TRATAMIENTO DE RIESGOS INFORMÁTICOS DEL ÁREA DE TI DE LA EMPRESA CENTRO DE DIAGNOSTICO AUTOMOTOR MOTOCENTRO S.A.S

OMAR ROSAS ALDANA

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

TRATAMIENTO DE RIESGOS INFORMÁTICOS DEL ÁREA DE TI DE LA EMPRESA CENTRO DE DIAGNOSTICO AUTOMOTOR MOTOCENTRO S.A.S

OMAR ROSAS ALDANA

Proyecto de Grado presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

ING. JOEL CARROLL
Director Proyecto de Grado

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

NOTA DE ACEPTACIÓN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá D.C., 19 de diciembre de 2023

DEDICATORIA

En primer lugar doy gracias a Dios por darme salud y la oportunidad de cumplir una nueva meta en mi vida profesional iluminada siempre de sabiduría, a Nora mi esposa que me apoyó y comprendió en esta nueva etapa de estudio dándome una voz de aliento cuando en varias ocasiones sentí no poder continuar; a mis hijos Juan, Salomé y Santiago que son la razón de mi existir, por comprender y aceptar no dedicarles el tiempo que se merecen; a mi madre Ana Sofia por inculcarme desde niño el amor por el estudio, siempre tendré muy presente su frase "*el mayor tesoro que podemos tener es el estudio*", a mi padre Alvaro por trasmitirme su valentía ante cualquier situación, a mí mismo para demostrarme que todo sacrificio tiene una recompensa.

AGRADECIMIENTOS

Agradezco al grupo de tutores de la Universidad Nacional Abierta y a Distancia UNAD, quienes con sus orientaciones me guiaron poco a poco hasta lograr cumplir este logro que en varias oportunidades lo veía muy difícil por la metodología de autoaprendizaje, pero que con dedicación se fueron viendo los frutos de muchas noches de desvelo, estrés, incertidumbre entre otros sentimientos que iban surgiendo a medida que avanzaban los periodos académicos. Mis más sinceros agradecimientos a la empresa CDA MOTOCENTRO SAS por confiar en mí y permitirme aplicar los conocimientos adquiridos a lo largo de la especialización en seguridad informática.

CONTENIDO

pág.

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

LISTA DE GRÁFICOS

LISTA DE ANEXOS

GLOSARIO

ACTIVO DE INFORMACIÓN: es un objeto tangible o intangible, análogo o digital que le genera valor a la organización, por ejemplo, los colaboradores, los documentos físicos, las bases de datos, el hardware, el software, el cableado y las redes, y los dispositivos de almacenamiento.

AMENAZA: posible acción o evento que se aprovecha de alguna vulnerabilidad de un sistema para causar algún tipo de daño acceso no deseado.

ANÁLISIS DE RIESGOS: (Process Hazards Analysis) es la acción sistemática que estudia los probables eventos y amenazas identificando los posibles daños a los activos de información y sus consecuencias.

CIBERSEGURIDAD: Conjunto de herramientas y procedimientos que se utilizan para proteger la información de los diferentes sistemas informáticos.

CONFIDENCIALIDAD: es un principio del SGSI, consisten en disponer los mecanismos necesarios para controlar el acceso a la información privada, sensible o clasificada.

CONTINUIDAD DEL SERVICIO: se encarga de impedir que una interrupción de servicios imprevista y grave tenga grandes consecuencias para el negocio. Estas interrupciones podrían venir derivadas no solo de fallos en la infraestructura (virus, ataques de denegación de servicio entre otros), sino también por desastres naturales (inundaciones, fuego, terremotos, etc.).

CONTROL DE ACCESO: validación de la identidad para garantizar el uso de un sistema o información, extinguiendo el uso no autorizado.

CONTROLES DE SEGURIDAD: acciones destinadas a garantizar la conservación de los activos, sistemas, instalaciones, datos y demás recursos informáticos.

CRIPTOGRAFÍA: es la ciencia de escribir mensajes cifrados, permite mantener la información segura cundo se transfiere entre distintos medios, evitando que al ser interceptada esta sea de utilidad.

DEFACEMENT: Ataque cibernético consistente en el enmascaramiento de un sitio web para dar al visitante o usuario la apariencia de no estar en el sitio web correcto, la estrategia consiste en cambiar la apariencia de la página web (imágenes, colores, etc.).

DISPONIBILIDAD: es un principio del SGSI, es la capacidad para el acceso y utilización oportuno de la información que ofrecen las organizaciones a los usuarios a través de los medios de comunicación (portal web, formularios web, Apps, etc.).

EQUIPOS: Están incluidos los equipos de cómputo, comunicaciones, extinción de incendios, respaldo de energía, audiovisuales, equipos de inspección entre otros.

HARDENING: endurecimiento, es la acción de eliminar todas las configuraciones por defecto, con el fin de mitigar las vulnerabilidades de las aplicaciones y la infraestructura que las soportan.

HARDWARE: parte tangible, conjunto de componentes físicos que conforman de un sistema.

IMPACTO: conjunto de consecuencias que puede originar un riesgo

INCIDENTE DE SEGURIDAD DE INFORMACIÓN: acceso o intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; impedimento en la operación normal de las redes, sistemas o recursos informáticos; violación a una Política de Seguridad de la Información.

INFRAESTRUCTURA: Conjunto de elementos o servicios que se consideran necesarios para el funcionamiento de una organización o para el desarrollo de una actividad.

INTEGRIDAD: es un principio del SGSI, define mecanismos que aseguran la fidelidad, exactitud y completitud de la información en todo momento.

MITIGAR: disminuir o reducir un riego

OFICIAL DE SEGURIDAD: persona encargada de administrar, implementar, actualizar y monitorear el Sistema de Gestión de Seguridad de la Información**.**

PLAN DE CONTINGENCIA: es un tipo de plan preventivo, predictivo y reactivo. Presenta una estructura estratégica y operativa que ayudará a controlar una situación de emergencia y a minimizar sus consecuencias negativas.

POLÍTICAS DE ORIGEN DE LAS CABECERAS: son las reglas establecidas para garantizar la seguridad en las comunicaciones a través del protocolo HTTP. La cabecera establece los permisos para acceder a los recursos seleccionados desde un servidor en un dominio que no corresponde al dominio al que pertenece.

PROBABILIDAD: grado de posibilidad de que suceda algún fenómeno o situación dadas algunas circunstancias

RIESGO RESIDUAL: riesgo que persiste después de la toma de medidas para tratar los riegos que se identificaron, previamente.

RIESGO: es el grado de exposición de un activo de información que hace que las amenazas saquen provecho de una vulnerabilidad provocando daños que impactan a la organización.

RIESGOS POTENCIALES: Situación o evento en que se ve afectada la adecuada prestación del servicio, provocada por agentes internos o externos a la organización.

ROLES: funciones que desempeñan una o varias personas dentro de la organización.

SEGURIDAD DE LA INFORMACIÓN: Acciones encaminadas a asegurar la preservación de la confidencialidad, integridad y disponibilidad de la información, también involucra otros atributos, como la autenticidad, la responsabilidad, el no repudio y la confiabilidad. Estos atributos aseguran que la información confidencial solo se divulgue a las partes autorizadas (confidencialidad), evite la modificación no autorizada de la información (integridad) y garantice que las partes autorizadas puedan acceder a los datos cuando lo solicite (disponibilidad).

SISTEMA DE GESTIÓN DE SEGURIDAD DE DA INFORMACIÓN: conjunto de políticas, procedimientos, recursos y actividades encaminadas en la administración de la información.

SISTEMA DE INFORMACIÓN: conjunto de componentes que interactúan entre sí para recolectar, administrar, procesar, recuperar, distribuir la información.

SOFTWARE: Es el conjunto de los programas de cómputo, procedimientos, reglas, documentación datos asociados que forman parte de las operaciones de un sistema de computación.

TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES: herramientas, recursos, equipos, programas informáticos, aplicaciones, que permiten el procesamiento, almacenamiento, transmisión de información.

TOLERANCIA AL RIESGO: nivel de riego aceptable que se está dispuesto a asumir.

TRATAMIENTO DEL RIESGO: Proceso de selección e implementación de medidas para modificar el riesgo.

VALORACIÓN DEL RIESGO: El riesgo identificado se debe evaluar de acuerdo con la gravedad de este, siendo esta baja, media o alta, y dependiendo de la influencia que pueda ejercer sobre el resultado final de la revisión Técnico-mecánica y de emisiones contaminantes.

VALORACIÓN: proceso para reconocer o apreciar un grado de valor.

RESUMEN

El presente proyecto contextualiza la importancia que hoy en día se le debe dar a la seguridad de los activos de información de cualquier organización, indistintamente de su naturaleza y tamaño, en vista de que a medida que crece el uso de la tecnología, en la misma proporción o mayor es el crecimiento de los ataques cibernéticos, en ese sentido toda organización debe plantear dentro de sus principales estrategias corporativas la de establecer un plan de tratamiento de riesgos de seguridad que garantice la mitigación de los ataques cibernéticos y mejore la seguridad en sus activos de información.

Ahora bien, este proyecto está orientado hacia la identificación de los activos de información del área de TI de la empresa CENTRO DE DIAGNOSTICO AUTOMOTOR MOTOCENTRO S.A.S., con un resultado de 76 activos de información tipificados de conformidad con los tipos de activos que plantea la metodología MAGERIT V3, entre los cuales están Claves Criptográficas, Servicio, Software y Hardware. Luego de la identificación y tipificación, el proyecto se enfoca en establecer la matriz de análisis y evaluación de los riesgos de seguridad de los activos de información de la empresa, aplicando la metodología mencionada anteriormente, se identifican los riesgos que tienen nivel Moderado e Inaceptable, de acuerdo con las dimensiones de la metodología aplicada, así mismo, según el impacto en la confidencialidad, integridad y disponibilidad de la información se establece los riesgos de seguridad que tienen nivel bajo, medio, alto y extremo.

Por último, en el presente proyecto se identifican las posibles vulnerabilidades de los activos de información del área de TI y se diseña el plan de tratamiento de riesgos de seguridad de la información aplicando los controles propuestos en el Anexo A de la norma ISO/IEC 27001 con el objetivo de mejorar los niveles de

seguridad de los activos de información mitigando los riesgos a los que pueden estar expuestos estos.

ABSTRACT

This project contextualizes the importance that today should be given to the security of information assets of any organization, regardless of its nature and size, in view that as the use of technology grows, in the same proportion or greater is the growth of cyber attacks, in this sense every organization should raise within its main corporate strategies, to establish a security risk treatment plan to ensure the mitigation of cyber attacks and improve the security of its information assets.

Now, this project is oriented towards the identification of the information assets of the IT area of the company CENTRO DE DIAGNOSTICO AUTOMOTOR MOTOCENTRO S.A.S., with a result of 76 information assets classified in accordance with the types of assets proposed by the MAGERIT V.3 methodology, among which are Cryptographic Keys, Service, Software and Hardware. After the identification and typification, the project focuses on establishing the analysis and evaluation matrix of the security risks of the company's information assets, applying the aforementioned methodology, the risks that have a Moderate and Unacceptable level are identified, In accordance with the dimensions of the applied methodology, likewise, according to the impact on the confidentiality, integrity and availability of the information, the security risks that have a low, medium, high and extreme level are established.

Finally, in this project the possible vulnerabilities of the information assets of the IT area are identified and the information security risk treatment plan is designed applying the controls proposed in Annex A of the ISO/IEC 27001 standard. with the aim of improving the security levels of information assets, mitigating the risks to which they may be exposed.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

El CENTRO DE DIAGNOSTICO AUTOMOTOR MOTOCENTRO S.A.S, es un organismo de inspección tipo A, acreditado por ONAC, bajo la norma técnica colombiana NTC ISO IEC 17200, en Revisión Técnico-Mecánica y de Emisiones Contaminantes en vehículos automotores Motocicletas 2T Motocicletas 4T.

Debe cumplir entre otras normas con la NTC 5385, NUMERAL 4.16 donde se habla de los requisitos de hardware y software, así como de los requisitos de seguridad de la información, aunque el organismo cuenta con un sistema de gestión enfocado en el cumplimiento de la NTC ISO IEC 17200; este no es lo suficientemente robusto para controlar los riesgos de seguridad de la información.

El CDA MOTOCENTRO S.A.S cuenta con una política de seguridad de la información, procedimientos de mantenimiento de equipos de cómputo, instructivos para la realización y restauración de copias de seguridad, bitácoras de fallos, sin embargo, no se ha tenido en cuenta en la identificación de los riesgos asociados a la seguridad de la información, tampoco se cuenta con un inventario completo y actualizado de todos los activos informáticos.

De esta manera al no tener definidos los riesgos ni los activos, el CDA MOTOCENTRO S.A.S no cuenta con los controles necesarios para hacer frente a las amenazas que puedan surgir y poner en riesgo la seguridad de la información, lo cual conlleva un gran problema para la organización al ser un organismo de inspección acreditado, que debe tener planes de contingencia y de continuidad de la prestación de sus servicios.

1.2 FORMULACIÓN DEL PROBLEMA

De conformidad con lo descrito anteriormente, se plantea la siguiente formulación del problema así: ¿Cómo el plan de tratamiento de riesgos de seguridad de la información permitirá mejorar la seguridad de los activos de información del área de TI del CDA MOTOCENTRO S.A.S.?

2 JUSTIFICACIÓN

Este proyecto nace como resultado del aumento de los ataques cibernéticos que hoy en día viven las organizaciones en nuestro país, de acuerdo con datos aportados por la fiscalía general, durante el periodo de enero a junio de 2021, los ataques en Colombia aumentaron un treinta por ciento en comparación con el mismo periodo del año inmediatamente anterior, pasando de 18.290 a 23.000 casos reportados. [1]

Como podemos evidenciar en el párrafo anterior, el crecimiento de ataques informáticos va en un crecimiento muy significativo por lo que se hace inevitable que las organizaciones garanticen los tres pilares fundamentales de la seguridad de la información, como lo son la integridad, confidencialidad y disponibilidad de la información, con el fin de mejorar no solo los niveles de seguridad, sino que también aumentar los niveles de competitividad y beneficio tanto empresarial como hacia sus clientes.

Ahora bien, dado que el CDA MOTOCENTRO S.A.S. es una empresa cuya infraestructura tecnológica no cuenta con los controles necesarios para mitigar las amenazas a las que están expuestos sus activos de información, tampoco cuenta con una identificación de estos que permita realizar una adecuada administración y gestión de los riesgos de seguridad de información, en tal sentido la misionalidad del CDA MOTOCENTRO S.A.S. es susceptible a verse afectada por riesgos como delitos informáticos, ocasionando tanto pérdidas económicas significativas como la integridad, confidencialidad y disponibilidad de la información almacenada y generada por la empresa.

[1] FOROS, SEMANA. www.semana.com [página web]. (9, diciembre, 2021). [Consultado el 18, marzo, 2022]. Disponible en Internet: <https://www.semana.com/nacion/articulo/que-retos-tiene-colombia-en-temas-de-ciberseguridad-expertos-lo-analizan/202100/>.

Con el desarrollo de este proyecto se realizará un análisis de riesgos de los activos de información, el cual permitirá identificar y clasificar eventos y amenazas dirigidas a la organización, ayudando a establecer medidas para minimizar los ataques hasta cierto nivel de impacto, al mismo tiempo el análisis de riesgos permitirá mejorar o restructurar el Plan de Seguridad de la Información - PSI con el que cuenta el CDA MOTOCENTRO S.A.S.

Con el resultado del análisis de riesgos se establecerá el plan de tratamiento de riesgos de seguridad de la información del CDA MOTOCENTRO S.A.S., el cual servirá de inicio para que a mediano plazo la empresa dentro de su planeación estratégica contemple la posibilidad de implementar el Sistema de Gestión de Seguridad de la Información, con el fin de salvaguardar toda la información y activos de la organización.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Proponer el plan de tratamiento de los riesgos informáticos en la empresa CDA MOTOCENTRO SAS, para mejorar la seguridad de los activos de información del área de TI, de conformidad con la metodología MAGERIT V3.

3.2 OBJETIVOS ESPECÍFICOS

3.2.1 Analizar la infraestructura tecnológica de MOTOCENTRO S.A.S. para establecer los activos de información del área de TI de la empresa, de conformidad con los tipos de activos que se plantean en la metodología MAGERIT V3.

3.2.2 Establecer la matriz del análisis y la evaluación de los riesgos de seguridad de los activos de información del área de TI de MOTOCENTRO S.A.S. para catalogarlos de acuerdo con su nivel de riesgo y de conformidad con las dimensiones de valoración propuestas en la metodología MAGERIT V3.

3.2.3 Diseñar el plan de tratamiento de riesgos de seguridad de la información de MOTOCENTRO S.A.S para mejorar los niveles de seguridad informática de los activos de información del área de TI, evitando se materialicen los riegos o minimizando su impacto, en caso de su materialización.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

Hoy en día el uso de las Tecnologías de la Información – TI en el ámbito laboral ha incrementado de manera significativa, así mismo la tecnología ha ido evolucionando con el pasar de los días, sin embargo, a medida que crece la aplicación de las TI y el progreso tecnológico avanza, los ataques cibernéticos aumentan y evolucionan de una manera más rápida, dado lo anterior surge la necesidad de aplicar metodologías y/o técnicas que permitan una gestión y administración del riesgo, y al mismo tiempo aumentar los niveles de seguridad en los activos informáticos en una organización, evitando que se materialicen los riesgos de estos, es por eso que a través de un plan de tratamiento de riesgos informáticos de la empresa CDA MOTOCENTRO SAS, se busca mitigar los ataques donde se atente contra los tres pilares de la información, es decir la integridad, disponibilidad y confidencialidad de esta.

En la actualidad existen varias metodologías enfocadas al análisis de riesgos informáticos, entre las más destacadas están: CORAS, CRAMM, MEHARI, MAGERIT, NIST SP 800:30, OCTAVE, frente a ello se empleó la metodología MAGERIT V3 con el fin de hacer una identificación de los activos susceptibles a un evento de seguridad, realizar una valoración de los activos críticos, identificar las principales amenazas y catalogarlas de acuerdo con su probabilidad de ocurrencia, como el impacto que generan, validar las medidas de seguridad existentes, identificar los riesgos residuales a los que la empresa queda expuesta y por ultimo diseñar el plan de tratamiento de riesgos informáticos de la empresa, para que a mediano plazo la empresa dentro de su planeación estratégica contemple la posibilidad de implementar el Sistema de Gestión de Seguridad de la Información.

4.2 MARCO CONCEPTUAL

MAGERIT: es una metodología enfocada al análisis y gestión de los riesgos de seguridad de la información, la cual fue creada por el Consejo Superior de Administración Electrónica de España[2], esta metodología brinda el método y las técnicas que permiten establecer el impacto que puede llegar a tener la seguridad de la información en una organización, debido a las vulnerabilidades que pueden existir en sus activos de información, las cuales son utilizadas por personas malintencionadas para realizar intentos de ataques cibernéticos; en ese sentido MAGERIT permite implementar medidas de control mediante un plan de tratamiento que garantice la mitigación de los riesgos.

ISO 27001: Es una norma internacional creada por la Organización Internacional de Normalización (ISO), y su función es de evitar que se generen incidentes relacionados con la Seguridad de la Información, independientemente si un incidente es leve o grave, éste representa un recurso económico para las empresas, en tal sentido al disminuir los incidentes se optimizan los recursos de las organizaciones.

Seguridad de la Información: es la unión de todas las técnicas y procedimientos que se deben tener a nivel de recurso humano como técnico, con el objetivo de salvaguardar los tres pilares fundamentales de la información, independientemente del medio en que se encuentre, los cuales que son:

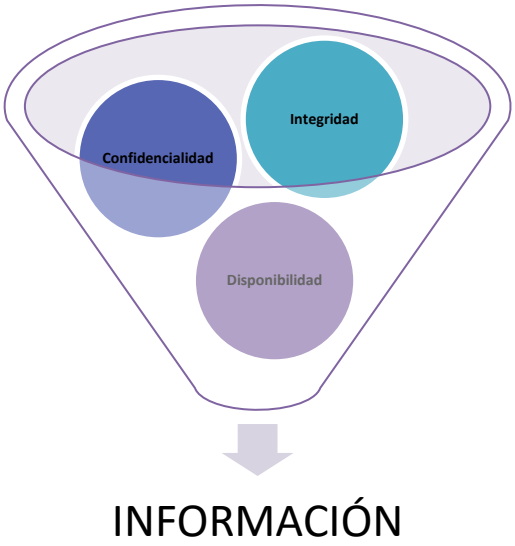
- **Confidencialidad**: garantizando que el acceso a los datos y su modificación sea realizado por las personas autorizadas para tal fin.
- **Integridad**: certificar que los datos no han sido manipulados por

[2] WELIVESECURITY ™ BY ESET ® (2013). MAGERIT: metodología práctica para gestionar riesgos [consultado: 20 de marzo de 2022]. Recuperado de: https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/

terceros de forma malintencionada, lo que garantiza que la información y sus procedimientos son exactos y completos.

- **Disponibilidad**: la información deberá estar accesible en todo momento que se requiera por los usuarios autorizados.

