Su objetivo es establecer un Estado avanzado, claro, efectivo, justo, participativo, diverso y equitativo, busca alcanzar un crecimiento económico completo y duradero que garantice los derechos determinados en la Constitución y los pactos internacionales, junto con la seguridad, la vida y la dignidad de las personas, la protección del medio ambiente, la diversidad y la prosperidad social.

4.4.2 Visión

El objetivo del Partido de la Unión por la Gente es convertirse en la fuerza política líder del país, a través de una propuesta amplia, inclusiva y diversa que fomente el respeto a la institucionalidad, el Estado Social y Democrático de Derecho, la seguridad humana, el bienestar social, el partido se propone alcanzar el desarrollo económico sostenible, la conservación del medio ambiente, la construcción de una paz duradera, la promoción de los derechos civiles y la igualdad de género, así como la inclusión de las comunidades diversas. Para ello, busca involucrar de manera activa a sus miembros en todo el territorio nacional.

4.4.3 Actividades realizadas por el partido

Campañas electorales: los partidos políticos en Colombia suelen llevar a cabo campañas electorales para promover a sus candidatos y atraer votantes. Esto puede incluir la realización de eventos públicos, la distribución de propaganda electoral, la publicidad en medios de comunicación, entre otros.

Participación en el Congreso: los partidos políticos en Colombia tienen representantes en el Congreso, quienes presentan y debaten proyectos de ley y políticas públicas. Además, pueden participar en comisiones y grupos de trabajo para discutir temas específicos.

Organización de eventos: los partidos políticos en Colombia suelen organizar eventos para sus seguidores y simpatizantes, como mítines, marchas y concentraciones. Estos eventos pueden ser una forma de promover su ideología y de demostrar su fuerza política.

Movilización de votantes: los partidos políticos en Colombia suelen movilizar a sus seguidores para que voten en las elecciones. Esto puede incluir el transporte de votantes a los centros de votación, la distribución de información sobre cómo votar y la realización de campañas para incentivar la participación electoral.

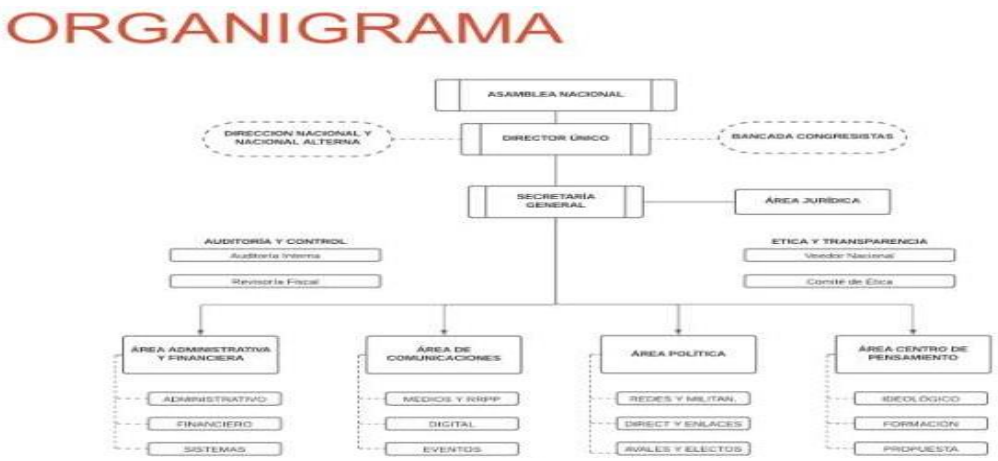
Formación política: los partidos políticos en Colombia pueden ofrecer formación política para sus seguidores y miembros. Esto puede incluir cursos, talleres y seminarios sobre temas políticos y sociales relevantes.

Participación en debates públicos: los partidos políticos en Colombia suelen participar en debates públicos para discutir temas relevantes y promover su ideología. Esto puede incluir debates en medios de comunicación, foros públicos y otros eventos similares.

Contacto con la ciudadanía: los partidos políticos en Colombia pueden llevar a cabo actividades para establecer contacto con la ciudadanía, como encuestas, entrevistas y reuniones con grupos comunitarios. Esto puede ayudarles a conocer las necesidades y preocupaciones de la población y a adaptar su plataforma política en consecuencia.

4.4.4 Estructura

Figura 4 Organigrama Partido de la U



Fuente: Partido de la U

Figura 5 Estructura Área Sistemas

Fuente: el Autor.

Tabla 1 Funciones Personal Sistemas

Cargo	Funciones
Coordinador de Sistemas	Administrar Red interna y Externa y dispositivos. Administrar S.I Administración Copias de Seguridad Garantizar la integración de datos y plataformas. Revisar diseño y ejecución de pruebas para desarrollos a presentar Coordinar cruces de información entre las diferentes bases de datos. Dirigir procesos de capacitación Administración de cuentas de correo electrónico Administración VPN Administración cuenta Zoom
Desarrollador (Tercero)	Ajustar sistemas según nuevos requerimientos Mantenimiento plataforma SIU y página Web
Auxiliar de Soporte	Brindar soporte técnico a funcionarios en ofimática Realizar mantenimiento a equipos y periféricos Realizar copias de seguridad Apoyar procesos de impresión y copias Apoyar gestión de usuarios y contraseñas Configurar internet Apoyo video conferencias

Fuente: El Autor.

4.4.5 Ubicación Física de la Compañía

Colombia – Bogotá. Cundinamarca

Calle 36 # 15-08 Teusaquillo.

4.5 ANTECEDENTES O ESTADO ACTUAL

Varios partidos políticos en Latinoamérica han implementado un SGSI para proteger su información y garantizar la integridad de sus procesos internos y su participación en el ámbito político. Algunos de estos partidos son el Movimiento Ciudadano en México, el Partido Alianza Verde en Colombia, el Partido Socialista de Chile y el Partido Nacional PAN de México. Estos partidos han implementado sus SGSI - ISO/IEC 27001 y han tomado medidas preventivas para resguardar su información.

4.5.1 Movimiento Ciudadano (México)

El partido ha implementado un SGSI para proteger la información confidencial de sus militantes y afiliados, así como garantizar la integridad de sus procesos internos y su participación en el ámbito político. El Movimiento Ciudadano ha destacado la importancia de ser transparentes y la rendir públicamente cuentas en su política de seguridad de la información.

4.5.2 Alianza Verde (Colombia)

El Partido Alianza Verde cuenta con un SGSI diseñado para detectar y gestionar los riesgos asociados a la seguridad, implantar políticas y procedimientos de seguridad, y garantizar la continuidad y que la información esté disponible. El SGSI se basa en la norma ISO/IEC 27001.

4.5.3 Partido Socialista de Chile

El partido cuenta con un SGSI implementado que tiene como objetivo garantizar que los datos sean confidenciales, íntegros y disponibles en cuanto a información que maneja el partido, minimizando los riesgos de seguridad y asegurando la normal operación del negocio en respuesta a eventos de seguridad. Su SGSI basado en ISO/IEC 27001.

4.5.4 Partido Nacional PAN de México

El partido ha sido certificado por el Instituto Nacional de Transparencia (INAI) por la ejecución de su SGSI, basado en ISO/IEC 27001. El PAN ha tomado medidas preventivas para resguardar la información que está bajo su responsabilidad.

4.6 MARCO LEGAL

En el caso de Colombia, el marco legal que se aplica a los SGSI es la Ley 1581 de 2012 y sus disposiciones.

La Ley 1581 de 2012[27] establece el régimen general de protección de datos de las personas e instituye las deberes que tienen tanto los titulares de los datos como las entidades encargadas de su gestión y protección. La Ley instituye que todas las empresas deben implementar protocolos de protección adecuados en cuanto a la administración de los datos personales, incluyendo el diseño y la implementación de un SGSI.

Además, la Ley 1273 de 2009[28] establece el marco legal para combatir delincuencia informática en el país. Esta ley Establece penalidades para los crímenes cibernéticos, como el acceso no autorizado a sistemas, la interceptación de datos y la alteración de datos. Por lo tanto, las empresas y organizaciones que implementan un SGSI también deben tener en cuenta estas regulaciones para proteger la información y la prevención de delitos informáticos.

El Decreto 1151 de 2008 es una normativa emitida por el Gobierno de Colombia, que Establece las directrices fundamentales de la estrategia de Gobierno en Línea. (GEL) del país[29]. Esta estrategia que la gestión pública sea transparente, mediante el uso de TICS promoviendo la intervención ciudadana y la simplificación de trámites y procesos.

El Decreto reglamenta parcialmente la Ley 962 de 2005, establece un marco jurídico para la eliminación o simplificación de trámites y procedimientos innecesarios o que obstaculizan el ejercicio de las obligaciones y el cumplimiento de los derechos de los ciudadanos ante el Estado.

Entre las disposiciones del Decreto 1151 de 2008, se encuentran la creación de la Comisión Intersectorial, la enunciación de directrices y criterios para la implementación de la GEL en las organizaciones gubernamentales, la promoción

[27] DAPRE Presidencia. Normativa. [Sitio Web]. [Consultado: 04 de abril de 2023]. Archivo Pdf. Disponible en: https://dapre.presidencia.gov.co/normativa/normativa/LEY%201581%20DEL%2017%20DE%20OCTUBRE%20DE%202012.pdf

[28] DAPRE Presidencia. Normativa. [Sitio Web]. [Consultado: 04 de abril de 2023]. Archivo Pdf. Disponible en: https://dapre.presidencia.gov.co/normativa/normativa/LEY%201273%20DEL%2023%20DE%20DICIEMBRE%20DE%202009.pdf

[29] Decreto 1151 de 2008. Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea de la República de Colombia, se reglamenta parcialmente la ley 962 de 2005, y se dictan otras disposiciones. Presidencia de la República de Colombia. [Sitio Web]. [Consultado: 04 de abril de 2023]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=32713.

del uso de firma electrónica y la obligatoriedad de la publicación de información en los sitios web de las entidades públicas.

La Ley 1712 de 2014, Ley de Transparencia y Acceso a la Información Pública Nacional, es una normativa emitida por el Gobierno de Colombia, se trata de una ley que busca asegurar el acceso a información pública y promover la transparencia en la gestión pública[30].

Esta ley establece los mecanismos y procedimientos para el acceder a la información pública en Colombia, así como las obligaciones de las entidades públicas en relación con la divulgación y publicación de la información que manejan. Además, la ley promueve la rendición de cuentas y la intervención ciudadana en los temas públicos.

[30] Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. Congreso de la República de Colombia. [Sitio Web]. [Consultado: 04 de abril de 2023]- Disponible en: https://www.secretariasenado.gov.co/senado/basedoc/ley_1712_2014.html.

5. DISEÑO METODOLÓGICO

5.1 FASE DIAGNÓSTICO SITUACIÓN ACTUAL E IDENTIFICACIÓN DE ACTIVOS

5.1.1 Contexto del Partido de la U: Área Administrativa

Identificación de la Organización:

Nombre de la Organización: Partido de la U.
Ubicación: Bogotá - Colombia, calle 36 # 15 – 08 Teusaquillo
Tipo de Organización: Partido Político.

5.1.2 Entorno Político:

Regulaciones: Las regulaciones colombianas incluyen la Ley Estatutaria 1581 de 2012, que regula la protección de datos personales y la Ley 1475 de 2011, que establece las normas para los partidos y movimientos políticos.

5.1.3 Stakeholders: Miembros del partido, líderes políticos, donantes, afiliados, empleados internos y externos, proveedores y autoridades gubernamentales.

5.1.4 Actividades Administrativas:

Procesos Administrativos: Procesos como la gestión de afiliados, recaudación de fondos, comunicaciones internas, campañas políticas y gestión de recursos humanos son cruciales.

Sistemas de Información: Sistemas para manejar datos de afiliados, registros financieros, correos electrónicos internos y plataformas de redes sociales utilizadas para campañas y comunicación política.

5.1.5 Riesgos y Amenazas:

Amenazas Externas: Amenazas como ciberataques, manipulación de información en redes sociales y robo de datos pueden tener un impacto significativo en la reputación del partido y la confianza pública.

Amenazas Internas: Acceso no autorizado a datos sensibles por parte de empleados descontentos o miembros del partido con agendas diferentes.

5.1.6 Objetivos de Seguridad:

Confidencialidad: Garantizar que los datos de los afiliados, donantes y estrategias políticas estén protegidos contra el acceso no autorizado.

Integridad: Evitar la manipulación de datos financieros y políticos, asegurando que la información no sea alterada sin autorización.

Disponibilidad: Asegurar que los sistemas estén disponibles para los miembros autorizados del partido en todo momento, especialmente durante las campañas políticas.

Alcance del SGSI:

Ámbito Geográfico: Oficina Administrativa del partido en Colombia y cualquier ubicación donde se almacenen o procesen datos administrativos.

Alcance Funcional: Procesos clave como la gestión de miembros, recaudación de fondos, gestión de campañas y comunicaciones internas estarán dentro del alcance del SGSI.

Normativas de Seguridad:

Estándares de Seguridad: Implementar controles basados en estándares como ISO/IEC 27001 para garantizar que los datos estén protegidos de acuerdo con las mejores prácticas internacionales.
Cultura de Seguridad:

Concientización: Realizar entrenamientos regulares sobre seguridad de la información para todos los empleados y miembros del partido, destacando la importancia de proteger la información confidencial.
Evaluación y Mejora Continua:

Auditorías y Evaluaciones: Programar auditorías regulares del SGSI para identificar áreas de mejora y garantizar que los controles estén siendo efectivos.
Retroalimentación: Obtener retroalimentación regular de los miembros y empleados para ajustar las medidas de seguridad según las necesidades y preocupaciones cambiantes.

La fase de evaluación de la situación actual y el reconocimiento de los aspectos relevantes y clasificación de activos ser hará a través de recolección de información, observación, revisión de documentos y entrevistas, realizar entrevistas con los responsables de área de la compañía, para conocer los activos informáticos que utilizan, identificar procesos y procedimientos empleados. Se emplearán listas de chequeo basados en controles de declaración de aplicabilidad SOA ISO27001 para identificar la situación actual del Partido en cuanto a seguridad y para establecer su estado de implementación y documentar hallazgos y recomendaciones. Esta técnica permite recopilar información de primera mano.

Después de recopilar la información de los activos TI, se identificarán activos TI y se realizará un análisis exhaustivo de los factores que podrían afectar que la información permanezca íntegra, disponible y confidencial. De esta forma, se identificarán activos críticos y los riesgos que afectarían la seguridad de la compañía.

La metodología empleada para identificar y clasificar los activos TI en un SGSI se basa en los siguientes pasos:

Identificación de los activos: Se realiza un inventario completo de los activos de TI que se encuentran en la compañía, incluyendo hardware, software, datos, redes y servicios.

Valoración de los activos: Se evalúa el valor de cada uno de los activos identificados, considerando su importancia para la organización y su impacto en caso de una posible pérdida de disponibilidad, integridad o confidencialidad.

Clasificación de los activos: Una vez identificados y valorados los activos de TI, se deben clasificar según su importancia y riesgo asociado, utilizando un criterio de clasificación definido previamente. Esta clasificación puede ser en función de la criticidad, la confidencialidad, la integridad o la disponibilidad de los activos.

Protección de los activos: Finalmente, se establecen medidas de seguridad adecuadas para cada categoría de activos clasificados, garantizando la protección adecuada de los mismos y mitigando los riesgos identificados.

5.2 ANÁLISIS DE RIESGOS

Se realizará análisis cualitativo y cuantitativo igualmente para evaluación de riesgos y amenazas asociados, análisis descriptivo para ordenar resultados. Se complementará la gestión de riesgos empleando la herramienta MAGERIT.

Con MAGERIT se evaluarán los riesgos asociados a los activos, siguiendo estos pasos:

Identificar los activos de información. Estos activos pueden incluir datos, sistemas, infraestructuras, entre otros.

Clasificar los activos de información: se debe clasificar cada uno de los activos de información según su importancia para el negocio y su nivel de sensibilidad.

Identificar las amenazas: reconocidos los activos TI se deben identificar las posibles amenazas a los que están expuestos. Estas amenazas pueden provenir del interior o exterior de la compañía.

Valorar la vulnerabilidad: Esto implica determinar las debilidades o fallas en la seguridad que podrían permitir que una amenaza tenga éxito.

Calcular el riesgo: después de evaluar las amenazas y vulnerabilidades, se debe calcular el riesgo asociado a cada activo de información. Esto implica establecer la posibilidad de que suceda una amenaza y el impacto al negocio.

Priorizar los riesgos: por último, se deben ordenar los riesgos identificados según su nivel de riesgo y su importancia para el negocio. Esto permitirá aunar los esfuerzos y recursos en aquellos riesgos que son más críticos y necesitan ser mitigados con mayor urgencia.

5.3 PROPONER POLÍTICAS Y CONTROLES

Basado en los 114 Controles de ISO27001 y su aplicabilidad, se identificarán los controles necesarios para diseñar el sistema de acuerdo a la norma ISO/IEC 27001:2022, basados en el análisis de riesgo realizado en la fase anterior a fin de mitigarlos. Luego, se procederá a diseñar una propuesta de políticas de seguridad personalizadas para la empresa para disminuir los riesgos identificados y mejorar la seguridad y su revisión periódica estableciendo roles y responsabilidades. La metodología para proponer políticas y controles:

Análisis de riesgos: Después de haber completado el análisis de los riesgos que afectan la compañía en materia de seguridad, se realiza una identificación de las debilidades y peligros potenciales que pueden poner riesgo los activos TI.
Definición de objetivos y políticas de seguridad: Una vez identificados los riesgos, se deben definen los objetivos y lineamientos de seguridad que se deben cumplir. Estas políticas deben estar en concordancia con la estrategia de la compañía y con los requisitos legales y regulatorios que afectan al sector de la compañía.

Selección de controles de seguridad: A partir de las políticas definidas, se seleccionan los controles que protejan los activos de TI de la compañía. Estos controles pueden ser técnicos, organizativos o legales, y se deben acomodar a los requisitos específicos de la compañía.

Alcance: Área administrativa Partido de la U.

6. ANÁLISIS SITUACIÓN ACTUAL PARTIDO DE LA U – OBJETIVO 1

La seguridad es un tema relevante actualmente, especialmente en el ámbito político. Los partidos políticos manejan gran cantidad de información sensible y confidencial, por lo que es fundamental que cuenten con sistemas de seguridad que les permitan protegerla de forma efectiva.

Por lo enunciado anteriormente en este capítulo se evalúa la actualidad del Partido de la U en cuanto a la gestión de la seguridad, a través de la aplicación de los controles establecidos por la norma ISO 27001. La evaluación se realizará mediante un análisis exhaustivo de los diferentes procesos, políticas y procedimientos que el partido tiene implementados para proteger su información, con el fin de detectar posibles debilidades y oportunidades de perfeccionamiento.

El resultado de esta evaluación permitirá al Partido de la U tener una visión clara de cómo se encuentra respecto a seguridad, lo que le permitirá tomar decisiones y medidas para fortalecer su SGSI y proteger de manera efectiva la información confidencial de sus militantes y afiliados. Revisando cada uno de los controles el Partido de la U puede evaluar de manera exhaustiva la realidad de su seguridad, identificar posibles vulnerabilidades o brechas en sus procesos, e incluir medidas preventivas para minimizar los riesgos y proteger sus datos.

Además, la implementación de estos controles también les permite estar acorde con los requisitos normativos y de índole legal relacionados con la protección de la información, generar confianza y credibilidad entre sus militantes y afiliados, y mejorar su imagen y reputación como organización comprometida con la seguridad

En el capítulo se ilustrará a grandes rasgos sobre la estructura del Partido de la U, su ubicación, número de empleados, estructura organizacional y TI, posteriormente después de evaluar documentos suministrados y entrevistas con líderes de área se realizó un diagnóstico de su situación actual basado en los controles ISO que tiene aplicados y la forma en la que son implementados, registrando hallazgos, estado del control y recomendaciones.

6.1 ANÁLISIS SITUACIÓN ACTUAL BASADO EN CONTROLES ISO 27001

Evaluación de la situación actual evaluando los 15 objetivos y 114 objetivos de la Norma.

Figura 6 Controles ISO

Anexo	Descripción Control
A5	POLITICAS DE SEGURIDAD
A6	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION.
A7	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
A8	GESTIÓN DE ACTIVOS
A9	CONTROL DE ACCESO
A10	CIFRADO
A11	SEGURIDAD FÍSICA Y AMBIENTAL
A12	SEGURIDAD EN LA OPERATIVA
A13	SEGURIDAD EN LAS TELECOMUNICACIONES
A14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
A15	RELACIONES CON SUMINISTRADORES.
A16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN
A17	ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
A18	CUMPLIMIENTO

Fuente: el Autor.

Basados en entrevistas con jefaturas de sistemas, jurídica, archivo y administrativa se pudieron establecer el cumplimiento o no de los controles asociados a los anexos anteriores, el proceso de apoyo en la revisión de documentos suministrados por el partido de la U, para poder identificar de esta manera la situación actual respecto a seguridad informática y establecer qué se está implementando, que no y se debe implementar y qué definitivamente no es necesario. Se realizará un análisis anexo por anexo identificando su cumplimiento, los hallazgos y las observaciones o recomendaciones.

A5 POLÍTICAS DE SEGURIDAD

Figura 7 Anexo 5

ISO 27002 Controles	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
5.1.1	Conjunto de políticas para la seguridad de la información.	IMPLEMENTAR	Se evidencian unas políticas obsoletas que no están ajustadas a las nuevas necesidades del negocio, incluso al cambio de su sede física e infraestructura TI	Crear e implementar políticas de Seguridad de la información ajustadas a la situación actual.
5.1.2	Revisión de las políticas para la seguridad de la información.	IMPLEMENTAR	No se evidencian revisiones y actualización de las políticas desde hace más de 5 años.	Se propone definir responsables y frecuencia de revisiones

Fuente: el autor.

Se evidencian unas políticas obsoletas que no se ajustan a la situación actual del Partido, incluso fueron desarrolladas hace más de 5 años y la sede ha cambiado 3 veces, no hay evidencia de responsables de aplicación y planes de capacitación al personal, los mismos desconocen su existencia, no se evidencian actualizaciones ni encargado del proceso.

A6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

Figura 8 Anexo 6.1

ISO 27002 Controles	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
6.1.1	Asignación de responsabilidades para la seguridad de la información.	IMPLEMENTAR	No se evidencian responsabilidades de seguridad de información	Definir roles y responsabilidades asociadas al proceso de seguridad de la información.
6.1.2	Segregación de tareas.	IMPLEMENTADO	En el Contrato o vínculo laboral suscrito	N/A
6.1.3	Contacto con las autoridades.	IMPLEMENTAR	No se evidencia responsable	Definir y documentar responsable de Seguridad encargado de contacto con Autoridades.
6.1.4	Contacto con grupos de interés especial.	IMPLEMENTAR	No se evidencia responsable	Definir y documentar responsable de Seguridad encargado de contacto con Autoridades.
6.1.5	Seguridad de la información en la gestión de proyectos.	IMPLEMENTAR	No se Evidencia	Incluir Gestión de proyectos con participación TI que garantice la Seguridad informática

Fuente: el Autor.

Este anexo indica que no se han encontrado roles y responsabilidades definidos en relación a temas de seguridad. Es posible que la organización no tenga claridad sobre quiénes son los responsables de implementar medidas de seguridad, supervisar su cumplimiento y tomar decisiones en caso de eventos de seguridad. Se asume que el responsable es el Coordinador de sistemas, pero no hay nada documentado ni establecido, no se contempla lo referente a trabajo remoto ni existe documentación alguna del préstamo de equipos, configuraciones y políticas asociadas al proceso. En general, la interpretación de estos hallazgos sugiere que la compañía necesita mejorar su cultura de seguridad y asegurarse de que las responsabilidades y procesos están claramente definidos y documentados. Se sugiere implementar las recomendaciones mencionadas para fortalecer la gestión de la seguridad.

Anexo 6.2 Dispositivos para movilidad y teletrabajo

Figura 9 Anexo 6.2

ISO 27002 Controles	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
6.2.1	Política de uso de dispositivos para movilidad.	IMPLEMENTAR	No se contemplan aspectos de teletrabajo en las políticas definidas ni está documentado procesos y controles	Incluir aspectos de teletrabajo en las políticas, documentar procesos y controles. se debe proteger la información a la que se tiene acceso, que es procesada o almacenada en lugares en los que se realiza teletrabajo.
6.2.2	Teletrabajo.	IMPLEMENTAR	No se contemplan aspectos de teletrabajo en las políticas definidas ni está documentado procesos y controles	Incluir aspectos de teletrabajo en las políticas, documentar procesos y controles. se debe proteger la información a la que se tiene acceso, que es procesada o almacenada en lugares en los que se realiza teletrabajo.

Fuente: el Autor

Según los hallazgos, se recomienda que la organización implemente una política de teletrabajo y defina los métodos y revisiones necesarios para proteger la seguridad en este contexto. Es relevante que se establezcan los roles y responsabilidades correspondientes, y se capacite a los trabajadores en el uso seguro de los dispositivos de movilidad. Además, se recomienda realizar una estimación de riesgos específica para el teletrabajo y se establezcan disposiciones de seguridad adecuadas para proteger los datos. Es importante que esta política de teletrabajo sea actualizada regularmente y que se realicen auditorías periódicas para garantizar su cumplimiento.

A7 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

Figura 10 Anexo 7.1

ISO 27002 Controles	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
7.1.1	Investigación de antecedentes.	IMPLEMENTADO	En el Contrato o vínculo laboral suscrito, recursos humanos y jurídica cumplen a cabalidad este aspecto	Para minimizar los riesgos en el manejo de la información, se realiza una revisión de los antecedentes de los nuevos empleados que serán contratados por la entidad. De esta manera, se podrá conocer su historial laboral y personal para asegurarse de que no haya antecedentes que puedan poner en riesgo la seguridad de la información de la organización
7.1.2	Términos y condiciones de contratación.	IMPLEMENTADO	En el Contrato o vínculo laboral suscrito, recursos humanos y jurídica cumplen a cabalidad este aspecto	Los contratos de los empleados deben incluir cláusulas que especifiquen las responsabilidades y los cuidados que deben tener con la información de la Entidad.

Fuente: el Autor.

Se evidencia el cumplimiento de este punto a cabalidad por parte del área jurídica y de recursos humanos, los antecedentes del personal son requeridos y estudiados y los contratos incluyen convenios confidenciales y seguridad.

Figura 11 Anexo 7.2

ISO 27002 Controles	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
7.2.1	Responsabilidades de gestión.	IMPLEMENTAR	Aunque los empleados están al tanto de sus responsabilidades es fundamental asegurar que los empleados mantengan su conocimiento actualizado y sean conscientes de cualquier cambio o actualización en los deberes relacionados con su trabajo	la Entidad debe proporcionar los medios adecuados para garantizar que sus empleados cumplan con sus deberes en Seguridad de la Información durante todo su ciclo laboral.
7.2.2	Concienciación, educación y capacitación en seguridad de la información	IMPLEMENTAR	No se Evidencia	Es importante que la Entidad desarrolle un programa continuo de formación y concientización en seguridad de la información dirigido a sus empleados y terceros relacionados, con el fin de crear una cultura de seguridad.
7.2.3	Proceso disciplinario.	IMPLEMENTADO	Incluido en los contratos.	N/A

Fuente: el Autor.

Es importante que el Partido se asegure de que los empleados reciban capacitaciones periódicas y actualizaciones sobre las responsabilidades relacionadas con la seguridad. Además, la organización debe proporcionar los recursos requeridos para que los empleados puedan cumplir con sus deberes de manera efectiva y eficiente. La finalidad de este programa es crear una cultura, promoviendo buenas prácticas.

Figura 12 Anexo 7.3.1

Control	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
7.3.1	Cese o cambio de puesto de trabajo.	IMPLEMENTADO	Incluido en los contratos.	Se debe informar a los empleados o contratistas, las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de contrato, los cuales deben cumplir.

Fuente: el Autor.

Después de revisar la lista de verificación relacionada con el dominio 7, se puede concluir que el partido está llevando a cabo una buena gestión en la contratación de personal. Se están utilizando herramientas para buscar antecedentes públicos y, en algunos casos, se están involucrando terceros para la contratación. Todo esto demuestra que el personal contratado no tiene problemas judiciales o pendientes con el estado u otras entidades. Se deben fortalecer procesos de capacitación y concientización del personal.

Anexo 8 Gestión de Activos

Figura 13 Anexo 8.1

Control	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
8.1.1	Inventario de activos.	MEDIANAMENTE IMPLEMENTADO	El área de Sistemas lleva un inventario básico de activos, Se debe fortalecer este aspecto.	La Entidad debe mantener un inventario de recursos o activos de información. Los dueños de la información deben clasificar la información basados en su valor, sensibilidad, riesgo de pérdida o compromiso.
8.1.2	Propiedad de los activos.	IMPLEMENTADO	El área de Sistemas lleva un inventario y tiene control sobre el mismo, es actualizado anualmente.	El área de sistemas debe llevar una supervisión y mantenimiento adecuados del inventario de activos de tecnología e información. Esto implica establecer responsabilidades sobre la posesión de dichos activos y la información que contienen, así como realizar un control riguroso sobre el licenciamiento de software.

Fuente: el Autor.

Se deben evaluar los activos que no están incluidos en el inventario actual y se agreguen al mismo. También es importante que se establezca un proceso para actualizar el inventario de forma periódica y se definan responsabilidades claras para su mantenimiento. Se recomienda que se realice una jornada de concientización y capacitación para todos los empleados, donde se expliquen las políticas y procedimientos establecidos, las actividades permitidas y prohibidas y las consecuencias de incumplir las reglas. Además, se debe determinar un proceso de monitoreo y seguimiento para verificar cumplimiento. Se sugiere que se realice una revisión periódica de los registros de actas de entrega y devolución

para asegurar que todos los activos sean devueltos al finalizar el ciclo laboral de un empleado o al finalizar el uso de un activo. También es importante establecer un proceso para la verificación y seguimiento de la devolución de activos.

Figura 14 Anexo 8.2

Control	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
8.2.1	Directrices de clasificación.	IMPLEMENTADO	En la actualidad este control es realizado por el área de archivo garantizando el cumplimiento de este.	N/A
8.2.2	Etiquetado y manipulado de la información.	IMPLEMENTADO	En la actualidad este control es realizado por el área de archivo garantizando el cumplimiento de este.	
8.2.3	Manipulación de activos.	IMPLEMENTAR	No se evidencia	Establecer procedimientos de manipulación de activos: Una vez identificados los activos de información, es necesario establecer procedimientos claros para su manipulación. Estos procedimientos deben cubrir todas las fases del ciclo de vida de los activos, incluyendo la adquisición, el uso y el mantenimiento, así como la disposición final.