Figura 1: Pilares de la seguridad de la información



Fuente: elaboración propia

Administración del Riesgo: La gestión de riesgos es un enfoque estructurado para manejar la incertidumbre relativa a una amenaza a través de una secuencia de actividades humanas que incluyen la identificación, el análisis y la evaluación de riesgo, para luego establecer las estrategias de su tratamiento utilizando recursos gerenciales.

Análisis del riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de este.

Causa: Elemento que origina el comienzo de una situación determinada que genera un efecto o consecuencia.

Consecuencia: Resultado de un evento que afecta los objetivos.

Control: Medida que mantienen y/o modifica un riesgo

Evaluación del riesgo: proceso en el cual se comparan los resultados del análisis del riesgo frente a los controles implementados, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

Evento: Ocurrencia o cambio de un conjunto particular de circunstancias

Fuente de Riesgo: Elemento que, por si solo o combinación con otros, tiene potencial de generar riesgo.

Gestión del Riesgo: actividades coordinadas para dirigir y controlar la organización con relación al riesgo.

Probabilidad: Posibilidad que algo suceda.

Riesgo: Posibilidad o probabilidad de que un evento pueda afectar las funciones de la entidad e impactar el logro de sus objetivos.

Tratamiento del riesgo: proceso por el cual se modifica el riesgo.

Activo: según la RAE “conjunto de todos los bienes y derechos con valor monetario que son propiedad de una empresa, institución o individuo”[3].

[3] RAL ACADEMIA ESPAÑOLA (2021), Diccionario de la lengua española. Recuperado de: https://dle.rae.es/activo

Activo de información: es todo aquello que guarda relación con el tratamiento de la información y que posee un valor para la empresa, independiente de su medio de almacenamiento que puede ser físico o magnético, por ejemplo, los registros físicos, sistemas de información, bases de datos entre otros.

Amenaza: Es cualquier suceso o acción que tiene la posibilidad de afectar los datos en los sistemas de información dentro de una organización, aprovechándose de alguna vulnerabilidad existente.

Vulnerabilidad: es una posible inseguridad en un sistema, la cual puede ser explotada por un ciberdelincuente con el fin de comprometer la seguridad de la información, en ese sentido se hace necesario identificarlas y eliminarlas de inmediato evitando consecuencias mayores.

Valoración: proceso para reconocer o apreciar un grado de valor.

Probabilidad: grado de posibilidad de que suceda algún fenómeno o situación dadas algunas circunstancias

Riesgo Residual: riesgo que persiste después de la toma de medidas para tratar los riegos que se identificaron, previamente.

Tolerancia al riesgo: nivel de riego aceptable que se está dispuesto a asumir.

Impacto: conjunto de consecuencias que puede originar un riesgo.

4.3 MARCO CONTEXTUAL

CDA MOTOCENTRO S.A.S. organismo de inspección tipo A, acreditado por la ONAC, para la realización de revisiones Técnico-Mecánica y de Emisiones Contaminantes en vehículos automotores Motocicletas 2T Motocicletas 4T.

Fue creada en el año de 2018 en el municipio de Duitama – Boyacá, e inició su atención al público en octubre de 2019, con un campo de acción inicialmente en el municipio, sin embargo, se ha ido extendiendo en los demás municipios que hacen parte de la provincia del Tundama (Belén, Busbanzá, Cerinza, Corrales, Floresta, Paipa, Santa Rosa de Viterbo y Tutazá) y en gran parte del departamento de Boyacá, debido a sus altos niveles de calidad en el servicio de revisión técnico-mecánica y de emisiones contaminantes con exclusividad para motocicletas.

Para el CDA MOTOCENTRO S.A.S. el usuario es la razón de ser por lo que se enfoca en la prestación del servicio de revisión técnico-mecánica y de emisiones contaminantes para motocicletas; siguiendo la normatividad que los rige entre las que están la NTC ISO IEC 17200 y NTC 5385, apoyados en tecnología de primer nivel en el área de diagnóstico automotor, talento humano idóneo y una excelente atención al usuario, contribuyendo con la protección del medio ambiente y actuando responsablemente con la sociedad en la seguridad vial.

4.4 MARCO LEGAL

Hoy en día en Colombia cada vez es más común oír hablar de ciberataques a las organizaciones tanto públicas como privadas, perjudicando lo más esencial y vital en una empresa que son sus activos de información, en ese sentido es necesario conocer, entender y cumplir la legislación relacionada con la ciberseguridad en nuestro país.

Para establecer un marco legal local, el cual concuerda con el mercado de la empresa CDA MOTOCENTRO S.A.S., relacionado con el presente proyecto aplicado se describen las siguientes leyes aplicables en el campo de la ciberseguridad en Colombia:

4.4.1 Ley 1273 de 2009 De la Protección de la información y de los datos.

Esta ley incluye dentro del código penal colombiano un nuevo mecanismo legal, denominado "De la Protección de la información y de los datos", el cual busca la preservación de la integridad, confidencialidad y disponibilidad de los datos y de los sistemas de información que utilicen las Tecnologías de la Información y las Comunicaciones - TIC

De acuerdo con la Ley 1273 de 2009 tenemos que los delitos informáticos en Colombia que atentan contra la Confidencialidad, la Integridad y la Disponibilidad de la información son los siguientes:

- **Acceso no autorizado a un SI o red:** ocurre cuando una persona sin la debida autorización accede en todo o en parte a un sistema de información o red los cuales cuentan o no con una protección a nivel de seguridad.
- **Obstaculización ilegitima de SI o red:** se da cuando se entorpece el acceso normal o el funcionamiento de un sistema de información o red.
- **Intercepción de datos:** se incurre en este delito cuando sin una orden judicial previa se intercepta información durante el proceso de envío o recepción de esta o que se encuentra contenida en un SI.
- **Daño informático:** ocurre cuando se destruye, daña, borra, deteriora, altera o suprima información digital sin tener la facultad para realizarlo.
- **Uso de malware:** se da cuando no se cuenta con la debida autorización para producir, enviar, adquirir, traficar, distribuir, vender, introducir o extraer del territorio nacional malware u otro software con efectos maliciosos.

- **Violación de datos personales:** se da cuando para beneficio propio o de un tercero se vende, sustrae, intercambie, ofrece, compre, intercepte o modifique datos personales contenidos en SI, BD o archivos.
- **Obtención de datos personales a través de suplantación de sitios web:** quien diseñe, venda, desarrolle, ejecute, trafique o envíe sitios web falsos que tengan la finalidad de capturar datos personas de forma ilícita.
- **Transferencia no consentida de activos:** incurre en este delito quien se lucre o se valga de cualquier manipulación informática, para obtener la transferencia no consentida de activos en daño de un tercero.

4.4.2 Ley estatutaria 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.

Esta ley tiene como propósito garantizar el derecho constitucional que tienen las personas a conocer, actualizar y rectificar la información que se haya recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

4.4.3 Ley estatutaria 1266 de 2008. Hábeas data, modificada por la Ley 2157 de 2021.

"*Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones."*[4]

[4] CONGRESO DE LA REPÚBLICA (2008). LEY ESTATUTARIA 1266 DE 2008. Recuperado de: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

5 DISEÑO METODOLÓGICO

5.1 TIPO DE INVESTIGACIÓN

El tipo de investigación a emplear en el presente proyecto será orientado hacia la investigación aplicada tecnológica, porque se basa en metodologías, normas y técnicas para realizar el análisis y gestión del riesgo con el objetivo de abordar el problema específico de la empresa CDA MOTOCENTRO S.A.S. que se centra en el tratamiento de los riesgos informáticos de sus activos de información.

5.2 METODOLOGÍA DE DESARROLLO

El presente proyecto aplicado está basado en la metodología MAGERIT V:3.0 para el análisis y gestión de riesgos relacionados con la seguridad de la información, la cual plantea las siguientes etapas o pasos a seguir como buenas prácticas para el análisis de riesgos:

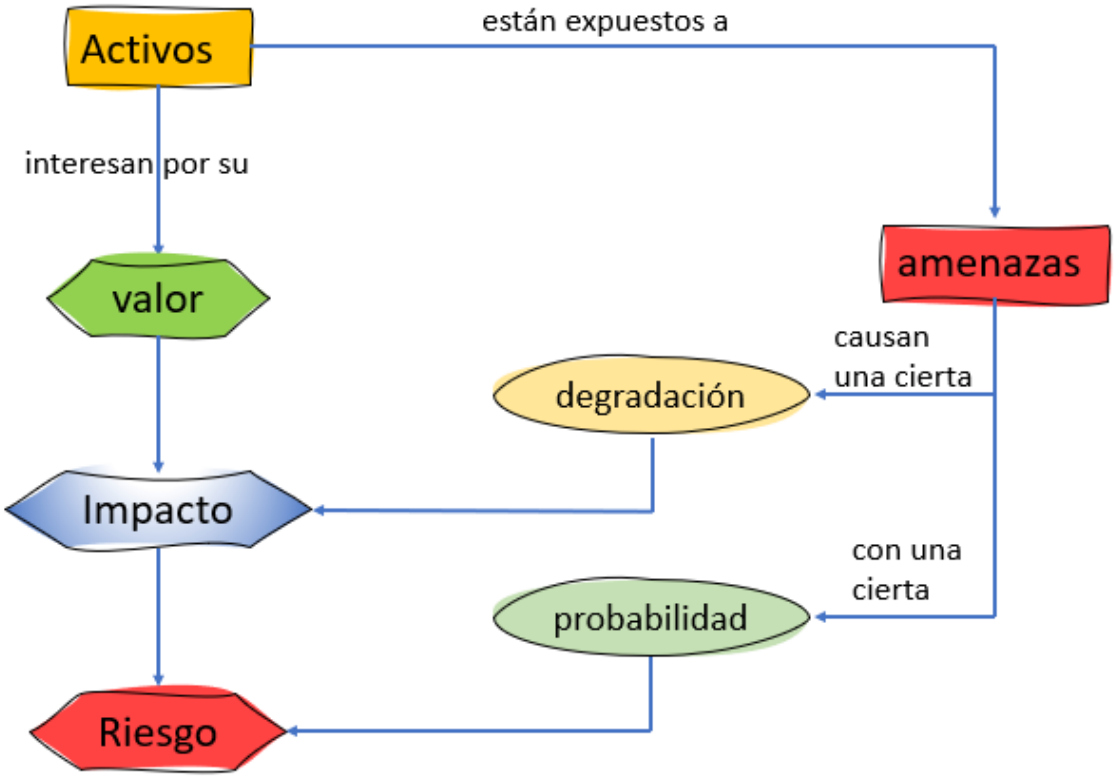
- Identificar los activos más importantes para la organización.
- Establecer a qué amenazas se exponen aquellos activos.
- Establecer las salvaguardas con las que se dispone y que tan eficaces son frente al riesgo identificado.
- "Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza."[5]
- "Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza."[6]

[5] Portal de Administración Electrónica. (2012). MAGERIT V.3: Metodología de Análisis y gestión de riesgos de los sistemas de información. Libro I Método [En línea]. Gobierno de España. Octubre de 2012. p. 22. Disponible en: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

[6] Ibid.

La siguiente ilustración permite un recorrido inicial por los diferentes pasos que plantea la metodología.

Figura 2: Pasos y elementos del análisis de riesgos



Fuente: Elaboración propia

5.2.1 Paso 1: Identificar los Activos

Dentro de un sistema de información existen dos componentes esenciales que son, en primer lugar, la información que se maneja, seguido de los servicios que brinda. En ese sentido los activos esenciales marcan la pauta para establecer los requisitos de seguridad para el resto de los componentes del sistema.

En ese orden de ideas y de conformidad con la metodología MAGERIT – V:3.0 los activos de información se pueden tipificar en:

- Esenciales [*essential*]
- Arquitectura del sistema [*arch]*
- Datos/Información [D]
- Claves Criptográficas [K]
- Servicios [S]
- Software [SW]
- Hardware [HW]
- Redes de comunicaciones [COM]
- Soportes de información [Media]
- Equipamiento auxiliar [AUX]
- Instalaciones [L]
- Personal [P]

Como se observa, los activos son de diferentes tipos, por lo tanto, las amenazas y las salvaguardas dependen del tipo de activo.

5.2.1.1 Dependencias.

Partiendo del punto que los activos esenciales son la información y los servicios prestados, sin embargo, estos activos van a depender de otros más comunes como lo son el hardware, las comunicaciones, las instalaciones y las personas.

Los activos forman árboles o grafos de dependencias donde la seguridad de los niveles superiores va a depender de los que se encuentren en los niveles inferiores. Es ahí donde entra el concepto de dependencias entre activos, que dicho en otras palabras es la forma como un activo superior se ve altamente afectado por un incidente de seguridad que haya sufrido un activo inferior.

Generalmente las dependencias se adaptan a la organización en donde se va a realizar el análisis de riesgos, sin embargo, se puede estructurar de la siguiente forma:

- Esenciales
    - Información
    - Servicios brindados
- Servicios internos
    - Que estructuran ordenadamente el SI
- Equipamiento informático
    - Software
    - Hardware
    - Comunicaciones
    - Dispositivos de almacenamiento: discos, cintas etc.
- Entorno: activos para garantizar las capas
    - Equipamiento y suministros
    - Mobiliario
- Servicios subcontratados
- Instalaciones físicas
- Personal
    - Usuarios
    - Administradores y operarios
    - Desarrolladores[7]

5.2.1.2 Valoración

[7] Ibid. P. 24

*"La valoración se puede ver desde la perspectiva de la '**necesidad de proteger**' pues cuanto más valioso es un activo, mayor nivel de protección requeriremos en la dimensión (o dimensiones) de seguridad que sean pertinentes*."[8]

La valoración es establecer el costo necesario para recuperarse de una incidencia que dejara el activo inutilizable. Dentro de los factores a considerar están:

- Costo de reposición: adquisición e instalación
- Costo de mano de obra (especializada) invertida en recuperar (el valor) del activo
- Lucro cesante: pérdida de ingresos
- Capacidad de operar: confianza de los usuarios y proveedores que se traduce en una pérdida de actividad o en peores condiciones económicas
- Sanciones por incumplimiento de la ley u obligaciones contractuales
- Daño a otros activos, propios o ajenos
- Daño a personas
- Daños medioambientales[9]

La valoración se puede dar cualitativa o cuantitativamente, dependiendo de los criterios de homogeneidad y relatividad.

5.2.1.3 Dimensiones

En los activos de información intervienen las siguientes dimensiones:

- su confidencialidad: ¿qué daño causaría que lo conociera quien no debe?
- su integridad: ¿qué perjuicio causaría que estuviera dañado o corrupto?

[8] Ibid.
[9] Ibid. P. 25

- su disponibilidad: ¿qué perjuicio causaría no tenerlo o no poder utilizarlo?[10]

A las dimensiones canónicas de la seguridad se pueden completar otras derivadas que permitan una percepción de los usuarios de los sistemas de información:

Autenticidad: *¿qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa*?[11]

Trazabilidad*: ¿qué daño causaría no saber a quién se le presta tal servicio? O sea, ¿quién hace qué y cuándo? ¿qué daño causaría no saber quién accede a qué datos y qué hace con ellos?*[12]

5.2.2 Paso 2: Establecer amenazas

Este paso radica en determinar las amenazas que afectarían en particular a cada activo de información.

5.2.2.1 Identificación de amenazas

De acuerdo con la metodología MAGERIT V:3.0 las amenazas se pueden clasificar en:

- De origen natural (terremotos, inundaciones, …)
- Del entorno (de origen industrial como contaminaciones, fallas eléctricas, …)
- Defectos de las aplicaciones (defectos en su diseño o en su implementación).
- Causadas por las personas de forma accidental (por error o por omisión).
- Causadas por las personas de forma deliberada (con ánimo de beneficiarse, causar daños y perjuicios).

[10] Ibid. P. 24
[11] Ibid.
[12] Ibid.

5.2.2.2 Valoración de las amenazas

Una vez determinado que una amenaza puede perjudicar a un activo, hay que valorar su influencia en el valor del activo, en dos sentidos:

- Degradación: cuán perjudicado resultaría el [valor del] activo
- Probabilidad: cuán probable o improbable es que se materialice la amenaza

De los anteriores sentidos surgen las siguientes escalas:

Figura 3: Degradación del valor

MA	muy alta	casi seguro	fácil
A	alta	muy alto	medio
M	media	posible	difícil
B	baja	poco probable	muy difícil
MB	muy baja	muy raro	extremadamente difícil

Fuente: PAE - MAGERIT V.3

Figura 4: Degradación del valor

MA	100	muy frecuente	a diario
A	10	frecuente	mensualmente
M	1	normal	una vez al año
B	1/10	poco frecuente	cada varios años
MB	1/100	muy poco frecuente	siglos

Fuente: PAE - MAGERIT V.3

5.2.3 Paso 3: Salvaguardas

"Se definen las salvaguardas o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo."[13]

5.2.3.1 Selección de Salvaguardas

Existe una gran variedad de posibles salvaguardas a considerar, en ese sentido es necesario hacer un filtro inicial para seleccionar las más relevantes de acuerdo con lo que hay que proteger, para ello se debe tener presente los siguientes aspectos:

- Tipo de activos a proteger, pues cada tipo se protege de una forma específica
- Dimensión o dimensiones de seguridad que requieren protección
- Amenazas de las que necesitamos protegernos
- Si existen salvaguardas alternativas

Además, es conveniente fijar un principio de proporcionalidad y tener en cuenta:

- El mayor o menor valor propio o acumulado sobre un activo, centrándonos en lo más valioso y obviando lo irrelevante
- La mayor o menor probabilidad de que una amenaza ocurra, centrándonos en los riesgos más importantes
- La cobertura del riesgo que proporcionan salvaguardas alternativas[14]

5.2.3.2 Efectos de las Salvaguardas

Las salvaguardas intervienen en la valoración del riesgo de dos formas:

[13] Ibid. P. 31
[14] Ibid.

- Reduciendo la probabilidad de las amenazas: llamadas comúnmente salvaguardas preventivas debido a que logran impedir que las amenazas se materialicen.
- Limitando el daño causado: hay salvaguardas que directamente limitan el posible daño, en cambio otras permiten detectar de inmediato el ataque para frenar que el daño causado avance. *Incluso algunas salvaguardas se limitan a permitir la pronta recuperación del sistema cuando la amenaza lo destruye*. En cualquiera de los casos, la amenaza se llega a materializar; sin embargo, se limitan las consecuencias.[15]

5.2.4 Paso 4: Impacto

"Dado un cierto conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de posible impacto que se denomina residual. Se dice que hemos modificado el impacto, desde un valor potencial a un valor residual.

El cálculo del impacto residual es sencillo. Como no han cambiado los activos, ni sus dependencias, sino solamente la magnitud de la degradación, se repiten los cálculos de impacto con este nuevo nivel de degradación.

La magnitud de la degradación tomando en cuenta la eficacia de las salvaguardas, es la proporción que resta entre la eficacia perfecta y la eficacia real.

El impacto residual puede calcularse acumulado sobre los activos inferiores, o repercutido sobre los activos superiores."[16]

[15] Ibid. P. 32
[16] Ibid. P. 35

5.2.5 Paso 5: Riesgo Residual

"Dado un cierto conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de riesgo que se denomina residual. Se dice que hemos modificado el riesgo, desde un valor potencial a un valor residual.

El cálculo del riesgo residual es sencillo. Como no han cambiado los activos, ni sus dependencias, sino solamente la magnitud de la degradación y la probabilidad de las amenazas, se repiten los cálculos de riesgo usando el impacto y la probabilidad residuales de ocurrencia.

La magnitud de la degradación se toma en consideración en el cálculo del impacto residual."[17]

Al igual que el impacto residual, el riesgo residual es acumulado o repercutido.

5.3 FUENTES Y TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN

Para la recolección de información del presente proyecto aplicado, la principal fuente será a través de visitas y contacto directo con la infraestructura tecnológica del CDA MOTOCENTRO S.A.S., así mismo, con el personal de TI quien conoce el estado actual de los sistemas de información que se utilizan en la empresa.

De otra parte, se hará uso de información consultada en Internet como lo son monografías, proyectos de grado, libros especializados, artículos entre otros, que estén directamente relacionados con el objeto de estudio y por supuesto información

[17] Ibid.

contenida tanto en la metodología MAGERIT V:3.0 como en la misma norma ISO/IEC 27001:2013.

5.4 POBLACIÓN Y MUESTRA

La población del presente proyecto está conformada por los activos de información del CDA MOTOCENTRO S.A.S. y la muestra será los activos del área de TI de la organización, área que maneja el core del negocio y donde se administra gran cantidad de información almacenada en las bases de datos del sistema de información propia para la operación del CDA.

6 DESARROLLO DE LOS OBJETIVOS

Hoy en día una organización debe ser inteligente y proactiva, enfocada a la planificación y la toma decisiones con un alto pensamiento apoyado en riesgos, con el propósito de anticiparse a las dificultades y lograr una óptima eficacia, a su vez, obtener cada vez excelentes resultados, previniendo las consecuencias negativas de las dinámicas del contexto, así mismo, promoviendo escenarios propicios que la impulsen a obtener los resultados planteados.

6.1 IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN DEL AREA DE TI DEL CDA MOTOCENTRO S.A.S.

Los activos de información en el entorno de la norma ISO/IEC 27001 corresponde a todo aquello que para una organización representa un valor y en ese sentido debe protegerlos.

La identificación de los activos de información toma un papel importante dentro de la seguridad de la información en una organización, debido a que permite identificar los activos de información a los que se les debe brindar mayor relevancia al momento de protegerlos.

De acuerdo con la metodología MAGERIT V. 3:0 los activos de información se pueden tipificar de la siguiente forma y empleando dentro de un paréntesis angular [] la abreviatura según el tipo de activo:

- [*essential*] Esenciales: en los sistemas de información existen dos puntos esenciales, los servicios que brindan y la información que se maneja, estos dos marcan la pauta a nivel de seguridad para los otros elementos del sistema. La [inf] información puede ser de carácter personal, vital y clasificada.

- [*arch]* Arquitectura del sistema*:* consiste en los componentes que permiten estructurar el sistema, como lo son su arquitectura interna y sus relaciones externas.
- [D] Datos/Información: la información o datos es el activo principal en una organización, asemejándolo con el cuerpo humano, son el corazón para brindar sus servicios. Los datos son almacenados de manera agrupada como ficheros o en bases de dato, facilitando su transmisión.
- [K] Claves Criptográficas: están son empleadas para proteger la información, combinando información secreta y pública.
- [S]Servicios: la función principal de este tipo de activo es satisfacer la necesidad de los usuarios en cuanto al servicio. En este tipo se encuentran aquellos servicios que brinda el Sistema de información.
- [SW] Software: también se le conoce como programas, desarrollos, aplicativos, etc., el software es quien se encarga de gestionar, analizar y transformar los datos. En este tipo de activo se encuentran todas aquellas labores que han sido automatizadas.
- [HW] Hardware: lo conforman todos los componentes físicos que permiten soportar tanto directa como indirectamente los diferentes servicios que brinda la organización, estos activos son el soporte para ejecución del software para el procesamiento y/o transmisión de la información.
- [COM] Redes de comunicaciones: a este tipo de activo corresponde los servicios de comunicaciones de terceros, que permiten la transmisión de información de un lugar a otro.
- [Media] Soportes de información: es cada uno de los dispositivos físicos que permiten el almacenamiento, ya sea permanente o temporal, de los datos.
- [AUX] Equipamiento auxiliar: compuesto por equipos que no están directamente relacionados con la información pero que sirven de soporte a los sistemas de información, dentro de los cuales se encuentran UPS, cableado, fibra óptica, armarios o Racks, entre otros.

- [L] Instalaciones: corresponde a la infraestructura física donde se encuentran alojados los sistemas de información y comunicaciones de la organización.
- [P] Personal: conformado por las personas que interactúan directamente con los sistemas de información.

Para la identificación de los activos de información del CDA MOTOCENTRO, se va a utilizar la matriz de análisis de riesgos de ciberseguridad del autor Luis Fernando Zambrano (ver **Anexo A** hoja **AVC**, columnas C,D,E), docente de la UNAD y director del curso Administración y Gestión del Riesgo, en la cual se consolida no solo la identificación de activos sino también el análisis, evaluación y tratamiento de los riesgos, dado que el enfoque de gestión de riesgos a aplicar está basado en la metodología MAGERIT. Este instrumento se utilizará como un anexo a este proyecto.

Adicional al registro de los activos de información en la matriz mencionada anteriormente, se realizó una visita y se hizo un registro fotográfico con la finalidad de conocer la infraestructura tecnológica de la empresa y la operación principal de la misma.

A continuación, se ilustran y describen varios de los activos de información que hacen parte de la infraestructura tecnológica de la empresa CDA MOTOCENTRO S.A.S., el listado completo de los activos de información se encuentra disponible en el Anexo A del presente proyecto:

6.1.1 Instalaciones del Centro de Diagnostico Automotor MOTOCENTRO S.A.S.: las cuales comprenden un área aproximadamente de 411 m^2, distribuidos en dos plantas, que brindan un espacio ideal para ejecutar el servicio de revisión técnico-mecánica y de emisiones contaminantes con la mejor calidad en el sector, dichas instalaciones están ubicadas en la ciudad de Duitama – Boyacá.

Figura 5: CDA MOTOCENTRO

Fuente: elaboración propia

6.1.2 [COM] Rack de comunicaciones: compartimento donde se encuentra ubicado el servidor principal de la organización, junto con el router, switch y DVR, desde allí se distribuye todo el cableado estructurado para la infraestructura tecnológica del CDA.

Figura 6: [COM] Rack de comunicaciones

Fuente: elaboración propia

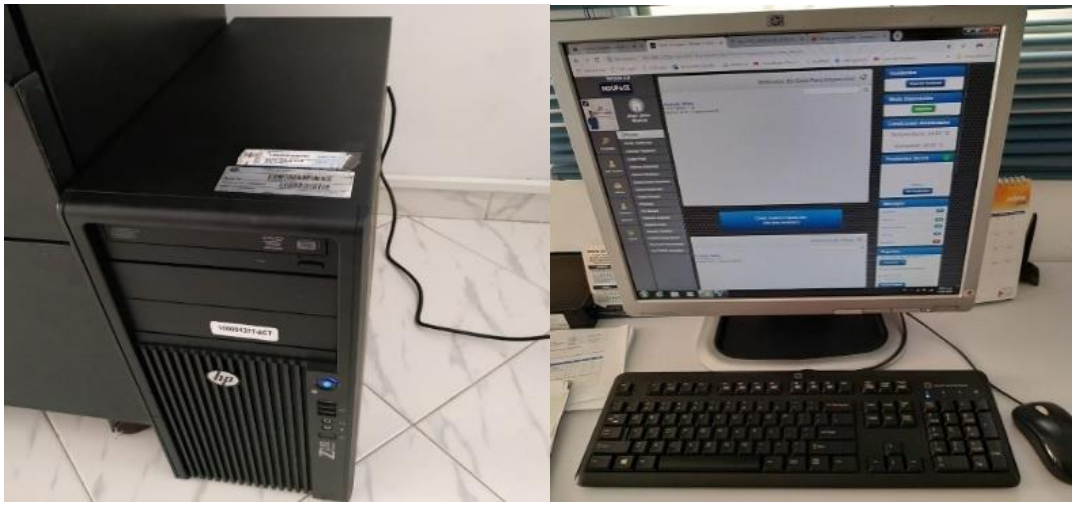
6.1.3 [HW] Servidor principal: equipo WorkStation de marca Hewllett Packard, con sistema operativo Windows 7 Professional, como SO anfitrión, en el cual se tiene virtualizada, a través del software VirtualBox, una maquina con sistema operativo Linux Server dentro del cual se tiene implementado el software Core del CDA denominado INDUPACK, este se encarga de suministrar los servicios necesarios para el funcionamiento de las aplicaciones de Revisión Técnico mecánica, así como el manejo de la base de datos general.

Figura 7: [HW] Servidor principal

Fuente: elaboración propia

6.1.4 [HW] Servidor de respaldo: equipo Workstation con las mismas características tanto físicas como lógicas que el servidor principal para que entre en funcionamiento en caso de una falla o incidente.

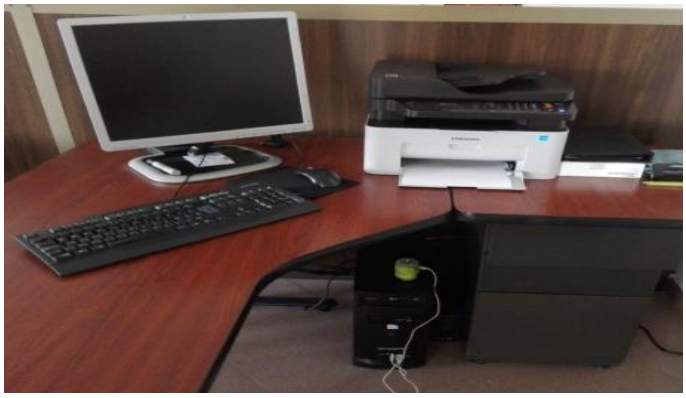
Figura 8: [HW] Servidor de respaldo



Fuente: elaboración propia

6.1.5 [HW] Equipo de cómputo TI: equipo de escritorio de marca ARGOM con sistema operativo Windows 10 Professional, desde el cual se accede a través de un servicio web al software INDUPACK (revisión técnico mecánica) dentro de la misma red LAN, cuenta con software utilitario para las diferentes laborales del Director TI, este equipo se utiliza además para generar los reportes de resultados de las pruebas realizadas, validar la información, generar copias de respaldo, interactuar con los servicios de vigilancia y control SICOV, monitoreo de cámaras, creación y edición de documentos, manejo de correo electrónico.

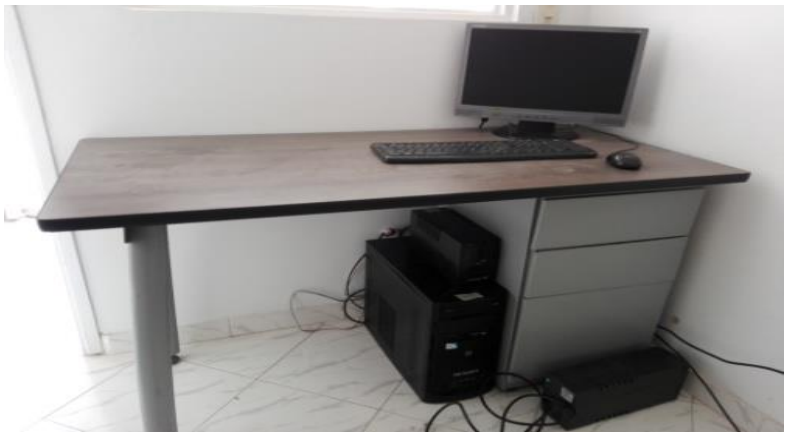
Figura 9: [HW] Equipo de cómputo TI



Fuente: elaboración propia

6.1.6 [HW] Equipo de cómputo coordinador operativo: Este esquipo cuenta con la capacidad de funcionar como respaldo de cualquier equipo incluyendo el servidor, maneja una copia de seguridad del servidor principal, así como todas las aplicaciones y configuraciones necesarias para permitir cumplir con cualquier función.

Figura 10: [HW] Equipo de cómputo coordinador operativo



Fuente: elaboración propia

6.1.7 [HW] Equipo de cómputo coordinador administrativo: cumple con las funciones de registro de información en la plataforma RUNT, adquisición de PIN de pago en la plataforma de supergiros, generación de facturas en la plataforma de la DAIN, para acceder a la aplicación de INDUPACK (revisión técnico-mecánica) alimentando información necesaria para los procesos de revisión, creación y edición de documentos, manejo de correo electrónico.

Figura 11: [HW] Equipo de cómputo coordinador administrativo

Fuente: elaboración propia

6.1.8 Equipos de impresión: activos empleados para la salida de los datos que son generados en los sistemas de información del CDA, como por ejemplo los resultados de la verificación para el cumplimiento de la revisión técnico-mecánica y emisión de gases contaminantes que se realizan a las motocicletas de 4 y 2 tiempos.

Figura 12: [HW] impresora 1 Samsung

Fuente: elaboración propia

Figura 13: [HW] impresora 2 Samsung

Fuente: elaboración propia

Figura 14: [HW] impresora 3 Cannon

Fuente: elaboración propia

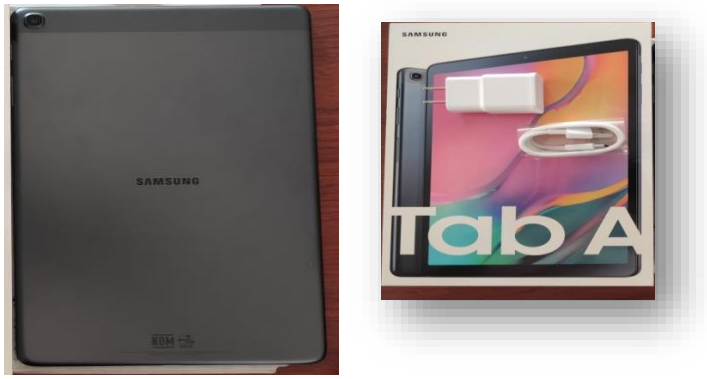
6.1.9 [HW] Tabletas Samsung: actualmente se cuenta con 3 de estos dispositivos con las mismas características de hardware y software, en las cuales se realiza todo el proceso de la revisión técnico-mecánica y emisión de gases contaminantes, equipos con sistema operativo Android 6.0.1, equipos que permiten realizar la inspección visual de la motocicleta mediante el uso de la APP Pre-revisión, seguidamente a través de la APP Pista se realiza todo el levantamiento de información como resultado del proceso de la revisión técnico-mecánica en las diferentes estaciones de la pista de inspección, permitiendo realizar registros fotográficos, validación de listas de chequeo de defectos, realizar pruebas de sonometría, análisis de gases, frenometro y prueba de medición luces; luego esta información en sincronizada con el software INDUPACK donde el Coordinador técnico del CDA puede realizar la verificación de los resultados obtenidos para aprobar o no la revisión.

Figura 15: [HW] Tableta 1 Samsung

Fuente: elaboración propia

6.1.10 [HW] Tableta 4 Samsung, esta Tablet cuenta con la APP Servicio que permite al acceso con privilegios más elevados para realizar labores de verificación, calibración y mantenimiento de los equipos de inspección.

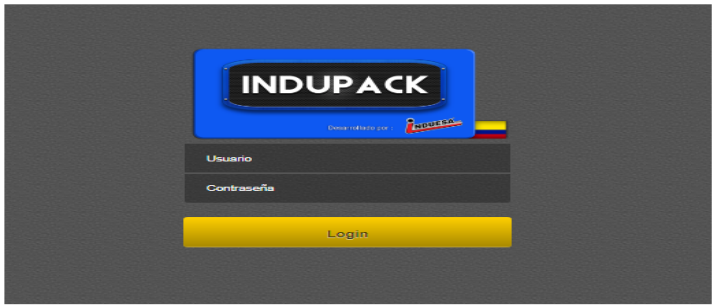
Figura 16: [HW] Tableta 4 Samsung



Fuente: elaboración propia

6.1.11 [SW] Software INDUPACK: es el Core del negocio del CDA MOTOCENTRO S.A.S. en el cual se realiza la gestión y administración de toda la data que se genera durante el proceso de la revisión técnico-mecánica y emisión de gases contaminantes, principal actividad de la empresa objeto del presente proyecto.

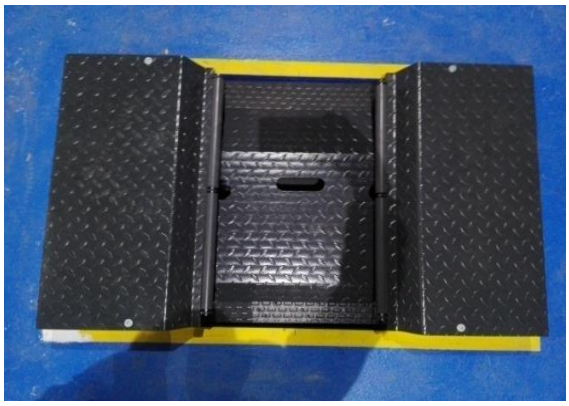
Figura 17: [SW] Software INDUPACK



Fuente: elaboración propia

6.1.12 [HW] Frenometro XEDRA: permite enviar al software INDUPACK los resultados de la prueba de verificación del estado y eficacia de los frenos de las motocicletas a través de la tarjeta de desarrollo Beaglebone, este equipo de inspección es capaz de medir las fuerzas de frenado y el peso del vehículo.

Figura 18: [HW] Frenometro XEDRA



Fuente: elaboración propia

6.1.13 [HW] Alineador de luces TECNOLUX: equipo de inspección encargado de la medición de la intensidad luminosa y el ángulo de inclinación de los haces de luz.

Figura 19: [HW] Alineador de luces TECNOLUX

Fuente: elaboración propia

6.1.14 [HW] Analizador de gases 4T MOTORSCAN: equipo de inspección utilizado para la medición de las emisiones contaminantes (CO, CO_2; HC).

Figura 20: [HW] Analizador de gases 4T MOTORSCAN

Fuente: elaboración propia

6.1.15 [HW] Termohigrómetro INDUESA: equipo encargado de monitorear la temperatura ambiente y la humedad relativa, con el fin de garantizar que las mediciones de emisiones contaminantes se realicen en condiciones controladas.

Figura 21: [HW] Termohigrómetro INDUESA

Fuente: elaboración propia

6.1.16 [HW] Sonómetro PCE: equipo de inspección encargado de la medición del ruido(decibelios) generado por el vehículo al realizar aceleraciones.

Figura 22: [HW] Sonómetro PCE

Fuente: elaboración propia

6.1.17 [HW] Cuentarrevoluciones Brain Bee: equipo de inspección para la medición de las revoluciones del motor RPM, también cuenta con la capacidad de medir la temperatura del motor esto para poder realizar las pruebas de emisiones de gases de forma correcta.

Figura 23: [HW] Cuentarrevoluciones Brain Bee

Fuente: elaboración propia

Como resultado de la identificación de activos de información de la empresa objeto de este proyecto, se tiene la Tabla 1. Resumen de activos de información, donde se puede visualizar la clasificación general y número de activos por el tipo de este, de conformidad con la metodología MAGERIT V: 3.0 y el uso del instrumento Matriz de Análisis de Riesgos del ingeniero Luis Fernando Zambrano.

Tabla 1. Resumen de activos de información

Tipo de activo	Cantidad
Tipo Dato	0
Tipo Claves Criptográficas	2
Tipo Servicio	2
Tipo Software	40
Tipo Hardware	32
Tipo Comunicaciones	0
Tipo Soporte de Información	0
Tipo Equipamiento Auxiliar	0

Tipo Instalaciones	0
Tipo Personal	0
Total de Activos	**76**

Así mismo se pudo identificar la ubicación que tienen los activos de información, la cual puede variar entre física o electrónica, como se evidencia en la Tabla 2. Resumen ubicación activos de información.

Tabla 2. Resumen ubicación activos de información.

Ubicación	
Física	8
Electrónica	68

Una vez identificados los activos, el tipo de activo, el propietario del activo y su ubicación, se da paso a realizar su valoración cualitativa y cuantitativa para iniciar el análisis y evaluación de los riesgos que se trabajará en el numeral 6.2 del presente proyecto aplicado.

6.2 MATRIZ DEL ANÁLISIS Y LA EVALUACIÓN DE LOS RIESGOS DE SEGURIDAD DE LOS ACTIVOS DE INFORMACIÓN DE CDA MOTOCENTRO S.A.S

La matriz de análisis y evaluación de riesgos es una herramienta visual que representa los riesgos potenciales que afectan a una organización, la matriz de riesgos se fundamenta en dos factores que se cruzan: la probabilidad de que ocurra el evento de riesgo y el impacto potencial que tendrá el evento de riesgo en el

negocio, en otras palabras, es una herramienta que le ayuda a visualizar la probabilidad frente a la gravedad de un riesgo potencial.

De acuerdo con la probabilidad y la gravedad, los riesgos se pueden clasificar como altos, moderados o bajos, como parte del proceso de gestión de riesgos, las organizaciones emplean matrices de riesgo para apoyarse a priorizar diferentes riesgos y establecer una estrategia de tratamiento adecuada.

En ese sentido, es tan importante tener un panorama preciso de todos los riesgos potenciales que afronta la organización, para que pueda evaluar su impacto y crear un plan de tratamiento de riesgos exitoso.

Los activos de información se catalogan de acuerdo con la confidencialidad, integridad y disponibilidad, cada uno de estos tres principios de seguridad se clasifica individualmente como muy bajo (MB), bajo (B), medio (M), alto (A) o muy alto (MA).

Por ejemplo, un activo de información puede tener un nivel de confidencialidad de "bajo", un nivel de integridad de "medio" y un nivel de disponibilidad de "alto" (es decir, B-M-A).

Las preguntas se clasifican por confidencialidad, integridad y disponibilidad, cada pregunta debe responderse secuencialmente, según las mejores capacidades de los propietarios de la información.

"*Un análisis de riesgos TIC es recomendable en cualquier Organización que dependa de los sistemas de información y comunicaciones para el cumplimiento de su misión.*"[18]

[18] Ibid. P. 16

De conformidad con la metodología MAGERIT V. 3.0 en la cual está basado en presente proyecto aplicado, para realizar la valoración de los activos para hacer su análisis y evaluación, se deben tener presente cinco dimensiones que son:

- Confidencialidad
- Integridad
- Disponibilidad
- Trazabilidad
- Autenticidad

Para la valoración de las anteriores dimensiones de cada uno de los activos de información, existe dos técnicas una de ellas es la **cualitativa**, que consiste en valorar cada una de las cinco dimensiones de acuerdo con la tabla cualitativa que comprende los siguientes valores Muy Bajo (MB), Bajo (B), Medio (M), Alto (A) y Muy Alto (MA). La otra técnica es la **cuantitativa,** la cual, una vez valoradas las dimensiones con un criterio cualitativo, de acuerdo con este se asigna un valor cuantitativo así:

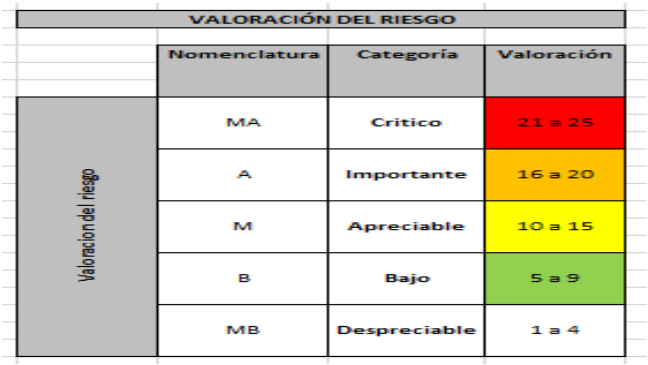
Tabla 3. Valoración de activos

Valor Cualitativo	**Valor Cuantitativo**
Muy Bajo	4
Bajo	9
Moderado	15
Alto	20
Muy Alto	25

Los valores cuantitativos son muy útiles, pero requieren de un mayor esfuerzo, al usar números para la valoración del riesgo al que puede estar expuesto el activo

permite realizar el promedio de las cinco (5) dimensiones y saber la categoría a la que pertenece el riesgo, de la siguiente forma:

Figura 24: Valoración del Riesgo



VALORACIÓN DEL RIESGO			
	Nomenclatura	Categoría	Valoración
Valoración 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: ZAMBRANO, Luis (2022). Matriz de análisis de riesgos de ciberseguridad. UNAD - Curso administración y gestión del riesgo.