Fuente: el Autor.

Se recomienda revisar periódicamente las directrices de clasificación, etiquetado y manipulación para asegurar que siguen siendo adecuadas y relevantes para la organización. Además, se debe considerar la posibilidad de brindar capacitación

periódica a los empleados que manejan información clasificada para asegurar que están al tanto de las directrices y saben cómo aplicarlas correctamente. Se recomienda implementar procedimientos claros para el manejo de activos de información en todas las fases de los activos, desde la compra hasta la disposición final. Estos procedimientos deben ser establecidos por la organización y deben cubrir las mejores prácticas de seguridad para proteger los activos críticos

Figura 15 Anexo 8.3

Control	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
8.3.1	Gestión de soportes extraíbles.	IMPLEMENTAR	No se evidencia	Definir una política y procedimientos para la gestión de soportes extraíbles que incluya su identificación, registro, almacenamiento, transporte, uso y disposición final.
8.3.2	Eliminación de soportes.	IMPLEMENTAR	Se realiza informalmente, pero no está contemplado en las políticas ni procedimientos.	Se debe efectuar copia de respaldo de toda la información considerada confidencial o sensible y que se encuentre contenida en los equipos de la Entidad. En especial se debe asegurar el respaldo de información cuando termine el vínculo laboral del funcionario
8.3.3	Soportes físicos en tránsito.	IMPLEMENTAR	No se Evidencia	Establecer procedimientos de seguridad para el transporte de soportes extraíbles entre diferentes lugares, registro de la entrega.

Fuente: el Autor.

Es importante establecer una política clara y detallada para la gestión de soportes extraíbles, capacitar al personal, implementar medidas de seguridad, llevar un

registro actualizado, eliminar de forma segura, y establecer procedimientos de seguridad para el transporte. Esto ayudará a proteger la información reservada.

Anexo 9 Control de Accesos

Figura 16 Anexo 9.1

Control	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
9.1.1	Política de control de accesos.	MEDIANAMENTE IMPLEMENTADO	existe documentación sobre esta política en la compañía, pero no hay una guía de capacitación periódica para reforzarla con todos los empleados.	El uso de la información de la Entidad debe ser controlado para prevenir accesos no autorizados. Los privilegios sobre la información deben ser otorgados y mantenidos de acuerdo con las necesidades de la operación, limitando el acceso sólo a lo que es requerido.
9.1.2	Control de acceso a las redes y servicios asociados.	MEDIANAMENTE IMPLEMENTADO	Se evidencia directorio Activo y carpetas de red con acceso restringido, previa solicitud del área administrativa a sistemas, reforzar revisiones periódicas de equipos y permisos otorgados.	Revisar periódicamente permisos de usuarios, alta y baja de usuarios, incluirlo en las políticas.

Fuente: el Autor.

Se evidencia que existe documentación al respecto en la compañía, pero no hay una guía de capacitación periódica para reforzarla con todos los empleados. En cuanto al control de acceso a recursos, se evidencia la existencia de un directorio activo y carpetas de red con acceso restringido, previa solicitud del área administrativa al área de sistemas, pero se requiere reforzar las revisiones

periódicas de equipos y permisos otorgados. En general, se observa una implementación mediana de ambas políticas.

9.2 Gestión de Acceso de usuario

Figura 17 Anexo 9.2

Control	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
9.2.1	Gestión de altas/bajas en el registro de usuarios.	IMPLEMENTADO	Administrativa vía correo electrónico notifica al área de sistemas de los usuarios que ingresan y egresan para crear o desactivar cuentas asociadas.	Los procedimientos deben incluir todo el ciclo de vida del acceso de los usuarios, desde el registro inicial hasta la baja.
9.2.2	Gestión de los derechos de acceso asignados a usuarios.	IMPLEMENTADO	Los derechos de acceso se asignan en función de los roles y responsabilidades de cada usuario en la organización	N/A
9.2.3	Gestión de los derechos de acceso con privilegios especiales.	IMPLEMENTAR	No se Evidencia	La Entidad puede restringir el acceso a la información y el personal autorizado puede usar tecnología de monitoreo de red y eventos de seguridad de la información.
9.2.4	Gestión de información confidencial de autenticación de usuarios.	IMPLEMENTADO	Los derechos de acceso son permisos para acceder a recursos del sistema según la responsabilidad en la organización. Cuando un empleado deja su puesto, el reemplazo tendrá acceso previa notificación.	los usuarios de la Entidad serán requeridos para que se autentiquen ellos mismos, previa obtención del acceso a la información.

Fuente: el Autor.

Se evidencia que el Partido ha implementado controles de acceso de usuario para usuarios nuevos y retirados en el registro de usuarios, y revoca o modifica

permisos según sea el caso, debe implementar y gestionar lo referente a permisos privilegiados para fortalecer el control.

Figura 18 Anexo 9.2 Continuación

Control	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
9.2.5	Revisión de los derechos de acceso de los usuarios.	IMPLEMENTADO	Periódicamente se revisar permisos y roles otorgados.	N/A
9.2.6	Retirada o adaptación de los derechos de acceso	IMPLEMENTAR	Cada usuario cuenta con un Usuario y contraseña única en Directorio activo, permisos que pueden ser retirados o modificados previa notificación del área administrativa a sistemas.	Usuarios deben identificarse y autenticarse para acceder a información de la entidad. La autenticación puede ser cambiada si hay un cambio de funciones o si el empleado ya no trabaja en la organización.

Fuente: El Autor

Se evidencia que se lleva a cabo una revisión regular de los permisos de acceso otorgados a los usuarios, lo cual está implementado. También se evidencia que cada usuario cuenta con un usuario y contraseña única en el Directorio Activo, y que los permisos pueden ser retirados o modificados previa notificación del área administrativa a sistemas.

Anexo 9.3 Responsabilidades del Usuario

Figura 19 Anexo 9.

Control	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
9.3.1	Uso de información confidencial para la autenticación.	IMPLEMENTADO	Cada usuario cuenta con un Usuario y contraseña única en Directorio activo y sistemas y recursos compartidos.	Cada usuario es responsable por sus acciones mientras usa cualquier recurso de información de la Entidad.

Fuente: El Autor.

Se evidencia que el acceso a información es previa autenticación, según los permisos previamente otorgados.

Figura 20 Anexo 9.4

Control	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
9.4.1	Restricción del acceso a la información.	IMPLEMENTADO	Los permisos son otorgados según funciones y responsabilidades previa solicitud del área administrativa a sistemas.	Se debe asegurar que los usuarios de la información, únicamente tengan acceso a lo que les concierne.
9.4.2	Procedimientos seguros de inicio de sesión.	MEDIANAMENTE IMPLEMENTADO	Existe pero no se evidencian capacitaciones ni sensibilización referente a la seguridad en el inicio de sesión.	La capacitación de usuarios en buenas prácticas de seguridad en la selección, uso y protección de claves o contraseñas es importante para validar su identidad y establecer derechos de acceso de manera segura a las instalaciones, equipos o servicios informático

Fuente: el Autor.

Se evidencia que la restricción del acceso a la información se encuentra implementada mediante la asignación de permisos según funciones y responsabilidades, previa solicitud del área administrativa a sistemas. Sin embargo, se indica que no se evidencian capacitaciones ni sensibilización referente a la seguridad en el inicio de sesión, por lo que se debe implementar una capacitación para los usuarios en cuanto a buenas prácticas de seguridad en lo referente a gestión de claves e inicio de sesión.

Figura 21 Continuación Anexo 9.4

Control	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
9.4.3	Gestión de contraseñas de usuario.	IMPLEMENTADO	En la política se encuentra establecida con los lineamientos a tener en cuenta en la definición de contraseñas.	Poseer algún grado de complejidad y no deben ser palabras comunes que se puedan encontrar en diccionarios, ni tener información personal, por ejemplo: fechas de cumpleaños, nombre de los hijos, placas de automóvil, etc. Tener mínimo diez caracteres alfanuméricos.
9.4.4	Uso de herramientas de administración de sistemas.	IMPLEMENTADO	Este control se encuentra implementado en el área de Sistemas y está funcionando acorde a la normatividad solicitada por la compañía.	El área de Sistemas del Partido, velará porque los recursos de la plataforma tecnológica y los servicios de red sean operados y administrados en condiciones controladas y de seguridad, que permitan un monitoreo posterior de la actividad de los usuarios

Fuente: El Autor

Se evidencian lineamientos de gestión de contraseñas de usuario está establecida claramente y que se debe cumplir con la complejidad y longitud mínima para garantizar la seguridad de los sistemas. Por otro lado, Se puede comprobar que se

están utilizando herramientas de gestión de sistemas de manera efectiva y cumpliendo con los requisitos establecidos por la empresa.

Figura 22 Continuación Anexo 9.4

Control	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
9.4.5	Control de acceso al código fuente de los programas.	IMPLEMENTADO	Este control se encuentra implementado en el área de Sistemas y está funcionando acorde a la normatividad solicitada por la compañía.	El área de Sistemas del Partido, como responsable de la administración de los sistemas de información, aplicativos y sus códigos fuente, propenderá para que estos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico.

Fuente: El Autor.

Se evidencia que el acceso al código fuente está restringido y está implementado adecuadamente.

Anexo 10. Cifrado

Figura 23 Anexo 10

Control	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
10.1.1	Política de uso de los controles criptográficos.	IMPLEMENTAR	No se evidencia	El partido se asegurará que la información considerada secreta o limitada esté protegida mediante el uso de técnicas de cifrado al ser almacenada o transmitida en cualquier forma. Esto se hace para garantizar que la información no sea comprometida o vista por personas no autorizadas y que su contenido permanezca seguro y no se altere en el proceso.
10.1.2	Gestión de claves.	IMPLEMENTAR	No se evidencia	El Partido debe proteger los tipos de claves de modificación o destrucción; las claves secretas y las privadas además requieren protección contra su distribución no autorizada.

Fuente: El Autor.

Se establece que la información considerada secreta o limitada debe ser protegida mediante técnicas de cifrado al ser almacenada o transmitida en cualquier forma, y que las claves privadas deben ser protegidas evitando que sean distribuidas de manera no autorizada y la modificación o destrucción. Sin embargo, no se evidencia la implementación de estas medidas por parte del partido.

Anexo 11 Seguridad Física y Ambiental

Figura 24 Anexo 11

Control	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
11.1.1	Perímetro de seguridad física.	IMPLEMENTADO MEDIANAMENTE	Existe un control básico de ingreso y egreso a las instalaciones mediante el registro en un formato que está contemplado en las políticas pero no es implementado, el cuarto de redes cuenta con acceso restringido y existe un formato de ingresos y egresos, solo el personal TI puede ingresar y externos autorizados previamente con personal TI de la compañía.	La seguridad física de la Entidad debe basarse en perímetros y áreas seguras, las cuales serán protegidas por medio de controles circundantes apropiados.
11.1.2	Controles físicos de entrada.	IMPLEMENTAR	No se evidencia registro de ingreso y egresos de los funcionarios y personal externo. No están previamente identificados, no se tiene un control efectivo en los accesos del personal.	La seguridad en las áreas físicas de una empresa debe ser proporcional al valor de la información que se maneja. Se deben implementar medidas de seguridad adecuadas, como cerraduras y sistemas de control de acceso, y prevenir el acceso no autorizado.

Fuente: El Autor

Se puede observar que la seguridad física del partido requiere mejoras en cuanto a la implementación y cumplimiento de políticas y controles establecidos. Se

recomienda enfocarse en fortalecer los controles de acceso y monitoreo de ingreso y egreso del personal y visitantes a las instalaciones.

Figura 25 Continuación anexo 11

Control	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
11.1.3	Seguridad de oficinas, despachos y recursos.	IMPLEMENTAR	No se evidencia registro de ingreso y egresos de los funcionarios y personal externo. No están previamente identificados, no se tiene un control efectivo en los accesos del personal.	Los ingresos y egresos de personal a las instalaciones de la Entidad, deben ser registrados; por consiguiente, los funcionarios y personal provisto por terceras partes deben cumplir completamente con los controles físicos implantados.
11.1.4	Protección contra las amenazas externas y ambientales.	IMPLEMENTAR	No se evidencia sistemas de control ambiental, no se evidencian sistemas de vigilancia y control, no se evidencia sistemas de alarmas.	El Partido debe proveer condiciones físicas y medioambientales adecuadas para proteger y operar correctamente sus recursos, especialmente su plataforma tecnológica en el centro de cómputo. Esto incluye sistemas de control ambiental, detección y extinción de incendios, protección contra descargas eléctricas, vigilancia y monitoreo, y alarmas ambientales

Fuente: el Autor.

El partido necesita efectuar medidas de seguridad pertinentes para proteger sus recursos y asegurar su información, es oportuna la implementación de sistemas de control de acceso y de vigilancia, así como la protección contra descargas eléctricas, el descubrimiento y extinción de incendios, entre otros. Además, se requiere que se implemente un registro de ingreso y egreso de personal para garantizar la seguridad física de la entidad.

Anexo 11 Continuación

Figura 26 Continuación Anexo 11

Control	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
11.1.5	El trabajo en áreas seguras.	IMPLEMENTAR	No se evidencian Controles	Se recomienda al Partido instalar y mantener los mecanismos de seguridad física y control de acceso necesarios para proteger el perímetro de sus instalaciones, y asegurará que estos mecanismos sean efectivos en su tarea de garantizar la seguridad.
11.1.6	Áreas de acceso público, carga y descarga.	No Aplica	No aplica	No aplica

Fuente: El Autor

Se evidencia que el Partido no cuenta con controles efectivos de seguridad física en sus instalaciones, ya que no hay registros de ingreso y egreso de personal, ni medidas de protección contra amenazas externas y ambientales.

Figura 27 Anexo 11.2

Control	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
11.2.1	Emplazamiento y protección de equipos.	MEDIANAMENTE IMPLEMENTADO	Equipos en lugares seguros, protegidos con contraseñas, se cuenta con UPS, se debe contemplar copias de seguridad externas, y plan ante desastres que no se evidencia, no hay sistema de vigilancia ni de refrigeración.	Es importante implementar sistemas de vigilancia y monitoreo, refrigeración adecuada y copias de seguridad externas para garantizar la disponibilidad y protección de la información. También es fundamental contar con un plan ante desastres y realizar evaluaciones periódicas para identificar debilidades y realizar ajustes necesarios.
11.2.2	Instalaciones de suministro.	MEDIANAMENTE IMPLEMENTADO	Se cuenta con UPS y equipos de respaldo, no se evidencia plan de mantenimiento preventivo.	Es importante asegurar que se cuente con un plan de suministros y que el mantenimiento de las redes eléctricas, de voz y de datos sea realizado por personal capacitado, autorizado e identificado Mantener un registro actualizado de los mantenimientos

Fuente: El Autor.

Se evidencia que la seguridad de los equipos no está completamente implementada. Si bien se han tomado algunas medidas como el emplazamiento de los equipos en lugares seguros y su protección con contraseñas, también existen debilidades en la implementación de copias de seguridad externas y un

plan ante desastres. Además, no hay un sistema de vigilancia ni de refrigeración adecuada. En cuanto a las instalaciones de suministro, se cuenta con UPS y equipos de respaldo, pero no se evidencia un plan de mantenimiento preventivo y es necesario asegurarse de que el mantenimiento sea realizado por personal capacitado y autorizado, manteniendo un registro actualizado de las actividades programadas. En resumen, se requiere implementar medidas adicionales que permitan que estén disponibles y protegidos.

Figura 28 Continuación Anexo 11.2

Control	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
11.2.3	Seguridad del cableado.	MEDIANAMENTE IMPLEMENTADO	Se evidencia cableado nuevo, se encuentra en canaletas, separado de áreas susceptibles a inundaciones. pero no se evidencia planes de revisión y mantenimiento	Se recomienda contar con un plan de mantenimiento de la red cableada y centro de datos.
11.2.4	Mantenimiento de los equipos.	IMPLEMENTADO	Se evidencia plan de mantenimiento preventivo semestral y registros asociados al proceso.	Continuar con el plan establecido dando estricto cumplimiento.
11.2.5	Salida de activos fuera de las dependencias de la empresa.	IMPLEMENTADO	Se evidencia la existencia de un formato de préstamo y salida de equipos y existen registros asociados debidamente firmados	Continuar con la implementación de este control estrictamente.
11.2.6	Seguridad de los equipos y activos fuera de las instalaciones.	IMPLEMENTAR	No se evidencia información ni documentación asociada a este control	Establecer procedimientos y lineamientos que garanticen la protección de equipos fuera de las instalaciones.

Fuente: el Autor.

Se evidencia que en términos generales los controles están implementados y aplicados, y es necesario establecer procedimientos y lineamientos que garanticen la protección de equipos fuera de las instalaciones.

Continuación Anexo 11.2

Control	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento.	MEDIANAMENTE IMPLEMENTADO	Se evidencia que aunque está documentado que todo movimiento o retirada de equipos debe estar a cargo del área de sistemas, en algunas ocasiones el personal no cuente con los procedimientos.	Es importante comunicar de manera clara y efectiva a todo el personal los procedimientos establecidos para el movimiento y retirada de equipos, y ofrecer capacitación y entrenamiento para implementarlos de manera efectiva. Se deben verificar y actualizar los procedimientos, establecer un proceso de revisión y seguimiento para garantizar su cumplimiento, y sancionar el incumplimiento.
11.2.8	Equipo informático de usuario desatendido.	IMPLEMENTADO	Para estaciones de trabajo conectadas en acceso remoto, se cuenta con controles de acceso que permiten garantizar el correcto uso de las aplicaciones dentro y fuera de la compañía.	N/A

Fuente: El Autor.

Se evidencia que la empresa tiene implementados controles de seguridad para la protección de los equipos, pero existen áreas de oportunidad para mejorar la seguridad física y el mantenimiento preventivo de los equipos y establecer lineamientos para la seguridad de los activos fuera de la compañía. Por otro lado, La empresa tiene medidas de seguridad establecidas para controlar el acceso a las estaciones de trabajo que se conectan de forma remota

Figura 29 Continuación Anexo 11.2

Control	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla.	MEDIANAMENTE IMPLEMENTADO	EL control se encuentra definido en las políticas pero se evidencian equipos despejados y desbloqueados continuamente.	Establecer configuración obligatoria de desbloqueo automático para equipos desatendidos, se recomienda capacitar y concientizar el personal

Fuente: El Autor.

En la política de la empresa se establece la necesidad de tener puestos de trabajo despejados y de bloquear la pantalla, sin embargo, se ha observado que esta política no se está implementando de manera adecuada, ya que se evidencian equipos despejados y desbloqueados de manera continua. Para mejorar esta situación, se sugiere establecer una configuración obligatoria de desbloqueo automático para equipos desatendidos y capacitar al personal para que comprendan la importancia de mantener la pantalla bloqueada y el equipo despejado, con el fin de prevenir posibles amenazas de seguridad.

ANEXO 12 SEGURIDAD EN LA OPERATIVA

Figura 30 Anexo 12.1

Control	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
12.1.1	Documentación de procedimientos de operación.	IMPLEMENTADO	El área de tecnología en la actualidad tiene documentada toda la información relacionada con la administración del SIU, manuales, procedimientos y políticas que permiten que este control se encuentre de forma correcta dentro de la compañía.	N/A
12.1.2	Gestión de cambios.	IMPLEMENTAR	No se Evidencia, Es fundamental tener un control de cambios adecuado para asegurar que toda la información relevante sea documentada y registrada en los controles correspondientes	Se recomienda que todo cambio a la infraestructura informática debe estar controlado y será realizado de acuerdo con los procedimientos de gestión de cambios.
12.1.3	Gestión de capacidades.	IMPLEMENTAR	No se evidencia	Se debe realizar una revisión periódica de los recursos de TI y de los requisitos de capacidad para ajustar los planes y procedimientos según sea necesario.

Fuente: El Autor.

El área de sistemas tiene toda la información necesaria documentada, lo que indica que este control está implementado de manera adecuada.

En cuanto a la gestión de cambios no se evidencia su implementación. Es fundamental contar con un control de cambios adecuado para garantizar que toda la información relevante sea documentada y registrada en los controles correspondientes. Es importante realizar una revisión periódica de los recursos de TI y de los requisitos de capacidad para ajustar los planes y procedimientos según sea necesario. Se recomienda implementar procedimientos de gestión de capacidades para garantizar una adecuada gestión de los recursos de TI.

Figura 31 Continuación Anexo 12.1

Control	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
12.1.4	Separación de entornos de desarrollo, prueba y producción.	IMPLEMENTADO	Se evidencian ambientes de desarrollo, producción y pruebas para el sistema de información y página Web	el área de Tecnología debe proveer los recursos necesarios para la implantación de controles que permitan la separación de ambientes de desarrollo, pruebas y producción

Fuente: El Autor.

Se evidencia el cumplimiento a cabalidad de este control se cuenta con ambientes separados para el desarrollo de software.

Figura 32 Anexo 12.2

Control	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
12.2.1	Controles contra el código malicioso.	MEDIANAMENTE IMPLEMENTADO	Se evidencia implementación actualizado y licenciado (Kasperksy) en cada uno de los equipos y firewall. No se evidencian planes de capacitación y concientización en cuento a seguridad informática	Contar con planes de capacitación de concientización y sensibilización en temas de seguridad informática dirigido al personal y partes interesadas.

Fuente: El Autor.

Se evidencia que se cuenta con antivirus licenciado y actualizado, no obstante, el personal no se encuentra capacitado en cuanto a lineamientos de seguridad.

Figura 33 Anexo 12.3

Control	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
12.3.1	Copias de seguridad de la información.	IMPLEMENTADO	Las copias de seguridad siempre se realizan por el área de Sistemas del Partido, tanto en servidores como en carpetas compartidas de red. Al final contrato se realiza backup total de equipos. No se evidencia redundancia externa de las copias	Se recomienda contar con copias de almacenamiento externas para garantizar la disponibilidad de la información en caso de desastre.

Fuente: El Autor.

Se efectúan mensualmente copias de seguridad se servidores y carpetas compartidas y al finalizar contratos, se sugiere tener redundancia externa.

Figura 34 Anexo 12.4

Control	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
12.4.1	Registro y gestión de eventos de actividad.	IMPLEMENTAR	Se evidencia control sólo en cuentas de correo electrónico, no se evidencia en sistema de información	El Partido vigilará constantemente cómo los funcionarios y personal externo utilizan los recursos tecnológicos y sistemas de información de la plataforma tecnológica
12.4.2	Protección de los registros de información.	IMPLEMENTAR	No se evidencia	El área de sistemas debe garantizar que los registros de auditoría de la plataforma tecnológica y los sistemas de información de la Entidad estén precisos y disponibles.
12.4.3	Registros de actividad del administrador y operador del sistema.	IMPLEMENTAR	No se evidencia	Es necesario examinar los registros de auditoría de los administradores y operadores de la plataforma tecnológica y sistemas de información para detectar problemas de seguridad y realizar una supervisión adecuada.
12.4.4	Sincronización de relojes.	IMPLEMENTADO	reloj sincronizado	N/A

Fuente: El Autor.

Se recomienda implementar un control para monitorear constantemente cómo los funcionarios y personal externo utilizan los recursos del Partido. Esto permitirá detectar posibles riesgos de seguridad y tomar medidas preventivas, se recomienda implementar un control que garantice auditoría cuente con registros de la plataforma tecnológica y los sistemas precisos y disponibles y se recomienda implementar un control que permita examinar los registros de auditoría con el fin de detectar posibles problemas de seguridad y realizar una supervisión adecuada.

Figura 35 Anexo 12.5

Control	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
12.5.1	Instalación del software en sistemas en producción.	IMPLEMENTAR	No se evidencia Documentado	A través del área de Sistemas, El partido designará responsables y establecerá procedimientos para controlar la instalación de software operativo, se cerciorará de contar con el soporte de los proveedores de dicho software y asegurará la funcionalidad de los sistemas de información que operan sobre la plataforma tecnológica cuando el software operativo es actualizado

Fuente: El Autor.

No se evidencia el control se recomienda establecer lineamientos y responsables.

Figura 36 Anexo 12.6

Control	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
12.6.1	Gestión de las vulnerabilidades técnicas.	IMPLEMENTAR	No se evidencia	A través del área de Sistemas se, revisará periódicamente la aparición de vulnerabilidades técnicas sobre los recursos de la plataforma tecnológica por medio de la realización periódica de pruebas de vulnerabilidades
12.6.2	Restricciones en la instalación de software.	IMPLEMENTADO	Está documentado y se evidencia que la instalación de software es realizada exclusivamente por el equipo de sistemas del partido.	La instalación de software en los computadores del partido, es una función exclusiva del área sistemas

Fuente: El Autor.

Se evidencia que no se ha implementado un control para la detección y gestión de vulnerabilidades técnicas. Se recomienda área de sistemas revisar habitualmente la existencia de vulnerabilidades técnicas sobre los recursos TI mediante la realización reiterada de pruebas de vulnerabilidades. se evidencia que está implementado y documentado que la instalación de software es efectuada exclusivamente por el equipo de sistemas del partido.

Figura 37 Anexo 12.7

Control	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
12.7.1	Controles de auditoría de los sistemas de información.	IMPLEMENTAR	No se evidencia auditorías a los sistemas de información	Auditoría debe llevar a cabo un monitoreo regular para verificar si se cumplen las políticas de la organización, evaluar qué tan avanzada está la implementación de los sistemas de información, revisar el estado de mantenimiento y determinar cómo se pueden mejorar los sistemas de información.

Fuente: El Autor.

Se evidencia que no se han implementado controles de auditoría de los SI. Se recomienda que el departamento de Auditoría lleve a cabo un monitoreo regular para verificar si se cumplen las políticas de la organización, evaluar qué tan avanzada está la implementación, revisar el estado de mantenimiento y determinar cómo se pueden mejorar.

Figura 38 Anexo 13.1

Control	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
13.1.1	Controles de red.	MEDIANAMENTE IMPLEMENTADO	Se evidencian controles de red mediante directorio activo, firewall interno y externo,	La Entidad implementará mecanismos de control a través del área de Tecnología para garantizar la disponibilidad de las redes de datos y los servicios que dependen de ellas, y para reducir los riesgos de seguridad de la información transmitida a través de dichas redes.
13.1.2	Mecanismos de seguridad asociados a servicios en red.	IMPLEMENTAR	No se evidencia	Informes de auditoría de seguridad de red Resultados de análisis de vulnerabilidades y pruebas de penetración Registros de monitoreo y registro de acceso a los servicios de red Informes de incidentes de seguridad y cómo se han abordado Certificaciones o acreditaciones de seguridad relevantes.

Fuente: El Autor.

En cuanto a los controles de red, se evidencia una implementación medianamente implementada mediante el uso de directorio activo, firewall interno y externo. Sin embargo, se requiere implementar mecanismos adicionales de control para garantizar la disponibilidad y reducir los riesgos. Por otro lado, en cuanto a los elementos de seguridad asociados a servicios de red, no se evidencia su implementación y se requiere implementar informes de auditoría de seguridad de red, resultados de vulnerabilidades identificadas y pruebas de intrusión, registros de monitoreo y accesos de red, informes de incidentes de seguridad y certificaciones o acreditaciones de seguridad relevantes.

Figura 39 Anexo 13.1 Continuación

Control	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
13.1.3	Segregación de redes.	IMPLEMENTAR	En la Actualidad se cuenta con un solo segmento de red y un dominio para todo el Partido	El área de Sistemas debe mantener las redes de datos segmentadas por dominios, grupos de servicios, grupos de usuarios, ubicación geográfica o cualquier otra tipificación que se considere conveniente para la Entidad

Fuente: El Autor.

Anexo 13.2

Control	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
13.2.1	Políticas y procedimientos de intercambio de información.	IMPLEMENTAR	No se evidencia	Es importante asegurar la información al compartirla con entidades externas, para lo cual se deben establecer procedimientos y controles necesarios que permitan un intercambio seguro.
13.2.2	Acuerdos de intercambio.	IMPLEMENTADO	Incluido en los contratos.	Definir los términos y condiciones de los acuerdos de confidencialidad o intercambio de información con terceros, y establecer las consecuencias legales en caso de que alguna de las partes incumpla lo acordado
13.2.3	Mensajería electrónica.	IMPLEMENTADO	El envío de correos electrónicos cuenta con antivirus y firewall garantizando protección	N/A

Fuente: El Autor

Se evidencia que la política y los procedimientos de intercambio aún no han sido implementados, mientras que los acuerdos de intercambio ya han sido definidos y establecidos en los contratos. Además, se evidencia que los correos electrónicos son enviados con medidas de protección como antivirus y firewall.

Figura 40 Continuación Anexo 13.2

Control	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
13.2.4	Acuerdos de confidencialidad y secreto.	IMPLEMENTADO	Estos acuerdos se establecen en los vínculos contractuales	El área Jurídica debe incluir en los contratos con terceras partes los acuerdos de confidencialidad o intercambio, estableciendo claramente las responsabilidades y obligaciones legales asignadas a dichos terceros en caso de divulgación no autorizada de información de los beneficiarios de la Entidad entregada para cumplir los objetivos misionales.

Fuente: El Autor.

Se evidencia el cumplimiento de este control, es contemplado en los contratos con proveedores.

Figura 41 Anexo 14

Control	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
14.1.1	Análisis y especificación de los requisitos de seguridad.	IMPLEMENTADO	Aunque se especifican requisitos de seguridad de la información en función de las necesidades de la compañía, no siempre son del conocimiento de todos los funcionarios.	Los requerimientos de seguridad de la información deben ser identificados previos al diseño de los sistemas de tecnología de la información.
14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes públicas.	IMPLEMENTADO	Incluye controles y políticas , Firewall interno y Externo	El área de Sistemas debe asegurar que los sistemas de información o aplicativos informáticos que pasan a través de redes públicas, incluyen controles de seguridad y cumplen con las políticas de seguridad de la información, con el fin de proteger la información de la Entidad de posibles ataques.
14.1.3	Protección de las transacciones por redes telemáticas.	NO IMPLEMENTAR	N/A	N/A

Fuente: El Autor.

Se evidencia el cumplimiento de estos controles en el Partido.