Seguido a la evaluación de las dimensiones, se procede a responder cada una de las preguntas que hacen parte de los atributos que establece la norma ISO/IEC 27001:2013, las preguntas son:

- ¿Es activo de información de terceros o de clientes que debe protegerse?
- Sistema expuesto en internet
- ¿Activo de información que debe ser restringido a un número limitado de empleados?
- Activo de información que debe ser restringido a personas externas
- Activo de información que puede ser alterado o comprometido para fraudes ó corrupción
- Activo de información que es muy crítico para el servicio hacia terceros

A los anteriores atributos se responde SI o NO, esto permite conocer la clasificación de los activos según su valor.

Mediante el uso de la matriz de análisis de riesgos de ciberseguridad, se puede también identificar la clasificación según el impacto de seguridad, es decir, si el

activo de información llega a ser conocido, utilizado o modificado por alguna persona o sistema sin la debida autorización, impactaría negativamente a los sistemas y/o procesos de la organización de manera leve, importante o grave.

Para la valoración cualitativa y cuantitativa de los activos de información del CDA MOTOCENTRO, se sigue utilizando la matriz de análisis de riesgos de ciberseguridad del autor Luis Fernando Zambrano (ver Anexo A hoja AVC, columnas desde la F hasta la T), docente de la UNAD y director del curso Administración y Gestión del Riesgo, dichas valoraciones nos permitirá conocer la valoración del riesgo de cada uno de los activos (ver Anexo A hoja VC columna C).

Como resultado de las valoraciones de activos de información de la empresa objeto de este proyecto, se tienen las siguientes tablas resumen que permiten visualizar de manera general la clasificación de los activos según su valor, según el impacto a la seguridad, así mismo conocer los niveles de riesgos de los activos, de conformidad con la metodología MAGERIT V: 3.0 y el uso del instrumento Matriz de Análisis de Riesgos del ingeniero Luis Fernando Zambrano.

Tabla 4. Clasificación de activos según su valor

Número de activos de clientes o terceros que deben protegerse	61
Activos de información expuestos en internet	47
Activos de información que deben ser restringidos a un número limitado de empleados	72
Número de activos de información que deben ser restringidos a personas externas	74
Activos de información que pueden ser alterados o comprometidos para fraudes o corrupción	70

Número de activos de información que son muy críticos para las operaciones internas	73
Número de activos de información que son muy críticos para el servicio hacia terceros	50

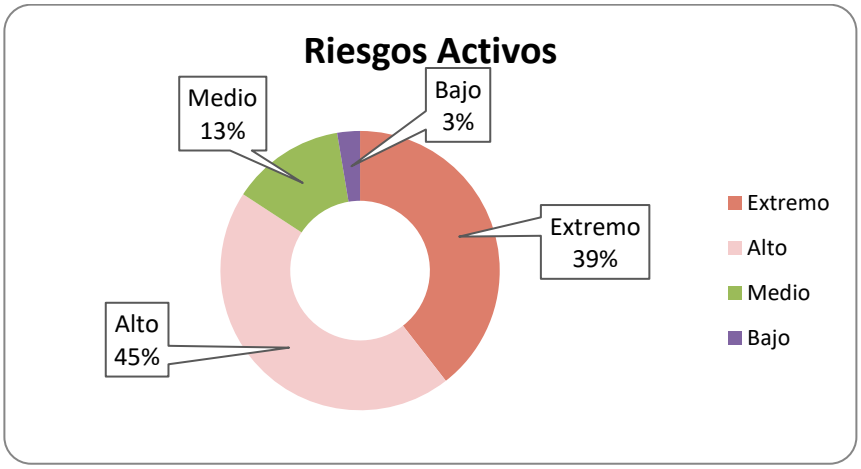
Tabla 5. Clasificación según impacto de seguridad

Leve	10
Importante	57
Grave	9

Tabla 6. Resumen de nivel de riesgo en los activos

NIVEL	CANTIDAD DE ACTIVOS
Extremo	30
Alto	34
Medio	10
Bajo	2

Gráfico 1. Representación porcentual de los riesgos según el nivel



De acuerdo con la identificación de los activos, su propietario, su tipo y su valoración cualitativa, el resultado es el que se evidencia en la Tabla 7.

Tabla 7. Identificación de activos, valoración cualitativa.

No.	DATOS DEL ACTIVO DE INFORMACION			DIMENSION				
	Nombre del activo de información	Propietario del activo	Tipo de Activo	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad
1	[SW] Windows 7 Professional	Abelardo Maldonado Maldonado	SOFTWARE	B	M	MA	MA	MA
2	[SW] Antivirus Avast	Abelardo Maldonado Maldonado	SOFTWARE	B	B	MA	MA	MA
3	[HW] Equipo WorkStation Servidor HP	Abelardo Maldonado Maldonado	HARDWARE	B	B	MA	MA	MA
4	[SW] Cobianbackup	Abelardo Maldonado Maldonado	SOFTWARE	B	B	MA	MA	MA
5	[SW] Linux Server virtualizado	Abelardo Maldonado Maldonado	SOFTWARE	B	B	MA	MA	MA
6	[SW] VirtualBox	Abelardo Maldonado Maldonado	SOFTWARE	MB	MB	MA	MA	MA
7	[HW] Switch TP-Link TL-SG1016D	Abelardo Maldonado Maldonado	HARDWARE	MB	MB	M	M	MA
8	[HW] Router Archer C2	Abelardo Maldonado Maldonado	HARDWARE	MB	MB	MA	MA	MA
9	[HW] DVR DAHUA 8ch	Abelardo Maldonado Maldonado	HARDWARE	MB	MB	MA	MA	MA
10	[SW] Base de datos Mysql 5.7.17	Abelardo Maldonado Maldonado	SOFTWARE	MB	MB	M	M	MA
11	[SW] RTMyEC (INDUCAPK)	Abelardo Maldonado Maldonado	SOFTWARE	MB	MB	MA	MA	MA
12	[SW] AnyDesk	Abelardo Maldonado Maldonado	SOFTWARE	MB	MB	M	M	MA
13	[SW] TeamViewer	Abelardo Maldonado Maldonado	SOFTWARE	MB	MB	MA	MA	MA
14	[HW] Telefono AT&T	Abelardo Maldonado Maldonado	HARDWARE	MB	MB	MA	MA	MA
15	[SW] Windows 10 Profesional 21H2	Victor Manuel Montañez Arandia	SOFTWARE	B	B	MA	MA	MA
16	[SW] Office professional plus 2016	Victor Manuel Montañez Arandia	SOFTWARE	B	B	A	A	A

No.	DATOS DEL ACTIVO DE INFORMACION			DIMENSION				
	Nombre del activo de información	Propietario del activo	Tipo de Activo	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad
17	[HW] Equipo de computo ARGOM	Victor Manuel Montañez Arandia	HARDWARE	B	B	MA	MA	MA
18	[SW] AudiWeb-FirmaFur	Victor Manuel Montañez Arandia	SOFTWARE	MA	B	MA	MA	B
19	[SW] SmartPSS	Victor Manuel Montañez Arandia	SOFTWARE	MA	B	MA	MA	B
20	[SW] RTMyEC (INDUCAPK)	Victor Manuel Montañez Arandia	SOFTWARE	MA	B	MA	MA	B
21	[HW] IMPRESORA 1 Samsung	Victor Manuel Montañez Arandia	HARDWARE	B	B	MA	B	MA
22	[HW] TABLET No 3 Samsung	Victor Manuel Montañez Arandia	HARDWARE	B	B	A	A	MA
23	[SW] Android 6.0.1	Victor Manuel Montañez Arandia	SOFTWARE	B	B	B	MA	MA
24	[K] Firma Digital	Victor Manuel Montañez Arandia	CRIPTOGRAFICAS	B	B	B	MA	MA
25	[HW] Telefono AT&T	Victor Manuel Montañez Arandia	HARDWARE	B	B	B	MA	MA
26	[SW] Windows 10 Profesional 21H2	Jhon Jairo Blanco	SOFTWARE	B	M	MA	MA	MA
27	[SW] Office professional plus 2016	Jhon Jairo Blanco	SOFTWARE	B	M	MA	MA	MA
28	[HW] Equipo de computo ARGOM	Jhon Jairo Blanco	HARDWARE	B	B	MA	MA	MA
29	[SW] AudiWeb	Jhon Jairo Blanco	SOFTWARE	B	M	MA	MA	MA
30	[S] hq.runt.com.co	Jhon Jairo Blanco	SERVICIOS	MA	B	MA	MA	A
31	[SW] Supergiros	Jhon Jairo Blanco	SOFTWARE	B	MB	MA	MA	MA
32	[SW] AnyDesk	Jhon Jairo Blanco	SOFTWARE	B	B	MA	MA	MA
33	[SW] RTMyEC (INDUCAPK)	Jhon Jairo Blanco	SOFTWARE	MA	B	MA	MA	B
34	[SW] AnyDesk	Jhon Jairo Blanco	SOFTWARE	B	B	MA	MA	MA
35	[SW] SmartPSS	Jhon Jairo Blanco	SOFTWARE	B	B	MA	MA	MA
36	[HW] IMPRESORA 3 Canon	Jhon Jairo Blanco	HARDWARE	B	M	MA	MA	MA
37	[K] Firma Digital	Jhon Jairo Blanco	CRIPTOGRAFICAS	B	B	MA	MA	MA
38	[HW] Telefono AT&T Base	Jhon Jairo Blanco	HARDWARE	B	M	MA	MA	MA
39	[SW] Windows 10 Profesional 21H2	Zulay Calderon Velandia	SOFTWARE	A	A	A	A	A
40	[SW] Office professional plus 2016	Zulay Calderon Velandia	SOFTWARE	A	A	A	A	A
41	[HW] Equipo de computo JANUS - Administrativo	Zulay Calderon Velandia	HARDWARE	B	B	B	B	B
42	[SW] AudiWeb	Zulay Calderon Velandia	SOFTWARE	A	A	A	A	A
43	[S] hq.runt.com.co	Zulay Calderon Velandia	SERVICIOS	B	B	A	MA	B
44	[SW] Supergiros	Zulay Calderon Velandia	SOFTWARE	A	B	MA	MA	A
45	[SW] AnyDesk	Zulay Calderon Velandia	SOFTWARE	B	B	A	A	MA
46	[SW] RTMyEC (INDUCAPK)	Zulay Calderon Velandia	SOFTWARE	MA	B	MA	MA	B
47	[SW] AnyDesk	Zulay Calderon Velandia	SOFTWARE	A	A	A	A	A
48	[SW] SmartPSS	Zulay Calderon Velandia	SOFTWARE	A	A	A	A	A
49	[HW] IMPRESORA 2 Samsung	Zulay Calderon Velandia	HARDWARE	B	B	B	B	B
50	[HW] FRENOMETRO	Jorge Andres Pineda	HARDWARE	A	A	A	A	A
51	[HW] ALINEADOR DE LUCES	Jorge Andres Pineda	HARDWARE	B	B	A	MA	B
52	[HW] SONOMETRO	Jorge Andres Pineda	HARDWARE	A	B	MA	MA	A
53	[HW] ANALIZADOR4T	Jorge Andres Pineda	HARDWARE	B	B	A	A	MA
54	[HW] ANALIZADOR2T	Jorge Andres Pineda	HARDWARE	B	MA	B	MA	B

No.	DATOS DEL ACTIVO DE INFORMACION			DIMENSION				
	Nombre del activo de información	Propietario del activo	Tipo de Activo	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad
55	[HW] TERMOHIGROMETRO	Jorge Andres Pineda	HARDWARE	A	A	A	A	A
56	[HW] TERMOHIGROMETRO RESPALDO	Jorge Andres Pineda	HARDWARE	B	B	A	MA	B
57	[HW] PROFUNDIMETRO PF 011	Jorge Andres Pineda	HARDWARE	A	B	MA	MA	A
58	[HW] PROFUNDIMETRO PF 012	Jorge Andres Pineda	HARDWARE	B	B	A	A	MA
59	[HW] MANOMETRO	Jorge Andres Pineda	HARDWARE	B	MA	B	MA	B
60	[HW] CUENTA REVOLUCIONES	Jorge Andres Pineda	HARDWARE	B	MA	B	MA	B
61	[HW] TABLET No 1 Samsung	Jorge Andres Pineda	HARDWARE	A	A	A	A	A
62	[HW] TABLET No 2 Samsung	Jorge Andres Pineda	HARDWARE	B	B	A	MA	B
63	[HW] TABLET No 4 Samsung	Jorge Andres Pineda	HARDWARE	A	B	MA	MA	A
64	[HW] HCO (Tarjeta Desarrollo Beaglebone) GASES	Jorge Andres Pineda	HARDWARE	B	B	A	A	MA
65	[HW] HCO (Tarjeta Desarrollo Beaglebone) FRENOMETRO	Jorge Andres Pineda	HARDWARE	B	MA	B	MA	B
66	[HW] HCO (Tarjeta Desarrollo Beaglebone) LUXOMETRO	Jorge Andres Pineda	HARDWARE	B	B	A	A	MA
67	[SW] LINUX ubuntu	Jorge Andres Pineda	SOFTWARE	B	MA	B	MA	B
68	[SW] LINUX ubuntu	Jorge Andres Pineda	SOFTWARE	B	B	A	A	MA
69	[SW] LINUX ubuntu	Jorge Andres Pineda	SOFTWARE	B	MA	B	MA	B
70	[SW] Android 6.0.1	Jorge Andres Pineda	SOFTWARE	B	B	A	A	MA
71	[SW] Android 6.0.1	Jorge Andres Pineda	SOFTWARE	B	MA	B	MA	B
72	[SW] Android 10	Jorge Andres Pineda	SOFTWARE	B	B	A	A	MA
73	[HW] Telefono AT&T	Jorge Andres Pineda	HARDWARE	B	MA	B	MA	B
74	[SW] APP Pista	Jorge Andres Pineda	SOFTWARE	B	B	A	A	MA
75	[SW] APP Pre-revision	Jorge Andres Pineda	SOFTWARE	B	MA	B	MA	B
76	[SW] APP Servicio	Jorge Andres Pineda	SOFTWARE	B	B	A	A	MA

Fuente: elaboración propia a partir del instrumento matriz de análisis de riesgos de ciberseguridad

A continuación, se evidencia el resultado obtenido de la valoración cuantitativa de conformidad con la valoración cualitativa anterior y de acuerdo con la tabla de valoración del riesgo, la ISO 27001:2013 y la metodología MAGERIT V: 3.0.

Tabla 8. Valoración cuantitativa de los activos de información

No	NOMBRE	RIESGO	AUTENTICIDAD	TRAZABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR
1	[SW] Windows 7 Professional	IMPORTANTE	9	15	25	25	25	20
2	[SW] Antivirus Avast	IMPORTANTE	9	9	25	25	25	19
3	[HW] Equipo WorkStation Servidor HP	IMPORTANTE	9	9	25	25	25	19
4	[SW] Cobianbackup	IMPORTANTE	9	9	25	25	25	19
5	[SW] Linux Server virtualizado	IMPORTANTE	9	9	25	25	25	19
6	[SW] VirtualBox	IMPORTANTE	4	4	25	25	25	17
7	[HW] Switch TP-Link TL-SG1016D	APRECIABLE	4	4	15	15	25	13
8	[HW] Router Archer C2	IMPORTANTE	4	4	25	25	25	17
9	[HW] DVR DAHUA 8ch	IMPORTANTE	4	4	25	25	25	17
10	[SW] Base de datos Mysql 5.7.17	APRECIABLE	4	4	15	15	25	13
11	[SW] RTMyEC (INDUCAPK)	IMPORTANTE	4	4	25	25	25	17
12	[SW] AnyDesk	APRECIABLE	4	4	15	15	25	13
13	[SW] TeamViewer	IMPORTANTE	4	4	25	25	25	17
14	[HW] Telefono AT&T	IMPORTANTE	4	4	25	25	25	17
15	[SW] Windows 10 Profesional 21H2	IMPORTANTE	9	9	25	25	25	19
16	[SW] Office professional plus 2016	IMPORTANTE	9	9	20	20	20	16
17	[HW] Equipo de computo ARGOM	IMPORTANTE	9	9	25	25	25	19
18	[SW] AudiWeb-FirmaFur	IMPORTANTE	25	9	25	25	9	19
19	[SW] SmartPSS	IMPORTANTE	25	9	25	25	9	19
20	[SW] RTMyEC (INDUCAPK)	IMPORTANTE	25	9	25	25	9	19
21	[HW] IMPRESORA 1 Samsung	APRECIABLE	9	9	25	9	25	15
22	[HW] TABLET No 3 Samsung	IMPORTANTE	9	9	20	20	25	17
23	[SW] Android 6.0.1	APRECIABLE	9	9	9	25	25	15
24	[K] Firma Digital	APRECIABLE	9	9	9	25	25	15
25	[HW] Telefono AT&T	APRECIABLE	9	9	9	25	25	15
26	[SW] Windows 10 Profesional 21H2	IMPORTANTE	9	15	25	25	25	20

No	NOMBRE	RIESGO	AUTENTICIDAD	TRAZABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR
27	[SW] Office professional plus 2016	IMPORTANTE	9	15	25	25	25	20
28	[HW] Equipo de computo ARGOM	IMPORTANTE	9	9	25	25	25	19
29	[SW] AudiWeb	IMPORTANTE	9	15	25	25	25	20
30	[S] hq.runt.com.co	CRITICO	25	9	25	25	20	21
31	[SW] Supergiros	IMPORTANTE	9	4	25	25	25	18
32	[SW] AnyDesk	IMPORTANTE	9	9	25	25	25	19
33	[SW] RTMyEC (INDUCAPK)	IMPORTANTE	25	9	25	25	9	19
34	[SW] AnyDesk	IMPORTANTE	9	9	25	25	25	19
35	[SW] SmartPSS	IMPORTANTE	9	9	25	25	25	19
36	[HW] IMPRESORA 3 Canon	IMPORTANTE	9	15	25	25	25	20
37	[K] Firma Digital	IMPORTANTE	9	9	25	25	25	19
38	[HW] Telefono AT&T Base	IMPORTANTE	9	15	25	25	25	20
39	[SW] Windows 10 Profesional 21H2	IMPORTANTE	20	20	20	20	20	20
40	[SW] Office professional plus 2016	IMPORTANTE	20	20	20	20	20	20
41	[HW] Equipo de computo JANUS - Administrativo	BAJO	9	9	9	9	9	9
42	[SW] AudiWeb	IMPORTANTE	20	20	20	20	20	20
43	[S] hq.runt.com.co	APRECIABLE	9	9	20	25	9	14
44	[SW] Supergiros	IMPORTANTE	20	9	25	25	20	20
45	[SW] AnyDesk	IMPORTANTE	9	9	20	20	25	17
46	[SW] RTMyEC (INDUCAPK)	IMPORTANTE	25	9	25	25	9	19
47	[SW] AnyDesk	IMPORTANTE	20	20	20	20	20	20
48	[SW] SmartPSS	IMPORTANTE	20	20	20	20	20	20
49	[HW] IMPRESORA 2 Samsung	BAJO	9	9	9	9	9	9
50	[HW] FRENOMETRO	IMPORTANTE	20	20	20	20	20	20
51	[HW] ALINEADOR DE LUCES	APRECIABLE	9	9	20	25	9	14
52	[HW] SONOMETRO	IMPORTANTE	20	9	25	25	20	20
53	[HW] ANALIZADOR4T	IMPORTANTE	9	9	20	20	25	17
54	[HW] ANALIZADOR2T	APRECIABLE	9	25	9	25	9	15
55	[HW] TERMOHIGROMETRO	IMPORTANTE	20	20	20	20	20	20
56	[HW] TERMOHIGROMETRO RESPALDO	APRECIABLE	9	9	20	25	9	14
57	[HW] PROFUNDIMETRO PF 011	IMPORTANTE	20	9	25	25	20	20
58	[HW] PROFUNDIMETRO PF 012	IMPORTANTE	9	9	20	20	25	17

No	NOMBRE	RIESGO	AUTENTICIDAD	TRAZABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR
59	[HW] MANOMETRO	APRECIABLE	9	25	9	25	9	15
60	[HW] CUENTA REVOLUCIONES	APRECIABLE	9	25	9	25	9	15
61	[HW] TABLET No 1 Samsung	IMPORTANTE	20	20	20	20	20	20
62	[HW] TABLET No 2 Samsung	APRECIABLE	9	9	20	25	9	14
63	[HW] TABLET No 4 Samsung	IMPORTANTE	20	9	25	25	20	20
64	[HW] HCO (Tarjeta Desarrollo Beaglebone) GASES	IMPORTANTE	9	9	20	20	25	17
65	[HW] HCO (Tarjeta Desarrollo Beaglebone) FRENOMETRO	APRECIABLE	9	25	9	25	9	15
66	[HW] HCO (Tarjeta Desarrollo Beaglebone) LUXOMETRO	IMPORTANTE	9	9	20	20	25	17
67	[SW] LINUX ubuntu	APRECIABLE	9	25	9	25	9	15
68	[SW] LINUX ubuntu	IMPORTANTE	9	9	20	20	25	17
69	[SW] LINUX ubuntu	APRECIABLE	9	25	9	25	9	15
70	[SW] Android 6.0.1	IMPORTANTE	9	9	20	20	25	17
71	[SW] Android 6.0.1	APRECIABLE	9	25	9	25	9	15
72	[SW] Android 10	IMPORTANTE	9	9	20	20	25	17
73	[HW] Telefono AT&T	APRECIABLE	9	25	9	25	9	15
74	[SW] APP Pista	IMPORTANTE	9	9	20	20	25	17
75	[SW] APP Pre-revision	APRECIABLE	9	25	9	25	9	15
76	[SW] APP Servicio	IMPORTANTE	9	9	20	20	25	17

Fuente: elaboración propia a partir del instrumento matriz de análisis de riesgos de ciberseguridad

6.3 PLAN DE TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD PARA LOS ACTIVOS DE INFORMACIÓN DEL CDA MOTOCENTRO S.A.S.

6.3.1 Declaración de aplicabilidad - SoA

Previo a establecer un plan de tratamiento sobre los riesgos de seguridad identificados sobre los activos de información de la empresa objetivo de este proyecto, se debe realizar la declaración de aplicabilidad o SoA, como comúnmente se conoce por sus siglas en ingles SoA - Statement of Applicability, de los diferentes

controles de seguridad de acuerdo con la ISO 27001:2013 necesarios para la gestión de riesgos.

Tabla 9. Declaración de aplicabilidad – SoA

ISO 27001:2013 Controles de Seguridad				Control seleccionado Si/No	Razón de la selección	Control implementado Si/No	Justificación de exclusión	Comentarios (visión general de la implementación)
Cláusula	**Sección**	**Objetivo de control**	**Control**					
5. Políticas de Seguridad	5.1	Dirección de la alta gerencia para la seguridad de la información						
Objetivo: Brindar orientación y soporte, por parte de la dirección, de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes	5.1.1	Políticas de seguridad de la información	Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes interesadas	Sí	La empresa cuenta con política de seguridad de la información establecida en su Sistema de Gestión de Calidad	SI		
	5.1.2	Revisión de las políticas de seguridad de la información	Las políticas para Seguridad de la Información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su idoneidad, adecuación y eficacia continúas	Sí	La empresa cuenta con política de seguridad de la información, sin embargo no se realiza una revisión periodica.	No		Revisar la política de seguridad de la información cada periodo de tiempo o cuando se presenten cambios importantes.
6. Organización de la Seguridad de la Información	6.1	Organización interna						
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementaci	6.1.1	Roles y responsabilidad de seguridad de la información	Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	Sí	No se encuentran definidos.	No		Creación de roles y responsablidades.

ISO 27001:2013 Controles de Seguridad				Control seleccionado Si/No	Razón de la selección	Control implementado Si/No	Justificación de exclusión	Comentarios (visión general de la implementación)
Cláusula	Sección	Objetivo de control	Control					
ón y la operación de la seguridad de la información dentro de la organización.	6.1.2	Separación de deberes	Las tareas y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional o el uso indebido de los activos de la organización	Sí	Se debe establecer muy bien los procesos y procedimientos para definir los límites de los usuarios respecto a los activos. Adicional en los computadores no se tienen definidos usuarios.	No		Creación de usuario de red personal para cada empleado.
	6.1.3	Contacto con autoridades	Se debe mantener contactos apropiados con las autoridades pertinentes.	Sí	No se cuenta con un directorio en caso de consultas, incidentes y emergencias relacionadas con la seguridad de la información.	No		Realizar una lista de contactos de las diferentes autoridades a nivel de seguridad de la información.
	6.1.4	Contacto con grupos de interés especial	Se deben mantener controles apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad	Sí	No hay contacto con autoridades relacionadas con la seguridad de la información y ciberseguridad.	No		El encargado de seguridad TI deberá tener contacto con las autoridades de ciberseguridad de la región y del país.
	6.1.5	Seguridad de la información en la gestión de proyectos	La seguridad de la información se debe tratar en la gestión de proyectos, independiente del tipo de proyecto.	Sí	No existe.	No		Solicitar en los contratos tecnológicos la identificación de los riesgos.
	6.2	Dispositivos móviles y teletrabajo						

ISO 27001:2013 Controles de Seguridad				Control seleccionado Si/No	Razón de la selección	Control implementado Si/No	Justificación de exclusión	Comentarios (visión general de la implementación)
Cláusula	**Sección**	**Objetivo de control**	**Control**					
Objetivo: Garantizar la seguridad del teletrabajo y el uso de los dispositivos moviles	6.2.1	Política de dispositivos móviles	Se deben adoptar una política unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	Sí	No existe.	No		División de las redes inalámbricas entre el área operativa y los visitantes. Diseñar política del uso de dispositivos móviles.
	6.2.2	Teletrabajo	Se deben implementar una política y medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo	No	No se realiza actividades de Teletrabajo		Actividades no realizadas	
7 Seguridad en los Recursos Humanos	7.1	Previo al empleo						
Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.	7.1.1	Verificación de antecedentes	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.	Sí	No se lleva a cabo una verificación de antecedentes a los candidatos.	No		Crear una política de Talento Humano y procedimiento de selección de personal, que permita realizar la valoración de antecedentes de acuerdo con la ley, durante el proceso de preselección de los empleados de la organización.

ISO 27001:2013 Controles de Seguridad				Control seleccionado Si/No	Razón de la selección	Control implementado Si/No	Justificación de exclusión	Comentarios (visión general de la implementación)
Cláusula	Sección	Objetivo de control	Control					
Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan**.**	7.1.2	Términos y condiciones del empleo	Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a seguridad de la información	Sí	Los empleados y contratistas firman acuerdo de confidencialidad, de conformidad con lo indicado en el Manual de Calidad Sección 2 - información corporativa	Si		Garantizar la firma del acuerdo de confidencialidad
	7.2	Durante el empleo						
	7.2.1	Responsabilidades de la Alta Gerencia	La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos de la organización.	Sí	Se debe fortalecer la politica de seguridad de la información establecida en la empresa para que se incluya compromisos tanto de la gerencia como los empleados en torno a mejorar la seguridad.	No		Diseñar un documento que contenga los diferentes compromisos de la seguridad de la información para que sea firmado por todos los colaboradores de la organización.
	7.2.2	Conciencia, educación y entrenamiento de seguridad de la información	Todos los empleados de la organización y donde sea pertinente, los contratistas deben recibir educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo	Sí	No existe capacitación a los colaboradores sobre seguridad de la información.	No		Mediante campañas de sensibilización en seguridad de la información, se capacitará a todos los empleados y contratistas de la organización.

ISO 27001:2013 Controles de Seguridad				Control seleccionado Si/No	Razón de la selección	Control implementado Si/No	Justificación de exclusión	Comentarios (visión general de la implementación)
Cláusula	Sección	Objetivo de control	Control					
	7.2.3	Proceso disciplinario	Se debe contar con un proceso formal y comunicado para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	Sí	Se tiene claro desde la política de seguridad de la información, la responsabilidad en caso de incumplimiento de dicha política, sin embargo, se requiere definir un procedimiento disciplinario para las faltas a nivel de seguridad de la información.	No		Establecer un procedimiento disciplinario a seguir relacionado con el incumplimiento de las normas establecidas en la empresa en lo que concierne a la seguridad de la información, de acuerdo con la normatividad vigente.
	7.3	Terminación y cambio de empleo						
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo	7.3.1	Termino de responsabilidades o cambio de empleo	Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben redefinir, comunicar al empleado o contratista y se deben hacer cumplir.	Sí		Si		Se tiene establecido un acuerdo de confidencialidad que lo debe firmar tanto empleados como contratistas de la empresa, donde también se establece que una vez no exista vínculo con la empresa se debe mantener la reserva de la información organizacional.
8 Gestión de Activos	8.1	Responsabilidad de los activos						

ISO 27001:2013 Controles de Seguridad				Control seleccionado Si/No	Razón de la selección	Control implementado Si/No	Justificación de exclusión	Comentarios (visión general de la implementación)
Cláusula	Sección	Objetivo de control	Control					
Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección adecuadas.	8.1.1	Inventario de activos	Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos	Sí		Sí		Con el desarrollo de este proyecto aplicado, se realiza el levantamiento del inventario de activos de información del área de TI de la empresa y se documenta.
	8.1.2	Propiedad de activos	Los activos mantenidos en el inventario deben ser propios.	Sí		Sí		Dentro del inventario de activos de información realizado, se establece el propietario del activo relacionado.
	8.1.3	Uso aceptable de los activos	Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	Sí	En la politica de seguridad establecida por la empresa, se define el compromiso del uso responsable de los equipos e información de la organización, sin embargo, se debe ampliar el alcance a todos los activos de información.	No		Establecer un acta de entrega a los propietarios de los activos de información dentro de la organización, donde se defina su uso responsable.

ISO 27001:2013 Controles de Seguridad				Control seleccionado Si/No	Razón de la selección	Control implementado Si/No	Justificación de exclusión	Comentarios (visión general de la implementación)
Cláusula	Sección	Objetivo de control	Control					
	8.1.4	Devolución de activos	Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	Sí		No		Se dispondrá dentro de la política de seguridad de información que todo empleado que labore para la empresa al terminar su contrato debe devolver los activos en las condiciones iniciales.
	8.2	Clasificación de la información						
Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.	8.2.1	Clasificación de la información	La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	Sí	No existe la clasificación de la información.	No		Se debe establecer una política de clasificación de la información en la cual se detalle según los diferentes criterios de acuerdo con la criticidad y susceptibilidad a modificación o divulgación no autorizada.
	8.2.2	Etiquetado de la información	Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	Sí	No existe un procedimiento para el etiquetado de la información	No		Cuando se establezca la política de clasificación de la información se debe incluir el procedimiento para etiquetar la información de acuerdo con su criticidad en: pública, uso interno, restringida y confidencial.

ISO 27001:2013 Controles de Seguridad				Control seleccionado Si/No	Razón de la selección	Control implementado Si/No	Justificación de exclusión	Comentarios (visión general de la implementación)
Cláusula	Sección	Objetivo de control	Control					
	8.2.3	Manejo de activos	Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	Sí	No existe un procedimiento para el manejo de activos	No		Se debe establecer una adecuada clasificación y manejo de los activos de información dejando todo documentado. Adicionalmente se debe implementar el uso del directorio activo con el fin de restringir el acceso a la información y de acuerdo a las funciones de cada cargo se dará los privilegios estrictamente necesarios.
	8.3	Manejo de medios						
Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios	8.3.1	Gestión de medios removibles	Se deben implementar procedimientos para la gestión de medio removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	Sí	No existe un procedimiento para la gestión de medios removibles	No		Se dispondrá dentro de las políticas de seguridad de la información, el bloqueo de los puertos de los equipos de escritorio y portátiles que hacen parte de la empresa.
	8.3.2	Eliminación de medios	Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	Sí		No		Se dispondrá dentro de las políticas de seguridad de la información, la eliminación segura de la información según el tipo del medio.

ISO 27001:2013 Controles de Seguridad				Control seleccionado Si/No	Razón de la selección	Control implementado Si/No	Justificación de exclusión	Comentarios (visión general de la implementación)
Cláusula	Sección	Objetivo de control	Control					
	8.3.3	Transporte de medios físicos	Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	Sí		No		Cuando se requiera el traslado de información en físico, este contará según el tipo del medio, de cifrado con llave pública o el envío por correo certificado si la información es documentación por escrito.
9 Control de Acceso	9.1	Requerimientos de negocio para el control de acceso						
Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.	9.1.1	Política de control de acceso	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.	Sí		Si		La empresa cuenta con política de control de acceso, se debe garantizar su cumplimiento.
	9.1.2	Acceso a redes y servicios de red	Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	Sí		No		Se otorgará los permisos de acceso a la red según el rol y las funciones del cargo.
	9.2	Gestión de accesos de usuario						

ISO 27001:2013 Controles de Seguridad				Control seleccionado Si/No	Razón de la selección	Control implementado Si/No	Justificación de exclusión	Comentarios (visión general de la implementación)
Cláusula	Sección	Objetivo de control	Control					
Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.	9.2.1	Registro y baja del usuario	Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	Sí	No se cuenta con un proceso para el registro y baja de usuarios.	No		Se debe fortalecer la política de control acceso donde se establezca el registro de nuevos usuarios y el de baja para personal que se retira de la empresa.
	9.2.2	Provisión de acceso a usuarios	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.	Sí		No		Dentro de la política de control de acceso se establecerá los accesos necesarios por cada rol asignado, cambio de permisos al cambiar de funciones y deshabilitación en periodos de vacaciones o similares.
	9.2.3	Gestión de derechos de acceso privilegiados	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	Sí		No		Se fortalecerá la política de control de acceso para que solo los administradores del sistema y los soportes TI tengan privilegios de administrador sobre los equipos.
	9.2.4	Gestión de información de autenticación secreta de usuarios	La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	Sí		No		Dentro de la política de control de acceso, se establecerá que las credenciales de cada usuario tendrán una vigencia de 45 días y su cambio es obligatorio al

ISO 27001:2013 Controles de Seguridad				Control seleccionado Si/No	Razón de la selección	Control implementado Si/No	Justificación de exclusión	Comentarios (visión general de la implementación)
Cláusula	Sección	Objetivo de control	Control					
								caducar, esto se realizará desde la gestión de usuarios.
	9.2.5	Revisión de derechos de acceso de usuarios	Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	Sí		No		Se llevará el control de los usuarios a través de la gestión de usuarios y se tendrán actualizados los permisos según el rol establecido.
	9.2.6	Eliminación o ajuste de derechos de acceso	Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	Sí		No		Se llevará el control de los usuarios a través de la gestión de usuarios y se harán los ajustes requeridos.
	9.3	Responsabilidades del usuario						
Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.	9.3.1	Uso de información de autenticación secreta	Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	Sí		Si		Se harán campañas para la sensibilización del buen uso de las contraseñas de los sistemas, de conformidad con la política de contraseñas establecida por la empresa.

ISO 27001:2013 Controles de Seguridad				Control seleccionado Si/No	Razón de la selección	Control implementado Si/No	Justificación de exclusión	Comentarios (visión general de la implementación)
Cláusula	Sección	Objetivo de control	Control					
	9.4	Control de acceso de sistemas y aplicaciones						
Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.	9.4.1	Restricción de acceso a la información	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	Sí		No		Dentro de la política de control de acceso, se restringirá el acceso a la información a través de la gestión de usuarios.
	9.4.2	Procedimientos de inicio de sesión seguro	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	Sí	En la política de control de acceso establecida por la empresa, está definido un máximo de tres intentos infructuosos para inactivar el usuario.	Si		Garantizar el cumplimiento de la política de control de acceso
	9.4.3	Sistema de gestión de contraseñas	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	Sí		No		Dentro de la política de control de acceso, cada plataforma o programa tendrá su usuario y contraseña la cual solicitará al ingresar.
	9.4.4	Uso de programas y utilidades privilegiadas	Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	Sí		No		Dentro de la política de seguridad de la información, se limitará el uso de los programas a los que estén aprobados por la gerencia, solo las áreas de soporte tendrán privilegios de

ISO 27001:2013 Controles de Seguridad				Control seleccionado Si/No	Razón de la selección	Control implementado Si/No	Justificación de exclusión	Comentarios (visión general de la implementación)
Cláusula	Sección	Objetivo de control	Control					
								administración sobre los equipos y sistemas.
	9.4.5	Control de acceso al código fuente del programa	Se debe restringir el acceso a los códigos fuente de los programas.	No	Actividades no realizadas	No	La empresa no desarrolla software.	
10 Criptografía	10.1	Controles criptográficos						
Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o la integridad de la información	10.1.1	Política en el uso de controles criptográficos	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	Sí		Sí		Utilización de protocolos seguros cifrados (HTTPS) en la página web de la empresa.
	10.1.2	Gestión de llaves	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.	Sí		No		Fortalecer la política de seguridad de la información, donde se incluya el uso, protección y duración de las llaves criptográficas.
11 Seguridad Física y del Entorno	11.1	Áreas seguras						
Objetivo: Prevenir el acceso físico no autorizado, el daño e la interferencia a la información y a las instalaciones	11.1.1	Perímetro de seguridad físico	Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o critica, e instalaciones	Sí		Si		Monitoreo por un CCTV y sistema de alarma para el acceso a la empresa.

ISO 27001:2013 Controles de Seguridad				Control seleccionado Si/No	Razón de la selección	Control implementado Si/No	Justificación de exclusión	Comentarios (visión general de la implementación)
Cláusula	Sección	Objetivo de control	Control					
de procesamiento de información de la organización.			de manejo de información.					
	11.1.2	Controles físicos de entrada	Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	Sí		No		Se debe implementar un registro de visitas o acceso al rack de comunicaciones en bitácoras.
	11.1.3	Seguridad de oficinas, habitaciones y facilidades	Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.	Sí		No		Acceso restringido al público al área de TI, se solicita autorización de ingreso a la persona encargada.
	11.1.4	Protección contra amenazas externas y del ambiente	Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	Sí	La empresa cuenta con protección contra incendios (sensores y extintores), protección eléctrica, sin embargo, se deben implementar medidas en caso de inundación, las cuales no están controladas.	No		Diseño del plan de emergencias

ISO 27001:2013 Controles de Seguridad				Control seleccionado Si/No	Razón de la selección	Control implementado Si/No	Justificación de exclusión	Comentarios (visión general de la implementación)
Cláusula	Sección	Objetivo de control	Control					
	11.1.5	Trabajo en áreas seguras	Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	Sí		No		Restricción de equipos de fotografía y vídeo a áreas restringidas, control de ingreso de dispositivos electrónicos como tabletas, portátiles, teléfonos y dispositivos de almacenamiento.
	11.1.6	Áreas de entrega y carga	Se deben controlar los puntos de acceso tales como las áreas de despacho y carga y otros puntos por donde pueden entrar personas no autorizadas y, si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	Sí		No		Inspección de ingreso y salida de personas, vehículos y elementos.
	11.2	Equipo						
Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.	11.2.1	Instalación y protección de equipo	Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	Sí		No		Elaboración de plan de contingencia y emergencia.
	11.2.2	Servicios de soporte	Los equipos se deben proteger contra fallas de energía y otras interrupciones	Sí		Si		Se cuenta con instalación de UPS y sistema de corriente regulada.

ISO 27001:2013 Controles de Seguridad				Control seleccionado Si/No	Razón de la selección	Control implementado Si/No	Justificación de exclusión	Comentarios (visión general de la implementación)
Cláusula	Sección	Objetivo de control	Control					
			causadas por fallas en los servicios de suministro.					
	11.2.3	Seguridad en el cableado	El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.	Sí		No		Sistema de administración de la red, se bloquean puertos y puntos de red no usados.
	11.2.4	Mantenimiento de equipos	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Sí		Si		Se cuenta con procedimiento de mantenimiento a los equipos de cómputo, impresoras, equipos servidor, se registra el mantenimiento en la hoja de vida del equipo.
	11.2.5	Retiro de activos	Los equipos, información o software no se deben retirar de su sitio sin autorización previa	Sí		No		Todos los activos tanto de software como de hardware deberán estar aprobados por el Director de TI y del Gerente.
	11.2.6	Seguridad del equipo y activos fuera de las instalaciones	Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los	No		No	No se cuenta con equipos y/o activos por fuera de la empresa.	No se podrá retirar los equipos de cómputo de la oficina.

ISO 27001:2013 Controles de Seguridad				Control seleccionado Si/No	Razón de la selección	Control implementado Si/No	Justificación de exclusión	Comentarios (visión general de la implementación)
Cláusula	Sección	Objetivo de control	Control					
			diferentes riesgos de trabajar fuera de dichas instalaciones.					
	11.2.7	Eliminación segura o reuso del equipo	Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición o reúso.	Sí		No		Se eliminará de forma segura la información que se encuentre en los equipos cuando sean dados de baja o cuando se vaya a asignar de nuevo.
	11.2.8	Equipo de usuario desatendido	Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	Sí		No		A través de la configuración se dispondrá de bloqueo de equipo por inactividad.
	11.2.9	Política de escritorio limpio y pantalla limpia	Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	Sí		No		Fortalecer la política de seguridad de la información, para incluir el no uso del escritorio para guardar documentación ni dejar visible los accesos a las aplicaciones.
12 Seguridad en las Operaciones	12.1	Procedimientos Operacionales y Responsabilidades						

ISO 27001:2013 Controles de Seguridad				Control seleccionado Si/No	Razón de la selección	Control implementado Si/No	Justificación de exclusión	Comentarios (visión general de la implementación)
Cláusula	Sección	Objetivo de control	Control					
Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.	12.1.1	Documentación de procedimientos operacionales	Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.	Sí		No		Se debe documentar los procesos más relevantes, mantenimiento de equipos, copias de seguridad, manejo de medios, entre otros y publicar en un sitio controlado.
	12.1.2	Gestión de cambios	Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	Sí		No		Establecer la metodología para la gestión de cambio y llevar un registro de los cambios en los sistemas de información mediante registros y manejo de eventos y logs.
	12.1.3	Gestión de la capacidad	Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	Sí		No		Se realizarán planes para la optimización de los recursos TI y la seguridad de la información.
	12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Se deben separar los ambientes de desarrollo, pruebas y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	No		No	La empresa no desarrolla software.	