Anexo 14.2

Figura 42 Anexo 14.2

Control	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
14.2.1	Política de desarrollo seguro de software.	IMPLEMENTADO	El desarrollo siempre se realiza en su respectivo ambiente y se tiene en cuenta las políticas instauradas para su desarrollo seguro.	Es necesario garantizar que los sistemas de información desarrollados interna o externamente cumplan con los requisitos de seguridad esperados, las mejores prácticas de desarrollo seguro de aplicaciones y se realicen pruebas de aceptación y seguridad al software desarrollado.
14.2.2	Procedimientos de control de cambios en los sistemas.	IMPLEMENTAR	No se evidencia	el área de sistemas debe contar con sistemas de control de versiones para administrar los cambios de los sistemas de información de la Entidad.
14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	IMPLEMENTAR	No se evidencia	El área de sistemas debe realizar pruebas en todos los sistemas cuando se cambia el sistema operativo de los equipos de cómputo de la Entidad, para evaluar los posibles efectos secundarios.

Fuente: El Autor

Se evidencia que se realiza el desarrollo en un ambiente adecuado y se tienen en cuenta las políticas establecidas. Sin embargo, en cuanto a los procedimientos de control de cambios en los sistemas y la revisión técnica de las aplicaciones, no se evidencia su implementación. Se recomienda establecer control de versiones para administrar los cambios en los sistemas y realizar pruebas en todos los sistemas al cambiar el sistema operativo de los equipos para evaluar posibles efectos en su normal operación y seguridad.

Figura 43 Continuación Anexo 14.2

Control	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
14.2.4	Restricciones a los cambios en los paquetes de software.	IMPLEMENTADO	Cambios realizados sólo por personal autorizado del área técnica.	la realización de un cambio tecnológico en un paquete de software entregado por un tercero, que no considere los requerimientos de seguridad de la Información hace que la Entidad esté expuesta a riesgos.
14.2.5	Uso de principios de ingeniería en protección de sistemas.	IMPLEMENTADO	Se establecen controles en la implementación del sistema de información cumpliendo con regulaciones y normatividad	N/A
14.2.6	Seguridad en entornos de desarrollo.	IMPLEMENTADO	el desarrollo se realiza considerando el ambiente de desarrollo provisto por la compañía y su proveedor de servicios.	a Entidad implementará y protegerá los ambientes necesarios para el desarrollo e integración de sistemas durante todo el ciclo de vida del sistema.

Fuente: El Autor.

Se evidencia que la entidad ha implementado medidas como contar con una política de desarrollo seguro de software, limitaciones respecto cambios de software y seguridad en entornos de desarrollo. Sin embargo, aún falta implementar medios de control de cambios y revisión a nivel técnico de las aplicaciones posterior a los cambios.

Figura 44 Anexo 14.2 Continuación

Control	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
14.2.7	Externalización del desarrollo de software.	IMPLEMENTADO	En la actualidad los ajustes del sistema son realizados por un tercero, se firman acuerdos de confidencialidad	El área de sistemas debe establecer controles de acceso y procedimientos para los ambientes de desarrollo de los garantizando que los desarrolladores tengan acceso limitado y controlado a los datos y archivos de producción.
14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas.	IMPLEMENTADO	Se realizan fases de desarrollo y pruebas en ambientes de pruebas para asegurar la calidad del software antes de implementarlo en producción.	En el ciclo de vida de los sistemas, se deben aplicar las buenas prácticas y lineamientos de desarrollo seguro desde la fase de diseño hasta la puesta en marcha, y los desarrolladores deben contemplar esto en todo momento.
14.2.9	Pruebas de aceptación.	MEDIANAMENTE IMPLEMENTADO	No se evidencia, se verifica correcto funcionamiento pero no se formaliza mediante actas	Posterior a las pruebas, verifica el correcto funcionamiento del desarrollo, se firman actas de aceptación de pruebas de entrega correcta del desarrollo.

Fuente: El Autor.

Se puede decir que la evidencia de la implementación de la política de pruebas de aceptación es medianamente implementada, ya que, aunque se comprueba el adecuado funcionamiento del desarrollo, no se formaliza mediante documentos de aceptación. Es importante que se establezcan procedimientos formales para la ejecución de pruebas de aceptación y se documenten los resultados de las mismas en actas que permitan garantizar la entrega correcta del desarrollo.

14.3 Datos de prueba

Control	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
14.3.1	Protección de los datos utilizados en pruebas.	IMPLEMENTADO	incluido en los contratos.	El área de Sistemas protegerá los datos de prueba utilizados por los desarrolladores, evitando la divulgación de información confidencial de los ambientes de producción.

Fuente: El Autor.

Se evidencia que el área de sistemas ha implementado la protección de los datos utilizados en pruebas, incluyendo esta medida en los contratos correspondientes. Esto es importante para que la información sea confidencial de los ambientes de producción, evitando su divulgación y uso inapropiado durante las pruebas de desarrollo de software.

Anexo 15. Relaciones con Suministradores

Control	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
15.1.1	Política de seguridad de la información para suministradores.	MEDIANAMENTE IMPLEMENTADO	Se evidencian cláusulas de confidencialidad en los contratos	la entidad implementará controles para supervisar y garantizar que las terceras partes con las que se relaciona cumplan con las políticas y procedimientos de seguridad de la información establecidos por la entidad. Esto se hace para asegurar que la información y servicios proporcionados por estas terceras partes sean seguros y protejan la información de la entidad
15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores.	IMPLEMENTADO	Incluidos en contratos con proveedores	N/A
15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones.	NO IMPLEMENTAR	N/A	N/A

Fuente: El Autor.

Se evidencian cláusulas de confidencialidad en los contratos la entidad, implementa controles para supervisar y garantizar que las terceras partes con las que se relaciona cumplan lineamientos de seguridad establecidos por la entidad. Esto se hace para asegurar que los datos y servicios proporcionados por estas terceras partes sean seguros y protejan la información de la entidad.

Figura 45 Anexo 15.2

Control	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
15.2.1	Supervisión y revisión de los servicios prestados por terceros.	IMPLEMENTADO	Cada contrato cuenta con un supervisor garante del cumplimiento	El área de Sistemas debe identificar y monitorear los riesgos relacionados con terceras partes o los servicios provistos por ellas, haciendo extensiva esta actividad a la cadena de suministro de los servicios de tecnología o comunicaciones provistos.
15.2.2	Gestión de cambios en los servicios prestados por terceros.	IMPLEMENTAR	No Se evidencia	Los supervisores de contratos con terceros deben gestionar los cambios en los servicios provistos por los proveedores para mantener los niveles de cumplimiento de servicio y seguridad establecidos, y monitorear los riesgos emergentes con el apoyo del área de Seguridad de la Información.

Fuente: El Autor.

Cada contrato cuenta con un supervisor responsable del cumplimiento, no se evidencia una gestión formal de los cambios de condiciones de servicios de los proveedores. Los supervisores de contratos con terceros deben gestionar los cambios para conservar los niveles de cumplimiento y seguridad establecidos, y monitorear los riesgos emergentes con el apoyo del área sistemas.

Figura 46 Anexo 16

Control	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
16.1.1	Responsabilidades y procedimientos.	IMPLEMENTAR	No se evidencia	La Entidad incentivará a los funcionarios y personal externo a reportar incidentes relacionados con la seguridad de la información y los medios de procesamiento, incluyendo plataformas tecnológicas, sistemas de información, medios físicos de almacenamiento y personas.
16.1.2	Notificación de los eventos de seguridad de la información.	IMPLEMENTAR	No se evidencia	Los propietarios de los activos de información deben notificar de manera temprana al área técnica cualquier incidente de seguridad que identifiquen o que consideren pueda ocurrir.
16.1.3	Notificación de puntos débiles de la seguridad.	IMPLEMENTAR	No se Evidencia	Si un funcionario tiene conocimiento de una pérdida o divulgación no autorizada de información clasificada como uso interno, reservada o restringida, debe informarlo al área de Sistemas.

Fuente: El Autor.

Se evidencia que, en cuanto a las responsabilidades y procedimientos, hay una implementación pendiente ya que no se evidencia la incentivación por parte de la entidad a los funcionarios y personal externo para reportar incidentes de seguridad. También se debe implementar la notificación temprana de cualquier incidente de seguridad identificado por los responsables de los activos y la notificación de puntos débiles de seguridad, como la pérdida o divulgación no autorizada de información clasificada, que debe ser informada al área de sistemas para su registro y gestión adecuada.

Figura 47 Continuación Anexo 16.1

Control	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones.	IMPLEMENTAR	No se evidencia evaluación de impacto de cualquier novedad que atente contra la seguridad de la información.	El área técnica debe analizar los incidentes de seguridad recibidos y activar el protocolo de contacto con las autoridades si lo considera necesario.
16.1.5	Respuesta a los incidentes de seguridad.	IMPLEMENTAR	No se evidencia	El área técnica debe asignar personal capacitado para investigar los incidentes de seguridad, identificar las causas, encontrar soluciones y prevenir futuras ocurrencias.
16.1.6	Aprendizaje de los incidentes de seguridad de la información.	IMPLEMENTAR	No se evidencia	el área técnica debe crear bases de conocimiento con soluciones para los incidentes de seguridad, con la colaboración del área de Tecnología y la Secretaría General, para acelerar la respuesta ante futuros incidentes.

Fuente: El Autor.

No se evidencia implementación de los controles, es importante que el área técnica implemente los procedimientos necesarios para valorar los eventos de seguridad, responder a los incidentes y aprender de ellos para mejorar la seguridad en la entidad.

Figura 48 Continuación Anexo 16.1

Control	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
16.1.7	Recopilación de evidencias.	IMPLEMENTAR	No se evidencia, Es importante recopilar evidencia en todos los casos para garantizar la seguridad de la información y llevar un registro del caso para su trazabilidad.	En cada incidente de seguridad, se debe realizar una evaluación detallada y recopilar las pruebas necesarias. Los incidentes deben ser evaluados según sus circunstancias y escalados al Comité de Seguridad de la Información si es necesario.

Fuente: El Autor

No se evidencia recopilación de evidencias de incidentes que sirvan de insumo para futuros eventos.

Anexo 17 aspectos de la seguridad de la información en la gestión de la continuidad del negocio

Figura 49 Anexo 17.1

Control	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
17.1.1	Planificación de la continuidad de la seguridad de la información.	IMPLEMENTAR	No se evidencian acciones que garanticen continuidad del negocio, sólo existen copias de seguridad alojadas en instalaciones	se debe crear y probar periódicamente procedimientos para recuperar la información crítica de la Entidad de manera oportuna y razonable sin comprometer la seguridad establecida
17.1.2	Implantación de la continuidad de la seguridad de la información.	IMPLEMENTAR	No se evidencia	En caso de contingencias o eventos catastróficos que afecten la operación del partido, es importante contar con recursos adecuados para garantizar una respuesta efectiva de los funcionarios y procesos y asegurar la continuidad de las operaciones.
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	IMPLEMENTAR	No se Evidencia	Es importante realizar pruebas periódicas del plan de recuperación ante desastres y/o continuidad de negocio para asegurar su efectividad y documentar las pruebas.

Fuente: El Autor.

No se han implementado acciones adecuadas para garantizar la normal operación del Partido en caso de contingencias o eventos catastróficos que puedan afectar la operación del partido. No se han creado ni probado periódicamente procedimientos para recuperar la información crítica de la entidad, y no se han asignado recursos adecuados para garantizar una respuesta positiva de los funcionarios y procesos en caso de contingencias.

Figura 50 Anexo 17.2

Control	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
17.2.1	Disponibilidad de instalaciones para el procesamiento de la información.	NO IMPLEMENTAR	N/A	

Fuente: El autor.

Anexo 18. Cumplimiento

Figura 51 Anexo 18.1

Control	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
18.1.1	Identificación de la legislación aplicable.	IMPLEMENTADO	El partido se asegura de cumplir con la normativa actual y de adaptarse a su marco de trabajo y contexto empresarial.	El área de sistemas debe asegurarse de que el software instalado en los recursos de la plataforma tecnológica cumpla con los requisitos legales y de licenciamiento aplicables.
18.1.2	Derechos de propiedad intelectual (DPI).	IMPLEMENTADO	En los contratos de la compañía se establecen los derechos de propiedad y autoría sobre todo lo creado dentro del entorno de trabajo.	Todo el personal de la entidad debe cumplir con las leyes de derechos de autor y licenciamiento de software.
18.1.3	Protección de los registros de la organización.	IMPLEMENTADO	Se protegen registros con medidas establecidas	el área Legal y técnica deben identificar y mantener actualizados los requisitos legales, reglamentarios y contractuales relacionados con los registros de la organización para protegerlos contra posibles amenazas.

Fuente: El Autor

Se evidencia que el Partido ha implementado satisfactoriamente los controles relacionados con legislación aplicable, propiedad intelectual y la protección de los datos. Es importante destacar que la entidad debe seguir implementando controles en las áreas donde se evidenció falta de implementación, como lo son la comunicación de sucesos de seguridad, la evaluación de impacto de novedades que atenten contra la seguridad, la asignación de personal capacitado para investigar incidentes de seguridad y la planificación, implantación y verificación de la continuidad.

Figura 52 Continuación Anexo 18.1

Control	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
18.1.4	Protección de datos y privacidad de la información personal.	IMPLEMENTADO	Existe una política de privacidad de Datos e información, sistemas contemplan protección de datos y Habeas Data	La Entidad, a través del área de Seguridad de la Información, se encargará de proteger los datos personales de sus beneficiarios, proveedores y otros terceros que le proporcionen información, cumpliendo con la Ley 1581 de 2012 de protección de datos personales.
18.1.5	Regulación de los controles criptográficos.	NO IMPLEMENTAR	N/A	N/A

Fuente: El Autor.

Se evidencia implementación en el control de protección de datos.

Figura 53 Anexo 18.2

Control	Descripción	ESTADO	Hallazgos u Observaciones	Recomendaciones
18.2.1	Revisión independiente de la seguridad de la información.	IMPLEMENTAR	No se evidencia	El Partido debe hacer revisiones regulares para asegurarse de que los controles establecidos cumplan con las normas de seguridad internacionales, como ISO 27001.
18.2.2	Cumplimiento de las políticas y normas de seguridad.	IMPLEMENTAR	Poner en marcha de políticas y garantizar su cumplimiento, designar responsables	todas las personas que trabajan o colaboran con la Entidad deben cumplir con las políticas de seguridad que se implementarán y realizar auditorías sorpresa a las diferentes áreas y procesos para verificar el cumplimiento de las políticas establecidas, reportar inconsistencias detectadas. Es importante que el personal cumpla con las políticas no solo por las auditorías, sino también como parte de sus responsabilidades como funcionarios de la entidad.
18.2.3	Comprobación del cumplimiento.	IMPLEMENTAR	No se evidencia, existen auditorías externas muy básicas que no contemplan todo lo referente a seguridad de la información y cumplimiento de políticas y normatividad	

Fuente: El Autor.

Se puede evidenciar que hay algunas acciones implementadas en el partido para garantizar la seguridad, pero también se pueden identificar algunas áreas de mejora. Es importante que se implementen las acciones faltantes asegurar la información y cumplir con los lineamientos de seguridad establecidos.

Así podemos dar cierre al capítulo número uno donde podemos evidenciar que pese a que el partido ha iniciado e implementado lineamientos en pro de proteger su información hay que reforzarlos e implementar controles asociados a procesos críticos con los que no cuenta actualmente, es necesario replantear la política con la que se cuenta reemplazándola por una más amplia, con sus respectivos responsables, controles, seguimiento y evaluación.

De los ciento catorce controles evaluados el partido cuenta con 50 implementados con recomendaciones, 15 medianamente implementados y 49 no implementados. Aunque el partido de la U ha implementado una cantidad significativa de controles de seguridad, la cantidad de controles no implementados indica que hay áreas de mejora en la seguridad de la información. La seguridad de la información es un proceso continuo que debe ser gestionado de manera adecuada y constante. Por lo tanto, se recomienda que el partido de la U continúe mejorando sus medidas de seguridad para reducir los riesgos y garantizar la protección de su información.

Es vital entonces la decisión y el respaldo de la dirección en la realización de este proyecto en pro de proteger su información, sus activos, capacitar su personal y estar a la vanguardia de los cambios reaccionando oportunamente y garantizando la operación del negocio.

7. IDENTIFICACIÓN Y EVALUACIÓN DE ACTIVOS

Para valorar los activos TI frente a la confidencialidad, integridad y disponibilidad, es necesario seguir un proceso sistemático que permita identificar y clasificar los activos críticos para la organización. Este proceso se puede dividir en los siguientes pasos:

Identificar los activos de TI: Es necesario realizar un inventario detallado de todos los activos de TI de la compañía, incluyendo servidores, aplicaciones, bases de datos, redes, dispositivos móviles y cualquier otro activo relevante.

Evaluar la importancia de los activos: Una vez que se han identificado todos los activos de TI, es necesario evaluar la importancia de cada uno de ellos para la organización. Esta evaluación se basa en estos criterios:

- Confidencialidad: ¿Cuán importante es la información que se almacena o procesa en el activo? ¿Qué daño podría causar si la información se revelara a personas no autorizadas?

- Integridad: ¿Cuán importante es que los datos almacenados o procesados en el activo sean precisos y completos? ¿Qué daño podría causar si los datos fueran alterados o eliminados?

- Disponibilidad: ¿Cuán importante es que el activo esté disponible en todo momento? ¿Qué daño podría causar si el activo estuviera no está disponible durante un período prolongado de tiempo?

Clasificar los activos según su importancia: Una vez que se han evaluado los activos de TI en concordancia con su relevancia para la compañía, es necesario clasificarlos en diferentes niveles según su criticidad.

Evaluar y clasificar los activos de TI es un paso crítico para garantizar la seguridad en una compañía. Los activos de TI incluyen cualquier recurso tecnológico que almacene, procese o transmita información, como computadoras, servidores, dispositivos de red, software, bases de datos y otros dispositivos de almacenamiento.

La evaluación y clasificación de los activos de TI permiten a una organización identificar los recursos críticos, definir su valor y estipular los recursos necesarios para protegerlos. Al clasificar los activos de TI en función de su importancia, los

equipos de seguridad de la información pueden establecer diferentes niveles de protección para cada uno, de manera que los activos críticos reciban una mayor atención en cuanto a medidas de seguridad y protección.

Además, la clasificación también ayuda a definir responsabilidades claras para la gestión de cada recurso. Se asigna a una persona responsable de un recurso crítico que supervise y controle su uso, acceso y protección. Esto asegura que cada recurso esté siendo gestionado y protegido de manera adecuada, disminuyendo el riesgo de brechas de seguridad o pérdida de información crítica.

Después de analizar la organización, se han identificado los activos TI. Para llevar a cabo este análisis, apoyados por el personal del departamento de Sistemas del partido, quienes proporcionaron información relevante para la identificación de dichos activos.

7.1 ACTIVOS IDENTIFICADOS

Tabla 2 Activos Identificados

CANTIDAD	DESCRIPCIÓN	UBICACIÓN	RESPONSABLE
2	SWITCH HP	CUARTO DE REDES	Técnico Sistemas
1	SWITCH D LINK	CUARTO DE REDES	Técnico Sistemas
1	SWITCH ARUBA	CUARTO DE REDES	Técnico Sistemas
1	PLANTA TELEFONICA	CUARTO DE REDES	Técnico Sistemas
2	DISCO DURO EXTERNO TOSHIBA	CUARTO DE REDES	Coordinador Sistemas
1	STORAGE THECUS	CUARTO DE REDES	Coordinador Sistemas
2	UPS	CUARTO DE REDES	Técnico Sistemas
1	SERVIDOR THINKSTATION	CUARTO DE REDES	Coordinador Sistemas
1	SERVIDOR IBM	CUARTO DE REDES	
4	REPETIDOR ACCESS POINT TP LINK	PRIMER y SEGUNDO PISO	Equipo de Sistemas
40	EQUIPOS HP + PANTALLA	OFICINAS	Empleados partido
43	CUENTAS DE CORREO	ADMIN SISTEMAS	Empleados – Coordinador Sistemas
1	FIREWALL	ADMIN SISTEMAS	Coordinador Sistemas - Sophos
1	INTERNET CANAL DEDICADO CLARO	ADMIN SISTEMAS	Sistemas - Claro
1	PÁGINA WEB (DOMINIO – HOSTING)	ADMIN SISTEMAS	Admin web Godaddy-prodominios
1	SISTEMA DE INFORMACIÓN	ADMIN SISTEMAS	Admin Web-Azure
40	LICENCIAS OFFICE 2010	ADMIN SISTEMAS	Técnico Sistemas, Empleados

Continuación Tabla 2

CANTIDAD	DESCRIPCIÓN	UBICACIÓN	
40	LICENCIAS WINDOWS 10	ADMIN SISTEMAS	Técnico Sistemas, Empleados
1	SIIGO	ADMIN SISTEMAS	Siigo
40	ANTIVIRUS KASPERSKY	ADMIN SISTEMAS	Kasperky – Técnico sistemas
1	DISCO DURO 8 TB SEAGATE	SOPORTE	Técnico sistemas
1	DISCO DURO TOSHIBA 1TB	SOPORTE	Jefe Administrativa
1	FIREWALL WEB SIU	ADMIN SISTEMAS	Admin Web y programador
1	DIRECTORIO ACTIVO	ADMIN SISTEMAS	Coordinador sistemas
80	PERSONAL	RECURSOS HUMANOS	Recursos Humanos

Fuente: Partido de la U

Los ACTIVOS TI de una empresa pueden clasificarse en varias categorías, como:

- Hardware: equipos físicos utilizados para procesar, almacenar y comunicar información.
- Software: programas informáticos que se ejecutan en los equipos para realizar diversas tareas.
- Redes: infraestructura de red que conecta los dispositivos y permite la comunicación y el intercambio de datos.
- Servicios: servicios informáticos que proporcionan soporte y mantenimiento a los sistemas y equipos de la empresa.
- Datos: información valiosa almacenada y procesada por los sistemas de la empresa.

7.2 CATEGORIZACIÓN ACTIVOS

Tabla 3 Categorización Activos

Categoría	Activo	Descripción
Hardware	Switch HP	Equipo de red HP para interconexión de dispositivos.
Hardware	Switch D Link	Equipo de red D-Link para interconexión de dispositivos.
Hardware	Switch Aruba	Equipo de red Aruba para interconexión de dispositivos.
Hardware	Planta telefónica	Sistema de telefonía utilizado para gestionar llamadas internas y externas.
Hardware	Disco duro externo Toshiba	Unidad de almacenamiento externa para realizar copias de seguridad y almacenamiento de datos.
Hardware	Storage Thecus	Unidad de almacenamiento en red para compartir archivos y realizar copias de seguridad.
Hardware	UPS	Fuente de alimentación ininterrumpida para proporcionar energía en caso de fallos eléctricos.
Hardware	Servidor Thinkstation	Servidor ThinkStation para alojar aplicaciones y servicios.
Hardware	Servidor IBM	Servidor IBM para alojar aplicaciones y servicios.
Hardware	Repetidor Access Point TP Link	Dispositivo utilizado para ampliar la cobertura de una red Wi-Fi.
Hardware	Equipos HP + pantalla y accesorios	Equipo de cómputo HP que incluye pantalla y accesorios.
Hardware/software	Firewall	Controla y filtra el tráfico de red que entra y sale de una red informática
Hardware	Disco duro 8 TB Seagate	Unidad de almacenamiento interno con capacidad de 8 TB.
Hardware	Disco duro Toshiba 1TB	Unidad de almacenamiento interno con capacidad de 1 TB.
Software	Licencias Office 2010	Licencias de software para el paquete de aplicaciones Microsoft Office 2010.

Categoría	Activo	Descripción
Software	Licencias Windows 10	Licencias de software para el sistema operativo Windows 10.
Software	Antivirus Kaspersky	Software de seguridad para protección contra virus y malware.
Software	Sistema contable Siigo	Sistema de software contable y administrativo.
Redes	Internet canal dedicado Claro	Canal de internet dedicado proporcionado por la empresa Claro.
Servicios	Cuentas de correo	Cuentas de correo electrónico para los empleados de la empresa.
Datos	Página web (dominio-hosting)	Página web de la empresa alojada en un servidor web y registrada en un dominio.
Datos	Sistema de información	Conjunto de datos utilizados para la gestión de procesos y servicios de la empresa.
Servicio	Directorio activo	Administrador centralizado cuentas de dominio
Personal	Empleados	Operan e interactúan con infraestructura TI

Fuente: El Autor.

7.3 EVALUACIÓN ACTIVOS

Para determinar el nivel de riesgo de un activo en cuanto a confidencialidad, integridad y disponibilidad, se pueden utilizar los siguientes criterios:

7.3.1 Confidencialidad:

Alto riesgo: si la divulgación o acceso no autorizado de la información puede causar un daño significativo o catastrófico a la organización o a terceros.

Medio riesgo: si la divulgación o acceso no autorizado de la información puede causar un daño moderado a la organización o a terceros.

Bajo riesgo: si la divulgación o acceso no autorizado de la información no causa daño significativo a la organización o a terceros.

7.3.2 Integridad:

Alto riesgo: si la alteración no autorizada de la información puede causar un daño significativo o catastrófico a la organización o a terceros.

Medio riesgo: si la alteración no autorizada de la información puede causar un daño moderado a la organización o a terceros.

Bajo riesgo: si la alteración no autorizada de la información no causa daño significativo a la organización o a terceros.

7.3.3 Disponibilidad:

Alto riesgo: si la falta de disponibilidad de la información o del activo puede causar un daño significativo o catastrófico a la organización o a terceros.

Medio riesgo: si la falta de disponibilidad de la información o del activo puede causar un daño moderado a la organización o a terceros.

Bajo riesgo: si la falta de disponibilidad de la información o del activo no causa daño significativo a la organización o a terceros.

Tabla 4 Criterios de Evaluación

Alto (3)	Daño Significativo o catastrófico
Medio (2)	Daño moderado
Bajo (1)	No causa daños significativos

Fuente: El Autor.

Criticidad: Crítico: cuando el valor resultante de la suma es igual o superior a 7.

Moderado: cuando el valor resultante de la suma es mayor o igual a 4 y menor que 7.

Bajo: cuando el valor resultante de la suma es menor que 4.

Tabla 5 Valoración Activos

Activo	Integridad	Confidencialidad	Disponibilidad
Switch HP	Medio (2)	Bajo (1)	Alto (3)
Switch D Link	Medio (2)	Bajo (1)	Alto (3)
Switch Aruba	Medio (2)	Bajo (1)	Alto (3)
Planta telefónica	Bajo (1)	Bajo (1)	Medio (2)
Disco duro externo Toshiba	Medio (2)	Alto (3)	Medio (2)
Storage Thecus	Alto (3)	Alto (3)	Alto (3)
UPS	Bajo (1)	Bajo (1)	Alto (3)
Servidor Thinkstation	Alto (3)	Alto (3)	Alto (3)
Servidor IBM	Alto (3)	Alto (3)	Alto (3)
Repetidor Access Point TP Link	Medio (2)	Bajo (1)	Medio (2)
Equipos HP + pantalla y accesorios	Medio (2)	Medio (2)	Medio (2)
Cuentas de correo	Medio (2)	Alto (3)	Medio (2)
Internet canal dedicado Claro	Bajo (1)	Bajo (1)	Medio (2)

Activo	Integridad	Confidencialidad	Disponibilidad
Página web (dominio-hosting)	Alto (3)	Alto (3)	Alto (3)
Licencias Office 2010	Bajo (1)	Bajo (1)	Bajo (1)
Licencias Windows 10	Bajo (1)	Bajo (1)	Bajo (1)
Antivirus Kaspersky	Alto (3)	Alto (3)	Medio (2)
Disco duro 8 TB Seagate	Medio (2)	Alto (3)	Medio (2)
Disco duro Toshiba 1TB	Medio (2)	Alto (3)	Medio (2)
Sistema contable Siigo	Alto (3)	Alto (3)	Medio (2)
Sistema de información SIU	Alto (3)	Alto (3)	Medio (2)
Firewall Web	Alto (3)	Alto (3)	Medio (2)
Firewall interno/externo	Alto (3)	Alto (3)	Medio (2)
Directorio Activo	Alto (3)	Alto (3)	Medio (2)
Personal	Alto (3)	Alto (3)	Alto (3)

Fuente: El Autor.

Tabla 6 Criticidad Activos

Activo	Criticidad	Valoración
Switch HP	6	Medio
Switch D Link	6	Medio
Switch Aruba	6	Medio
Planta telefónica	4	Medio
Disco duro externo Toshiba	7	Alto
Storage Thecus	9	Alto
UPS	5	Medio
Servidor Thinkstation	9	Alto
Servidor IBM	9	Alto
Repetidor Access Point TP Link	5	Medio
Equipos HP + pantalla y accesorios	6	Medio
Cuentas de correo	7	Alto
Internet canal dedicado Claro	4	Medio

Activo	Criticidad	Valoración
Página web (dominio-hosting)	9	Alto
Licencias Office 2010	3	Bajo
Licencias Windows 10	3	Bajo
Antivirus Kaspersky	8	Alto
Disco duro 8 TB Seagate	7	Alto
Disco duro Toshiba 1TB	7	Alto
Sistema contable Siigo	8	Alto
Sistema de información SIU	8	Alto
Firewall Web	8	Alto
Firewall interno/externo	8	Alto
Directorio Activo	8	Alto
Personal	9	Alto

Fuente: El Autor.

Basados en la información obtenida los siguientes activos críticos en términos de confidencialidad, integridad y disponibilidad y se deben aunar esfuerzos para protegerlos:

- Storage Thecus
- Personal
- Servidor Thinkstation y servidor IBM
- Página web (dominio-hosting)
- Antivirus Kaspersky
- Disco duro 8 TB Seagate, Toshiba 1TB
- Sistema contable Siigo
- Sistema de información SIU
- Firewall Web, Firewall interno/externo
- Cuentas de Correo

Estos activos son críticos debido a que tienen una alta importancia para el funcionamiento y la seguridad de la organización, y su pérdida o compromiso podría tener consecuencias graves para la empresa. Es importante que estos activos reciban una atención especial en términos de protección y medidas de seguridad.

7.4 SUGERENCIAS PARA SALVAGUARDAR ACTIVOS CRÍTICOS

Para el Caso en estudio se categorizan las salvaguardas según el catálogo de elementos para cada activo incluyendo categoría a la que pertenecen y se realiza una evaluación de las salvaguardas propuestas basadas en EAR, PILAR y MAGERIT 3 según los criterios que se enuncian a continuación.

Figura 54 EAR (Estrategia, Arquitectura, Regulación)

Fase	Estrategia	Arquitectura	Regulación
Anticipación (A)	Evitar amenazas proactivamente.	Diseñar sistemas robustos y seguros.	Cumplir con normativas de seguridad.
Resistencia (R)	Reducir el impacto y recuperarse.	Implementar medidas de seguridad.	Cumplir con regulaciones específicas.
Capacidad de Crisis (C)	Manejar crisis y recuperarse.	Establecer protocolos de respuesta.	Cumplir con regulaciones de gestión de crisis.