ISO 27001:2013 Controles de Seguridad				Control seleccionado Si/No	Razón de la selección	Control implementado Si/No	Justificación de exclusión	Comentarios (visión general de la implementación)
Cláusula	Sección	Objetivo de control	Control					
	12.2	Protección de Software Malicioso						
Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.	12.2.1	Controles contra software malicioso	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.	Sí		Si		Se cuenta con software antimalware con actualizaciones automáticas y escaneo del sistema diario y en tiempo real.
	12.3	Respaldo						
Objetivo: Proteger contra la perdida de datos	12.3.1	Respaldo de información	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.	Sí		No		Se debe establecer una política de backup y restauración, con posibilidad de respaldo en la nube.
	12.4	Bitácoras y monitoreo						
Objetivo: Registrar eventos y generar evidencia	12.4.1	Bitácoras de eventos	Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	Sí		No		Se debe implementar procedimiento para la revisión de los logs de eventos de los usuarios de red y comportamiento de seguridad de la red.
	12.4.2	Protección de información en bitácoras	Las instalaciones y la información de registro se deben proteger contra alteración y	Sí		No		Por medio de la gestión de usuarios se debe controlar el acceso no autorizado.

ISO 27001:2013 Controles de Seguridad				Control seleccionado Si/No	Razón de la selección	Control implementado Si/No	Justificación de exclusión	Comentarios (visión general de la implementación)
Cláusula	Sección	Objetivo de control	Control					
			acceso no autorizado.					
	12.4.3	Bitácoras de administrador y operador	Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	Sí		No		Se mantiene el registro de administradores del sistema.
	12.4.4	Sincronización de relojes	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	Sí		No		Con el controlador de dominio se ajustan todos los relojes del sistema.
	12.5	Control de software operacional						
Objetivo: Asegurarse de la integridad de los sistemas operacionales	12.5.1	Instalación de software en sistemas operacionales	Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	Sí		No		Solo el área de TI podrá realizar instalación de software.
	12.6	Gestión de vulnerabilidades técnicas						

ISO 27001:2013 Controles de Seguridad				Control seleccionado Si/No	Razón de la selección	Control implementado Si/No	Justificación de exclusión	Comentarios (visión general de la implementación)
Cláusula	Sección	Objetivo de control	Control					
Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas	12.6.1	Gestión de vulnerabilidades técnicas	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 medidas apropiadas para tratar el riesgo asociado.	Sí		No		A través del antivirus y las actualizaciones de Windows se gestiona las vulnerabilidades.
	12.6.2	Restricciones en la instalación de software	Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios.	Sí		No		Solo el área de TI podrá realizar instalación de software.
	12.7	Consideraciones de auditoría de sistemas de información						
Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos	12.7.1	Controles de auditoría de sistemas de información	Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	Sí		No		Se debe establecer un plan de auditorías con el fin de no impactar la operación.
13 Seguridad en las Comunicaciones	13.1	Gestión de seguridad en red						

ISO 27001:2013 Controles de Seguridad				Control seleccionado Si/No	Razón de la selección	Control implementado Si/No	Justificación de exclusión	Comentarios (visión general de la implementación)
Cláusula	Sección	Objetivo de control	Control					
Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.	13.1.1	Controles de red	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	Sí		No		Se realizará segmentación de la red. Se debe definir la política de red inalámbrica operativa y red de invitados.
	13.1.2	Seguridad en los servicios en red	Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	Sí		No		Autenticación en la red utilizando el controlador de dominio, registro a la red para la red inalámbrica de invitados. Se debe ver la posibilidad de implementar un firewall.
	13.1.3	Segregación en redes	Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	Sí		No		Se utilizará segmentación de la red a través de VLAN, para aislar la Red de servidor de la red operativa y de visitantes.
	13.2	Transferencia de información						

ISO 27001:2013 Controles de Seguridad				Control seleccionado Si/No	Razón de la selección	Control implementado Si/No	Justificación de exclusión	Comentarios (visión general de la implementación)
Cláusula	Sección	Objetivo de control	Control					
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa**.**	13.2.1	Políticas y procedimientos para la transferencia de información	Se debe contar con políticas, procedimientos y controles de transferencia información formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	Sí		No		Se debe establecer las políticas y procedimientos dentro del SGC de la empresa para garantizar la integridad y confidencialidad de la información, con el fin de restringir la transferencia de información a través de correos no corporativos, y en lo posible hacer uso de métodos o técnicas criptográficas, así como el uso de medios seguros para la transmisión de datos.
	13.2.2	Acuerdos en la transferencia de información	Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.	Sí		No		Se acuerda con los empleados, proveedores, contratista el uso adecuado de la información a través de los medios de transmisión electrónica utilizando canales seguros y cifrados.

ISO 27001:2013 Controles de Seguridad				Control seleccionado Si/No	Razón de la selección	Control implementado Si/No	Justificación de exclusión	Comentarios (visión general de la implementación)
Cláusula	Sección	Objetivo de control	Control					
	13.2.3	Mensajería electrónica	Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	Sí		No		Utilización de mensajería electrónica (corporativa) con cifrado de extremo a extremo y que guarde la política de confidencialidad de la información.
	13.2.4	Acuerdos de confidencialidad o no-revelación	Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	Sí		Si		Se cuenta con acuerdos de confidencialidad que deben ser firmados por empleados, contratistas y proveedores de servicio.
14 Adquisición, Desarrollo y Mantenimiento de Sistemas	14.1	Requerimientos de seguridad en sistemas de información						
Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye	14.1.1	Análisis y especificación de requerimientos de seguridad	Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	Sí		No		Se establece con los contratistas desarrolladores de software la inclusión de mecanismos de seguridad de la información.

ISO 27001:2013 Controles de Seguridad				Control seleccionado Si/No	Razón de la selección	Control implementado Si/No	Justificación de exclusión	Comentarios (visión general de la implementación)
Cláusula	Sección	Objetivo de control	Control					
también los requisitos para sistemas de información que prestan servicios sobre redes.	14.1.2	Aseguramiento de servicios de aplicación en redes públicas	La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	Sí		No		El tráfico de la red se realiza mediante protocolos de transferencia seguros.
	14.1.3	Protección de transacciones en servicios de aplicación	La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	Sí		No		Se utilizará el uso de certificados para las aplicaciones más sensibles.
	14.2	Seguridad en el proceso de desarrollo y soporte						
Objetivo: Asegurar que la seguridad de la información este diseñada e implementada dentro del ciclo de vida	14.2.1	Política de desarrollo seguro	Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.	Sí		No		Se establece con los contratistas desarrolladores de software la aplicación de metodologías de desarrollo seguro.

ISO 27001:2013 Controles de Seguridad				Control seleccionado Si/No	Razón de la selección	Control implementado Si/No	Justificación de exclusión	Comentarios (visión general de la implementación)
Cláusula	Sección	Objetivo de control	Control					
de desarrollo de los sistemas de información.	14.2.2	Procedimientos de control de cambios del sistema	Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.	Sí		No		A través de control de cambios, se establecen el versionamiento de las aplicaciones.
	14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa	Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	Sí		No		Se elabora plan de validación y realización de pruebas cuando se realice algún cambio en los sistemas.
	14.2.4	Restricción de cambios en paquetes de software	Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	Sí		No		Desarrollo seguro de aplicaciones, solo los administradores del sistema podrán realizar cambios.
	14.2.5	Principios de seguridad en la ingeniería de sistemas	Se deben establecer documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de	Sí		No		Acuerdos entre los desarrolladores de software y el área de TI, para que se establecen las políticas de uso de metodologías de desarrollo seguro.

ISO 27001:2013 Controles de Seguridad				Control seleccionado Si/No	Razón de la selección	Control implementado Si/No	Justificación de exclusión	Comentarios (visión general de la implementación)
Cláusula	Sección	Objetivo de control	Control					
			sistemas de información.					
	14.2.6	Entorno de desarrollo seguro	Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	Sí		No		Los desarrolladores solo tendrán acceso a los recursos establecidos para ello, no se le permite el ingreso a los sistemas productivos.
	14.2.7	Desarrollo tercerizado	La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	Sí		No		Se establecerá con los contratistas desarrolladores sobre la propiedad intelectual del software, acuerdos de licenciamiento dentro de los contratos.
	14.2.8	Pruebas de seguridad del sistema	Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.	Sí		No		Antes de la aplicación de nuevas versiones de software, se harán pruebas en ambientes previos.
	14.2.9	Pruebas de aceptación del sistema	Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.	Sí		No		Se harán pruebas antes de la salida a producción.
	14.3	Datos de prueba						

ISO 27001:2013 Controles de Seguridad				Control seleccionado Si/No	Razón de la selección	Control implementado Si/No	Justificación de exclusión	Comentarios (visión general de la implementación)
Cláusula	**Sección**	**Objetivo de control**	**Control**					
Objetivo: Asegurar la protección de los datos usados para pruebas.	14.3.1	Protección de datos de prueba	Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.	Sí		No		Todas las pruebas se harán en los ambientes de desarrollo y ambientes previos
15 Relaciones con Proveedores	15.1	Seguridad de la información en relaciones con el proveedor						
Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.	15.1.1	Política de seguridad de la información en las relaciones con el proveedor	Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.	Sí		No		En la política de seguridad de la información se establece los ANS con los proveedores y contratistas.
	15.1.2	Atención de tópicos de seguridad en los acuerdos con el proveedor	Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	Sí		No		Se estipula los entregables y producto final de acuerdo a los ANS y el manejo de la información.

ISO 27001:2013 Controles de Seguridad				Control seleccionado Si/No	Razón de la selección	Control implementado Si/No	Justificación de exclusión	Comentarios (visión general de la implementación)
Cláusula	Sección	Objetivo de control	Control					
	15.1.3	Cadena de suministros de tecnologías de la información y comunicaciones	Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	Sí		No		Se estipula con los proveedores de servicios tecnológicos los requisitos legales y políticas de seguridad de la información.
	15.2	Gestión de entrega de servicios de proveedor						
Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores	15.2.1	Monitoreo y revisión de servicios del proveedor	Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	Sí		No		Supervisión de los contratos desde el área de TI.
	15.2.2	Gestión de cambios a los servicios del proveedor	Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y las mejoras de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos de negocio involucrados, y la revaluación de los riesgos.	Sí		No		Se establece comité de control de cambios quienes revisarán los contratos con los proveedores.

ISO 27001:2013 Controles de Seguridad				Control seleccionado Si/No	Razón de la selección	Control implementado Si/No	Justificación de exclusión	Comentarios (visión general de la implementación)
Cláusula	**Sección**	**Objetivo de control**	**Control**					
16 Gestión de Incidentes de Seguridad de la Información	16.1	Gestión de incidentes de seguridad de la información y mejoras						
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.	16.1.1	Responsabilidades y procedimientos	Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	Sí		No		Se debe establecer un procedimiento para la gestión de incidentes de seguridad de la información.
	16.1.2	Reporte de eventos de seguridad de la información	Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	Sí		No		Cada incidente de seguridad se documentará y se llevará registro y se dispondrá en un repositorio para su consulta.
	16.1.3	Reporte de debilidades de seguridad de la información	Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	Sí		No		Los reportes se harán al buzón de correo electrónico del área de seguridad de la información.

ISO 27001:2013 Controles de Seguridad				Control seleccionado Si/No	Razón de la selección	Control implementado Si/No	Justificación de exclusión	Comentarios (visión general de la implementación)
Cláusula	Sección	Objetivo de control	Control					
	16.1.4	Valoración y decisión de eventos de seguridad de la información	Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	Sí		No		Se categorizará los eventos de seguridad de acuerdo a los estándares.
	16.1.5	Respuesta a incidentes de seguridad de la información	Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	Sí		No		De acuerdo a los análisis, se dispondrá de las soluciones y controles a los incidentes reportados.
	16.1.6	Aprendizaje de incidentes de seguridad de la información	El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o impacto de incidentes futuros.	Sí		No		Con los incidentes presentados, se crearán la resolución de los incidentes.
	16.1.7	Colección de evidencia	La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	Sí		No		Se realizará una base de datos con las soluciones encontradas en la resolución de los incidentes reportados.

ISO 27001:2013 Controles de Seguridad				Control seleccionado Si/No	Razón de la selección	Control implementado Si/No	Justificación de exclusión	Comentarios (visión general de la implementación)
Cláusula	**Sección**	**Objetivo de control**	**Control**					
17 Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio	17.1	Continuidad de la seguridad de la información						
Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.	17.1.1	Planeación de la continuidad de la seguridad de la información	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.	Sí		No		Se debe diseñar el plan de contingencia para la continuidad del negocio.
	17.1.2	Implementación de la continuidad de la seguridad de la información	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 adversa.	Sí		No		Se debe diseño el plan de contingencia.
	17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementado	Sí		No		Plan de contingencia, se debe tener en cuenta todos los sistemas TI críticos para la operación del negocio.

ISO 27001:2013 Controles de Seguridad				Control seleccionado Si/No	Razón de la selección	Control implementado Si/No	Justificación de exclusión	Comentarios (visión general de la implementación)
Cláusula	Sección	Objetivo de control	Control					
			s, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.					
	17.2	Redundancias						
Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.	17.2.1	Disponibilidad de facilidades de procesamiento de información	Las instalaciones de procesamientos de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	Sí		No		Contemplar tener al menos dos proveedores de servicio de internet y sistema redundante en el servidor principal.
18 Cumplimiento	18.1	Cumplimiento con Requerimientos Legales y Contractuales						
Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.	18.1.1	Identificación de legislación aplicable y requerimientos contractuales	Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.	Sí		No		Aplicación de la norma actual sobre SGSI.

ISO 27001:2013 Controles de Seguridad				Control seleccionado Si/No	Razón de la selección	Control implementado Si/No	Justificación de exclusión	Comentarios (visión general de la implementación)
Cláusula	Sección	Objetivo de control	Control					
	18.1.2	Derechos de propiedad intelectual (IPR)	Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.	Sí		No		Tener todo el software bajo licencia y los programas desarrollados por terceros deben tener la cesión de los derechos de autor sobre el software.
	18.1.3	Protección de registros	Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	Sí		No		Organización de la red para la toma de registros, control sobre los repositorios, y los programas cuentan con logs de auditoría.
	18.1.4	Privacidad y protección de información personal identificable (PIR)	Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige e la legislación y la reglamentación pertinentes, cuando sea aplicable.	Sí		Si		Se encuentra implementada la autorización de tratamiento de datos personales de acuerdo a la ley vigente.
	18.1.5	Regulación de controles criptográficos	Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y	Sí		No		Se usará la criptografía para salvaguardar la información más sensible.

ISO 27001:2013 Controles de Seguridad				Control seleccionado Si/No	Razón de la selección	Control implementado Si/No	Justificación de exclusión	Comentarios (visión general de la implementación)
Cláusula	Sección	Objetivo de control	Control					
			reglamentación pertinentes.					
	18.2	Revisiones de seguridad de la información						
Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.	18.2.1	Revisión independiente de seguridad de la información	El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información), se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	Sí		No		Se dispondrá dentro de la política de seguridad de la información la ejecución de auditoría cada cierto tiempo que se considere oportuno o cada vez que se presente cambios importantes en los sistemas.
	18.2.2	Cumplimiento con políticas y estándares de seguridad	Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro	Sí		No		Se quiere de personal calificado y con conocimientos en las normas de seguridad de la información como ISO/IEC 27000, leyes vigentes al respecto. Tener un asesor en SGSI.

ISO 27001:2013 Controles de Seguridad				Control seleccionado Si/No	Razón de la selección	Control implementado Si/No	Justificación de exclusión	Comentarios (visión general de la implementación)
Cláusula	Sección	Objetivo de control	Control					
			requisito de seguridad.					
	18.2.3	Revisión del cumplimiento técnico	Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	Sí		No		Revisión periódica de los sistemas TI para la ejecución de plan de mejoras en cada área.

Fuente: elaboración propia

Para una mejor visualización y comprensión de la declaración de aplicabilidad de los controles de seguridad del Anexo A de la norma ISO/IEC 27001:2013, se invita a acceder al Anexo A - Matriz Análisis de Riesgos CDA Motocentro.xlsx en la hoja SoA, matriz que hace parte integral de este proyecto aplicado.

6.3.2 Análisis de amenazas

De acuerdo con la metodología empleada para el desarrollo de este proyecto aplicado, que corresponde a MAGERIT V.3, y lo indicado en el numeral 5.2.2 del punto 5.2. METODOLOGÍA DE DESARROLLO del capítulo 5. DISEÑO METOLÓGICO del presente documento, se identificaron las posibles amenazas de los activos de información del área de TI de la empresa CDA MOTOCENTRO S.A.S., según la clasificación (De origen natural, del entorno, defecto de aplicaciones, causadas por las personas de forma accidental, y causadas por las personas de forma deliberada), partiendo de su valoración cualitativa y cuantitativa se realizó la valoración de dichas amenazas según la probabilidad de vulneración y la clasificación de la gestión actual.

De lo anterior se pudo calcular el valor del riesgo neto, la criticidad neta, así como el valor del riesgo y criticidad residuales con el fin de definir el nivel de aceptación del riesgo. El resultado obtenido es la identificación de 153 posibles amenazas de las cuales 5 tienen Nivel Moderado y 145 Nivel Inaceptable, como se puede observar en la siguiente tabla.

Tabla 10. Análisis de amenazas de los activos de información

No. De Amenazas y Vulnerabilidades	Activos de Información	Nombre del activo de información	Valoración del Riesgo de los Activos	Amenazas Metodología MAGERIT	Vulnerabilidades	Niveles de aceptación del .	Probabilidad de vulneración	Cálculo del riesgo neto	Criticidad neta	Calificación de Gestión	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Criticidad residual
1	SOFTWARE	[SW] Windows 7 Professional	20	[I5] Avería de origen físico o lógico	Uso de versión obsoleta de sistema operativo.	I	5	**100**	**C**	**1**		**100**	**C**
2	SOFTWARE	[SW] Windows 7 Professional	20	[I5] Avería de origen físico o lógico	Falta procedimiento de mantenimiento.	I	4	**80**	**C**	**4**	Existe política de mantenimiento de computadores y se encuentra documentado bajo procedimiento de la empresa	**20**	**I**
3	SOFTWARE	[SW] Windows 7 Professional	20	[A6] Abuso de privilegios de acceso	Spyware: CVE-2015-0016: Vulnerabilidad de elevación de privilegios de directorio transversal.	I	5	**100**	**C**	**1**		**100**	**C**
4	SOFTWARE	[SW] Windows 7 Professional	20	[E8] Difusión de software dañino	Spyware: CVE-2010-2568: Vulnerabilidad en Shell de Microsoft Windows.	I	5	**100**	**C**	**1**		**100**	**C**
5	HARDWARE	[HW] Equipo de computo JANUS - Administrativo	9	[I5] Avería de origen físico o lógico	Problemas de mantenimiento.	M	4	**36**	**C**	**4**	Existe política de mantenimiento de computadores y se encuentra documentado bajo procedimiento de la empresa	**9**	**B**
6	HARDWARE	[HW] Equipo de computo JANUS - Administrativo	9	[I5] Avería de origen físico o lógico	Envejecimiento del hardware.	I	4	**36**	**C**	**1**		**36**	**C**
7	HARDWARE	[HW] Equipo de computo JANUS - Administrativo	9	[A11] Acceso no autorizado	Posibilidad de utilizar un acceso oculto.	I	5	**45**	**C**	**1**		**45**	**C**
8	HARDWARE	[HW] Equipo de computo JANUS - Administrativo	9	[A11] Acceso no autorizado	El dispositivo utilizado permite usos diferentes de los previstos.	I	4	**36**	**C**	**1**		**36**	**C**

No. De Amenazas y Vulnerabilidades	Activos de Información	Nombre del activo de información	Valoración del Riesgo de los Activos	Amenazas Metodología MAGERIT	Vulnerabilidades	Niveles de aceptación del .	Probabilidad de vulneración	Cálculo del riesgo neto	Criticidad neta	Calificación de Gestión	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Criticidad residual
9	HARDWARE	[HW] Router Archer C2	17	[I6] Corte del suministro eléctrico	Hardware sensible a las perturbaciones eléctricas.	I	5	**85**	**C**	**1**		**85**	**C**
10	HARDWARE	[HW] Router Archer C2	17	[I6] Corte del suministro eléctrico	Terminal de comunicación que no dispone de alimentación auxiliar.	I	3	**51**	**C**	**1**		**51**	**C**
11	HARDWARE	[HW] Router Archer C2	17	[A26] Ataque destructivo	Falta de hardware de repuesto.	I	3	**51**	**C**	**1**		**51**	**C**
12	HARDWARE	[HW] Router Archer C2	17	[A26] Ataque destructivo	Fragilidad del hardware.	I	4	**68**	**C**	**1**		**68**	**C**
13	SOFTWARE	[SW] Linux Server virtualizado	19	[E19] Fugas de información	CVE-2022-26966: Se descubrió un problema en el kernel de Linux antes del 5.16.12. drivers/net/usb/sr9700.c permite a los atacantes obtener información confidencial de la memoria del montón a través de longitudes de marco manipuladas desde un dispositivo.	I	3	**57**	**C**	**1**		**57**	**C**
14	SOFTWARE	[SW] Linux Server virtualizado	19	[E20] Vulnerabilidades de los programas (software)	CVE-2022-25265: En el kernel de Linux hasta el 5.16.10, ciertos archivos binarios pueden tener el atributo exec-all si se crearon aproximadamente en 2003 (p. ej., con GCC 3.2.2 y el kernel de Linux 2.4.20). Esto puede provocar la ejecución de bytes ubicados en regiones supuestamente no ejecutables de un archivo.	I	3	**57**	**C**	**1**		**57**	**C**