Fuente: Elaboración propia

Figura 55 PILAR (Prevención, Identificación, Limitación, Análisis, Respuesta)

PILAR	Descripción
Prevención (P)	Implementar medidas para prevenir posibles amenazas y ataques.
Identificación (I)	Identificar y clasificar las amenazas cuando ocurren en tiempo real.
Limitación (L)	Limitar el alcance de las amenazas y reducir sus posibles impactos.
Análisis (A)	Analizar y evaluar la naturaleza y el impacto de las amenazas.
Respuesta (R)	Responder adecuadamente a las amenazas cuando se producen.

Fuente: Elaboración propia

Figura 56 MAGERIT 3

MAGERIT 3	Descripción
Activo (A)	Proteger la disponibilidad, integridad, confidencialidad, autenticidad y legalidad de la información.
Requisito (R)	Establecer los requisitos para la gestión de riesgos, incluyendo los procedimientos para identificar, evaluar y gestionar los riesgos.
Control (C)	Implementar medidas de seguridad y controles para gestionar y reducir los riesgos identificados.

Fuente: Elaboración propia

7.4.1 Discos Duros Externos

Encriptación de datos sensible, verificación periódica de la integridad de los datos almacenados, realizar copias de seguridad de manera regular para evitar pérdida de datos en caso de un fallo del dispositivo.

Figura 57 Discos Duros

Código	Salvaguarda	Categoría MAGERIT	EAR	PILAR	MAGERIT 3
DC.001	Cifrado de la información	Protección de los Datos / Información	A	C	A
DI.001	Aseguramiento de la integridad	Protección de los Datos / Información	R	A	C
DA.001	Copias de seguridad de los datos	Protección de los Datos / Información	C	R	R
H.AC.001	Control de acceso lógico	Protecciones Generales u Horizontales	A	A	A
DR.001	Retención de Datos	Protección de los Datos / Información	A	C	C
MP.A.001	Aseguramiento de la disponibilidad	Protección de los soportes de información	A	I	I
HV.tools.AV.001	Herramienta contra código dañino	Protecciones Generales u Horizontales	A	A	A
H.IR.001	Gestión de incidencias	Protecciones Generales u Horizontales	A	R	R
PS.AT.001	Formación y Concienciación	Salvaguarda relativa al personal	C	C	C
H.AU.001	Registro y Auditoría	Protecciones Generales u Horizontales	R	A	A

Fuente: Elaboración propia

7.4.2 Storage Thecus

Configuración adecuada de seguridad, como control de acceso a la red y autenticación de usuario, implementación de mecanismos de copia de seguridad y recuperación ante desastres.

Figura 58 Storage

Código	Salvaguarda	Categoría MAGERIT	EAR	PILAR	MAGERIT 3
H.AC.002	Control de acceso lógico	Protecciones Generales u Horizontales	A	A	A
H.IA.001	Identificación y autenticación	Protecciones Generales u Horizontales	A	A	A
DA.002	Copias de seguridad de los datos	Protección de los Datos / Información	C	R	R
BC.DRP. 001	Plan de Recuperación de Desastres	Continuidad de Operaciones	C	R	R

Fuente: Elaboración Propia

7.4.3 Personal

Establecer políticas y procedimientos claros, limitar el acceso menor privilegio, monitorear el acceso y uso de la información, es importante proteger los dispositivos de almacenamiento, como unidades USB, discos duros externos, entre otros, para evitar la extracción de información sensible de la compañía, educar al personal, realizar auditorías regulares.

Figura 59 Personal

Código	Salvaguarda	Categoría MAGERIT	EAR	PILAR	MAGERIT 3
G.Plan.001	Planificación de la Seguridad	Salvaguardas de Tipo Organizativo	A	P	C
H.AC.003	Control de acceso lógico	Protecciones Generales u Horizontales	A	L	C
H.AU.002	Registro y Auditoría	Protecciones Generales u Horizontales	A	I	C
MP.A.002	Aseguramiento de la disponibilidad	Protección de los Soportes de Información	A	P	C
PS.AT.002	Formación y Concienciación	Salvaguarda relativa al personal	C	I	C
H.IR.002	Gestión de incidencias	Protecciones Generales u Horizontales	R	I	A

Fuente: Elaboración Propia

7.4.4 Servidores

Configuración adecuada de seguridad, como autenticación de usuario, control de acceso a la red y firewalls de software, actualización regular de firmware y parches de seguridad, realizar copias de seguridad de manera regular y almacenarlas en un lugar seguro

Figura 60 Servidores

Código	Salvaguarda	Categoría MAGERIT	EAR	PILAR	MAGERIT 3
H.IA.002	Identificación y autenticación	Protecciones Generales u Horizontales	A	P	C
H.AC.004	Control de acceso lógico	Protecciones Generales u Horizontales	A	P	C
SA.001	Aseguramiento de la Disponibilidad	Protección de Servicios	A	P	C
H.VM.001	Gestión de Vulnerabilidades	Protecciones Generales u Horizontales	A	P	C
DA.003	Copias de seguridad de los datos	Protección de los Datos / Información	C	R	R

Fuente: Elaboración propia.

7.4.5 Cuentas de correo

Utilización de contraseñas fuertes y complejas, implementación de políticas de seguridad de correo electrónico, como filtrado de spam y correo no deseado, autenticación multifactorial, monitorear constantemente las cuentas para detectar posibles intentos de acceso no autorizado.

Figura 61 Correo

Código	Salvaguarda	Categoría MAGERIT	EAR	PILAR	MAGERIT 3
H.IA.003	Identificación y autenticación	Protecciones Generales u Horizontales	A	P	C
S.email.001	Protección del correo electrónico	Protección de los Servicios	A	P	C
H.AU.003	Monitorear constantemente las cuentas para detectar posibles intentos de acceso no autorizado	Protecciones Generales u Horizontales	C	I	C

Fuente: Elaboración propia

7.4.6 Página web (dominio-hosting)

Configuración adecuada de seguridad, como autenticación de usuario, encriptación de datos y firewalls con reglas establecidas y revisadas periódicamente, actualización regular de software y parches de seguridad.

Figura 62 Página

Código	Salvaguarda	Categoría MAGERIT	EAR	PILAR	MAGERIT 3
H.IA.004	Identificación y autenticación	Protecciones Generales u Horizontales	A	P	C
DC.002	Cifrado de la información	Protección de los Datos / Información	A	P	C
SA.002	Aseguramiento de la Disponibilidad	Protección de Servicios	A	P	C
H.VM.002	Gestión de Vulnerabilidades	Protecciones Generales u Horizontales	A	P	C

Fuente: Elaboración propia.

7.4.7 Antivirus Kaspersky

Configuración adecuada de seguridad, como actualización regular de firmas de virus y escaneo programado de archivos y carpetas.

Figura 63 Antivirus

Código	Salvaguarda	Categoría MAGERIT	EAR	PILAR	MAGERIT 3
HV.tools. AV.001	(Ctrl) enta contra código dañino	Protecciones Generales u Horizontales	A	P	C
H.tools.SF V.001	Verificación de Funciones de Seguridad	Protecciones Generales u Horizontales	A	P	C

Fuente: Elaboración propia

7.4.9 Sistema contable Siigo

Configuración adecuada de seguridad, como autenticación de usuario, control de acceso a la red y encriptación de datos, actualización regular de software y parches de seguridad.

Figura 64 Siigo

Código	Salvaguarda	Categoría MAGERIT	EAR	PILAR	MAGERIT 3
H.IA.005	Identificación y autenticación	Protecciones Generales u Horizontales	A	P	C
H.AC.005	Control de acceso lógico	Protecciones Generales u Horizontales	A	P	C
DC.003	Cifrado de la información	Protección de los Datos / Información	A	P	C
H.VM.003	Gestión de Vulnerabilidades	Protecciones Generales u Horizontales	A	P	C

Fuente: Elaboración Propia.

7.4.10 Sistema de información SIU

Configuración adecuada de seguridad, como autenticación de usuario multifactorial, control de acceso a la red y encriptación de datos, actualización regular de software y parches de seguridad.

Figura 65 SIU

Código	Salvaguarda	Categoría MAGERIT	EAR	PILAR	MAGERIT 3
H.IA.006	Identificación y autenticación	Protecciones Generales u Horizontales	A	P	C
H.AC.006	Control de acceso lógico	Protecciones Generales u Horizontales	A	P	C
DC.004	Cifrado de la información	Protección de los Datos / Información	A	P	C
H.VM.004	Gestión de Vulnerabilidades	Protecciones Generales u Horizontales	A	P	C

Fuente: Elaboración Propia.

7.4.11 Firewall Web

Configuración adecuada de seguridad, como control de acceso a la red y encriptación de datos, actualización regular de firmware y parches de seguridad.

Figura 66 Firewall

Código	Salvaguarda	Categoría MAGERIT	EAR	PILAR	MAGERIT 3
H.AC.007	Control de Acceso Lógico	Protecciones Generales u Horizontales	A	P	C
DC.00	Cifrado de la Información	Protección de los Datos/Información	A	P	C
HW.CM01	Protección de los Equipos informáticos	Cambios, actualizaciones y mantenimiento	A	P	C

Fuente: Elaboración Propia.

7.5 SUGERENCIAS GENERALES PARA PROTEGER LOS DIFERENTES ACTIVOS DE LA ORGANIZACIÓN

Switches: Configuración adecuada de seguridad, como autenticación de puerto y control de acceso a la red, actualización regular de firmware y parches de seguridad, restringir el acceso físico a los switches solo a personal autorizado, monitoreo de actividad en red.

Planta telefónica: Restringir el acceso físico al equipo, Configuración adecuada de autenticación de usuario y contraseñas seguras, implementar medidas de control de acceso para asegurarse de que solo los usuarios autorizados puedan hacer uso de las funcionalidades de la planta telefónica. Monitorear constantemente el tráfico de llamadas para detectar posibles intentos de fraude.

UPS: Monitoreo regular del estado y carga de la batería, ubicación segura y protegida de riesgos físicos y climáticos, configurar adecuadamente la UPS para evitar posibles fallos que puedan afectar la disponibilidad del sistema.

Repetidor Access Point TP Link: Configuración adecuada de seguridad, como autenticación de usuario, control de acceso a la red y encriptación de datos, actualización regular de firmware y parches de seguridad, restringir el acceso físico a los dispositivos solo a personal autorizado.

Equipos HP + pantalla y accesorios: Configuración adecuada de seguridad, como autenticación de usuario y control de acceso a la red, verificación regular de actualizaciones de seguridad y parches.

Internet canal dedicado Claro: revisión reglas de firewalls de hardware y software, monitoreo regular de la red y actividad sospechosa, establecer contraseñas seguras y cambiarlas periódicamente.

Directorio activo: Asignar permisos de acceso adecuados, encriptar la información almacenada, implementar controles de auditoría, realizar copias de seguridad y verificarlas para restaurar la información rápidamente, establecer políticas de seguridad.

Así podemos dar cierre al capítulo número dos donde podemos evidenciar que el partido de aunar esfuerzos para la protección de sus activos y garantizar la normal operación de su infraestructura, dado que se han evidenciado activos críticos que necesitan reforzar seguridad y garantizar su buen funcionamiento.

8. EVALUACIÓN DE AMENAZAS Y VULNERABILIDADES CON MAGERIT

La importancia de emplear MAGERIT radica en su capacidad para proporcionar un marco sólido y coherente para la gestión de riesgos de seguridad de la información, lo que permite a las organizaciones proteger sus activos de información de manera efectiva y cumplir con los requisitos normativos, al tiempo que optimizan la inversión en seguridad y se adaptan a un entorno de amenazas en constante evolución.

Evaluar las amenazas y vulnerabilidades de los activos TI del Partido de la U es esencial por varias razones:

Protección de Datos Sensibles: Los partidos políticos manejan información confidencial sobre sus miembros, donantes, estrategias electorales y políticas. Evaluar las amenazas ayuda a proteger esta información vital de posibles filtraciones o ataques cibernéticos.

Integridad del Proceso Electoral: La seguridad de los sistemas de votación electrónica y la gestión de datos electorales son críticos para garantizar elecciones justas y transparentes. La evaluación de vulnerabilidades contribuye a prevenir manipulaciones o intrusiones en estos sistemas.

Reputación y Confianza Pública: Un incidente de seguridad en los activos TI de un partido político puede erosionar la confianza de los votantes y socavar su reputación. La evaluación proactiva puede ayudar a evitar crisis de relaciones públicas.

Ciberseguridad Global: En un mundo interconectado, los partidos políticos pueden ser blanco de ataques cibernéticos de actores internos y externos. Evaluar amenazas y vulnerabilidades es esencial para anticipar y responder a estas amenazas.

Cumplimiento Legal: En muchos países, existen regulaciones y leyes que exigen la protección de datos personales y la seguridad cibernética. La falta de cumplimiento puede dar lugar a sanciones legales y multas. La evaluación ayuda a garantizar el cumplimiento normativo.

Continuidad Operativa: Los sistemas de TI son críticos para las operaciones diarias de un partido político. La evaluación de vulnerabilidades ayuda a asegurar la disponibilidad y la continuidad de estas operaciones, incluso en situaciones de crisis.

8.1. IDENTIFICACIÓN DE AMENAZAS

En este punto, el objetivo principal es analizar y comprender las posibles amenazas que pueden afectar los activos del Partido. Para hacerlo, se utilizará una lista de amenazas específicas que se encuentran en el Catálogo de Elementos de Magerit Versión 3. El propósito es identificar estas amenazas y evaluar cuán significativas son en el proyecto en cuestión.

8.2. CLASIFICACIÓN

De acuerdo a Magerit Versión 3, las amenazas se dividen en cuatro grupos o tipos diferentes.

Desastres naturales [N]
De origen Industrial [I]
Errores y fallos no intencionados [E]
Ataques Intencionados [A]

8.2.1 Identificación de amenazas asociadas a los activos

Figura 67 Amenazas Asociadas a Activos

Activo	Amenazas Asociadas
Switch HP	[I6] Corte del suministro eléctrico [I5] Avería de origen físico o lógico [E24] Caída del sistema por agotamiento de recursos [A11] Acceso no autorizado [E2] Errores del administrador [A6] Abuso de Privilegios de Acceso [A24] Denegación de servicio [A25] Robo [A26] Ataque destructivo
Switch D Link	[I6] Corte del suministro eléctrico [I5] Avería de origen físico o lógico [E24] Caída del sistema por agotamiento de recursos [A11] Acceso no autorizado [E2] Errores del administrador [A6] Abuso de Privilegios de Acceso [A24] Denegación de servicio [A25] Robo [A26] Ataque destructivo
Switch Aruba	[I6] Corte del suministro eléctrico [I5] Avería de origen físico o lógico [E24] Caída del sistema por agotamiento de recursos [A11] Acceso no autorizado [E2] Errores del administrador [A6] Abuso de Privilegios de Acceso [A24] Denegación de servicio [A25] Robo

Fuente: El Autor

Figura 68 Amenazas 2

Activo	Amenazas Asociadas
Planta telefónica	[I2] Daños por agua (internos) [I5] Avería de origen físico o lógico [I6] Corte del suministro eléctrico [E2] Errores del administrador [E23] Errores de mantenimiento / actualización de equipos (hardware) [A11] Acceso no autorizado [A25] Robo
Disco duro externo Toshiba	[A11] Acceso no autorizado [A25] Robo [E14] Escapes de información [E18] Destrucción de información [E15] Alteración accidental de la información [E19] Fugas de información [E25] Pérdida de equipos
Storage Thecus	[A11] Acceso no autorizado [A25] Robo [E14] Escapes de información [E18] Destrucción de información [E15] Alteración accidental de la información [E19] Fugas de información [E25] Pérdida de equipos
UPS	[N1] Fuego [N2] Daños por agua [N*] Desastres naturales [E23] Errores de mantenimiento / actualización de equipos (hardware) [A7] Uso no previsto [A23] Manipulación de los equipos [A25] Robo

Fuente El Autor.

Figura 69 Amenazas 3

Activo	Amenazas Asociadas
Servidor Thinkstation	[I11] Emanaciones electromagnéticas [E2] Errores del administrador [E25] Pérdida de equipos [A6] Abuso de privilegios de acceso [A7] Uso no previsto [A11] Acceso no autorizado [A23] Manipulación de los equipos [A24] Denegación de servicio [A25] Robo
Servidor IBM	[I11] Emanaciones electromagnéticas [E2] Errores del administrador [E25] Pérdida de equipos [A6] Abuso de privilegios de acceso [A7] Uso no previsto [A11] Acceso no autorizado [A23] Manipulación de los equipos [A24] Denegación de servicio [A25] Robo
Repetidor Access Point TP Link	[E2] Errores del administrador [E9] Errores de [re-]encaminamiento [E15]] Alteración accidental de la información [E19] Fugas de información [E25] Pérdida de equipos [A5] [A5] Suplantación de la identidad del usuario [A6] Abuso de privilegios de acceso [A7] Uso no previsto [A10] Alteración de secuencia [A11] Acceso no autorizado [A12] Análisis de tráfico [A14] Interceptación de información (escucha) [A19] Divulgación de información [A24] Denegación de servicio

Fuente: El Autor

Figura 70 Amenazas 4

Activo	Amenazas Asociadas
Equipos HP + pantalla y accesorios	[I11] Emanaciones electromagnéticas [E2] Errores del administrador [E1] Errores de los usuarios [E25] Pérdida de equipos [I5] Avería de origen físico o lógico [A6] Abuso de privilegios de acceso [A11] Acceso no autorizado [A23] Manipulación de los equipos
Cuentas de correo	[A11] Acceso no autorizado [A5] Suplantación de la identidad del usuario [A15] Modificación deliberada de la información [E20] Vulnerabilidades de los programas [A25] Robo [A14] Interceptación de información (escucha) [E19] Fugas de información [A26] Ataque destructivo
Internet canal dedicado Claro	[E2] Errores del administrador [E4] Errores de configuración [A11] Acceso no autorizado [I9] Interrupción de otros servicios y suministros esenciales [A12] Análisis de tráfico [A14] Interceptación de información (escucha) [A19] Divulgación de información

Fuente: El Autor.

Figura 71 Amenazas

Activo	Amenazas Asociadas
Página web (dominio-hosting)	[E19] Fugas de información [E20] Vulnerabilidades de los programas (software) [E21] Errores de mantenimiento / actualización de programas (software) [A6] Abuso de privilegios de acceso [A8] Difusión de software dañino [A11] Acceso no autorizado

Fuente: El Autor

Figura 72 Amenazas 5

Activo	Amenazas Asociadas
Licencias Office 2010	[E1] Errores de los usuarios [E2] Errores del administrador [E8] Difusión de software dañino [E20] Vulnerabilidades de los programas (software) [E21] Errores de mantenimiento / actualización de programas (software) [A5] Suplantación de la identidad del usuario [A6] Abuso de privilegios de acceso [A11] Acceso no autorizado [A15] Modificación deliberada de la información [A19] Divulgación de información [A22] Manipulación de programas
Licencias Windows 10	[E1] Errores de los usuarios [E2] Errores del administrador [E8] Difusión de software dañino [E20] Vulnerabilidades de los programas (software) [E21] Errores de mantenimiento / actualización de programas (software) [A5] Suplantación de la identidad del usuario [A6] Abuso de privilegios de acceso [A11] Acceso no autorizado [A15] Modificación deliberada de la información [A19] Divulgación de información [A22] Manipulación de programas

Fuente: El Autor

Figura 73 Amenazas 6

Activo	Amenazas Asociadas
Antivirus Kaspersky	[E1] Errores de los usuarios [E2] Errores del administrador [E8] Difusión de software dañino [E20] Vulnerabilidades de los programas (software) [E21] Errores de mantenimiento / actualización de programas (software) [A5] Suplantación de la identidad del usuario [A6] Abuso de privilegios de acceso [A11] Acceso no autorizado [A15] Modificación deliberada de la información [A19] Divulgación de información [A22] Manipulación de programas
Disco duro 8 TB Seagate	[A11] Acceso no autorizado [A25] Robo [E14] Escapes de información [E18] Destrucción de información [E15] Alteración accidental de la información [E19] Fugas de información [E25] Pérdida de equipos
Disco duro Toshiba 1TB	[A11] Acceso no autorizado [A25] Robo [E14] Escapes de información [E18] Destrucción de información [E15] Alteración accidental de la información [E19] Fugas de información [E25] Pérdida de equipos

Fuente: El Autor

Figura 74 Amenazas 7

Activo	Amenazas Asociadas
Sistema contable Siigo	[E1] Errores de los usuarios [E2] Errores del administrador [E8] Difusión de software dañino [E15] Alteración accidental de la información [E19] Fugas de información [E20] Vulnerabilidades de los programas (software) [E21] Errores de mantenimiento / actualización de programas (software) [A5] Suplantación de la identidad del usuario [A6] Abuso de privilegios de acceso [A7] Uso no previsto [A11] Acceso no autorizado [A15] Modificación deliberada de la información [A19] Divulgación de información [A22] Manipulación de programas
Sistema de información SIU	[E1] Errores de los usuarios [E2] Errores del administrador [E8] Difusión de software dañino [E15] Alteración accidental de la información [E19] Fugas de información [E20] Vulnerabilidades de los programas (software) [E21] Errores de mantenimiento / actualización de programas (software) [A5] Suplantación de la identidad del usuario [A6] Abuso de privilegios de acceso [A7] Uso no previsto [A11] Acceso no autorizado [A15] Modificación deliberada de la información [A19] Divulgación de información [A22] Manipulación de programas

Fuente: El Autor

Figura 75 Amenazas 8

Activo	Amenazas Asociadas
Firewall Web	[E2] Errores del administrador [A6] Abuso de privilegios de acceso [A7] Uso no previsto [A11] Acceso no autorizado [A15] Modificación deliberada de la información [A22] Manipulación de programas
Firewall interno/externo	[E2] Errores del administrador [A6] Abuso de privilegios de acceso [A7] Uso no previsto [A11] Acceso no autorizado [A15] Modificación deliberada de la información [A22] Manipulación de programas [E25] Pérdida de equipos [A23] Manipulación de los equipos
Directorio Activo	[E1] Errores de los usuarios [E2] Errores del administrado [E4] Errores de configuración [E15] Alteración accidental de la información [A5] Suplantación de la identidad del usuario [A6] Abuso de privilegios de acceso [A11] Acceso no autorizado [A15] Modificación deliberada de la información [A19] Divulgación de información [A24] Denegación de servicio

Fuente: El Autor

Figura 76 Amenazas 9

Activo	Amenazas Asociadas
Personal	[E15] Alteración accidental de la información [E19] Fugas de información [A15] Modificación deliberada de la información [A19] Divulgación de información [A29] Extorsión [A30] Ingeniería social (picaresca)

Fuente: El Autor.

8.3. VALORACIÓN DE AMENAZAS

A continuación, se valorarán las amenazas y su frecuencia tomando como referencia los activos del partido de la U, su frecuencia e impacto en los pilares de la seguridad basados en MAGERIT.

Figura 77 Impacto y Valoración Amenazas

IMPACTO		VALOR
Muy alto	[MA]	100%
Alto	[A]	75%
Medio	[M]	50%
Bajo	[B]	20%
Muy bajo	[MB]	5%

Fuente: Magerit V.3 - Libro II - Catálogo de Elementos

Figura 78 Frecuencia Amenazas

Valor			Criterio
100	Frecuencia muy alta	FMA	1 vez al día
70	Frecuencia alta	FA	1 vez cada semana
50	Frecuencia media	FM	2 vez cada 2 meses
10	Frecuencia baja	FB	1 vez cada 6 meses
5	Frecuencia media baja	FMB	1 vez al año

Fuente: El Autor.

A continuación, se evidencia la percepción de la frecuencia y el impacto de las amenazas en diferentes dimensiones de seguridad basada en la información recopilada durante charlas no formales con empleados de la empresa de cada uno de los activos. El análisis se hace basado en las dimensiones que cada categoría impacta según el catálogo de elementos de MAGERIT.

Figura 79 Valoración Amenazas Switches

ACTIVO	AMENAZA	FRECUENCIA	% IMPACTO DIMENSIÓN				
			[A]	[C]	[I]	[D]	[T]
Switches HP, Dlink y Aruba	[I6] Corte del suministro eléctrico	10				100%	
	[I5] Avería de origen físico o lógico	5				100%	
	[E24] Caída del sistema por agotamiento de recursos	5				100%	
	[A11] Acceso no autorizado	10		75%	75%		
	[E2] Errores del administrador	5		100%	100%	100%	
	[A6] Abuso de Privilegios de Acceso	10		50%	50%	75%	
	[A24] Denegación de servicio	5				100%	
	[A25] Robo	10		75%		75%	
	[A26] Ataque destructivo	5				100%	

Fuente: El Autor

Figura 80 Valoración Amenazas Planta Telefónica

ACTIVO	AMENAZA	FRECUENCIA	% IMPACTO DIMENSIÓN				
			[A]	[C]	[I]	[D]	[T]
Planta Telefónica	[I2] Daños por Agua	5				100%	
	[I6] Corte del suministro eléctrico	10				100%	
	[I5] Avería de origen físico o lógico	5				100%	
	[E23] Errores de mantenimiento / actualización de equipos (hardware)	10				100%	
	[A11] Acceso no autorizado	10		50%	50%		
	[E2] Errores del administrador	5		50%	50%	100%	
	[A25] Robo	10		50%		75%	

Fuente: El Autor

Figura 81 Valoración Amenazas Discos y Storage

ACTIVO	AMENAZA	FRECUENCIA	% IMPACTO DIMENSIÓN				
			[A]	[C]	[I]	[D]	[T]
Discos Duros Externos y Storage	[A11] Acceso no autorizado	10		100%	75%		
	[A25] Robo	10		100%		75%	
	[E14] Escapes de información	10		100%			
	[E18] Destrucción de información	5				100%	
	[E15] Alteración accidental de la información	10			75%		
	[E19] Fugas de información	5		100%			
	[E25] Pérdida de equipos	50		100%		75%	

Fuente: El Autor

Figura 82 Valoración Amenazas UPS

ACTIVO	AMENAZA	FRECUENCIA	% IMPACTO DIMENSIÓN				
			[A]	[C]	[I]	[D]	[T]
UPS	[N1] Fuego	5				100%	
	[I2] Daños por Agua	10				100%	
	[N*] Desastres naturales	5				100%	
	[E23] Errores de mantenimiento / actualización de equipos	50				100%	
	[A7] Uso no previsto	10		50%	50%	50%	
	[A23] Manipulación de los equipos	5		50%		75%	
	[A25] Robo	10		20%		100%	

Fuente: El Autor

Figura 83 Valoración Amenazas Servidores

ACTIVO	AMENAZA	FRECUENCIA	% IMPACTO DIMENSIÓN				
			[A]	[C]	[I]	[D]	[T]
Servidores Thinkstation e IBM	[I11] Emanaciones electromagnéticas	5		75%			
	[E2] Errores del administrador	10		100%	100%	100%	
	[A6] Abuso de privilegios de acceso	10		100%	100%	75%	
	[A11] Acceso no autorizado	50		100%	100%		
	[A7] Uso no previsto	10		50%	50%	50%	
	[A24] Denegación de servicio					100%	
	[A23] Manipulación de los equipos	5		75%		75%	
	[A25] Robo	10		100%		100%	

Fuente: El Autor

Figura 84 Valoración Amenazas Access Point

ACTIVO	AMENAZA	FRECUENCIA	% IMPACTO DIMENSIÓN				
			[A]	[C]	[I]	[D]	[T]
Access Points	[E2] Errores del Administrador	10		50%	50%	50%	
	[E9] Errores de [re-]encaminamiento	10		50%			
	[E15]] Alteración accidental de la información	10		75%			
	[E19] Fugas de información	5				100%	
	[E25] Pérdida de equipos [A5]	10		20%		75%	
	[A5] Suplantación de la identidad del usuario	5		50%	50%	75%	
	[E25] Pérdida de equipos	50		20%		75%	
	[A6] Abuso de privilegios de acceso	10		50%	50%	75%	
	[A7] Uso no previsto	10		50%	50%	75%	
	[A10] Alteración de secuencia	5			75%		
	[A11] Acceso no autorizado	10		100%	75%		
	[A12] Análisis de tráfico	10			100%		
	[A14] Interceptación de información (escucha)	5		100%			
	[A19] Divulgación de información	10		100%			
	[A24] Denegación de servicio	5		75%		100%	

Fuente: El Autor

Figura 85 Valoración Amenazas Equipos

ACTIVO	AMENAZA	FRECUENCIA	% IMPACTO DIMENSIÓN				
			[A]	[C]	[I]	[D]	[T]
Equipos Hp + Pantalla y Accesorios	[I11] Emanaciones electromagnéticas	5		75%			
	[E2] Errores del administrador	10		100%	100%	100%	
	[E1] Errores de los Usuarios	50		100%	100%	100%	
	[E25] Pérdida de equipos	10		100%		100%	
	[I5] Avería de origen físico o lógico	50				75%	
	[A11] Acceso no autorizado	50		100%	100%		
	[A6] Abuso de privilegios de acceso	10		75%	100%	50%	
	[A23] Manipulación de los equipos	5		75%		75%	
	[A25] Robo	10		100%		100%	

Fuente: El Autor

Figura 86 Valoración Amenazas Correos

ACTIVO	AMENAZA	FRECUENCIA	% IMPACTO DIMENSIÓN				
			[A]	[C]	[I]	[D]	[T]
Cuentas de Correo	[A11] Acceso no autorizado	10		100%	100%		
	[A5] Suplantación de la identidad del usuario	10		100%	100%	100%	
	[A15] Modificación deliberada de la información	10			100%		
	[E20] Vulnerabilidades de los programas	5		100%	50%	75%	
	[A25] Robo	5		100%		75%	
	[A14] Interceptación de información (escucha)	5		75%			
	[E19] Fugas de información	5		100%			
	[A26] Ataque destructivo	10				50%	

Fuente: El Autor

Figura 87 Valoración Amenazas Internet

ACTIVO	AMENAZA	FRECUENCIA	% IMPACTO DIMENSIÓN				
			[A]	[C]	[I]	[D]	[T]
Internet Canal Dedicado	[E2] Errores del administrador	5		75%	50%	100%	
	[E4] Errores de Configuración	10			75%		
	[A11] Acceso no autorizado	10		75%	75%		
	[I9] Interrupción de otros servicios y suministros esenciales	10				100%	
	[A12] Análisis de tráfico	5			100%		
	[A14] Interceptación de información (escucha)	5		100%			
	[A19] Divulgación de información	5		75%			

Fuente: El Autor

Figura 88 Valoración Amenazas Página Web

ACTIVO	AMENAZA	FRECUENCIA	% IMPACTO DIMENSIÓN				
			[A]	[C]	[I]	[D]	[T]
Página Web-Dominio y Hosting	[E19] Fugas de información	5		100%			
	[E20] Vulnerabilidades de los programas	5		100%	50%	75%	
	[E21] Errores de mantenimiento / actualización de programas (software)	10				100%	
	[E1] Errores de los Usuarios	10		100%	100%	100%	
	[A6] Abuso de privilegios de acceso	10		75%	100%	100%	
	[A8] Difusión de software dañino	10		100%	100%	100%	
	[A11] Acceso no autorizado	5		100%	100%		

Fuente: El Autor

Figura 89 Valoración Amenazas Licencias

ACTIVO	AMENAZA	FRECUENCIA	% IMPACTO DIMENSIÓN				
			[A]	[C]	[I]	[D]	[T]
Licencias Office2010, Windows 10 y Kaspersky	[E1] Errores de los Usuarios	50		100%	100%	100%	
	[E2] Errores del administrador	10		100%	100%	100%	
	[A8] Difusión de software dañino	10		100%	100%	100%	
	[E20] Vulnerabilidades de los	5		100%	50%	75%	
	[E21] Errores de mantenimiento / actualización de programas (software)	10				100%	
	[A5] Suplantación de la identidad del	10		75%	75%	75%	
	[A11] Acceso no autorizado	50		100%	100%		
	[A6] Abuso de privilegios de acceso	10		75%	100%	50%	
	] Modificación deliberada de la informa	10			75%		
	[A19] Divulgación de información	10		75%			

Fuente: El Autor

Figura 90 Valoración Amenazas Sistemas

ACTIVO	AMENAZA	FRECUENCIA	% IMPACTO DIMENSIÓN				
			[A]	[C]	[I]	[D]	[T]
Sistema Contable SIIGO y SIU	[E1] Errores de los Usuarios	50		100%	100%	100%	
	[E2] Errores del administrador	10		100%	100%	100%	
	[A8] Difusión de software dañino	10		100%	100%	100%	
	[E15]] Alteración accidental de la información	10		75%			
	[E19] Fugas de información	10		100%			
	[E20] Vulnerabilidades de los programas	5		100%	75%	75%	
	[E21] Errores de mantenimiento / actualización de programas (software)	10				100%	
	[A5] Suplantación de la identidad del usuario	10		100%	100%	100%	
	[A11] Acceso no autorizado	50		100%	100%		
	[A6] Abuso de privilegios de acceso	10		100%	100%	50%	
	[A15] Modificación deliberada de la información	10			75%		
	[A19] Divulgación de información	10		100%			
	[A7] Uso no previsto	10		75%	75%	75%	
	[A22] Manipulación de programas	10		100%	100%	100%	

Fuente: El Autor

Figura 91 Valoración Firewall

ACTIVO	AMENAZA	FRECUENCIA	% IMPACTO DIMENSIÓN				
			[A]	[C]	[I]	[D]	[T]
Firewall Interno y Web	[E2] Errores del administrador	10		100%	100%	100%	
	[A11] Acceso no autorizado	50		100%	100%		
	[A6] Abuso de privilegios de acceso	10		100%	100%	50%	
	[A15] Modificación deliberada de la información	10			75%		
	[A22] Manipulación de programas	10		100%	100%	100%	

Fuente: El Autor

Figura 92 Valoración D.A

ACTIVO	AMENAZA	FRECUENCIA	% IMPACTO DIMENSIÓN				
			[A]	[C]	[I]	[D]	[T]
D.A	[E1] Errores de los Usuarios	50		100%	100%	100%	
	[E2] Errores del administrador	10		100%	100%	100%	
	[E4] Errores de Configuración	10			100%		
	[E15]] Alteración accidental de la información	10		75%			
	[A5] Suplantación de la identidad del usuario	10		100%	100%	100%	
	[A11] Acceso no autorizado	50		100%	100%		
	[A6] Abuso de privilegios de acceso	10		100%	100%	50%	
	[A15] Modificación deliberada de la información	10			75%		
	[A19] Divulgación de información	10		100%			
	[A7] Uso no previsto	10		75%	75%	75%	
	[A24] Denegación de servicio					100%	

Fuente: El Autor

Figura 93 Valoración Personal

ACTIVO	AMENAZA	FRECUENCIA	% IMPACTO DIMENSIÓN				
			[A]	[C]	[I]	[D]	[T]
Personal	[E15]] Alteración accidental de la información	10		100%			
	[E19] Fugas de información	10		100%			
	[A15] Modificación deliberada de la información	10			100%		
	[A19] Divulgación de información	10		100%			
	[A29] Extorsión	10		100%	100%	100%	
	[A30] Ingeniería social (picaresca)	10		100%	100%	100%	

Fuente: El Autor

8.4 RIESGOS ASOCIADOS

Figura 94 Valoración 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: El Autor.

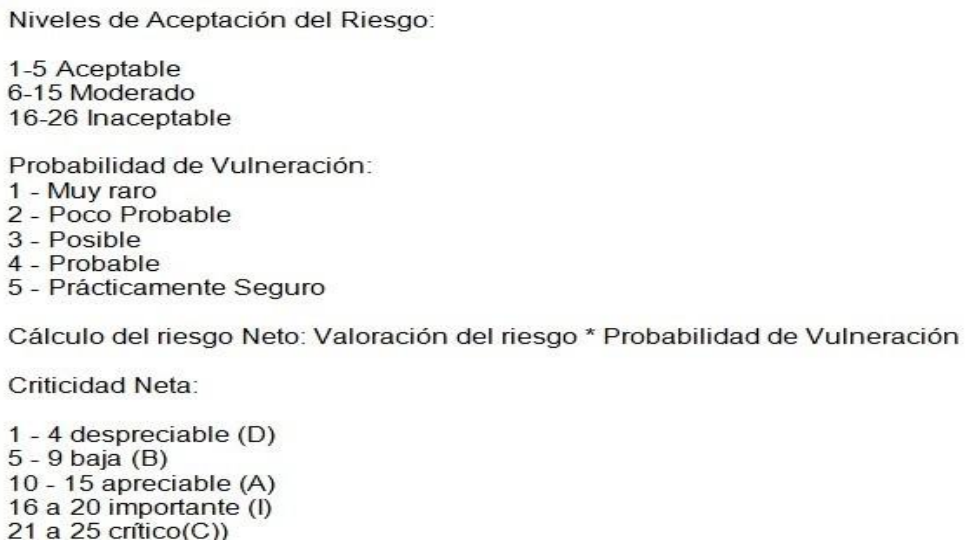
Figura 95 Valoración Riesgos

	Nombre	Riesgo	AUTENTICIDAD	TRAZABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILI	VALOR
1	Microsoft Windows Server 2008 R2 Standard	BAJO	9	9	9	9	9	9
2	Switch Hp	IMPORTANTE	15	15	9	15	25	16
3	Switch D Link	IMPORTANTE	15	15	9	15	25	16
4	Switch Aruba	IMPORTANTE	15	15	9	15	25	16
5	Planta telefónica	APRECIABLE	9	9	9	9	15	10
6	Disco duro externo Toshiba	APRECIABLE	15	9	20	15	9	14
7	Storage Thecus	CRITICO	25	25	25	25	25	25
8	UPS	APRECIABLE	9	9	9	9	25	12
9	Servidor Thinkstation	CRITICO	25	25	25	25	25	25
10	Servidor IBM	CRITICO	25	25	25	25	25	25
11	Repetidor Access Point TP Link	APRECIABLE	9	9	9	15	15	11
12	Equipos HP + pantalla y accesorios	APRECIABLE	15	15	15	15	15	15
13	Cuentas de correo	APRECIABLE	9	9	25	15	15	15
14	Internet canal dedicado Claro	APRECIABLE	15	9	9	9	15	11
15	Página web (dominio-hosting)	CRITICO	25	25	25	25	25	25
16	Licencias Office 2010	BAJO	9	9	9	9	9	9
17	Licencias Windows 10	BAJO	9	9	9	9	9	9
18	Antivirus Kaspersky	IMPORTANTE	15	15	25	25	15	19
19	Disco duro 8 TB Seagate	APRECIABLE	15	9	20	15	9	14
20	Disco duro Toshiba 1TB	APRECIABLE	15	9	20	15	9	14
21	Sistema contable Siigo	IMPORTANTE	25	9	25	25	15	20
22	Sistema de información SIU	IMPORTANTE	25	9	25	25	15	20
23	Firewall Web	IMPORTANTE	15	15	25	25	15	19
24	Firewall interno/externo	IMPORTANTE	15	15	25	25	15	19
25	Directorio Activo	IMPORTANTE	15	15	25	25	15	19
26	Personal	APRECIABLE	25	25	9	9	9	15

Fuente: El Autor.

Se procede a asociar las vulnerabilidades de las amenazas asociadas a los activos y evaluar los riesgos según los siguientes criterios:

Figura 96 Criterios Magerit



Fuente: Centro Criptológico Nacional. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT versión 3). [Sitio Web]. [Consultado: 04 de abril de 2023]. Archivo Pdf. Disponible en: https://www.ccn-cert.cni.es/pdf/magerit-v3-1-manual-completo.pdf

Figura 97 Swicthes HP, TPlink, Aruba

Activos de Información	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas Metodología Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Probabilidad de vulneración	Calculo del riesgo neto	Criticidad neta
HARDWARE	Switch HP	16	[I6] Corte del suministro eléctrico	Interrupción del Servicio	I	4	64	C
HARDWARE	Switch HP	16	[I5] Avería de origen físico o lógico	Falla de Hardware no detectada	I	3	48	C
HARDWARE	Switch HP	16	[E24] Caída del sistema por agotamiento de recursos	Falta de Monitoreo y Alertas	I	2	32	C
HARDWARE	Switch HP	16	[A11] Acceso no autorizado	Débil Autenticación y Autorización	M	3	48	C
HARDWARE	Switch HP	16	[E2] Errores del administrador	Falta de capacitación o la negligencia del administrador en la configuración y gestión del dispositivo	M	2	32	C
HARDWARE	Switch HP	16	[A6] Abuso de privilegios de acceso	Falta de una adecuada gestión de los permisos y privilegios de acceso en el dispositivo	M	2	32	C
HARDWARE	Switch HP	16	[A24] Denegación de servicio	Insuficiente protección del Switch HP contra ataques, sin IDS	I	2	32	C
HARDWARE	Switch HP	16	[A25] Robo	Falta medidas de seguridad en las instalaciones, sistema de control de acceso y vigilancia	M	1	16	I
HARDWARE	Switch HP	16	[A26] Ataque destructivo	Falta de protección física, acceso no autorizado a las instalaciones donde se encuentra el Switch	I	1	16	I

Fuente: El Autor.

Figura 98 Análisis Riesgos y Vulnerabilidades Planta Telefónica

Activos de Información	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas Metodología Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Probabilidad de vulneración	Calculo del riesgo neto	Criticidad neta
HARDWARE	Planta telefónica	10	[N2] Daños por agua	Falta de protección contra inundaciones o escapes de agua en las instalaciones.	A	3	30	C
HARDWARE	Planta telefónica	10	[I5] Avería de origen físico o lógico	Falta de mantenimiento preventivo y Correctivo a la Planta.	M	3	30	C
HARDWARE	Planta telefónica	10	[I6] Corte del suministro eléctrico	Falta de Redundancia, UPS	M	4	40	C
HARDWARE	Planta telefónica	10	[E2] Errores del administrador	Falta de supervisión y control adecuados por parte del administrador de la planta telefónica.	M	1	10	B
HARDWARE	Planta telefónica	10	[E23] Errores de mantenimiento / actualización de equipos (hardware)	Fallos en el mantenimiento y actualización de los equipos de hardware de la planta telefónica	A	3	30	C

Fuente el Autor

Figura 99 Riesgos y Vulnerabilidades Discos Duros Externos y Storage

Activos de Información	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas Metodología Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Probabilidad de vulneración	Calculo del riesgo neto	Criticidad neta
HARDWARE	Disco duro externo Toshiba	14	[A11] Acceso no autorizado	Falta de autenticación adecuada para acceder al disco duro externo Toshiba	M	3	42	C
HARDWARE	Disco duro externo Toshiba	14	[A25] Robo	Almacenamiento físico inadecuado del disco duro externo Toshiba	M	4	56	C
HARDWARE	Disco duro externo Toshiba	14	[E19] Fugas de información	Falta de cifrado o protección de datos en el disco duro externo	M	4	56	C
HARDWARE	Disco duro externo Toshiba	14	[E18] Destrucción de información	Falta de copias de seguridad regulares y adecuadas de los datos almacenados en el disco duro externo	I	2	28	C
HARDWARE	Disco duro externo Toshiba	14	[E15] Alteración accidental de la información	No implementación de mecanismos de protección contra escritura en el disco duro externo	M	2	28	C
HARDWARE	Disco duro externo Toshiba	14	[E25] Pérdida de equipos	Almacenamiento físico inadecuado del disco duro externo Toshiba, Falta de controles en el acceso a instalaciones	M	3	42	C

Fuente: El autor.

Figura 100 Riesgos y Vulnerabilidades UPS

Activos de Información	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas Metodología Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Probabilidad de vulneración	Calculo del riesgo neto	Criticidad neta
HARDWARE	UPS	12	[N1] Fuego	falta de medidas de prevención y extinción de incendios en la ubicación donde se encuentra la UPS	M	1	12	A
HARDWARE	UPS	12	[N2] Daños por agua	Falta de protección adecuada contra el agua o la humedad en el entorno donde se encuentra la UPS, ubicación inadecuada	M	3	36	C
HARDWARE	UPS	12	[E23] Errores de mantenimiento/ actualización de equipos (hardware)	Falta de mantenimiento preventivo y Correctivo a la UPS	M	2	24	C
HARDWARE	UPS	12	[A7] Uso no previsto	Falta de un plan o política de uso adecuado y restricciones de acceso.	M	1	12	A
HARDWARE	UPS	12	[A23] Manipulación de los equipos	Fallas de Control de Acceso al Data Center	M	1	12	A
HARDWARE	UPS	12	[A25] Robo	Fallas de Control de Acceso al Data Center	M	1	12	A

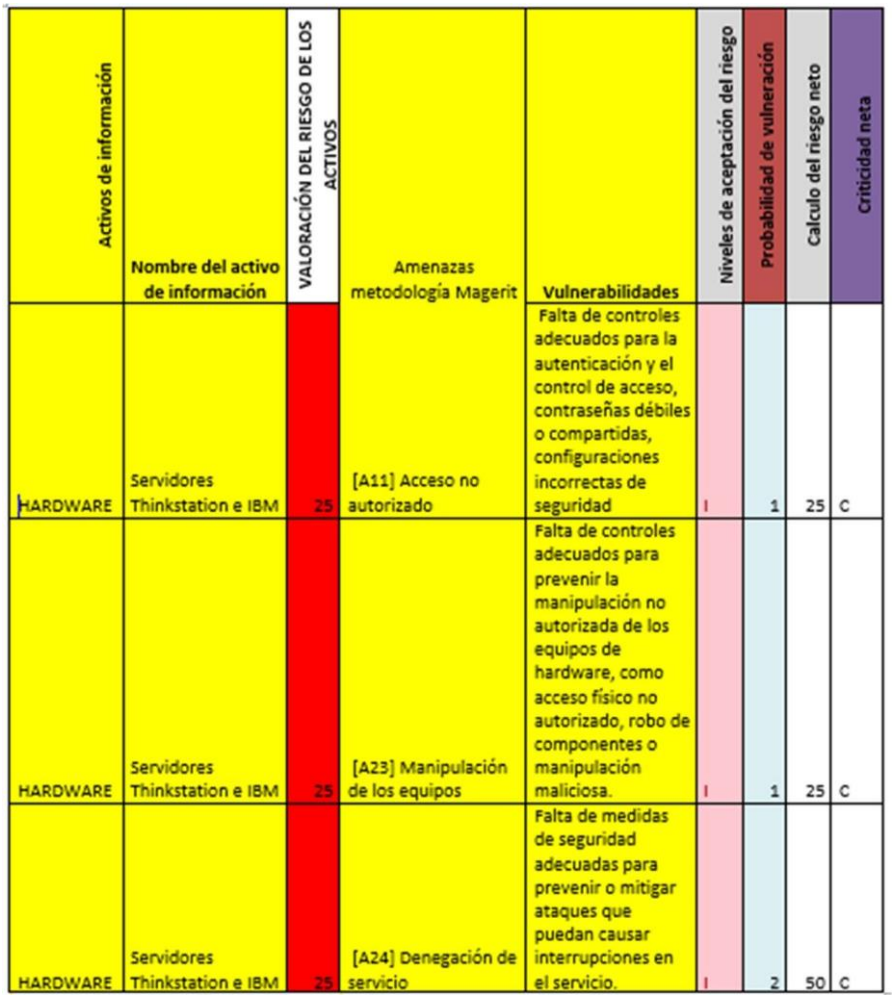
Fuente: El autor.

Figura 101 Análisis Riesgos y Vulnerabilidades Servidores

Activos de Información	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas Metodología Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Probabilidad de vulneración	Calculo del riesgo neto	Criticidad neta
HARDWARE	Servidor Thinkstation e IBM	25	[I11] Emanaciones electromagnéticas	Falta de blindaje electromagnético en el servidor	M	1	25	C
HARDWARE	Servidor Thinkstation e IBM	25	[E2] Errores del administrador	Falta de capacitación o formación adecuada del personal administrador	I	1	25	C
HARDWARE	Servidor Thinkstation e IBM	25	[E25] Pérdida de equipos	Falta de medidas de seguridad adecuadas para proteger físicamente el servidor	I	2	50	C
HARDWARE	Servidor Thinkstation e IBM	25	[A7] Uso no previsto	Falta de restricciones de acceso, la ausencia de un seguimiento de las actividades realizadas en el servidor o la falta de capacitación para los usuarios	I	2	50	C

Fuente: El Autor

Figura 102 Continuación Análisis Riesgos y Vulnerabilidades Servidores



Activos de información	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas metodología Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Probabilidad de vulneración	Calculo del riesgo neto	Criticidad neta
HARDWARE	Servidores Thinkstation e IBM	25	[A11] Acceso no autorizado	Falta de controles adecuados para la autenticación y el control de acceso, contraseñas débiles o compartidas, configuraciones incorrectas de seguridad	I	1	25	C
HARDWARE	Servidores Thinkstation e IBM	25	[A23] Manipulación de los equipos	Falta de controles adecuados para prevenir la manipulación no autorizada de los equipos de hardware, como acceso físico no autorizado, robo de componentes o manipulación maliciosa.	I	1	25	C
HARDWARE	Servidores Thinkstation e IBM	25	[A24] Denegación de servicio	Falta de medidas de seguridad adecuadas para prevenir o mitigar ataques que puedan causar interrupciones en el servicio.	I	2	50	C

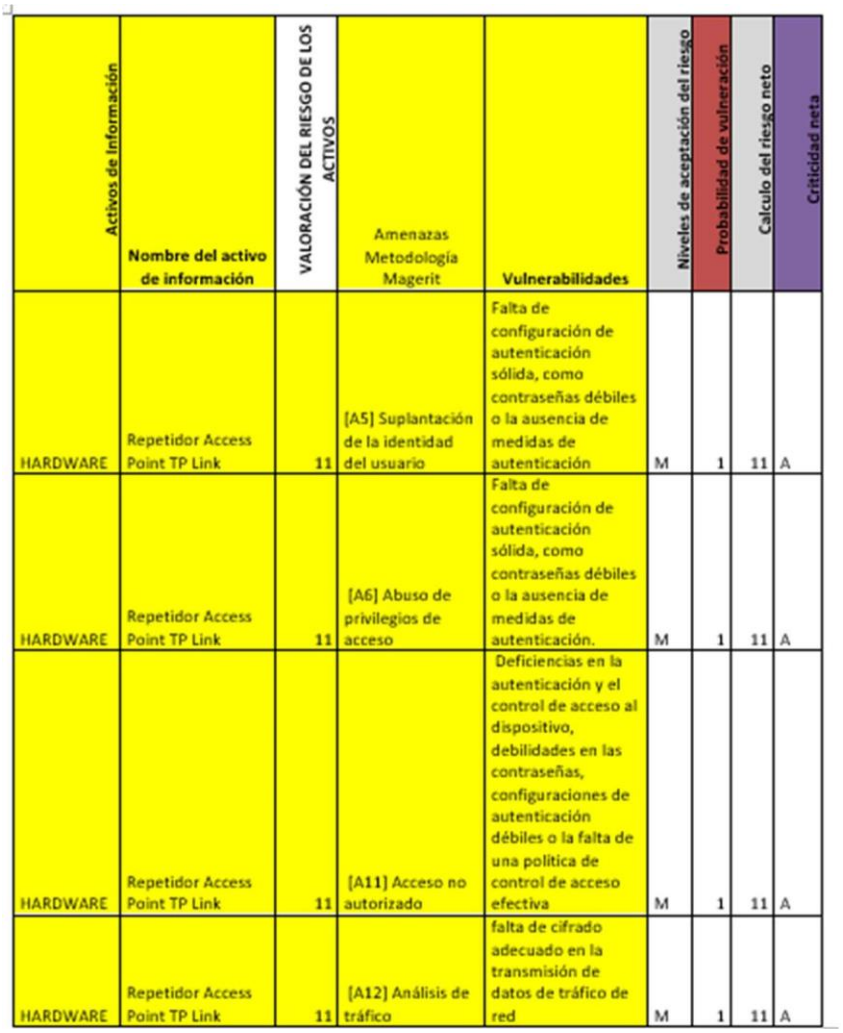
Fuente: El Autor.

Figura 103 Riesgos y Vulnerabilidades Access Point

Activos de Información	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas Metodología Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Probabilidad de vulneración	Calculo del riesgo neto	Criticidad neta
HARDWARE	Repetidor Access Point TP Link	11	[E2] Errores del administrador	Falta de capacitación o conocimiento adecuado por parte del administrador de red que configura o administra el dispositivo.	M	2	22	C
HARDWARE	Repetidor Access Point TP Link	11	[E9] Errores de [re-]encaminamiento	Configuración inadecuada de las rutas de red o la falta de conocimiento del personal encargado de la gestión y configuración del dispositivo	M	2	22	C
HARDWARE	Repetidor Access Point TP Link	11	[E15] Alteración accidental de la información	falta de controles de acceso adecuados o con la manipulación no intencionada de la configuración del dispositivo	M	2	22	C
HARDWARE	Repetidor Access Point TP Link	11	[E19] Fugas de información	falta de controles de seguridad adecuados para proteger la información transmitida a través del dispositivo	M	2	22	C
HARDWARE	Repetidor Access Point TP Link	11	[E25] Pérdida de equipos	falta de medidas de seguridad física para proteger el dispositivo contra robos o pérdida	A	3	33	C

Fuente: El Autor.

Figura 104 Continuación Riesgos y Vulnerabilidades Access Point



Activos de Información	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas Metodología Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Probabilidad de vulneración	Calculo del riesgo neto	Criticidad neta
HARDWARE	Repetidor Access Point TP Link	11	[A5] Suplantación de la identidad del usuario	Falta de configuración de autenticación sólida, como contraseñas débiles o la ausencia de medidas de autenticación	M	1	11	A
HARDWARE	Repetidor Access Point TP Link	11	[A6] Abuso de privilegios de acceso	Falta de configuración de autenticación sólida, como contraseñas débiles o la ausencia de medidas de autenticación.	M	1	11	A
HARDWARE	Repetidor Access Point TP Link	11	[A11] Acceso no autorizado	Deficiencias en la autenticación y el control de acceso al dispositivo, debilidades en las contraseñas, configuraciones de autenticación débiles o la falta de una política de control de acceso efectiva	M	1	11	A
HARDWARE	Repetidor Access Point TP Link	11	[A12] Análisis de tráfico	falta de cifrado adecuado en la transmisión de datos de tráfico de red	M	1	11	A

Fuente: El Autor.

Figura 105 Riesgos y Vulnerabilidades Equipos + Pantalla y Accesorios

Activos de Información	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas Metodología Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Probabilidad de vulneración	Calculo del riesgo neto	Criticidad neta
HARDWARE	Equipos HP + pantalla y accesorios	15	[I11] Emanaciones electromagnéticas	Falta de medidas de protección contra la emisión de radiaciones electromagnéticas	A	1	15	A
HARDWARE	Equipos HP + pantalla y accesorios	15	[E2] Errores del administrador	Falta de capacitación adecuada del personal administrador en la configuración, gestión y mantenimiento de estos dispositivos.	A	2	30	C
HARDWARE	Equipos HP + pantalla y accesorios	15	[E1] Errores de los usuarios	Falta de Capacitación en temas referentes a seguridad de la información y uso seguro de equipos	M	2	30	C
HARDWARE	Equipos HP + pantalla y accesorios	15	[E25] Pérdida de equipos	Falta de medidas de seguridad física para proteger estos activos	I	3	45	C
HARDWARE	Equipos HP + pantalla y accesorios	15	[I5] Avería de origen físico o lógico	Falta de medidas preventivas o de mantenimiento adecuadas para evitar estas averías, equipos muy viejos	M	3	45	C
HARDWARE	Equipos HP + pantalla y accesorios	15	[A6] Abuso de privilegios de acceso	Falta de control y gestión adecuada de los privilegios de acceso.	M	2	30	C
HARDWARE	Equipos HP + pantalla y accesorios	15	[A11] Acceso no autorizado	Deficiencias en la gestión de la autenticación y la falta de medidas de seguridad adecuadas para prevenir accesos no autorizados	M	1	15	A
HARDWARE	Equipos HP + pantalla y accesorios	15	[A23] Manipulación de los equipos	Falta de medidas de seguridad física y control de acceso para proteger estos activos	M	2	30	C

Fuente: El Autor.

Figura 106 Riesgos y Vulnerabilidades Cuentas de Correo

Activos de información	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas metodología Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Probabilidad de vulneración	Calculo del riesgo neto	Criticidad neta
SERVICIOS	Cuentas de correo	15	[A11] Acceso no autorizado	Falta de medidas adecuadas de autenticación y control de acceso.	M	1	15	A
SERVICIOS	Cuentas de correo	15	[A5] Suplantación de la identidad del usuario	Falta de Capacitación en temas referentes a seguridad de la información.	M	2	30	C
SERVICIOS	Cuentas de correo	15	[A15] Modificación deliberada de la información	Falta de controles de seguridad adecuados para prevenir la modificación no autorizada de los correos electrónicos y garantizar la integridad de los contenidos de los mensajes en las cuentas de correo.	M	1	15	A
SERVICIOS	Cuentas de correo	15	[E20] Vulnerabilidades de los programas (software)	Falta de aplicación de actualizaciones y parches.	M	1	15	A
SERVICIOS	Cuentas de correo	15	[A25] Robo	Debilidades en la autenticación y el control de acceso de las cuentas de correo electrónico, Falta capacitación personal en ingeniería social	I	2	30	C
SERVICIOS	Cuentas de correo	15	[A14] Interceptación de información (escucha)	Falta de cifrado adecuado en las comunicaciones de correo electrónico.	M	1	15	A
SERVICIOS	Cuentas de correo	15	[E19] Fugas de información	Falta de controles adecuados sobre el acceso y la gestión de las cuentas de correo electrónico.	M	1	15	A
SERVICIOS	Cuentas de correo	15	[A26] Ataque destructivo	Falta de implementación de medidas de seguridad robustas, como la autenticación de dos factores, políticas de contraseñas sólidas, detección de malware sistemas de filtrado de correo electrónico .	I	3	45	C

Fuente: El Autor.

Figura 107 Riesgos y Vulnerabilidades Internet Dedicado

Activos de Información	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas metodología Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Probabilidad de vulneración	Calculo del riesgo neto	Criticidad neta
SERVICIOS	Internet canal dedicado Claro	11	[E2] Errores del administrador	Configuraciones incorrectas, puertos o servicios abierto	M	1	11	A
SERVICIOS	Internet canal dedicado Claro	11	[E4] Errores de configuración	Falta de parches o actualizaciones	M	1	11	A
SERVICIOS	Internet canal dedicado Claro	11	[A11] Acceso no autorizado	Falta de autenticación multifactor (MFA)	I	2	22	C
SERVICIOS	Internet canal dedicado Claro	11	[I9] Interrupción de otros servicios y suministros esenciales	Falta de redundancia en la conexión de Internet o la dependencia exclusiva de un único proveedor de servicios	I	2	22	C
SERVICIOS	Internet canal dedicado Claro	11	[A12] Análisis de tráfico	Falta de medidas adecuadas de cifrado y monitoreo del tráfico de datos	M	1	11	A
SERVICIOS	Internet canal dedicado Claro	11	[A19] Divulgación de información	Ausencia de políticas y controles de acceso adecuados para proteger la información transmitida a través de la conexión de Internet dedicada.	I	2	22	C

Fuente: El Autor.