No. De Amenazas y Vulnerabilidades	Activos de Información	Nombre del activo de información	Valoración del Riesgo de los Activos	Amenazas Metodología MAGERIT	Vulnerabilidades	Niveles de aceptación del	Probabilidad de vulneración	Cálculo del riesgo neto	Criticidad neta	Calificación de Gestión	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Criticidad residual
15	SOFTWARE	[SW] Linux Server virtualizado	19	[A6] Abuso de privilegios de acceso	CVE-2022-23276: Vulnerabilidad de elevación de privilegios de contenedores de SQL Server para Linux.	I	3	**57**	**C**	**1**		**57**	
16	SOFTWARE	[SW] Linux Server virtualizado	19	[A6] Abuso de privilegios de acceso	CVE-2022-0646: Se encontró un uso incorrecto después de la liberación en el subsistema del Protocolo de transporte de componentes de administración (MCTP) del kernel de Linux en la forma en que el usuario activa cancel_work_sync después de unregister_netdev durante la eliminación del dispositivo. Un usuario local podría usar esta falla para bloquear el sistema o escalar sus privilegios en el sistema. Es actual desde Linux Kernel 5.17-rc1 (cuando se introdujo mctp-serial.c) hasta 5.17-rc5.	I	3	**57**	**C**	**1**		**57**	**C**
17	SOFTWARE	[SW] Linux Server virtualizado	19	[E21] Errores de mantenimiento / actualización de programas (software)	Averías en los equipos	I	4	**76**	**C**	**1**		**76**	**C**
18	SOFTWARE	[SW] Linux Server virtualizado	19	[I5] Avería de origen físico o lógico	Fuga de información	I	4	**76**	**C**	**1**		**76**	**C**

No. De Amenazas y Vulnerabilidades	Activos de Información	Nombre del activo de información	Valoración del Riesgo de los Activos	Amenazas Metodología MAGERIT	Vulnerabilidades	Niveles de aceptación del .	Probabilidad de vulneración	Cálculo del riesgo neto	Criticidad neta	Calificación de Gestión	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Criticidad residual
19	SOFTWARE	[SW] Linux Server virtualizado	19	[E21] Errores de mantenimiento / actualización de programas (software)	Falla del equipo	I	5	**95**	**C**	**4**	Existe politica de mantenimiento de computadores y se encuentra documentado bajo procedimiento de la empresa	**24**	**C**
20	SOFTWARE	[SW] Linux Server virtualizado	19	[E1] Errores de los usuarios	Fuga de información	I	4	**76**	**C**	**1**		**76**	**C**
21	SOFTWARE	[SW] Linux Server virtualizado	19	[I5] Avería de origen físico o lógico	Averías en los equipos por perdida en el suministro de energía	I	4	**76**	**C**	**3**	La empresa cuenta con UPS sin embargo, falta politica para continuidad del negocio	**25**	**C**
22	SOFTWARE	[SW] Linux Server virtualizado	19	[I5] Avería de origen físico o lógico	Averías en los equipos por Fenómenos meteorológicos y Condiciones medioambientales del Data Center	I	4	**76**	**C**	**1**		**76**	**C**
23	HARDWARE	[HW] Equipo WorkStation Servidor HP	19	[I5] Avería de origen físico o lógico	Problemas de mantenimiento.	I	4	**76**	**C**	**4**	Existe politica de mantenimiento de computadores y se encuentra documentado bajo procedimiento de la empresa	**19**	**I**
24	HARDWARE	[HW] Equipo WorkStation Servidor HP	19	[I5] Avería de origen físico o lógico	Envejecimiento del hardware.	I	4	**76**	**C**	**1**		**76**	**C**
25	HARDWARE	[HW] Equipo WorkStation Servidor HP	19	[A11] Acceso no autorizado	Posibilidad de utilizar un acceso oculto.	I	5	**95**	**C**	**1**		**95**	**C**
26	HARDWARE	[HW] Equipo WorkStation Servidor HP	19	[A11] Acceso no autorizado	El dispositivo utilizado permite usos diferentes de los previstos.	I	4	**76**	**C**	**1**		**76**	**C**
27	HARDWARE	[HW] Switch TP-Link TL-SG1016D	13	[I6] Corte del suministro eléctrico	Hardware sensible a las perturbaciones eléctricas.	I	5	**65**	**C**	**1**		**65**	**C**

No. De Amenazas y Vulnerabilidades	Activos de Información	Nombre del activo de información	Valoración del Riesgo de los Activos	Amenazas Metodología MAGERIT	Vulnerabilidades	Niveles de aceptación del .	Probabilidad de vulneración	Cálculo del riesgo neto	Criticidad neta	Calificación de Gestión	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Criticidad residual
28	HARDWARE	[HW] Switch TP-Link TL-SG1016D	13	[I6] Corte del suministro eléctrico	Terminal de comunicación que no dispone de alimentación auxiliar .	I	3	**39**	**C**	**1**		**39**	**C**
29	HARDWARE	[HW] Switch TP-Link TL-SG1016D	13	[A26] Ataque destructivo	Falta de hardware de repuesto.	I	3	**39**	**C**	**1**		**39**	**C**
30	HARDWARE	[HW] Switch TP-Link TL-SG1016D	13	[A26] Ataque destructivo	Fragilidad del hardware.	I	4	**52**	**C**	**1**		**52**	**C**
31	SOFTWARE	[SW] Antivirus Avast	19	[A6] Abuso de privilegios de acceso	CVE-2022-26522 y CVE-2022-26523: estas vulnerabilidades permiten a los atacantes escalar privilegios que les permiten deshabilitar productos de seguridad, sobrescribir componentes del sistema, corromper el sistema operativo o realizar operaciones maliciosas sin obstáculos.	I	3	**57**	**C**	**1**		**57**	**C**
32	SOFTWARE	[SW] Cobianbackup	19	[A5] Suplantación de la identidad del usuario	CVE-2017-11318: El cliente Cobian Backup versión 11, permite a atacantes de tipo man-in-the-middle agregar y ejecutar nuevas tareas de copia de seguridad cuando el servidor maestro es suplantado. Además, el atacante puede ejecutar comandos del sistema de remotamente mediante la violación de eventos de copia de seguridad previa.	I	4	**76**	**C**	**1**		**76**	**C**
33	SOFTWARE	[SW] Cobianbackup	19	[E15] Alteración accidental de la información	Privilegios inadecuados.	I	3	**57**	**C**	3	Existe política de backup pero no se encuentra documentado no hay control de acceso a los backups.	**19**	**I**

No. De Amenazas y Vulnerabilidades	Activos de Información	Nombre del activo de información	Valoración del Riesgo de los Activos	Amenazas Metodología MAGERIT	Vulnerabilidades	Niveles de aceptación del	Probabilidad de vulneración	Cálculo del riesgo neto	Criticidad neta	Calificación de Gestión	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Criticidad residual
34	SOFTWARE	[SW] Cobianbackup	19	[E2] Errores del administrador	Falta de un control de los procesos críticos.	I	3	**57**	**C**	**3**	Existe política de backup pero no se encuentra documentado.	**19**	**I**
35	SOFTWARE	[SW] VirtualBox	17	[A6] Abuso de privilegios de acceso	CVE-2021-35542: Vulnerabilidad en el producto Oracle VM VirtualBox de Oracle Virtualization (componente: Core). La versión compatible que se ve afectada es anterior a la 6.1.28. La vulnerabilidad fácilmente explotable permite que un atacante con privilegios altos inicie sesión en la infraestructura donde se ejecuta Oracle VM VirtualBox para comprometer Oracle VM VirtualBox. Los ataques exitosos de esta vulnerabilidad pueden resultar en la capacidad no autorizada de provocar un bloqueo o un bloqueo repetible con frecuencia (DOS completo) de Oracle VM VirtualBox	I	4	**68**	**C**	**1**		**68**	**C**
36	SOFTWARE	[SW] VirtualBox	17	[A11] Acceso no autorizado	CVE-2021-2285: La vulnerabilidad fácilmente explotable permite que un atacante no autenticado inicie sesión en la infraestructura donde se ejecuta Oracle VM VirtualBox para comprometer Oracle VM VirtualBox. Si bien la vulnerabilidad está en Oracle VM VirtualBox, los ataques pueden afectar significativamente a	I	5	**85**	**C**	**1**		**85**	**C**

No. De Amenazas y Vulnerabilidades	Activos de Información	Nombre del activo de información	Valoración del Riesgo de los Activos	Amenazas Metodología MAGERIT	Vulnerabilidades	Niveles de aceptación del .	Probabilidad de vulneración	Cálculo del riesgo neto	Criticidad neta	Calificación de Gestión	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Criticidad residual
					productos adicionales. Los ataques exitosos de esta vulnerabilidad pueden dar como resultado el acceso no autorizado a datos críticos o el acceso completo a todos los datos accesibles de Oracle VM VirtualBox.								
37	HARDWARE	[HW] DVR DAHUA 8ch	17	[I6] Corte del suministro eléctrico	Hardware sensible a las perturbaciones eléctricas.	I	5	**85**	**C**	**1**		**85**	**C**
38	HARDWARE	[HW] DVR DAHUA 8ch	17	[A26] Ataque destructivo	Falta de hardware de repuesto.	I	3	**51**	**C**	**1**		**51**	**C**
39	HARDWARE	[HW] DVR DAHUA 8ch	17	[A26] Ataque destructivo	Fragilidad del hardware.	I	3	**51**	**C**	**1**		**51**	**C**
40	SOFTWARE	[SW] Base de datos Mysql 5.7.17	13	[A6] Abuso de privilegios de acceso	CVE-2017-10294: Vulnerabilidad en el componente MySQL Server de Oracle MySQL (subcomponente: Server: Optimizer). Las versiones compatibles que se ven afectadas son la 5.6.37 y anteriores y la 5.7.19 y anteriores. La vulnerabilidad fácilmente explotable permite que un atacante con privilegios altos con acceso a la red a través de múltiples protocolos comprometa el servidor MySQL. Los ataques exitosos de esta vulnerabilidad pueden resultar en la capacidad no autorizada de provocar un bloqueo o un bloqueo repetible (DOS completo) de MySQL Server.	I	3	**39**	**C**	**1**		**39**	**C**

No. De Amenazas y Vulnerabilidades	Activos de Información	Nombre del activo de información	Valoración del Riesgo de los Activos	Amenazas Metodología MAGERIT	Vulnerabilidades	Niveles de aceptación del	Probabilidad de vulneración	Cálculo del riesgo neto	Criticidad neta	Calificación de Gestión	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Criticidad residual
					CVSS 3.0 Puntaje base 4.9 (Impactos de disponibilidad)								
41	SOFTWARE	[SW] RTMyEC (INDUCAPK)	17	[I5] Avería de origen físico o lógico	Falta procedimiento de mantenimiento para el software.	I	3	**51**	**C**	**1**		**51**	**C**
42	SOFTWARE	[SW] RTMyEC (INDUCAPK)	17	[E21] Errores de mantenimiento / actualización de programas (software)	Falta procedimiento de actualización.	I	3	**51**	**C**	**1**		**51**	**C**
43	SOFTWARE	[SW] RTMyEC (INDUCAPK)	17	[A7] Uso no previsto	Uso de base de datos personales.	I	3	**51**	**C**	**1**		**51**	**C**
44	SOFTWARE	[SW] Office professional plus 2016	16	[E20] Vulnerabilidades de los programas (software)	MS16-095: La habitual actualización acumulativa para Microsoft Internet Explorer que además soluciona nueve nuevas vulnerabilidades. La más grave de ellas podría permitir la ejecución remota de código si un usuario visita, con Internet Explorer, una página web especialmente creada (CVE-2016-3288 al CVE-2016-3290, CVE-2016-3293, CVE-2016-3321, CVE-2016-3322, CVE-2016-3326, CVE-2016-3327 y CVE-2016-3329). CVE-2022-21840 Paquete de servicio 1 de Microsoft SharePoint Foundation 2016, Ejecución remota de código estado Crítico	I	4	**64**	**C**	**1**		**64**	**C**
45	SOFTWARE	[SW] Office professional plus 2016	16	[E20] Vulnerabilidades de los programas (software)	CVE-2022-21840 Microsoft Excel 2016 (edición de 64 bits) Ejecución remota de código Crítico	I	4	**64**	**C**	**1**		**64**	**C**

No. De Amenazas y Vulnerabilidades	Activos de Información	Nombre del activo de información	Valoración del Riesgo de los Activos	Amenazas Metodología MAGERIT	Vulnerabilidades	Niveles de aceptación del .	Probabilidad de vulneración	Cálculo del riesgo neto	Criticidad neta	Calificación de Gestión	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Criticidad residual
					CVE-2018-0792 Microsoft Word 2016 in Microsoft Office 2016 allows a remote code execution vulnerability due to the way objects are handled in memory, aka "Microsoft Word Remote Code Execution Vulnerability". This CVE is unique from CVE-2018-0794.								
46	SOFTWARE	[SW] AnyDesk	13	[A6] Abuso de privilegios de acceso	CVE-2021-40854: AnyDesk anterior a 6.2.6 y 6.3.x anterior a 6.3.3 permite que un usuario local obtenga privilegios de administrador mediante el uso de la función Abrir registro de chat para iniciar un proceso de Bloc de notas privilegiado que puede iniciar otras aplicaciones.	I	3	**39**	**C**	**1**		**39**	**C**
47	SOFTWARE	[SW] AnyDesk	13	[E8] Difusión de software dañino	CVE-2020-35483: AnyDesk anterior a 6.1.0 en Windows, cuando se ejecuta en modo portátil en un sistema donde el atacante tiene acceso de escritura al directorio de la aplicación, permite que este atacante comprometa una cuenta de usuario local a través de una configuración de solo lectura para un archivo troyano gcapi.dll .	I	3	**39**	**C**	**1**		**39**	**C**
48	SOFTWARE	[SW] AnyDesk	13	[E19] Fugas de información	CVE-2021-44426: Se descubrió un problema en AnyDesk antes de 6.2.6 y 6.3.x antes de 6.3.5. Es	I	3	**39**	**C**	**1**		**39**	**C**

No. De Amenazas y Vulnerabilidades	Activos de Información	Nombre del activo de información	Valoración del Riesgo de los Activos	Amenazas Metodología MAGERIT	Vulnerabilidades	Niveles de aceptación del	Probabilidad de vulneración	Cálculo del riesgo neto	Criticidad neta	Calificación de Gestión	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Criticidad residual
					posible cargar un archivo arbitrario en el directorio local ~/Downloads/ de la víctima si la víctima está utilizando el cliente Windows de AnyDesk para conectarse a una máquina remota, si un atacante también está conectado de forma remota con AnyDesk a la misma máquina remota. La carga se realiza sin ninguna aprobación o acción por parte de la víctima.								
49	SOFTWARE	[SW] TeamViewer	17	[E19] Fugas de información	CVE-2021-35005: Esta vulnerabilidad permite a los atacantes locales revelar información confidencial sobre las instalaciones afectadas de TeamViewer. Un atacante primero debe obtener la capacidad de ejecutar código con pocos privilegios en el sistema de destino para aprovechar esta vulnerabilidad. La falla específica existe dentro del servicio de TeamViewer. El problema se debe a la falta de una validación adecuada de los datos proporcionados por el usuario, lo que puede resultar en una lectura más allá del final de una matriz asignada. Un atacante puede aprovechar esto junto con otras vulnerabilidades para	I	3	**51**	**C**	**1**		**51**	**C**

No. De Amenazas y Vulnerabilidades	Activos de Información	Nombre del activo de información	Valoración del Riesgo de los Activos	Amenazas Metodología MAGERIT	Vulnerabilidades	Niveles de aceptación del	Probabilidad de vulneración	Cálculo del riesgo neto	Criticidad neta	Calificación de Gestión	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Criticidad residual
					ejecutar código arbitrario en el contexto de SYSTEM								
50	SOFTWARE	[SW] TeamViewer	17	[E8] Difusión de software dañino	CVE-2021-34859: Esta vulnerabilidad permite a atacantes remotos ejecutar código arbitrario en las instalaciones afectadas de TeamViewer 15.16.8.0. Se requiere la interacción del usuario para explotar esta vulnerabilidad, ya que el objetivo debe visitar una página maliciosa o abrir un archivo malicioso. La falla específica existe en el análisis de archivos TVS. El problema se debe a la falta de una validación adecuada de los datos proporcionados por el usuario, lo que puede provocar una condición de corrupción de la memoria. Un atacante puede aprovechar esta vulnerabilidad para ejecutar código en el contexto del proceso actual	I	4	**68**	**C**	**1**		**68**	**C**
51	SOFTWARE	[SW] TeamViewer	17	[E20] Vulnerabilidades de los programas (software)	CVE-2019-11769: Se descubrió un problema en TeamViewer 14.2.2558. La actualización del producto como usuario no administrativo requiere la introducción de credenciales administrativas en la GUI. Posteriormente, estas credenciales se procesan en Teamviewer.exe, lo que permite	I	3	**51**	**C**	**1**		**51**	**C**

No. De Amenazas y Vulnerabilidades	Activos de Información	Nombre del activo de información	Valoración del Riesgo de los Activos	Amenazas Metodología MAGERIT	Vulnerabilidades	Niveles de aceptación del	Probabilidad de vulneración	Cálculo del riesgo neto	Criticidad neta	Calificación de Gestión	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Criticidad residual
					que cualquier aplicación que se ejecute en el mismo contexto de usuario no administrativo las intercepte en texto no cifrado dentro de la memoria del proceso. Mediante el uso de esta técnica, un atacante local puede obtener credenciales administrativas para elevar los privilegios. Esta vulnerabilidad se puede aprovechar inyectando código en Teamviewer.exe que intercepta las llamadas a GetWindowTextW y registra las credenciales procesadas.								
52	SOFTWARE	[SW] Windows 10 Profesional 21H2	19	[E20] Vulnerabilidades de los programas (software)	CVE-2017-0144 El servidor SMBv1 en Microsoft Windows Vista SP2; Windows Server 2008 SP2 y R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold y R2; Windows RT 8.1; y Windows 10 Gold, 1511 y 1607; y Windows Server 2016 permite a atacantes remotos ejecutar código arbitrario a través de paquetes manipulados, vulnerabilidad también conocida como "Windows SMB Remote Code Execution Vulnerability". Esta vulnerabilidad es diferente a la descrita en CVE-2017-0143, CVE-2017-0145, CVE-2017-0146 y CVE-2017-0148.	I	3	**57**	**C**	**1**		**57**	**C**

No. De Amenazas y Vulnerabilidades	Activos de Información	Nombre del activo de información	Valoración del Riesgo de los Activos	Amenazas Metodología MAGERIT	Vulnerabilidades	Niveles de aceptación del	Probabilidad de vulneración	Cálculo del riesgo neto	Criticidad neta	Calificación de Gestión	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Criticidad residual
					CVE-2022-24525 Vulnerabilidad de elevación de privilegios de la pila de actualización de Windows. Fecha de publicación: 2022-03-09 Fecha de última actualización: 2022-03-15								
53	SOFTWARE	[SW] Windows 10 Profesional 21H2	19	[E20] Vulnerabilidades de los programas (software)	CVE-2022-24508 Vulnerabilidad de ejecución remota de código de cliente/servidor de Windows SMBv3 CVE-2022-24503 668 Vulnerabilidad de divulgación de información del cliente del protocolo de escritorio remoto.	I	3	**57**	**C**	**1**		**57**	**C**
54	HARDWARE	[HW] Equipo de computo ARGOM	19	[I5] Avería de origen físico o lógico	Problemas de mantenimiento.	I	4	**76**	**C**	**4**	Existe politica de mantenimiento de computadores y se encuentra documentado bajo procedimiento de la empresa	**19**	**I**
55	HARDWARE	[HW] Equipo de computo ARGOM	19	[I5] Avería de origen físico o lógico	Envejecimiento del hardware.	I	4	**76**	**C**	**1**		**76**	**C**
56	HARDWARE	[HW] Equipo de computo ARGOM	19	[A11] Acceso no autorizado	Posibilidad de utilizar un acceso oculto.	I	5	**95**	**C**	**1**		**95**	**C**
57	HARDWARE	[HW] Equipo de computo ARGOM	19	[A11] Acceso no autorizado	El dispositivo utilizado permite usos diferentes de los previstos.	I	4	**76**	**C**	**1**		**76**	**C**
58	SOFTWARE	[SW] AudiWeb-FirmaFur	19	[E21] Errores de mantenimiento / actualización de programas (software)	Falta procedimiento de actualización.	I	3	**57**	**C**	**1**		**57**	**C**