Figura 108 Riesgos y Vulnerabilidades Página web

Activos de Información	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas Metodología Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Probabilidad de vulneración	Calculo del riesgo neto	Criticidad neta
SOFTWARE	Página web (dominio-hosting)	25	[E19] Fugas de información	Configuraciones incorrectas en el servidor web o en la base de datos pueden dejar expuesta información crítica	I	1	25	C
SOFTWARE	Página web (dominio-hosting)	25	[E20] Vulnerabilidades de los programas (software)	Falta de actualización o parcheo de software utilizado en la página web.	I	3	75	C
SOFTWARE	Página web (dominio-hosting)	25	[E21] Errores de mantenimiento / actualización de programas (software)	Falta de actualización o parcheo de software utilizado en la página web.	I	3	75	C
SOFTWARE	Página web (dominio-hosting)	25	[A6] Abuso de privilegios de acceso	Falta de controles adecuados de autenticación y autorización en la página web.	I	1	25	C
SOFTWARE	Página web (dominio-hosting)	25	[A8] Difusión de software dañino	Errores en la validación de entrada de Datos, Vulnerabilidades de software	I	2	50	C
SOFTWARE	Página web (dominio-hosting)	25	[A11] Acceso no autorizado	El sitio web no implementa suficientes medidas para verificar y autorizar a los usuarios que intentan acceder a ciertas áreas o funcionalidades del sitio	I	2	50	C

Fuente: El Autor

Figura 109 Riesgos y Vulnerabilidades Office y Windows

Activos de información	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas metodología Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Probabilidad de vulneración	Calculo del riesgo neto	Criticidad neta
SOFTWARE	Licencias Office 2010 – Windows 10	9	[E1] Errores de los usuarios	falta de capacitación o conciencia de los usuarios sobre los términos y condiciones de las licencias, así como sobre las restricciones y políticas de uso del software	A	2	18	I
SOFTWARE	Licencias Office 2010 – Windows 10	9	[E2] Errores del administrador	No aplicar actualizaciones o parches de seguridad necesarios para mantener el software en conformidad con las licencias y protegerlo contra vulnerabilidades conocidas	M	2	18	I
SOFTWARE	Licencias Office 2010 – Windows 10	9	[E8] Difusión de software dañino	falta de restricciones adecuadas para la instalación de software en los dispositivos que utilizan estas licencias.	M	2	18	I
SOFTWARE	Licencias Office 2010 – Windows 10	9	[E20] Vulnerabilidades de los programas (software)	Falta de actualización o parcheo de software Empleado	A	1	9	B
SOFTWARE	Licencias Office 2010 – Windows 10	9	[E21] Errores de mantenimiento / actualización de programas (software)	Falta de actualización o parcheo de software Empleado	A	1	9	B
SOFTWARE	Licencias Office 2010 – Windows 10	9	[A5] Suplantación de la identidad del usuario	falta de autenticación sólida o medidas de seguridad insuficientes para verificar la identidad de los usuarios que acceden a las licencias	M	2	18	I
SOFTWARE	Licencias Office 2010 – Windows 10	9	[A6] Abuso de privilegios de acceso	falta de políticas de acceso, auditoría insuficiente o la asignación inapropiada de roles y permisos en relación con las licencias.	M	1	9	B

Fuente: El Autor

Figura 110 Continuación Riesgos y Vulnerabilidades Office y Windows

Activos de información	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas metodología Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Probabilidad de vulneración	Calculo del riesgo neto	Criticidad neta
SOFTWARE	Licencias Office 2010 – Windows 10	9	[A11] Acceso no autorizado	falta de autenticación robusta, contraseñas débiles o la falta de controles de acceso adecuados para evitar que usuarios no autorizados utilicen las licencias de manera indebida	M	1	9	B
SOFTWARE	Licencias Office 2010 – Windows 10	9	[A15] Modificación deliberada de la información	Falta de integridad y controles de seguridad que permitan proteger las licencias contra modificaciones no autorizadas.	A	1	9	B
SOFTWARE	Licencias Office 2010 – Windows 10	9	[A19] Divulgación de información	falta de cifrado o el acceso no autorizado a la información de licencia	M	1	9	B
SOFTWARE	Licencias Office 2010 – Windows 10	9	[A22] Manipulación de programas	falta de validación adecuada de las actualizaciones o parches del software	M	1	9	B

Fuente: El Autor

Figura 111 Riesgos y Vulnerabilidades Antivirus

Activos de Información	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas Metodología Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Probabilidad de vulneración	Calculo del riesgo neto	Criticidad neta
SOFTWARE	Antivirus Kaspersky	19	[E1] Errores de los usuarios	falta de capacitación o conciencia de los usuarios sobre los términos y condiciones de las licencias, así como sobre las restricciones y políticas de uso del software	A	2	38	C
SOFTWARE	Antivirus Kaspersky	19	[E2] Errores del administrador	No aplicar actualizaciones o parches de seguridad necesarios para mantener el software en conformidad con las licencias y protegerlo contra vulnerabilidades conocidas	M	2	38	C
SOFTWARE	Antivirus Kaspersky	19	[E8] Difusión de software dañino	Falta de restricciones adecuadas para la instalación de software en los dispositivos que utilizan estas licencias.	M	2	38	C
SOFTWARE	Antivirus Kaspersky	19	[E20] Vulnerabilidades de los programas (software)	Falta de actualización o parcheo de software Empleado	A	3	57	C

Fuente: El Autor

Figura 112 Continuación Riesgos y Vulnerabilidades Antivirus

Activos de información	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas Metodología Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Probabilidad de vulneración	Calculo del riesgo neto	Criticidad neta
SOFTWARE	Antivirus Kaspersky	19	[E21] Errores de mantenimiento / actualización de programas (software)	Falta de actualización o parcheo de software Empleado	A	3	57	C
SOFTWARE	Antivirus Kaspersky	19	[A5] Suplantación de la identidad del usuario	falta de autenticación sólida o medidas de seguridad insuficientes para verificar la identidad de los usuarios que acceden a las licencias	M	2	38	C
SOFTWARE	Antivirus Kaspersky	19	[A6] Abuso de privilegios de acceso	falta de políticas de acceso, auditoria insuficiente o la asignación inapropiada de roles y permisos en relación con las licencias.	M	1	19	I
SOFTWARE	Antivirus Kaspersky	19	[A11] Acceso no autorizado	falta de autenticación robusta, contraseñas débiles o la falta de controles de acceso adecuados para evitar que usuarios no autorizados utilicen las licencias de manera indebida	M	1	19	I
SOFTWARE	Antivirus Kaspersky	19	[A15] Modificación deliberada de la información	Falta de integridad y controles de seguridad que permitan proteger las licencias contra modificaciones no autorizadas.	A	1	19	I
SOFTWARE	Antivirus Kaspersky	19	[A19] Divulgación de información	falta de cifrado o el acceso no autorizado a la información de licencia	M	1	19	I
SOFTWARE	Antivirus Kaspersky	19	[A22] Manipulación de programas	falta de validación adecuada de las actualizaciones o parches del software	M	1	19	I

Fuente: El Autor.

Figura 113 Riesgos y Vulnerabilidades SIIGO

Activos de Información	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas metodología Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Probabilidad de vulneración	Calculo del riesgo neto	Criticidad neta
SOFTWARE	Sistema contable Siigo	20	[E1] Errores de los usuarios	Falta de capacitación o conciencia insuficiente de los usuarios sobre las prácticas de seguridad y el uso adecuado del sistema Siigo	M	2	40	C
SOFTWARE	Sistema contable Siigo	20	[E2] Errores del administrador	Falta de capacitación o errores del administrador en la configuración y administración del sistema Siigo	M	2	40	C
SOFTWARE	Sistema contable Siigo	20	[E8] Difusión de software dañino	Falta de protección contra la difusión de software malicioso o dañino en el sistema Siigo.	M	1	20	I
SOFTWARE	Sistema contable Siigo	20	[E19] Fugas de información	Insuficientes controles de acceso y protección de datos en el sistema Siigo que pueden llevar a fugas de información confidencial.	I	2	40	C
SOFTWARE	Sistema contable Siigo	20	[E20] Vulnerabilidades de los programas (software)	Falta de Actualizaciones y parcheo	M	1	20	I
SOFTWARE	Sistema contable Siigo	20	[E21] Errores de mantenimiento / actualización de programas (software)	Falta de Actualizaciones y parcheo	M	1	20	I
SOFTWARE	Sistema contable Siigo	20	[A5] Suplantación de la identidad del usuario	Falta de autenticación y control de acceso, monitoreo y seguimiento usuarios	I	2	40	C
SOFTWARE	Sistema contable Siigo	20	[A6] Abuso de privilegios de acceso	Deficiencias en la gestión de privilegios de acceso en el sistema Siigo	I	2	40	C

Fuente: El Autor.

Figura 114 Continuación Riesgos y Vulnerabilidades SIIGO

Activos de Información	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas metodología Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Probabilidad de vulneración	Calculo del riesgo neto	Criticidad neta
SOFTWARE	Sistema contable Siigo	20	[A7] Uso no previsto	Insuficiente control y supervisión de las actividades de los usuarios en el sistema Siigo, lo que podría dar lugar a un uso no previsto y potencialmente perjudicial de la plataforma.	I	2	40	C
SOFTWARE	Sistema contable Siigo	20	[A11] Acceso no autorizado	Falta de medidas adecuadas de autenticación y control de acceso en el sistema Siigo	M	1	20	I
SOFTWARE	Sistema contable Siigo	20	[A15] Modificación deliberada de la información	Insuficiente control y supervisión de las actividades de los usuarios en el sistema Siigo, lo que podría dar lugar a un uso no previsto y potencialmente perjudicial de la plataforma.	I	2	40	C
SOFTWARE	Sistema contable Siigo	20	[A19] Divulgación de información	Insuficiente control sobre la divulgación de información confidencial almacenada en el sistema contable Siigo	I	2	40	C
SOFTWARE	Sistema contable Siigo	20	[A22] Manipulación de programas	Insuficiente control sobre la manipulación de programas y sistemas en el sistema contable Siigo	I	2	40	C

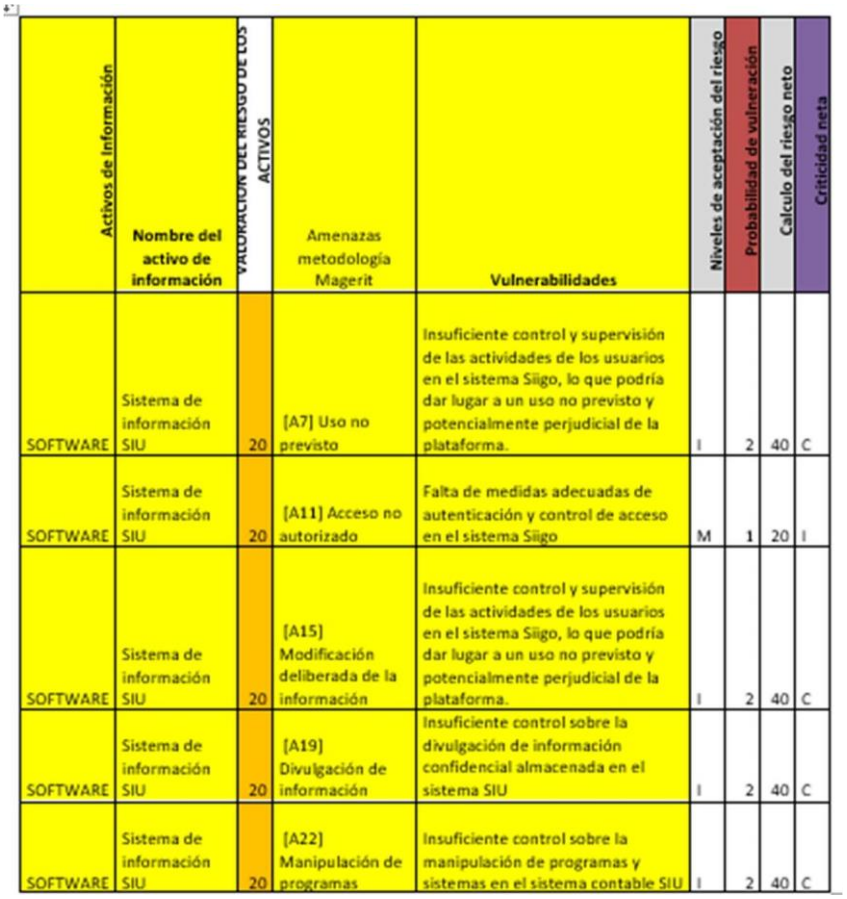
Fuente: El Autor.

Figura 115 Riesgos y Vulnerabilidades SIU

Activos de Información	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas metodología Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Probabilidad de vulneración	Calculo del riesgo neto	Criticidad neta
SOFTWARE	Sistema de información SIU	20	[E1] Errores de los usuarios	Falta de capacitación o conciencia insuficiente de los usuarios sobre las prácticas de seguridad y el uso adecuado del sistema SIU	M	2	40	C
SOFTWARE	Sistema de información SIU	20	[E2] Errores del administrador	Falta de capacitación o errores del administrador en la configuración y administración del sistema SIU	M	2	40	C
SOFTWARE	Sistema de información SIU	20	[E8] Difusión de software dañino	Falta de protección contra la difusión de software malicioso o dañino en el sistema SIU	M	1	20	I
SOFTWARE	Sistema de información SIU	20	[E19] Fugas de información	Insuficientes controles de acceso y protección de datos en el sistema Siigo que pueden llevar a fugas de información confidencial.	I	2	40	C
SOFTWARE	Sistema de información SIU	20	[E20] Vulnerabilidades de los programas (software)	Falta de Actualizaciones y parcheo	M	1	20	I
SOFTWARE	Sistema de información SIU	20	[E21] Errores de mantenimiento / actualización de programas (software)	Falta de Actualizaciones y parcheo	M	1	20	I
SOFTWARE	Sistema de información SIU	20	[A5] Suplantación de la identidad del usuario	Falta de autenticación y control de acceso, monitoreo y seguimiento usuarios	I	2	40	C
SOFTWARE	Sistema de información SIU	20	[A6] Abuso de privilegios de acceso	Deficiencias en la gestión de privilegios de acceso en el sistema SIU	I	2	40	C

Fuente: El Autor

Figura 116 Continuación Riesgos y Vulnerabilidades SIU



Activos de Información	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas metodología Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Probabilidad de vulneración	Calculo del riesgo neto	Criticidad neta
SOFTWARE	Sistema de información SIU	20	[A7] Uso no previsto	Insuficiente control y supervisión de las actividades de los usuarios en el sistema Siigo, lo que podría dar lugar a un uso no previsto y potencialmente perjudicial de la plataforma.	I	2	40	C
SOFTWARE	Sistema de información SIU	20	[A11] Acceso no autorizado	Falta de medidas adecuadas de autenticación y control de acceso en el sistema Siigo	M	1	20	I
SOFTWARE	Sistema de información SIU	20	[A15] Modificación deliberada de la información	Insuficiente control y supervisión de las actividades de los usuarios en el sistema Siigo, lo que podría dar lugar a un uso no previsto y potencialmente perjudicial de la plataforma.	I	2	40	C
SOFTWARE	Sistema de información SIU	20	[A19] Divulgación de información	Insuficiente control sobre la divulgación de información confidencial almacenada en el sistema SIU	I	2	40	C
SOFTWARE	Sistema de información SIU	20	[A22] Manipulación de programas	Insuficiente control sobre la manipulación de programas y sistemas en el sistema contable SIU	I	2	40	C

Fuente: El Autor.

Figura 117 Riesgos y Vulnerabilidades Firewall

Activos de Información	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas metodología Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Probabilidad de vulneración	Calculo del riesgo neto	Criticidad neta
SOFTWARE	Firewall Web	19	[E2] Errores del administrador	Configuración incorrecta de Reglas	I	1	19	I
SOFTWARE	Firewall Web	19	[A6] Abuso de privilegios de acceso	Falta de adecuado control y supervisión de los privilegios de acceso otorgados a los administradores o usuarios autorizados del firewall	I	1	19	I
SOFTWARE	Firewall Web	19	[A7] Uso no previsto	Falta de políticas y procedimientos claros para el uso autorizado y restricciones de uso no autorizado del firewall.	I	1	19	I
SOFTWARE	Firewall Web	19	[A11] Acceso no autorizado	Falta de medidas de seguridad adecuadas que protejan contra el acceso no autorizado a la configuración y los recursos del firewall.	I	2	38	C
SOFTWARE	Firewall Web	19	[A15] Modificación deliberada de la información	Falta de controles de seguridad adecuados que protejan contra la modificación no autorizada de la configuración y los datos almacenados en el firewall	I	1	19	I
SOFTWARE	Firewall Web	19	[A22] Manipulación de programas	No existe registro y monitoreo de cambios	I	2	38	C

Fuente: El Autor.

Figura 118 Riesgos y Vulnerabilidades Directorio Activo

Activos de Información	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS	Amenazas metodología Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Probabilidad de vulneración	Calculo del riesgo neto	Criticidad neta
SERVICIOS	Directorio Activo	19	[E1] Errores de los usuarios	la falta de capacitación o conciencia en seguridad de los usuarios finales, lo que puede llevar a acciones inadvertidas o negligentes	I	2	38	C
SERVICIOS	Directorio Activo	19	[E2] Errores del administrador	falta de un proceso adecuado de gestión de cambios y configuraciones, lo que podría llevar a cambios no autorizados o incorrectos en la configuración del Directorio Activo	I	1	19	I
SERVICIOS	Directorio Activo	19	[E4] Errores de configuración	falta de configuración adecuada o la configuración incorrecta de los objetos y permisos en el Directorio Activo	I	1	19	I
SERVICIOS	Directorio Activo	19	[E15] Alteración accidental de la información	falta de controles adecuados para prevenir cambios no deseados o inadvertidos en la información almacenada en el Directorio Activo	I	1	19	I
SERVICIOS	Directorio Activo	19	[A5] Suplantación de la identidad del usuario	falta de medidas de seguridad adecuadas para autenticar y verificar la identidad de los usuarios que acceden al sistema, altas, bajas y revocatorias	I	2	38	C
SERVICIOS	Directorio Activo	19	[A6] Abuso de privilegios de acceso	falta de controles adecuados para limitar y supervisar el acceso de los usuarios con privilegios a la información almacenada en el directorio.	I	2	38	C

Fuente: El Autor.

Figura 119 Continuación Riesgos y Vulnerabilidades Directorio Activo

Activos de Información	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS	Amenazas metodología Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Probabilidad de vulneración	Calculo del riesgo neto	Criticidad neta
SERVICIOS	Directorio Activo	19	[A11] Acceso no autorizado	falta de controles adecuados que permitan la autenticación y autorización de los usuarios de manera segura y precisa.	I	2	38	C
SERVICIOS	Directorio Activo	19	[A19] Divulgación de información	Falta de controles adecuados para proteger la confidencialidad de los datos almacenados en el Directorio Activo.	I	2	38	C
SERVICIOS	Directorio Activo	19	[A24] Denegación de servicio	Falta de planes de continuidad del negocio	I	2	38	C

Fuente: El Autor.

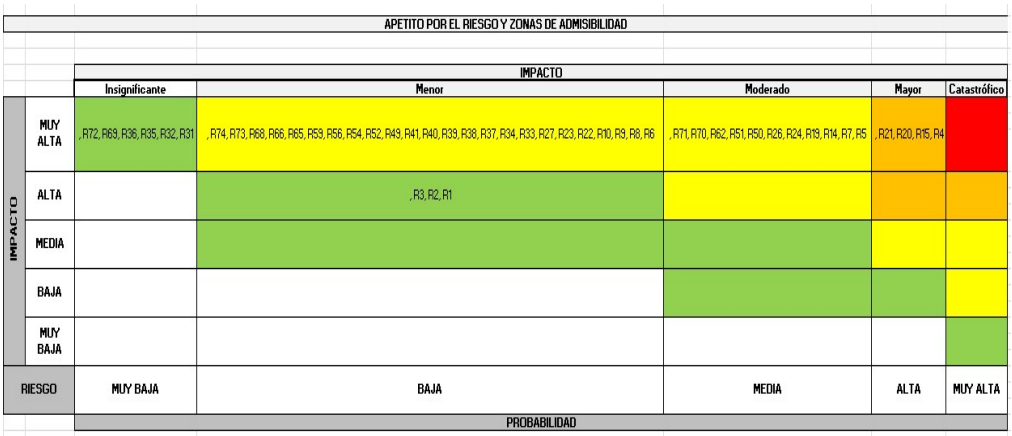
Figura 120 Riesgos y Vulnerabilidades Personal

Activos de Información	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas Metodología Magerit	Vulnerabilidades	Niveles de aceptación del riesgo	Probabilidad de vulneración	Calculo del riesgo neto	Criticidad neta
PERSONAL	Personal	15	[E15] Alteración accidental de la información	Falta de conciencia o capacitación adecuada del personal en cuanto a la importancia de mantener la integridad de la información y evitar alteraciones accidentales.	I	3	45	C
PERSONAL	Personal	15	[E19] Fugas de información	Falta de conciencia o capacitación adecuada del personal en cuanto a la importancia de proteger la información sensible y evitar su divulgación no autorizada	I	3	45	C
PERSONAL	Personal	15	[A15] Modificación deliberada de la información	Falta de controles adecuados para prevenir la modificación no autorizada de los datos por parte del personal	I	3	45	C
PERSONAL	Personal	15	[A29] Extorsión	Falta de capacitación y concientización	I	2	30	C
PERSONAL	Personal	15	[A30] Ingeniería social (picaresca)	Falta de capacitación y concientización	I	4	60	C

Fuente: El Autor

A continuación, se muestra el resumen riesgo Vs impacto en la figura 91.

Figura 121 Impacto



APETITO POR EL RIESGO Y ZONAS DE ADMISIBILIDAD						
		IMPACTO				
		Insignificante	Menor	Moderado	Mayor	Catastrófico
IMPACTO	MUY ALTA	, R72, R69, R36, R35, R32, R31	, R74, R73, R68, R66, R65, R53, R56, R54, R52, R49, R41, R40, R39, R38, R37, R34, R33, R27, R23, R22, R10, R9, R8, R6	, R71, R70, R62, R51, R50, R26, R24, R19, R14, R7, R5	, R21, R20, R15, R4	
	ALTA		, R3, R2, R1			
	MEDIA					
	BAJA					
	MUY BAJA					
RIESGO		MUY BAJA	BAJA	MEDIA	ALTA	MUY ALTA
		PROBABILIDAD				

Fuente: El Autor.

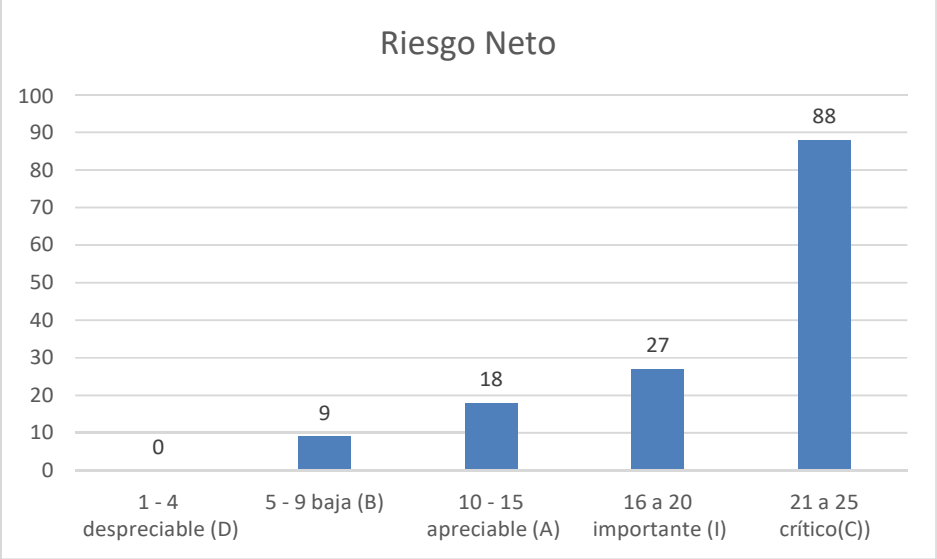
Se identificaron 139 riesgos potenciales que de ser materializados afectan la continuidad del negocio del Partido de la U, encontramos que 14 de ellos son Aceptables en cuanto a Niveles de aceptación del riesgo, 67 son moderados y 58 son críticos y se debe prestar especial atención en el momento de formular políticas y establecer controles para su mitigación.

Figura 122 Niveles de Aceptación

Fuente: El Autor.

En cuanto a Criticidad Neta tenemos: Baja 9, Apreciable 18, Importante 27, Crítico 88

Figura 123 Riesgo Neto



Fuente: El Autor.

Recomendaciones:

Políticas de Gestión de Riesgos: El Partido de la U debe formular políticas claras de gestión de riesgos que establezcan los procedimientos para Reconocer, analizar, gestionar y vigilar de forma constante los posibles peligros.

Controles de Mitigación: Es fundamental establecer medidas prácticas para reducir los riesgos clave identificados, lo que puede implicar fortalecer las defensas cibernéticas, reforzar la seguridad física y ofrecer entrenamiento en seguridad a los empleados.

Priorización de Riesgos: Dado que se han identificado numerosos riesgos, es importante priorizar la asignación de recursos y esfuerzos para abordar primero los riesgos críticos que tienen un impacto significativo en la continuidad del negocio.

Monitoreo Continuo: La administración de riesgos es un esfuerzo en constante evolución. Se requiere una supervisión continua para evaluar qué tan bien funcionan las medidas de seguridad establecidas y para identificar cualquier nuevo riesgo que pueda surgir en el camino.

Resiliencia Organizacional: La organización debe desarrollar una cultura de resiliencia, que incluya planes de contingencia y de respuesta a incidentes, para asegurarse de que esté preparada para hacer frente a situaciones de riesgo materializado.

Auditorías y Revisiones: Llevar a cabo evaluaciones regulares y análisis detallados de los controles y políticas para garantizar que sigan siendo efectivos y estén alineados con las cambiantes condiciones y amenazas.

Se puede concluir para cerrar este capítulo se han identificado un total de 139 riesgos potenciales que podrían afectar la continuidad del negocio del Partido de la U. Esta cantidad indica que existen múltiples áreas de riesgo que deben ser gestionadas.

Niveles de Aceptación del Riesgo: Se ha determinado que 16 de los riesgos son aceptables, 68 son moderados y 55 son críticos. Esta clasificación proporciona una visión clara de cuáles son los riesgos que requieren una atención inmediata y cuáles pueden manejarse con prioridad inferior.

Criticidad Neta: La distribución de los riesgos en función de la criticidad neta muestra que la mayoría de los riesgos se clasifican como "Críticos" (70), lo que indica que son de alta importancia para la organización y deben tratarse con seriedad.

9. DEFINICIÓN DE POLÍTICAS Y CONTROLES DE SEGURIDAD

En la era digital actual, las organizaciones enfrentan una creciente complejidad y sofisticación en las amenazas cibernéticas. Los partidos políticos, como el Partido de la U, no están exentos de estos riesgos. La seguridad se ha transformado en un pilar fundamental para cualquier entidad, especialmente para aquellas que manejan datos sensibles y confidenciales de sus miembros y ciudadanos en general. En este contexto, Aplicar medidas de seguridad de acuerdo con las directrices establecidas en la normativa ISO 27001 se presenta como una estrategia esencial para mitigar riesgos, proteger los datos y mantenerlos íntegros y confidenciales, así como para garantizar la continuidad y reputación del partido.

La norma ISO 27001 instaura un marco robusto Para crear, poner en práctica, conservar y perfeccionar constantemente un sistema que administra la seguridad de la información. Al adoptar esta norma, el Partido de la U estaría tomando medidas proactivas y efectivas para asegurar los datos y tecnologías contra amenazas internas y externas. Esta justificación se apoya en varios puntos clave:

- Protección de Datos Sensibles: Los partidos políticos manejan información sensible sobre sus miembros, donantes y ciudadanos. Implementar controles ISO 27001 asegura que esta información esté protegida contra accesos no autorizados, asegurando la privacidad y confidencialidad de los datos.

- Cumplimiento Legal y Normativo: Cumplir con la norma ISO 27001 demuestra el compromiso del partido con las normativas y reglas vinculadas a la salvaguardia de información. Además, ayuda a cumplir con requisitos legales como la legislación que garantiza la seguridad de la información personal. Personales en Colombia, garantizando así el cumplimiento normativo.

- Mitigación de Riesgos: La detección y análisis de posibles peligros son componentes fundamentales dentro de los estándares establecidos por ISO 27001. Al conocer y comprender los riesgos, el partido puede implementar medidas específicas para mitigarlos, reduciendo así la probabilidad de incidentes de seguridad.

- Confianza y Reputación: La adopción de estándares reconocidos internacionalmente como ISO 27001 evidencia la dedicación y responsabilidad del Partido de la U con la seguridad. Esto construye confianza tanto entre los miembros del partido como en la ciudadanía en general, fortaleciendo la reputación de la organización.

Para formalizar estos principios, el Partido de la U debería formular una Política de Seguridad sólida. Esta política que contemple, entre otros aspectos:

La dedicación y liderazgo de los altos ejecutivos: Una declaración clara del compromiso de la alta dirección del partido con la seguridad y el cumplimiento de la norma.

Alcance y Responsabilidades: Definir el alcance del sistema y las responsabilidades de las partes interesadas en la Aplicación y sostenimiento del sistema.

Gestión de Riesgos: Establecer procesos para detectar, examinar y administrar los riesgos de seguridad de forma regular y sistemática.

Formación y Concienciación: Garantizar que todos los miembros del partido estén capacitados y conscientes de las políticas y procedimientos de seguridad.

Evaluación y Mejora Continua: Establecer procesos para la revisión periódica del SGSI, identificar áreas de mejora y asegurar la continuidad de la mejora continua.

En resumen, aplicar medidas siguiendo las pautas de ISO 27001 y desarrollar una política de seguridad son pasos cruciales para el Partido de la U. No solo protegerán los datos valiosos del partido, sino que también fortalecerán la confianza de los miembros y ciudadanos, asegurando la integridad y reputación del partido en el panorama político y social.

9.1 APLICACIÓN CONTROLES RIESGOS MÁS RELEVANTES

Se realiza una aplicación de controles a los riesgos más relevantes basados en IOS27001, a fin de contrarrestar los mismos, se tomará cada activo y según amenaza detectada se identificará control y se determinará como se aplica.

Figura 124 Controles Switches

Activo	Amenaza	Vulnerabilidad	Control ISO	Cómo se aplica
Switch Hp	[I6] Corte del suministro eléctrico	Interrupción del Servicio	A17.1.2 Implementación de la continuidad de la seguridad de la información --Control: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la	Desarrollar un plan de continuidad del negocio que incluya medidas específicas para mantener la seguridad de la información durante un corte de energía eléctrica.
Switch Hp, Tplink, Aruba	[I5] Avería de origen físico o lógico	Falla de Hardware no detectada	A11.2.4 Mantenimiento de los equipos. -- Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e	Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad
Switch Hp, Tplink, Aruba	[E24] Caída del sistema por agotamiento de recursos	Falta de Monitoreos y Alertas	A11.2.4 Mantenimiento de los equipos. -- Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e	Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad
Switch Hp, Tplink, Aruba	[A24] Denegación de servicio	Insuficiente protección del Switch sin IDS	A13.1.1 Controles de redes	Implementar un IDS e IPS para control y
Switch Hp, Tplink, Aruba	[A26] Ataque Destructivo	Insuficiente protección del Switch sin IDS	A13.1.1 Controles de redes	Implementar un IDS e IPS para control y

Fuente: El Autor.

Figura 125 Controles Discos Duros y Storage

Activo	Amenaza	Vulnerabilidad	Control ISO	Cómo se aplica
Disco Duros Externos y Storage	[E18] Destrucción de la información	Falta de copias de seguridad regulares y adecuadas de los datos almacenados en el disco duro externo	A12.3.1 Respaldo de la información	Control: Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.

Fuente: El Autor.

Figura 126 Controles Servidores

Activo	Amenaza	Vulnerabilidad	Control ISO	Cómo se aplica
Servidor Thinkstation e IBM	[E2] Errores del Administrador	Falta de capacitación o formación adecuada del personal administrador	A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información.	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.
Servidor Thinkstation e IBM	[E25] Pérdida de Equipos	Falta de medidas de seguridad física para proteger el dispositivo contra robos o pérdida	A11.1.2 Controles de Acceso Físico	Control: Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.
Servidor Thinkstation e IBM	[A7] Uso No Previsto	Falta de restricciones de acceso, la ausencia de un seguimiento de las actividades realizadas en el servidor o la falta de capacitación para los usuarios	A9.2.3 Gestión de derechos de acceso privilegiado	Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado

Fuente: Elaboración Propia.

Figura 127 Controles Servidores 2

Activo	Amenaza	Vulnerabilidad	Control ISO	Cómo se aplica
Servidor Thinkstation e IBM	[A11] Acceso no Autorizado	Falta de controles adecuados para la autenticación y el control de acceso, contraseñas débiles o compartidas, configuraciones incorrectas de seguridad	A9.1.1 Política de control de acceso -- Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.	Control: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
Servidor Thinkstation e IBM	[A23] Manipulación de los equipos	Falta de controles adecuados para prevenir la manipulación no autorizada de los equipos de hardware, como acceso físico no autorizado, robo de componentes o manipulación maliciosa.	A11.1.3 Seguridad de oficinas, recintos e instalaciones.	Control: Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones..
Servidor Thinkstation e IBM	[A24] Denegación de Servicio	Falta de medidas de seguridad adecuadas para prevenir o mitigar ataques que puedan causar interrupciones en el servicio.	A13.1.1 Controles de redes	Implementar un IDS e IPS para control y monitoreo

Fuente: El Autor.

Figura 128 Controles Equipos

Activo	Amenaza	Vulnerabilidad	Control ISO	Cómo se aplica
Equipos Hp + Pantalla	[E25] Pérdida de equipos	Falta de medidas de seguridad física para proteger estos activos	A11.1.3 Seguridad de oficinas, recintos e instalaciones.	Control: Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.

Fuente: El Autor.

Figura 129 Controles Cuentas Correo

Activo	Amenaza	Vulnerabilidad	Control ISO	Cómo se aplica
Cuentas Correo	[A25] Robo	Debilidades en la autenticación y el control de acceso de las cuentas de correo electrónico, Falta capacitación personal en ingeniería social	A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información.	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia
Cuentas Correo	[A26] Ataque destructivo	Falta de implementación de medidas de seguridad robustas, como la autenticación de dos factores, políticas de contraseñas sólidas, detección de malware en archivos adjuntos de correo electrónico y sistemas de filtrado de correo electrónico inadecuados.	A.12.2.1 Controles contra codigo malicioso	Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.

Fuente: El Autor.

Figura 130 Controles Canal dedicado Claro

Activo	Amenaza	Vulnerabilidad	Control ISO	Cómo se aplica
Internet canal dedicado Claro	[A11] Acceso no autorizado	Falta de autenticación multifactor (MFA)	A12.4.1 Registro de eventos	Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
Internet canal dedicado Claro	[I9] Interrupción de otros servicios y suministros esenciales	Falta de redundancia en la conexión de Internet o la dependencia exclusiva de un único proveedor de servicios	A.17.1.1 Planificación de la continuidad de la seguridad de la información	Control: La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
Internet canal dedicado Claro	[A19] Divulgación de la información	Ausencia de políticas y controles de acceso adecuados para proteger la información transmitida a través de la conexión de Internet dedicada.	A13.1.1 Controles de Redes	Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.

Fuente: El Autor.

Figura 131 Controles Página Web

Activo	Amenaza	Vulnerabilidad	Control ISO	Cómo se aplica
Página Web	[E19] Fugas de información	Configuraciones incorrectas en el servidor web o en la base de datos pueden dejar expuesta información crítica	A.14.2.1 - Política de Desarrollo seguro	Control: Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.
Página Web	[E20] Vulnerabilidades de los programas (software)	Falta de actualización o parcheo de software utilizado en la página web.	A.12.6.1 Gestión de Vulnerabilidades técnicas	Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las
Página Web	[E21] Errores de mantenimiento / actualización de programas (software)	Falta de actualización o parcheo de software utilizado en la página web.	A.12.6.1 Gestión de Vulnerabilidades técnicas	Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las

Fuente: Elaboración Propia.

Figura 132 Continuación Controles Página Web

Activo	Amenaza	Vulnerabilidad	Control ISO	Cómo se aplica
Página Web	[A6] Abuso de Privilegios de Acceso	Falta de controles adecuados de autenticación y autorización en la página web.	A9.1.1 Políticas de Control de Acceso	Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.
Página Web	[A8] Difusión de software dañino	Errores en la validación de entrada de Datos, Vulnerabilidades de software	A.12.2.1 Controles contra codigo malicioso	Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los
Página Web	[A11] Acceso No Autorizado	Errores en la validación de entrada de Datos, Vulnerabilidades de software	A.12.6.1 Gestión de Vulnerabilidades técnicas	Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las

Fuente: El Autor.

Figura 133 Controles Siigo

Activo	Amenaza	Vulnerabilidad	Control ISO	Cómo se aplica
Sistema Contable Siigo	[E19] Fugas de Información	Insuficientes controles de acceso y protección de datos en el sistema Siigo que pueden llevar a fugas de información confidencial.	A9.1.1 Política de control de acceso --Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.	Control: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
Sistema Contable Siigo	[A5] Suplantación de la identidad del usuario	Falta de autenticación y control de acceso, monitoreo y segumiento usuarios	A9.1.1 Política de control de acceso --Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.	Control: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
Sistema Contable Siigo	[A6] Abuso de privilegios de acceso	Deficiencias en la gestión de privilegios de acceso en el sistema Siigo	A9.1.1 Política de control de acceso --Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.	Control: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.

Fuente: El Autor.

Figura 134 Continuación Controles Siigo

Activo	Amenaza	Vulnerabilidad	Control ISO	Cómo se aplica
Sistema Contable Siigo	[A7] Uso no previsto	Insuficiente control y supervisión de las actividades de los usuarios en el sistema Siigo, lo que podría dar lugar a un uso no previsto y potencialmente perjudicial de la plataforma.	A14.4.1 Registro de eventos	Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
Sistema Contable Siigo	[A19] Divulgación de información	Insuficiente control sobre la divulgación de información confidencial almacenada en el sistema contable Siigo	A8.2.1 Clasificación de la información	Control: La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
Sistema Contable Siigo	[A22] Manipulación de Programas	Insuficiente control sobre la manipulación de programas y sistemas en el sistema contable Siigo	A14.4.1 Registro de eventos	Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.

Fuente: El Autor.

Figura 135 Controles SIU

Activo	Amenaza	Vulnerabilidad	Control ISO	Cómo se aplica
Sistema de información SIU	[E19] Fugas de información	Insuficientes controles de acceso y protección de datos en el sistema Siigo que pueden llevar a fugas de información confidencial.	A9.1.1 Política de control de acceso --Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.	Control: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
Sistema de información SIU	[A5] Suplantación de la identidad del usuario	Deficiencias en la gestión de privilegios de acceso en el sistema SIU	A9.1.1 Política de control de acceso --Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad	Control: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
Sistema de información SIU	[A5] Suplantación de la identidad del usuario	Falta de autenticación y control de acceso, monitoreo y segumiento usuarios	A9.1.1 Política de control de acceso --Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad	Control: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.

Fuente: El Autor.

Figura 136 Continuación Controles SIU

Activo	Amenaza	Vulnerabilidad	Control ISO	Cómo se aplica
Sistema de información SIU	[A22] Manipulación de Programas	Insuficiente control sobre la manipulación de programas y sistemas en el sistema contable Siigo	A14.4.1 Registro de eventos	Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.

Fuente: El Autor.

Figura 137 Continuación Controles SIU

Activo	Amenaza	Vulnerabilidad	Control ISO	Cómo se aplica
Sistema de información SIU	[A6] Abuso de privilegios de acceso	Deficiencias en la gestión de privilegios de acceso en el sistema SIU	A9.1.1 Política de control de acceso --Control: Se debe establecer, documentar y revisar una	Control: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
Sistema de información SIU	[A7] Uso no previsto	Insuficiente control y supervisión de las actividades de los usuarios en el sistema Siigo, lo que podría dar lugar	A14.4.1 Registro de eventos	Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la
Sistema de información SIU	[A15] Modificación Deliberada de información	Insuficiente control y supervisión de las actividades de los usuarios en el sistema Siigo, lo que podría dar lugar	A14.4.1 Registro de eventos	Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la
Sistema de información SIU	[A19] Divulgación de información	Insuficiente control sobre la divulgación de información confidencial almacenada en el sistema SIU	A8.2.1 Clasificación de la información	Control: La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.

Fuente: El Autor.

Figura 138 Controles Firewall Web

Activo	Amenaza	Vulnerabilidad	Control ISO	Cómo se aplica
Firewall Web	[E2] Errores del administrador	Configuración incorrecta de Reglas	A12.4.3 Registros del adminsitrador y del operador	Control: Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con
Firewall Web	[A6] Abuso de privilegios de acceso	Deficiencias en la gestión de privilegios de acceso en el sistema SIU	A9.1.1 Política de control de acceso --Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la	Control: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
Firewall Web	[A7] Uso no previsto	Falta de políticas y procedimientos claros para el uso autorizado y restricciones de uso no autorizado del	A14.4.1 Registro de eventos	Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de

Fuente: El Autor.

Figura 139 Continuación Controles Firewall Web

Activo	Amenaza	Vulnerabilidad	Control ISO	Cómo se aplica
Firewall Web	[A11] Acceso no autorizado	Falta de medidas de seguridad adecuadas que protejan contra el acceso no autorizado a la configuración y los recursos del firewall.	A9.1.1 Política de control de acceso -- Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.	Control: Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
Firewall Web	[A15] Modificación deliberada de la información	Falta de controles de seguridad adecuados que protejan contra la modificación no autorizada de la configuración y los datos almacenados en	A14.4.1 Registro de eventos	Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
Firewall Web	[A22] Manipulación de programas	No existe registro y monitoreo de cambios	A14.4.1 Registro de eventos	Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.

Fuente: El Autor.

Figura 140 Controles Directorio Activo

Activo	Amenaza	Vulnerabilidad	Control ISO	Cómo se aplica
Directorio Activo	[E1] Errores de los usuarios	Falta de capacitación o conciencia en seguridad de los usuarios finales, lo que puede llevar a acciones inadvertidas o negligentes	A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información.	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.
Directorio Activo	[E2] Errores del administrador	Falta de un proceso adecuado de gestión de cambios y configuraciones, lo que podría llevar a cambios no autorizados o incorrectos en la configuración del	A12.4.3 Registros del adminsitrador y del operador	Control: Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.
Directorio Activo	[E4] Errores de configuración	Falta de configuración adecuada o la configuración incorrecta de los objetos y permisos en el Directorio Activo	A14.4.1 Registro de eventos	Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.

Fuente: El Autor.

Figura 141 Controles Directorio Activo

Activo	Amenaza	Vulnerabilidad	Control ISO	Cómo se aplica
Directorio Activo	[E15] Alteración accidental de la información	Falta de controles adecuados para prevenir cambios no deseados o inadvertidos en la información almacenada en el Directorio Activo	A14.4.1 Registro de eventos	Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
Directorio Activo	[A5] Suplantación de la identidad del usuario	Falta de medidas de seguridad adecuadas para autenticar y verificar la identidad de los usuarios que acceden al sistema, altas,	A9.2.2 Suministro Acceso Usuarioa	Control: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.
Directorio Activo	[A6] Abuso de privilegios de acceso	Falta de controles adecuados para limitar y supervisar el acceso de los usuarios con privilegios a la información almacenada en el	A9.1.1 Política de control de acceso -- Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.	Control: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.

Fuente: El Autor.

Figura 142 Continuación Controles Directorio Activo

Activo	Amenaza	Vulnerabilidad	Control ISO	Cómo se aplica
Directorio Activo	[A11] Acceso No Autorizado	Falta de controles adecuados que permitan la autenticación y autorización de los usuarios de manera segura y	A9.1.2 Acceso a redes y a servicios en red	Control: Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
Directorio Activo	[A19] Divulgación de información	Falta de controles adecuados para proteger la confidencialidad de los datos almacenados en el Directorio	A8.2.1 Clasificación de la información	Control: La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
Directorio Activo	[A25] Denegación del servicio	Falta de planes de continuidad del negocio	A17.1.2 Implementación de la continuidad de la seguridad de la información	Control: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación

Fuente: Elaboración Propia

Figura 143 Controles Personal

Activo	Amenaza	Vulnerabilidad	Control ISO	Cómo se aplica
Personal	[E15] Alteración accidental de la información	Falta de conciencia o capacitación adecuada del personal en cuanto a la importancia de mantener la integridad de la información y evitar alteraciones accidentales.	A7.2.2 Toma de conciencia, educación y formación en la seguridad de la información.	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.
Personal	[E19] Fugas de información	Falta de conciencia o capacitación adecuada del personal en cuanto a la importancia de proteger la información sensible y evitar su divulgación no autorizada	A7.2.2 Toma de conciencia, educación y formación en la seguridad de la información.	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.

Fuente: El Autor.

Figura 144 Controles Personal

Activo	Amenaza	Vulnerabilidad	Control ISO	Cómo se aplica
Personal	[A15] Modificación deliberada de la información	Falta de controles adecuados para prevenir la modificación no autorizada de los datos por	A9.2.2 Suministro de acceso de usuarios	Control: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.
Personal	[A29] Extorsión	Falta de capacitación y concientización	A7.2.2 Toma de conciencia, educación y formación en la seguridad de la información.	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.
Personal	[A30] Ingeniería social (picaresca)	Falta de capacitación y concientización	A7.2.2 Toma de conciencia, educación y formación en la seguridad de la información.	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.

Fuente: El Autor.

9.2 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARTIDO DE LA U

Introducción: Esta política define las reglas y acciones que el Partido de la U seguirá para proteger su información. Su propósito es garantizar la seguridad de los datos y prevenir pérdidas, robos, cambios no autorizados o uso indebido de la información.

Alcance: Este documento está destinado a personas afiliadas, empleados, contratistas, proveedores de servicios y cualquier otra parte que utilice o acceda a la información y la infraestructura tecnológica del Partido de La Unión por la Gente.

Objetivo: Garantizar que los datos del Partido de la u se conserven confidenciales, íntegros, mediante la implementación de medidas de seguridad robustas. Asegurar que la información sensible esté protegida contra accesos no autorizados, manipulación indebida y pérdida accidental, para salvaguardar la reputación y la confianza del partido y sus miembros.

Responsables: En el marco de esta política, se establecen claramente los responsables de su implementación y cumplimiento. Las siguientes personas y roles son designados como responsables de garantizar la seguridad de la información en el Partido de La U:

El Partido establece las siguientes responsabilidades:

- Empleados: cumplimiento de las políticas implementadas.

- La gerencia es responsable de: Aprobar la Política de Seguridad y garantizar su cumplimiento.

- El área TI es la responsable de capacitar y sensibilizar al personal en todo lo referente políticas de seguridad, es importante capacitar al personal en las políticas para asegurar que todos comprendan la importancia de aplicarlas de manera adecuada. también se debe capacitar al personal en la recuperación de datos y sistemas críticos en caso de una interrupción o pérdida de datos.

- Responsable de seguridad: es responsable de dirigir y organizar la ejecución y cumplimiento de las políticas de seguridad de la información. Su tarea es establecer los protocolos necesarios para asegurar la seguridad

del partido. Además, debe revisar regularmente estas políticas para garantizar que sigan siendo apropiadas y eficaces.

- Responsable gestión de activos de TI: este rol es el encargado de gestionar y proteger los activos de ti de la organización. el responsable de la gestión de activos de ti debe asegurarse de que se sigan las políticas de seguridad al adquirir, desplegar y retirar activos de ti. también es responsable de mantener un registro actualizado de los activos de ti y de asegurarse de que estén protegidos adecuadamente.

- Responsable de recursos humanos: este rol es el encargado de garantizar que los funcionarios del partido estén al tanto de las políticas de seguridad y de que se les proporcione la formación necesaria para cumplirlas. también es responsable de tramitar acceso del personal a los sistemas y datos de la organización, así como de garantizar que los funcionarios acaten las políticas de seguridad instituidas.

- Responsable de cumplimiento normativo: el área jurídica es la encargada de garantizar que la organización siga las leyes y normas de seguridad pertinentes, debe asegurarse de que las políticas cumplan con los normativas legales y requisitos gubernamentales, y de que se lleven a cabo auditorías y revisiones periódicas para evaluar el cumplimiento.

- Responsables de Departamentos y Unidades: Los jefes de los diferentes departamentos y unidades dentro del Partido de La U son responsables de garantizar que sus equipos comprendan y cumplan con las políticas de seguridad de la información. Esto incluye la capacitación regular de los empleados, la implementación de controles de seguridad específicos y la supervisión de las actividades diarias para asegurar el cumplimiento de estas políticas.

- Comité de Seguridad de la Información: Se establecerá un Comité de Seguridad de la Información que estará compuesto por representantes de diferentes áreas del partido. Este comité será responsable de revisar regularmente las políticas de seguridad, identificar posibles riesgos y proponer medidas correctivas para mejorar la seguridad de la información.

9.1.1 Directrices

La Organización se compromete a implementar las siguientes directrices son importante para asegurar la protección adecuada de la información manejada por la empresa:

Confidencialidad:

El Partido de la U garantiza la confidencialidad de la información que maneja, protegiéndola de accesos no autorizados y evitando su divulgación.

- Se establecen políticas y procedimientos para acceder a la información y se establecen medidas de control de acceso para asegurar que sólo personal autorizado pueda acceder a la información.

- Los empleados y colaboradores de Partido de la U, deberán firmar un acuerdo de confidencialidad antes de acceder a la información de la organización y se comprometen a no divulgar información una vez terminada su vinculación.

- Se crearán usuarios únicos con permisos según las funciones del empleado, asignando el mínimo privilegio, una vez finalizado contrato se inactivarán las cuentas. No se admite compartir credenciales por motivos de seguridad.

- Se protegerá la información confidencial mediante el uso de técnicas de encriptación y autenticación, se recomienda uso de VPN.

- Se implementan de medidas de seguridad física y lógica en las instalaciones y sistemas de la organización para controlar el ingreso y egreso.

Integridad

El Partido de la U, garantiza la integridad de la información que maneja, protegiéndola de alteraciones no autorizadas.

- Se establecen directrices y procesos para la administración. y actualización de la información y se establecen medidas de control de cambios para asegurar que sólo personal autorizado pueda modificar la información.

- Se realizarán copias de seguridad frecuentes para evitar pérdidas o corrupciones de la misma, están a cargo del área de sistemas, no se admite guardar localmente información sensible. El equipo de sistemas configurará en los equipos de la compañía carpetas compartidas en servidores a los cuales se les hace backup total mensualmente para que toda la información sea alojada en ellas.

- Las copias de seguridad deben reposar no sólo en las cintas magnéticas guardadas en las instalaciones, se deben salvaguardar también en la nube y mecanismos de almacenamiento externos, garantizando la redundancia y para evitar pérdida total de información en caso de desastre. Son responsabilidad del área técnica.

- Se verificará la integridad de los datos mediante técnicas de validación y verificación para garantizar que los datos no han sido modificados sin permiso. Se hará mediante el uso de algoritmos de hash son técnicas matemáticas que generan un valor único (hash) para cada conjunto de datos. Si los datos cambian, el hash también cambiará, lo que permite detectar cambios no autorizados., se emplearán también firmas digitales.

- Se implementarán actualizaciones y parches regulares en los sistemas del partido. Estas medidas son esenciales para prevenir vulnerabilidades que den pie a modificaciones no autorizadas en los datos, manteniendo así la integridad de nuestra información

Disponibilidad

El Partido de la U, garantiza que la información manejada esté disponible, asegurando su acceso por parte de los usuarios autorizados.

- Se establecen políticas y procedimientos, medidas esenciales para mantener y gestionar los sistemas y aplicaciones de la organización, asegurando que estén disponibles y funcionando correctamente, el mantenimiento preventivo y correctivo es responsabilidad del área técnica y se deberá realizar una verificación de equipos dos veces al año y se debe generar registro con reportes y hallazgos.

- Se establecen acciones de emergencia o planes alternativos. y recuperación de catástrofes para reducir el efecto de las interrupciones en la disponibilidad de la información.

- Se establecen acuerdos de garantía de servicio para garantizar que estén disponibles tanto los servicios como los sistemas críticos.

9.1.2 Políticas de Control de Acceso

- El acceso a los recursos de la empresa se otorgará según las necesidades específicas de cada usuario y se basará en el principio de "menos privilegios". Todos los accesos a la red de la empresa deben ser monitoreados y auditados regularmente. Cada empleado tendrá su usuario y contraseña que debe ser administrado privadamente.

- El requerimiento de altas y bajas será solicitado por recursos humanos vía correo electrónico al área técnica, indicando fecha de inicio y dado el caso fecha de fin del vínculo, se especificará recursos que empleará y rol que desempeñará en la compañía.

- El acceso a data center está restringido a personal del área técnica previo registro de formato de ingreso, si una persona externa debe ingresar debe tener previa autorización y la visita contar con presencia permanente de personal técnico del Partido.

- Todo personal que ingresa a la compañía sea interno o externo será registrado en su ingreso y egreso, de igual manera serán registrados los equipos externos ingresados verificando seriales al ingresar y salir.

- Se implementarán firewalls en los puntos de entrada a la red corporativa para bloquear tráfico no autorizado.

- Los empleados que accedan a la red de la empresa desde ubicaciones remotas deben utilizar una conexión VPN segura.

- Política de Gestión de Sesiones y Cierre de Sesión: Las sesiones de usuario se cerrarán automáticamente después de 15 minutos de inactividad para evitar accesos no supervisados.

- Los usuarios deben cerrar sesión al final de cada jornada laboral para proteger los datos y aplicaciones.

- Los empleados tendrán acceso solo a las aplicaciones y datos necesarios para sus roles específicos, según lo determinado por políticas de acceso basadas en roles.

- Los administradores de sistemas tendrán acceso a herramientas administrativas especiales, mientras que los empleados regulares tendrán acceso limitado a estas funciones.

- Los proveedores externos solo tendrán acceso a los sistemas y datos necesarios para realizar sus funciones contratadas y este acceso será revocado inmediatamente al finalizar su contrato.

- Los proveedores deben someterse a auditorías regulares de seguridad Asegurar que se sigan las normas de seguridad establecidas por el Partido.

- La información delicada debe ser encriptada cuando se está moviendo de un lugar a otro y cuando está almacenada para prevenir el ingreso no autorizado.

- Se implementará autenticación multifactorial para acceder a bases de datos que contienen información altamente confidencial.

9.1.3 Política de seguridad de dispositivos

- Todos los dispositivos del partido deben tener un software antivirus actualizado y tener activada la función de cortafuegos. Además, es necesario limitar la conexión de dispositivos personales a la red, a menos que estén debidamente autorizados.

- Los equipos deberán tener opción de bloqueo automático cuando se evidencia inactividad.

- Los equipos deben ser usados exclusivamente para cumplir tareas de la compañía.

- Todos los dispositivos y sistemas operativos deben mantenerse actualizados con los últimos parches y actualizaciones de seguridad. Se realizarán revisiones regulares para garantizar la aplicación oportuna de estos parches, es responsabilidad exclusiva del área TI esta tarea.

- El área TI es la única autorizada a realizar cambios en configuraciones, reubicar equipos. Si el empleado presenta algún inconveniente debe contactar su personal de inmediato.

- Solo se permitirá la instalación y ejecución de software autorizado y licenciado en los dispositivos de la empresa. Los empleados no pueden descargar o instalar software sin la aprobación de TI.

- Antes de ser retirados del servicio, los dispositivos serán limpiados de datos de forma segura para prevenir la recuperación de información sensible. Los dispositivos serán desechados de acuerdo con las regulaciones ambientales y de seguridad de datos.

- Los dispositivos deben estar físicamente protegidos contra el robo o acceso no autorizado. Se implementarán precauciones físicas, como cerraduras y dispositivos de alerta, según sea necesario.

- Se realizarán copias de seguridad frecuentes en todos los dispositivos y estas copias se almacenarán de forma segura y fuera del sitio. Las restauraciones de datos serán probadas periódicamente para garantizar su integridad.

- La política de seguridad de dispositivos y equipos será revisada y actualizada periódicamente para asegurar su relevancia y efectividad en respuesta a las amenazas y tecnologías emergentes.

9.1.4 Política de Gestión de Datos

- La información de los clientes y proveedores debe ser protegida mediante el uso de medidas de seguridad apropiadas, como la encriptación. Se deben tomar medidas para garantizar que los datos se almacenen solo en los lugares donde sea necesario y se eliminan de forma segura cuando ya no sean necesarios.

- Se instaura un período de retención de cinco años para los datos de clientes después de concluir el vínculo comercial. Los datos se eliminarán de forma segura al finalizar este período, a menos que se requiera una retención más larga por razones legales.

- Se implementará un sistema de autenticación basado en roles. Solo los empleados con autorización específica tendrán acceso a los datos de clientes y proveedores. El acceso se revisará trimestralmente para garantizar la relevancia de los permisos.

- Se implementarán firmas electrónicas para comprobar la autenticidad y consistencia de los documentos importantes de los clientes. Además, se realizarán comprobaciones regulares de checksum para asegurar que los datos no hayan sido alterados.

- Todas las transferencias de datos de clientes se realizarán a través de conexiones cifradas SSL/TLS.

- Se realizarán auditorías trimestrales de los registros de acceso a los datos de clientes. Cualquier acceso no autorizado se investigará y se tomarán medidas correctivas inmediatas.

- Se establecerá
- Un grupo de especialistas en incidentes formado por empleados de TI, Jurídica y relaciones públicas. Se mantendrá un plan de respuesta actualizado que incluya los pasos específicos a seguir en caso de una violación de datos.

9.1.5 Política de concienciación y formación

- Cada nuevo empleado en el Partido recibirá una orientación detallada sobre las Políticas y Normas de Seguridad relevantes para su área de trabajo y las responsabilidades específicas que implican por parte del área TI y recursos humanos. También se les informará sobre las posibles consecuencias si no cumplen con estas políticas.

- Todos los empleados, incluyendo funcionarios nuevos y antiguos, deberán participar en una capacitación anual obligatoria sobre las últimas amenazas de seguridad informática, técnicas de phishing, manejo seguro de contraseñas y prácticas seguras de navegación en línea, después de la capacitación anual obligatoria, los empleados deberán aprobar una prueba de conocimiento para evaluar su comprensión de las políticas y prácticas de

seguridad informática. Aquellos que no aprueben la prueba deberán recibir capacitación adicional

- El equipo TI llevará a cabo simulacros regulares, simulacros de correos electrónicos falsos para evaluar la habilidad de los empleados en detectar intentos de fraude por correo electrónico. Aquellos que caigan en el simulacro recibirán capacitación adicional y orientación.

- Los empleados serán informados inmediatamente sobre las últimas amenazas de seguridad y tácticas de ataque a través de correos electrónicos informativos, mensajes en el sistema interno y seminarios web de capacitación en vivo.

9.1.6 Política de Copias de seguridad

- El Equipo TI realizará backups regularmente para evitar pérdidas o corrupciones de la misma, están a cargo del área de sistemas, no se admite guardar localmente información sensible. El equipo de sistemas configurará en los equipos de la compañía carpetas compartidas en servidores a los cuales se les hace backup total mensualmente para que toda la información sea alojada en ellas.

- El equipo TI llevará a cabo pruebas periódicas de restauración de datos desde las copias de seguridad para verificar la la autenticidad y la habilidad para recuperación de los datos. Los resultados de estas pruebas serán documentados y revisados regularmente.

- Las copias de seguridad se almacenarán en un lugar seguro y fuera del sitio para proteger los datos contra desastres naturales, incendios u otros eventos que puedan afectar las instalaciones de la empresa. Se utilizarán servicios de almacenamiento en la nube o se almacenarán en un centro de datos externo.

- Todas las copias de seguridad se encriptarán para probar la confidencialidad de los datos almacenados. Se utilizarán algoritmos de encriptación seguros para proteger la información durante la transmisión y el almacenamiento.

- El equipo TI mantendrá un registro detallado de todas las actividades relacionadas con las copias de seguridad, incluyendo fechas, horas, tipos de datos respaldados y resultados de las operaciones de backup. Estos registros se revisarán periódicamente como parte de las auditorías internas.

- Solo el personal autorizado del equipo TI tendrá acceso a las copias de seguridad se establecerán medidas para regular el acceso y prevenir la entrada no permitida a los datos respaldados.

- Las políticas de copias de seguridad se revisarán anualmente para asegurarse de que estén alineadas con las necesidades operativas y los cambios en la infraestructura tecnológica de la empresa. Las actualizaciones se realizarán según sea necesario.

9.1.7 Política de gestión de incidentes de seguridad

- Todos los incidentes de seguridad deben ser informados inmediatamente al área TI, quien tomará las medidas necesarias para mitigar el impacto. Se debe indagar para establecer la causa de los incidentes y se deben tomar acciones con el fin de evitar sucesos parecidos en el mañana.

- Implementar procedimientos claros y específicos para notificar los incidentes de seguridad. Esto incluirá detalles sobre a quién notificar, cómo notificar y qué información incluir en el informe de incidente. Los procedimientos serán comunicados a todos los empleados y partes interesadas relevantes.

- Se establecerá un sistema de clasificación de incidentes para evaluar la gravedad y el impacto de cada incidente. Los incidentes se clasificarán en diferentes niveles (por ejemplo, bajo, medio, alto) para priorizar las respuestas y las medidas de mitigación.

- Después de cada incidente, se llevará a cabo un análisis de causa raíz para identificar las razones subyacentes del incidente. Esto ayudará a entender las vulnerabilidades y debilidades en el sistema de seguridad y a tomar medidas para prevenir incidentes similares en el futuro.

- Plan de contingencia detallado que describe las acciones específicas a seguir en caso de diferentes tipos de incidentes de seguridad. El plan incluye roles y responsabilidades claras para las personas dentro del grupo de reacción a eventos y las medidas técnicas y operativas a implementa.

- Todos los empleados recibirán capacitación periódica en concientización sobre incidentes para que puedan reconocer y reportar posibles incidentes de seguridad. Esta capacitación incluirá ejemplos de incidentes, cómo identificar señales de alerta y cómo notificar los incidentes al equipo de respuesta.

- Después de cada incidente, se realizará una revisión retrospectiva para evaluar la efectividad de la respuesta y las medidas tomadas. Las lecciones aprendidas se utilizarán para mejorar los procesos y la preparación para futuros incidentes.

9.1.8 Políticas de acceso a internet

- El servicio de internet debe ser empleado exclusivamente para cumplir con tareas de la compañía, este servicio cuenta con restricciones configuradas por el área técnica.

- La red cuenta con firewall interno y externo para la protección de la información enviada y recibida.

- No está permita la descarga de videos, películas o música.

- Emplear HTTPS para garantizar conexión segura.

- El equipo TI no asumirá la responsabilidad por problemas de conectividad y comunicación causados por el proveedor del servicio. Sin embargo, se encargará de comunicarse con el proveedor para presentar los reclamos correspondientes en caso de inconvenientes externos.

- Los usuarios del servicio de navegación en Internet, al utilizarlo, aceptan las siguientes condiciones:

- Sus actividades en Internet estarán sujetas a monitoreo, con la prohibición de acceder a sitios no autorizados y la transmisión de archivos reservados o confidenciales no autorizados.

- Está prohibida la descarga de software sin la autorización explícita de la Oficina de TI.

9.1.9 Software

Gestión de Software

- El equipo TI se encargará de establecer las estrategias para reemplazar sistemas y programas informáticos obsoletos.

- TI será responsable de sugerir y adquirir programas informáticos avanzados conforme a las pautas especificadas para la adquisición de equipos y software según las normativas del Partido.

Autorización y Control de Software:

- Para obtener nuevas licencias o actualizaciones de sistemas operativos, software comercial, bases de datos, comunicaciones, así como equipos y repuestos informáticos, se requerirá el asesoramiento y aprobación técnica de TI antes de cualquier adquisición.

- Cualquier usuario o funcionario que desee instalar software propiedad del Partido deberá justificar su necesidad y obtener la autorización de TI, con la aprobación de su supervisor. Deben especificar el dispositivo donde se instalará el software y el período durante el cual será utilizado.

- Se considerará una infracción grave si los usuarios o funcionarios instalan cualquier tipo de programa en sus dispositivos que no haya sido autorizado por TI.

- En caso de reinstalación, el personal de TI deberá eliminar por completo la versión anterior antes de proceder con la instalación de la nueva**.**

Instalación y Supervisión:

- El equipo de Sistemas se encargará de instalar y supervisar el software básico en todos los dispositivos informáticos.

- El área TI ofrecerá asesoramiento y supervisión para la instalación de software informático y de telecomunicaciones.

- Se garantizará que solo se instale software con licencia del Partido y que cumpla con los derechos especificados en la licencia, tanto en equipos informáticos como en dispositivos basados en sistemas informáticos.

Control y Prohibiciones:

- La instalación de programas gratuitos (freeware) o sin costo estará sujeta a la autorización de TI, cumpliendo con la ley de propiedad intelectual.

- Queda prohibida la instalación de software no licenciado, juegos u otros programas no relacionados con las funciones laborales. TI supervisará el cumplimiento y realizará inventarios periódicos de software instalado en los dispositivos del Partido.

Actualización y Protección:

- La autorización para adquirir y actualizar software será responsabilidad de la Secretaría General a través de TI.

- TI gestionará las actualizaciones del software común según las necesidades del Partido y garantizará que todos los equipos tengan software de seguridad básico, como antivirus y firewall.

Auditoría del Software:

- TI llevará a cabo auditorías anuales para asegurar que los programas instalados cuenten con licencias válidas. En caso de versiones de prueba que requieran licencia, los funcionarios deberán justificar la necesidad para adquirir el software.

Desarrollo de Software

- Antes de iniciar Antes de iniciar cualquier proyecto de desarrollo de software, se realizará una evaluación minuciosa de riesgos para detectar posibles debilidades y peligros.

- Se seguirán prácticas de desarrollo seguro, incluyendo la aplicación de medidas de protección, como la validación de entrada, la autenticación adecuada y la autorización restrictiva para prevenir vulnerabilidades comunes.

- Todo código desarrollado será revisado por un equipo de seguridad antes de su implementación para identificar y corregir posibles debilidades y errores de seguridad.

- Se realizarán pruebas de seguridad exhaustivas, incluyendo pruebas de penetración y análisis estáticos y dinámicos del código, para identificar y remediar vulnerabilidades antes del despliegue.

- Las vulnerabilidades identificadas durante el desarrollo o después de la implementación serán gestionadas y corregidas de manera oportuna para evitar posibles explotaciones.

- La seguridad será integrada en todas las etapas del ciclo de vida del desarrollo de software, desde la concepción hasta el mantenimiento, para asegurar la continuidad de las prácticas seguras.

- Todos los aspectos del desarrollo seguro, incluyendo evaluaciones de riesgos, controles implementados y resultados de pruebas de seguridad, serán documentados y registrados para futuras referencias y auditorías.

- El desarrollo de software cumplirá con las normativas pertinentes en el ámbito de seguridad y privacidad de datos para garantizar el cumplimiento legal y evitar posibles sanciones.

- Se manejarán ambientes de prueba aislados para validaciones previas entes de publicar en producción, se manejarán ambientes separados.

9.10.11 Política de Proveedores

- Antes de establecer relaciones comerciales con un proveedor, se realizará una evaluación exhaustiva de seguridad para garantizar que se adhieran a normas de seguridad adecuadas y preservar la privacidad, y que la información compartida permanezca íntegra y disponible.

- Todos los contratos con proveedores incluirán cláusulas específicas sobre seguridad de la información, detallando las responsabilidades del proveedor para resguardar la información compartida y garantizar el cumplimiento de las políticas de seguridad establecidas.

- Se establecerán procedimientos claros para otorgar acceso a los proveedores solo a los datos requeridos para prestar sus servicios. El acceso será revisado y actualizado regularmente.

- Los proveedores serán instruidos y requeridos para manejar los datos sensibles de forma segura, implementando medidas de encriptación y controles de acceso adecuados.

- Se establecerán sistemas de vigilancia para observar las acciones de los proveedores y reconocer cualquier conducta inusual o sospechosa que pudiera amenazar la seguridad de los datos.

- Los proveedores estarán obligados a informar inmediatamente sobre cualquier incidente de seguridad que afecte los datos compartidos. Se establecerán procedimientos claros para manejar y mitigar estos incidentes de manera eficiente

- Se realizarán evaluaciones periódicas de seguridad para asegurar que los proveedores mantengan los estándares de seguridad acordados. Esto puede incluir auditorías de seguridad y evaluaciones de vulnerabilidad.

- Los proveedores serán entrenados en las políticas y prácticas de seguridad de la organización para garantizar que estén al tanto de las expectativas y normativas de seguridad.

- Los proveedores serán responsables de cumplir con todas las leyes y regulaciones de seguridad aplicables. La organización se reserva el derecho de rescindir la relación si se incumplen estas normativas.

- Los proveedores serán requeridos para establecer planes de respaldo y continuidad del negocio para garantizar la disponibilidad de la información incluso en situaciones de emergencia o interrupciones del servicio.

9.1.12 Políticas contratación personal

- Se llevarán a cabo verificaciones por parte del área jurídica de antecedentes educativos, laborales y penales según lo permita la ley para asegurar que los empleados potenciales no representen un riesgo para la seguridad.

- Cada empleado firmará un acuerdo de confidencialidad y protección de datos para garantizar la seguridad de la información sensible del partido.

- Todos los empleados deberán completar una capacitación en seguridad en concordancia a las pautas de ISO 27001. Esto incluirá educación sobre prácticas seguras, manejo de datos confidenciales y protección contra amenazas cibernéticas.

- Cada empleado será responsable de proteger la información a la que tenga acceso. Se fomentará una cultura de seguridad donde los empleados comprendan la función que desempeñan en salvaguardar los recursos de información.

- Los empleados recibirán capacitación periódica para mantenerse actualizados sobre las últimas amenazas de seguridad y las mejores prácticas para mitigar riesgos.

- Se realizarán evaluaciones periódicas de los riesgos asociados con el personal, incluyendo la revisión de accesos y privilegios, para asegurar que los derechos de acceso estén alineados con las responsabilidades laborales y la política de mínimos privilegios.

- Todos los procesos de contratación y retención de personal cumplirán con las leyes y regulaciones locales afines con la privacidad y la seguridad.

- Se establecerán sistemas de monitoreo para inspeccionar las actividades de los empleados y garantizar el cumplimiento de las políticas de seguridad.

- Cualquier evento relacionado con la seguridad que involucre a empleados será investigado minuciosamente, y se tomarán medidas disciplinarias si se encuentra que un empleado ha comprometido la seguridad.

9.1.13 Política cuentas de Correo

- Las cuentas de correo electrónico de la organización se utilizarán únicamente para cuestiones laborales y comunicaciones oficiales. Se prohíbe el uso personal de las cuentas de correo electrónico.

- Todas las solicitudes de creación y eliminación de cuentas de correo electrónico deben ser enviadas por Recursos Humanos al equipo TI a través de correo electrónico. La notificación debe incluir la fecha de inicio o finalización del vínculo laboral, el área correspondiente y los recursos necesarios.

9.1.14 Política de Medios de Almacenamiento Externos:

- Queda estrictamente prohibido el uso de dispositivos de almacenamiento externos (como USB, discos duros externos) en los sistemas de la organización. Esta medida se toma para prevenir la propagación de virus y malware a través de medios extraíbles.

- Si, por alguna razón, se requiere el uso de un dispositivo externo, debe tener previa autorización del área TI y este debe ser escaneado por el software antivirus de la organización antes de ser conectado a cualquier computadora de la red.
- Todos los datos y archivos deben ser almacenados en los servidores y dispositivos de almacenamiento internos designados por la empresa. Se debe evitar guardar información confidencial en dispositivos externos sin la aprobación explícita de las autoridades competentes.

- Los empleados son responsables de asegurarse de que los archivos se almacenen correctamente en los sistemas internos de la empresa. Cualquier pérdida de datos o divulgación de información confidencial debido al uso indebido de dispositivos externos será responsabilidad del empleado involucrado.

9.1.15 Políticas página Web:

- Acceso y Autorización: Solo personal autorizado tiene acceso a las áreas administrativas del sitio web.

- Se deben utilizar contraseñas fuertes y se deben cambiar regularmente.

- Los usuarios deben tener roles y permisos asignados de manera apropiada para prevenir el acceso no permitido a los datos confidenciales.

- Protección de Datos: La información de los usuarios debe ser cifrada durante la transmisión utilizando protocolos seguros como HTTPS.

- Es necesario aplicar acciones de resguardo para asegurar los datos almacenados, incluyendo cifrado en reposo y restricciones de acceso basadas en roles.

Desarrollo y Mantenimiento Seguro

- Todo el código debe seguir las prácticas de seguridad más efectivas incluyendo la validación de entrada, prevención de inyecciones SQL y protección contra Cross-Site Scripting y Cross-Site Request Forgery.

- Se debe mantener el software del sitio web actualizado, incluyendo el sistema de gestión de contenido (CMS), los plugins y las bibliotecas utilizadas.

- Se deben implementar sistemas de monitoreo para supervisar la actividad del sitio web y detectar cualquier actividad inusual o intentos de acceso no autorizado.

- Los registros de acceso deben ser revisados regularmente para identificar posibles amenazas de seguridad.

Respuesta a Incidentes

- Se debe establecer un proceso de respuesta a incidentes para manejar rápidamente cualquier violación de seguridad o incidente de seguridad.

- Los usuarios y las partes interesadas deben ser notificados en caso de que se descubra una violación de datos que afecte su privacidad

9.2 REVISIÓN SEGUIMIENTO

Cada año, se examinarán las políticas para decidir si es necesario hacer modificaciones.

En este capítulo se han establecido políticas sólidas y controles robustos basados en la norma ISO 27001. Esta iniciativa representa un hito significativo en el compromiso personal y colectivo con la protección de la información vital.

Las políticas de seguridad de la información se han diseñado con precisión para guiar acciones y decisiones futuras. Brindan una estructura sólida sobre la cual construir, asegurando que estén plenamente conscientes de la importancia de mantener un entorno seguro y protegido para datos y activos del partido.

La implementación de controles respaldados por ISO 27001 refuerza y equipa al partido con las herramientas necesarias para enfrentar los desafíos cambiantes de la seguridad digital. Estos controles no solo minimizan riesgos, sino que también ayudan a detectar amenazas potenciales y a mantener las operaciones de manera segura.

Este capítulo no solo representa un logro, sino también un compromiso continuo. Con la seguridad de la información, ya evidencia un esfuerzo por proteger la integridad de los datos y la fortalecer la confianza en la compañía de todas las partes interesadas.

Al mirar hacia el futuro, se plantea seguir fortaleciendo la postura de seguridad, mantener la confianza de aquellos que dependen del partido y de salvaguardar los datos críticos.

10 CONCLUSIONES

Después de una evaluación exhaustiva de la situación actual del Partido de La U en términos de seguridad de la información, se identificaron áreas críticas que requerían atención inmediata y medidas preventivas para salvaguardar los activos digitales del partido. La implementación de políticas y controles basados en la norma ISO 27001 se perfiló como la hoja de ruta esencial para mejorar la postura de seguridad del partido. Este análisis proporcionó una visión detallada de los riesgos asociados a los activos, resaltando la importancia de establecer una cultura de seguridad y la necesidad de una mejora continua para adaptarse a las amenazas cambiantes.

Situación Actual

El Partido de La U necesitaba actualizar y revisar sus políticas de seguridad, establecer roles y responsabilidades claras, documentar procesos y controles, capacitar a los empleados, llevar un inventario de recursos y activos de tecnología de la información, contar con copias de almacenamiento externas y supervisar el uso de recursos tecnológicos para mejorar su gestión de incidentes y garantizar la disponibilidad de información en caso de desastre.

En ese momento, habían implementado el 43.86% de los controles de seguridad de la norma ISO 27001, algunos con recomendaciones, el 13.16% estaban medianamente implementados y el 42.98% no se habían implementado.

Valoración e identificación Activos

Respecto a sus activos, el Partido de La U necesitaba implementar algunos controles y medidas correctivas y preventivas para asegurar sus activos críticos, como redundancia, planes de contingencia y capacitación del personal. Los servidores y sistemas de información requerían medidas de seguridad para garantizar alta integridad y confidencialidad, como control de acceso y encriptación.

Los dispositivos de red necesitaban medidas de seguridad, como autenticación, para protegerse de posibles ataques. La página web del partido necesitaba encriptación de datos, control de acceso y autenticación para proteger su alta integridad, confidencialidad y disponibilidad.

Los dispositivos de almacenamiento y el antivirus Kaspersky necesitaban medidas de seguridad, como encriptación de datos y actualizaciones periódicas, para mantener su alta integridad y confidencialidad. Los equipos de escritorio y repetidores de acceso requerían control de acceso y autenticación para su disponibilidad y confidencialidad media.

Las licencias de Office 2010 y Windows 10 necesitaban mantenerse actualizadas para evitar posibles vulnerabilidades. Los firewalls internos/externos y web necesitaban actualizaciones y escaneos periódicos para garantizar su alta integridad y confidencialidad, así como un directorio activo con permisos de menor privilegio y revisiones periódicas.

Se implementaron controles para mitigar los riesgos catalogados como críticos y se prestó especial cuidado también a los catalogados como importantes, con el objetivo de garantizar la continuidad del negocio y evitar la pérdida de información. Fue fundamental implementar controles efectivos para mitigar los riesgos críticos identificados, lo que incluía mejorar la seguridad de la información, implementar medidas de seguridad física y capacitar al personal en seguridad.

Riesgos

La identificación de riesgos asociados a los activos permitió a la organización priorizar sus recursos y esfuerzos de seguridad. Al entender qué activos eran más críticos y qué amenazas podían afectarlos, el Partido pudo asignar recursos de manera más efectiva, enfocándose en proteger los activos más valiosos y vulnerables. Esta priorización informada mejoró la eficiencia en la implementación de controles y garantizó una protección adecuada para los activos que eran fundamentales para la continuidad del negocio.

Esta reflexión final sobre el trabajo previamente realizado destaca cómo la identificación de riesgos proporcionó una base sólida para la toma de decisiones informada en toda la organización. Al comprender los riesgos específicos que enfrentaban los activos críticos, los líderes empresariales pudieron tomar decisiones estratégicas relacionadas con inversiones en seguridad, cumplimiento normativo y mitigación de riesgos. Esta comprensión también fue crucial para el desarrollo de planes de respuesta a incidentes y la preparación para situaciones de crisis, asegurando que el partido estuviera preparado para enfrentar y mitigar los riesgos identificados.

Controles y políticas

La identificación de riesgos críticos y la implementación de controles basados en la norma ISO 27001 reflejaron una evaluación exhaustiva de las amenazas y vulnerabilidades de seguridad de la información en el Partido de La U.

La implementación de políticas de seguridad y controles ISO 27001 marcó el inicio de un viaje de mejora continua. Fue fundamental revisar periódicamente estos controles para adaptarse a las amenazas emergentes y a los cambios en el entorno tecnológico.

Establecer políticas y controles sólidos no solo implicaba tecnología, sino también la creación de una cultura de seguridad. La concientización y el compromiso de los empleados fueron tan cruciales como las soluciones técnicas.

La implementación de políticas y controles también significó estar preparados para incidentes de seguridad. Establecer procedimientos claros para la respuesta a incidentes fue esencial para minimizar el impacto de las violaciones de seguridad. La revisión regular y la mejora continua fueron esenciales. La evaluación periódica de la efectividad de las políticas y controles aseguró que la organización estuviera siempre un paso adelante en la protección de su información valiosa.

Respuesta pregunta problema

¿Cómo mejorar la protección de la información sensible del Partido de la U, incluyendo datos de los afiliados, estrategias políticas, planes de campaña y otros activos importantes en un entorno de crecientes amenazas cibernéticas, mediante la implementación de un SGSI?

Analizando la problemática inicial planteada, centrada en la necesidad de mejorar la protección de la información sensible del Partido de la U, incluyendo datos de afiliados, estrategias políticas, planes de campaña y otros activos cruciales, en un entorno de crecientes amenazas cibernéticas, el diseño del SGSI emerge como una solución clave, el SGSI proporciona un enfoque integral que va más allá de la implementación de tecnologías de seguridad, abordando aspectos organizativos y humanos. Basándonos en el análisis exhaustivo de la situación actual del Partido de la U, se concluyó que el diseño de un SGSI era esencial para mejorar la protección de la información sensible, incluyendo datos de afiliados, estrategias políticas y planes de campaña, frente a las crecientes amenazas cibernéticas. Este SGSI, alineado con estándares internacionales como ISO 27001, abarcó la identificación y valoración de activos, la identificación de amenazas y salvaguardas, la valoración de riesgos, y la definición de controles y políticas de seguridad de la información. La implementación de medidas específicas, como la encriptación de datos, autenticación multifactor y concientización del personal, se recomendó para fortalecer la seguridad. Además, se destacó la importancia de fomentar una cultura de seguridad que involucre a todos los niveles del partido, asegurando un compromiso generalizado con la protección de la información en un entorno político digitalmente desafiante. Este enfoque integral no solo protegió los activos críticos, sino que también reforzó la confianza de afiliados y partes interesadas, posicionando al partido como resiliente frente a las amenazas emergentes.

Conclusión General

La evaluación detallada de la seguridad de la información en el Partido de La U subrayó la necesidad urgente de implementar medidas preventivas y correctivas basadas en la norma ISO 27001. La identificación de riesgos críticos y la implementación de controles específicos fueron esenciales para salvaguardar los activos digitales del partido. Sin embargo, la protección efectiva fue más allá de la tecnología; implicó la creación de una cultura organizacional de seguridad, destacando la importancia de la concientización y el compromiso de los empleados. La revisión continua de políticas y controles garantizará una adaptación efectiva a las amenazas emergentes, asegurando la integridad, confidencialidad y disponibilidad de la información del partido y, en última instancia, preservando la confianza de sus miembros y stakeholders.

11 RECOMENDACIONES

Las siguientes son recomendaciones para fortalecer la seguridad de la información en el Partido:

Situación Actual

Revisar y actualizar las políticas de seguridad, designar responsables y definir roles y responsabilidades, realizar revisiones exhaustivas de antecedentes de nuevos empleados y agregar disposiciones en acuerdos laborales que establezcan responsabilidades y medidas de precaución, proporcionar capacitaciones constantes a los empleados y desarrollar un programa continuo de formación y concientización en seguridad, administrar inventario de recursos o activos TI, establecer responsabilidades y controlar el licenciamiento de software, definir el uso aceptable de los activos de TI y desarrollar una guía de capacitación periódica para reforzar la política de control de accesos.

Contar con un sistema de monitoreo de red y eventos de seguridad de la información, capacitar a los usuarios respecto a prácticas de seguridad y establecer instrucciones seguras de inicio de sesión, implementar un adecuado control de cambios y realizar una revisión periódica de los recursos de TI y de los requisitos de capacidad, proporcionar los medios necesarios para separar los entornos de desarrollo, pruebas y producción, contar con copias de almacenamiento externas, vigilar constantemente el uso de recursos y sistemas de la infraestructura TI, examinar registros de auditoría y realizar pruebas de vulnerabilidades y realizar auditorías a los sistemas de información y establecer políticas de seguridad de la información para suministradores.

Recomendaciones activos

Establecer políticas y procedimientos claros: La compañía debe establecer políticas y procedimientos claros en cuanto al uso y manejo de la información sensible y confidencial. Estos procedimientos deben ser comunicados y entrenados al personal, y deben ser actualizados de forma regular, limitar el acceso: Se debe limitar el acceso a la información sensible y confidencial solamente a aquellos empleados que requieren el acceso para realizar sus tareas laborales. Además, se deben establecer medidas de control para evitar que los empleados accedan a información que no necesitan, monitorear el acceso y uso de la información: Se deben implementar sistemas de monitoreo para registrar el acceso y uso de la información sensible y confidencial. Esto permitirá detectar

posibles fugas de información y tomar medidas inmediatas para evitar la filtración de datos, proteger los dispositivos de almacenamiento: Es importante proteger los dispositivos de almacenamiento, como unidades USB, discos duros externos, entre otros, para evitar la extracción de información sensible de la compañía,

Educar al personal: Es importante educar al personal acerca de la importancia de la información sensible y confidencial, y las consecuencias de una fuga de información. Esto permitirá crear una cultura de seguridad de la información en la compañía y motivar al personal a tomar medidas de protección adecuadas, realizar auditorías regulares: La compañía debe realizar auditorías regulares para verificar el cumplimiento de las políticas y procedimientos establecidos, y detectar posibles vulnerabilidades en la seguridad de la información.

Recomendaciones Riesgos

Participación Activa de la Alta Dirección: Obtener el compromiso activo y visible de la alta dirección en el tratamiento y seguimiento de los riesgos. Asegurar que los recursos necesarios estén disponibles para implementar medidas de mitigación efectivas

A los riesgos catalogados como críticos aplicar controles de ISO27001 para mitigarlos y evitar que se materialicen y puedan ocasionar eventos catastróficos en los Datos y continuidad del negocio, contemplarlos en el momento de crear políticas.

Realizar un seguimiento y evaluación constante del plan de mitigación de riesgos, establecer responsables y periodicidad de revisiones, Considerar la posibilidad de realizar auditorías de seguridad de forma periódica para evaluar el cumplimiento de los controles y estándares y buscar certificaciones de seguridad de la información, como ISO 27001, para demostrar el compromiso con las mejores prácticas de seguridad.

Recomendaciones Controles y políticas

Esta política será revisada y actualizada regularmente para asegurar su relevancia y eficacia. Los cambios significativos en las tecnologías o las amenazas de seguridad requerirán revisiones inmediatas de la política.

Se debe establecer un programa de monitoreo continuo para evaluar la efectividad de los controles y ajustarlos según sea necesario, se recomienda realizar

auditorías internas periódicas para verificar el cumplimiento y la eficacia de los controles.

Proporcionar informes periódicos sobre el estado de la seguridad de la información y los incidentes a la alta dirección para mantenerlos informados y comprometidos.

Recomendación General

Para mejorar la seguridad de la información, el Partido de La U debe revisar políticas, definir roles, capacitar empleados y controlar el acceso. Es vital proteger dispositivos de almacenamiento, educar al personal y realizar auditorías periódicas. La alta dirección debe comprometerse activamente, aplicar controles de ISO 27001 y considerar auditorías de seguridad. La política debe actualizarse regularmente, y se debe implementar un programa de monitoreo continuo. Informar a la alta dirección periódicamente asegurará transparencia y compromiso en el mantenimiento de un entorno seguro.

BIBLIOGRAFÍA

Agencia Nacional de Seguridad Vial. Agencia Nacional de Seguridad Vial. [Sitio Web]. [Consultado: 15 de marzo 2023]. Disponible en: https://ansv.gov.co/

Agencia Nacional de Tierras. Agencia Nacional de Tierras. [Sitio Web]. [Consultado: 15 de marzo 2023]. Disponible en: https://www.ant.gov.co/

BEEKMAN, George y QUINN, Michael J. Introducción a la informática. (2018). Pearson Educación.

BRAUN, Virginia. y CLARKE, V. Reflecting on reflexive thematic analysis. Qualitative Research in Sport, Exercise and Health. 11(4), 589-597. [En Línea]. [Consultado: 9 abril de 2023]. Disponible en: https://doi.org/10.1080/2159676X.2019.1628806

Centro Criptológico Nacional. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT versión 3). [Sitio Web]. [Consultado: 04 de abril de 2023]. Archivo Pdf. Disponible en: https://www.ccn-cert.cni.es/pdf/magerit-v3-1-manual-completo.pdf

Consejo Nacional Electoral (CNE). Comunicado de prensa: CNE informa sobre intentos de ataques informáticos en la jornada electoral. [Sitio Web]. [Consultado: 12 de marzo de 2023]. Disponible en: https://cne.gov.co/portal/informacion-para-periodistas/comunicados-de-prensa/1822-cne-informa-sobre-intentos-de-ataques-informaticos-en-la-jornada-electoral

DAPRE Presidencia. Normativa. [Sitio Web]. [Consultado: 04 de abril de 2023]. Archivo Pdf. Disponible en: https://dapre.presidencia.gov.co/normativa/normativa/LEY%201273%20DEL%2023%20DE%20DICIEMBRE%20DE%202009.pdf

DAPRE Presidencia. Normativa. [Sitio Web]. [Consultado: 04 de abril de 2023]. Archivo Pdf. Disponible en: https://dapre.presidencia.gov.co/normativa/normativa/LEY%201581%20DEL%2017%20DE%20OCTUBRE%20DE%202012.pdf

Decreto 1151 de 2008. Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea de la República de Colombia, se reglamenta parcialmente la ley 962 de 2005, y se dictan otras disposiciones. Presidencia de la República de Colombia. [Sitio Web]. [Consultado: 04 de abril de 2023]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=32713.

Fuerza Alternativa Revolucionaria del Común (FARC). Ataque informático al sitio web de FARC. [Sitio Web]. [Consultado: 12 marzo de 2023]. Disponible en: https://www.farc-ep.co/noticias/ataque-informatico-al-sitio-web-de-farc.html.

HAIR, Joseph.; BLACK, William, BABIN, Barry y Anderson, Rolph. (2018). Análisis multivariante (7ma ed.). Cengage Learning.

International Organization for Standardization ISO 27001:2013 Information technology - Security techniques - Information security management systems – Requirement.[En línea]. [Consultado:9 de abril de 2023]. Disponible en: https://www.iso.org/standard/54534.html

ISO/IEC. Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requisitos (ISO/IEC 27001:2013). [Sitio Web]. [Consultado: 04 de abril de 2023]. Disponible en: https://www.iso.org/standard/54534.

LAUREANO, Ana, y ROMERO, Juan. Descriptive analysis: A method for identifying, summarizing and comparing data. Research in Psychotherapy: Psychopathology, Process and Outcome, 22(3), 391-399. [En línea]. [Consultado:9 de abril de 2023]. Disponible en: https://doi.org/10.4081/ripppo.2019.391.

Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. Congreso de la República de Colombia. [Sitio Web]. [Consultado: 04 de abril de 2023]- Disponible en: https://www.secretariasenado.gov.co/senado/basedoc/ley_1712_2014.html.

Ministerio de Defensa. Agencia Nacional de Seguridad Cibernética. [Sitio Web]. [Consultado: 9 de abril 2023]. Archivo Pdf. Disponible en: https://www.mindefensa.gov.co/irj/go/km/docs/Mindefensa/Documentos/descargas/Seguridad/AgenciaNacionaldeSeguridadCibernetica.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. Inicio. [Sitio Web]. [Consultado: 15 de marzo de 2023]. Disponible en: https://www.mintic.gov.co/portal/inicio/

Movimiento Ciudadano. Home. [Sitio Web]. [Consultado: 08 de abril de 2023]. Disponible en: https://movimientociudadano.mx/

NIST. (2019). Computer Security.[Sitio Web]. [Consultado: 4 de abril de 2023]. Disponible en: https://www.nist.gov/topics/computer-security

Partido Alianza. Home. [Sitio Web]. [Consultado: 08 de abril de 2023]. Disponible en: Verdehttps://www.alianzaverde.org.co/

Partido de la U. Partido de La Unión por la Gente. [Sitio Web]. [Consultado: 12 de marzo de 2023]. Disponible en: https://partidodelau.com/.

Partido Nacional PAN. Home: [Sitio Web]. [Consultado: 9 de abril de 2023]. Disponible en: https://www.pan.org.mx/

Partido Socialista de Chile. Home: [Sitio Web]. [Consultado: 9 de abril de 2023]. Disponible en: https://www.pschile.cl/

Personería de Bogotá. Sistema de Seguridad y Gestión de la información. [Sitio Web]. [Consultado: 12 de marzo de 2023]. https://www.personeriabogota.gov.co/sistemas-de-gestion/sistema-de-seguridad-y-gestion-de-la-informacion-sgsi

Registraduría Nacional del Estado Civil. Registraduría Nacional del Estado Civil Home. [Sitio Web]. [Consultado: 15 marzo de 2023]. Disponible en: https://www.registraduria.gov.co

ROJAS, Adriana. Filtración de datos del Partido Liberal afecta a más de 1,7 millones de afiliados. El Espectador. [Sitio Web]. [Consultado: 9 de abril de 2023]. Disponible en: https://www.elespectador.com/tecnologia/filtracion-de-datos-del-partido-liberal-afecta-a-mas-de-17-millones-de-afiliados-articulo-921898/

Unidad Administrativa Especial de Aeronáutica Civil. Aeronáutica Civil. [Sitio Web]. [Consultado: 12 de marzo de 2023]. https://www.aerocivil.gov.co

WHITMAN, Michael. y MATTFORD, Herbert .Principles of Information Security. (2020). (6th ed.). Cengage Learning.