No. De Amenazas y Vulnerabilidades	Activos de Información	Nombre del activo de información	Valoración del Riesgo de los Activos	Amenazas Metodología MAGERIT	Vulnerabilidades	Niveles de aceptación del .	Probabilidad de vulneración	Cálculo del riesgo neto	Criticidad neta	Calificación de Gestión	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Criticidad residual
59	SOFTWARE	[SW] SmartPSS	19	[E20] Vulnerabilidades de los programas (software)	Uso de versión obsoleta de aplicación.	I	3	**57**	**C**	**1**		**57**	**C**
60	HARDWARE	[HW] IMPRESORA 1 Samsung	15	[I5] Avería de origen físico o lógico	Problemas de mantenimiento.	I	4	**60**	**C**	**4**	Existe politica de mantenimiento de computadores y se encuentra documentado bajo procedimiento de la empresa	**15**	**A**
61	HARDWARE	[HW] IMPRESORA 1 Samsung	15	[I5] Avería de origen físico o lógico	Envejecimiento del hardware.	I	4	**60**	**C**	**1**		**60**	**C**
62	HARDWARE	[HW] IMPRESORA 1 Samsung	15	[I6] Corte del suministro eléctrico	Hardware sensible a las perturbaciones eléctricas.	I	5	**75**	**C**	**1**		**75**	**C**
63	HARDWARE	[HW] IMPRESORA 1 Samsung	15	[A26] Ataque destructivo	Falta de hardware de repuesto.	I	3	**45**	**C**	**1**		**45**	**C**
64	HARDWARE	[HW] IMPRESORA 1 Samsung	15	[A26] Ataque destructivo	Fragilidad del hardware.	I	4	**60**	**C**	**1**		**60**	**C**
65	HARDWARE	[HW] TABLET No 3 Samsung	17	[I5] Avería de origen físico o lógico	Problemas de mantenimiento.	I	4	**68**	**C**	**4**	Existe politica de mantenimiento de computadores y se encuentra documentado bajo procedimiento de la empresa	17	I
66	HARDWARE	[HW] TABLET No 3 Samsung	17	[I5] Avería de origen físico o lógico	Envejecimiento del hardware.	I	4	**68**	**C**	**1**		68	C
67	HARDWARE	[HW] TABLET No 3 Samsung	17	[I6] Corte del suministro eléctrico	Hardware sensible a las perturbaciones eléctricas.	I	5	**85**	**C**	**1**		85	C
68	HARDWARE	[HW] TABLET No 3 Samsung	17	[A26] Ataque destructivo	Falta de hardware de repuesto.	I	3	**51**	**C**	**1**		51	C
69	HARDWARE	[HW] TABLET No 3 Samsung	17	[A26] Ataque destructivo	Fragilidad del hardware.	I	4	**68**	**C**	**1**		68	C

No. De Amenazas y Vulnerabilidades	Activos de Información	Nombre del activo de información	Valoración del Riesgo de los Activos	Amenazas Metodología MAGERIT	Vulnerabilidades	Niveles de aceptación del	Probabilidad de vulneración	Cálculo del riesgo neto	Criticidad neta	Calificación de Gestión	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Criticidad residual
70	SOFTWARE	[SW] Android 6.0.1	15	[E19] Fugas de información	CVE-2017-18643: Se descubrió un problema en los dispositivos móviles Samsung con el software M(6.x) y N(7.x). Hay divulgación de información de la dirección kbase_context de un nodo de memoria GPU. El ID de Samsung es SVE-2017-8907 (diciembre de 2017)	I	3	45	C	**1**		45	C
71	SOFTWARE	[SW] Android 6.0.1	15	[A6] Abuso de privilegios de acceso	CVE-2018-21087: Se descubrió un problema en los dispositivos móviles Samsung con el software L(5.x), M(6.x) y N(7.x). Hay un desbordamiento de búfer basado en almacenamiento dinámico de vnswap a través de la función de almacenamiento, con la escalada de privilegios resultante. El ID de Samsung es SVE-2017-10599 (enero de 2018).	I	3	45	C	**1**		45	C
72	SOFTWARE	[SW] Android 6.0.1	15	[E19] Fugas de información	CVE-2017-13269: Una vulnerabilidad de divulgación de información en el sistema Android (bluetooth). Producto: Android. Versiones: 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0, 8.1. ID de Android: A-68818034.	I	3	45	C	**1**		45	C
73	HARDWARE	[HW] Telefono AT&T	17	[I5] Avería de origen físico o lógico	Problemas de mantenimiento.	I	4	**68**	**C**	**4**	Existe politica de mantenimiento de computadores y se encuentra documentado bajo procedimiento de la empresa	17	I

No. De Amenazas y Vulnerabilidades	Activos de Información	Nombre del activo de información	Valoración del Riesgo de los Activos	Amenazas Metodología MAGERIT	Vulnerabilidades	Niveles de aceptación del	Probabilidad de vulneración	Cálculo del riesgo neto	Criticidad neta	Calificación de Gestión	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Criticidad residual
74	HARDWARE	[HW] Telefono AT&T	17	[I5] Avería de origen físico o lógico	Envejecimiento del hardware.	I	4	**68**	**C**	**1**		68	C
75	SOFTWARE	[SW] AudiWeb	20	[E21] Errores de mantenimiento / actualización de programas (software)	Falta procedimiento de actualización.	I	3	**60**	**C**	**1**		60	C
76	SOFTWARE	[SW] Supergiros	18	[E21] Errores de mantenimiento / actualización de programas (software)	Falta procedimiento de actualización.	I	3	**54**	**C**	**1**		54	C
77	SOFTWARE	[SW] Supergiros	18	[E20] Vulnerabilidades de los programas (software)	Uso de versión obsoleta de aplicación.	I	3	**54**	**C**	**1**		54	C
78	HARDWARE	[HW] IMPRESORA 3 Canon	20	[I5] Avería de origen físico o lógico	Problemas de mantenimiento.	I	4	**80**	**C**	**4**	Existe politica de mantenimiento de computadores y se encuentra documentado bajo procedimiento de la empresa	20	I
79	HARDWARE	[HW] IMPRESORA 3 Canon	20	[I5] Avería de origen físico o lógico	Envejecimiento del hardware.	I	4	**80**	**C**	**1**		80	C
80	HARDWARE	[HW] IMPRESORA 3 Canon	20	[I6] Corte del suministro eléctrico	Hardware sensible a las perturbaciones eléctricas.	I	5	**100**	**C**	**1**		100	C
81	HARDWARE	[HW] IMPRESORA 3 Canon	20	[A26] Ataque destructivo	Falta de hardware de repuesto.	I	3	**60**	**C**	**1**		60	C
82	HARDWARE	[HW] IMPRESORA 3 Canon	20	[A26] Ataque destructivo	Fragilidad del hardware.	I	4	**80**	**C**	**1**		80	C
83	HARDWARE	[HW] IMPRESORA 2 Samsung	9	[I5] Avería de origen físico o lógico	Problemas de mantenimiento.	M	4	**36**	**C**	**4**	Existe politica de mantenimiento de computadores y se encuentra documentado	9	B

No. De Amenazas y Vulnerabilidades	Activos de Información	Nombre del activo de información	Valoración del Riesgo de los Activos	Amenazas Metodología MAGERIT	Vulnerabilidades	Niveles de aceptación del .	Probabilidad de vulneración	Cálculo del riesgo neto	Criticidad neta	Calificación de Gestión	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Criticidad residual
											bajo procedimiento de la empresa		
84	HARDWARE	[HW] IMPRESORA 2 Samsung	9	[I5] Avería de origen físico o lógico	Envejecimiento del hardware.	I	4	**36**	**C**	**1**		36	C
85	HARDWARE	[HW] IMPRESORA 2 Samsung	9	[I6] Corte del suministro eléctrico	Hardware sensible a las perturbaciones eléctricas.	I	5	**45**	**C**	**1**		45	C
86	HARDWARE	[HW] IMPRESORA 2 Samsung	9	[A26] Ataque destructivo	Falta de hardware de repuesto.	I	3	**27**	**C**	**1**		27	C
87	HARDWARE	[HW] IMPRESORA 2 Samsung	9	[A26] Ataque destructivo	Fragilidad del hardware.	I	4	**36**	**C**	**1**		36	C
88	HARDWARE	[HW] FRENOMETRO	20	[I5] Avería de origen físico o lógico	Problemas de mantenimiento.	I	4	**80**	**C**	**4**	Existe política de mantenimiento de equipos y se encuentra documentado bajo procedimiento de la empresa	20	I
89	HARDWARE	[HW] FRENOMETRO	20	[I5] Avería de origen físico o lógico	Envejecimiento del hardware.	I	4	**80**	**C**	**1**		80	C
90	HARDWARE	[HW] FRENOMETRO	20	[I6] Corte del suministro eléctrico	Hardware sensible a las perturbaciones eléctricas.	I	4	**80**	**C**	**1**		80	C
91	HARDWARE	[HW] FRENOMETRO	20	[A26] Ataque destructivo	Falta de hardware de repuesto.	I	3	**60**	**C**	**1**		60	C
92	HARDWARE	[HW] ALINEADOR DE LUCES	14	[I5] Avería de origen físico o lógico	Problemas de mantenimiento.	M	4	**56**	**C**	**4**	Existe política de mantenimiento de equipos y se encuentra documentado bajo procedimiento de la empresa	14	A
93	HARDWARE	[HW] ALINEADOR DE LUCES	14	[I5] Avería de origen físico o lógico	Envejecimiento del hardware.	I	4	**56**	**C**	**1**		56	C
94	HARDWARE	[HW] ALINEADOR DE LUCES	14	[I6] Corte del suministro eléctrico	Hardware sensible a las perturbaciones eléctricas.	I	4	**56**	**C**	**1**		56	C
95	HARDWARE	[HW] ALINEADOR DE LUCES	14	[A26] Ataque destructivo	Falta de hardware de repuesto.	I	3	**42**	**C**	**1**		42	C

No. De Amenazas y Vulnerabilidades	Activos de Información	Nombre del activo de información	Valoración del Riesgo de los Activos	Amenazas Metodología MAGERIT	Vulnerabilidades	Niveles de aceptación del	Probabilidad de vulneración	Cálculo del riesgo neto	Criticidad neta	Calificación de Gestión	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Criticidad residual
96	HARDWARE	[HW] SONOMETRO	20	[I5] Avería de origen físico o lógico	Problemas de mantenimiento.	I	4	**80**	**C**	**4**	Existe política de mantenimiento de equipos y se encuentra documentado bajo procedimiento de la empresa	20	I
97	HARDWARE	[HW] SONOMETRO	20	[I5] Avería de origen físico o lógico	Envejecimiento del hardware.	I	4	**80**	**C**	**1**		80	C
98	HARDWARE	[HW] SONOMETRO	20	[I6] Corte del suministro eléctrico	Hardware sensible a las perturbaciones eléctricas.	I	4	**80**	**C**	**1**		80	C
99	HARDWARE	[HW] SONOMETRO	20	[A26] Ataque destructivo	Falta de hardware de repuesto.	I	3	**60**	**C**	**1**		60	C
100	HARDWARE	[HW] ANALIZADOR4T	17	[I5] Avería de origen físico o lógico	Problemas de mantenimiento.	I	4	**68**	**C**	**4**	Existe política de mantenimiento de equipos y se encuentra documentado bajo procedimiento de la empresa	17	I
101	HARDWARE	[HW] ANALIZADOR4T	17	[I5] Avería de origen físico o lógico	Envejecimiento del hardware.	I	4	**68**	**C**	**1**		68	C
102	HARDWARE	[HW] ANALIZADOR4T	17	[I6] Corte del suministro eléctrico	Hardware sensible a las perturbaciones eléctricas.	I	4	**68**	**C**	**1**		68	C
103	HARDWARE	[HW] ANALIZADOR4T	17	[A26] Ataque destructivo	Falta de hardware de repuesto.	I	3	**51**	**C**	**1**		51	C
104	HARDWARE	[HW] ANALIZADOR2T	15	[I5] Avería de origen físico o lógico	Problemas de mantenimiento.	I	4	**60**	**C**	**4**	Existe política de mantenimiento de equipos y se encuentra documentado bajo procedimiento de la empresa	15	A
105	HARDWARE	[HW] ANALIZADOR2T	15	[I5] Avería de origen físico o lógico	Envejecimiento del hardware.	I	4	**60**	**C**	**1**		60	C
106	HARDWARE	[HW] ANALIZADOR2T	15	[I6] Corte del suministro eléctrico	Hardware sensible a las perturbaciones eléctricas.	I	4	**60**	**C**	**1**		60	C
107	HARDWARE	[HW] ANALIZADOR2T	15	[A26] Ataque destructivo	Falta de hardware de repuesto.	I	3	**45**	**C**	**1**		45	C

No. De Amenazas y Vulnerabilidades	Activos de Información	Nombre del activo de información	Valoración del Riesgo de los Activos	Amenazas Metodología MAGERIT	Vulnerabilidades	Niveles de aceptación del .	Probabilidad de vulneración	Cálculo del riesgo neto	Criticidad neta	Calificación de Gestión	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Criticidad residual
108	HARDWARE	[HW] TERMOHIGROMETRO	20	[I5] Avería de origen físico o lógico	Problemas de mantenimiento.	I	4	**80**	**C**	**4**	Existe politica de mantenimiento de equipos y se encuentra documentado bajo procedimiento de la empresa	20	I
109	HARDWARE	[HW] TERMOHIGROMETRO	20	[I5] Avería de origen físico o lógico	Envejecimiento del hardware.	I	4	**80**	**C**	**1**		80	C
110	HARDWARE	[HW] TERMOHIGROMETRO	20	[I6] Corte del suministro eléctrico	Hardware sensible a las perturbaciones eléctricas.	I	4	**80**	**C**	**1**		80	C
111	HARDWARE	[HW] TERMOHIGROMETRO	20	[A26] Ataque destructivo	Falta de hardware de repuesto.	I	3	**60**	**C**	**1**		60	C
112	HARDWARE	[HW] TERMOHIGROMETRO RESPALDO	14	[I5] Avería de origen físico o lógico	Problemas de mantenimiento.	M	4	**56**	**C**	**4**	Existe política de mantenimiento de equipos y se encuentra documentado bajo procedimiento de la empresa	14	A
113	HARDWARE	[HW] TERMOHIGROMETRO RESPALDO	14	[I5] Avería de origen físico o lógico	Envejecimiento del hardware.	I	4	**56**	**C**	**1**		56	C
114	HARDWARE	[HW] TERMOHIGROMETRO RESPALDO	14	[I6] Corte del suministro eléctrico	Hardware sensible a las perturbaciones eléctricas.	I	4	**56**	**C**	**1**		56	C
115	HARDWARE	[HW] TERMOHIGROMETRO RESPALDO	14	[A26] Ataque destructivo	Falta de hardware de repuesto.	I	3	**42**	**C**	**1**		42	C
116	HARDWARE	[HW] MANOMETRO	15	[I5] Avería de origen físico o lógico	Envejecimiento del hardware.	I	4	**60**	**C**	1		60	C
117	HARDWARE	[HW] MANOMETRO	15	[A26] Ataque destructivo	Falta de hardware de repuesto.	I	3	**45**	**C**	**1**		45	C
118	HARDWARE	[HW] CUENTA REVOLUCIONES	15	[I5] Avería de origen físico o lógico	Problemas de mantenimiento.	I	4	**60**	**C**	**4**	Existe política de mantenimiento de equipos y se encuentra documentado bajo procedimiento de la empresa	15	A
119	HARDWARE	[HW] CUENTA REVOLUCIONES	15	[I5] Avería de origen físico o lógico	Envejecimiento del hardware.	I	4	**60**	**C**	**1**		60	C

No. De Amenazas y Vulnerabilidades	Activos de Información	Nombre del activo de información	Valoración del Riesgo de los Activos	Amenazas Metodología MAGERIT	Vulnerabilidades	Niveles de aceptación del	Probabilidad de vulneración	Cálculo del riesgo neto	Criticidad neta	Calificación de Gestión	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Criticidad residual
120	HARDWARE	[HW] CUENTA REVOLUCIONES	15	[A26] Ataque destructivo	Falta de hardware de repuesto.	I	3	**45**	**C**	**1**		45	C
121	HARDWARE	[HW] TABLET No 1 Samsung	20	[I5] Avería de origen físico o lógico	Problemas de mantenimiento.	I	4	**80**	**C**	**4**	Existe política de mantenimiento de computadores y se encuentra documentado bajo procedimiento de la empresa	20	I
122	HARDWARE	[HW] TABLET No 1 Samsung	20	[I5] Avería de origen físico o lógico	Envejecimiento del hardware.	I	4	**80**	**C**	**1**		80	C
123	HARDWARE	[HW] TABLET No 1 Samsung	20	[A26] Ataque destructivo	Falta de hardware de repuesto.	I	3	**60**	**C**	**1**		60	C
124	HARDWARE	[HW] TABLET No 1 Samsung	20	[A26] Ataque destructivo	Fragilidad del hardware.	I	4	**80**	**C**	**1**		80	C
125	HARDWARE	[HW] TABLET No 1 Samsung	20	[E19] Fugas de información	CVE-2017-18643: Se descubrió un problema en los dispositivos móviles Samsung con el software M(6.x) y N(7.x). Hay divulgación de información de la dirección kbase_context de un nodo de memoria GPU. El ID de Samsung es SVE-2017-8907 (diciembre de 2017)	I	3	60	C	**1**		60	C
126	HARDWARE	[HW] TABLET No 1 Samsung	20	[A6] Abuso de privilegios de acceso	CVE-2018-21087: Se descubrió un problema en los dispositivos móviles Samsung con el software L(5.x), M(6.x) y N(7.x). Hay un desbordamiento de búfer basado en almacenamiento dinámico de vnswap a través de la función de almacenamiento, con la escalada de privilegios resultante. El ID de	I	3	60	C	**1**		60	C

No. De Amenazas y Vulnerabilidades	Activos de Información	Nombre del activo de información	Valoración del Riesgo de los Activos	Amenazas Metodología MAGERIT	Vulnerabilidades	Niveles de aceptación del	Probabilidad de vulneración	Cálculo del riesgo neto	Criticidad neta	Calificación de Gestión	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Criticidad residual
					Samsung es SVE-2017-10599 (enero de 2018).								
127	HARDWARE	[HW] TABLET No 2 Samsung	14	[I5] Avería de origen físico o lógico	Problemas de mantenimiento.	M	4	**56**	**C**	**4**	Existe politica de mantenimiento de computadores y se encuentra documentado bajo procedimiento de la empresa	14	A
128	HARDWARE	[HW] TABLET No 2 Samsung	14	[I5] Avería de origen físico o lógico	Envejecimiento del hardware.	I	4	**56**	**C**	**1**		56	C
129	HARDWARE	[HW] TABLET No 2 Samsung	14	[A26] Ataque destructivo	Falta de hardware de repuesto.	I	3	**42**	**C**	**1**		42	C
130	HARDWARE	[HW] TABLET No 2 Samsung	14	[A26] Ataque destructivo	Fragilidad del hardware.	I	4	**56**	**C**	**1**		56	C
131	HARDWARE	[HW] TABLET No 2 Samsung	14	[E19] Fugas de información	CVE-2017-18643: Se descubrió un problema en los dispositivos móviles Samsung con el software M(6.x) y N(7.x). Hay divulgación de información de la dirección kbase_context de un nodo de memoria GPU. El ID de Samsung es SVE-2017-8907 (diciembre de 2017)	I	3	42	C	**1**		42	C
132	HARDWARE	[HW] TABLET No 2 Samsung	14	[A6] Abuso de privilegios de acceso	CVE-2018-21087: Se descubrió un problema en los dispositivos móviles Samsung con el software L(5.x), M(6.x) y N(7.x). Hay un desbordamiento de búfer basado en almacenamiento dinámico de vnswap a través de la función de almacenamiento, con la escalada de privilegios resultante. El ID de	I	3	42	C	**1**		42	C

No. De Amenazas y Vulnerabilidades	Activos de Información	Nombre del activo de información	Valoración del Riesgo de los Activos	Amenazas Metodología MAGERIT	Vulnerabilidades	Niveles de aceptación del	Probabilidad de vulneración	Cálculo del riesgo neto	Criticidad neta	Calificación de Gestión	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Criticidad residual
					Samsung es SVE-2017-10599 (enero de 2018).								
133	HARDWARE	[HW] TABLET No 4 Samsung	20	[I5] Avería de origen físico o lógico	Problemas de mantenimiento.	I	4	**80**	**C**	**4**	Existe politica de mantenimiento de computadores y se encuentra documentado bajo procedimiento de la empresa	20	I
134	HARDWARE	[HW] TABLET No 4 Samsung	20	[I5] Avería de origen físico o lógico	Envejecimiento del hardware.	I	4	**80**	**C**	**1**		80	C
135	HARDWARE	[HW] TABLET No 4 Samsung	20	[A26] Ataque destructivo	Falta de hardware de repuesto.	I	3	**60**	**C**	**1**		60	C
136	HARDWARE	[HW] TABLET No 4 Samsung	20	[A26] Ataque destructivo	Fragilidad del hardware.	I	4	**80**	**C**	**1**		80	C
137	HARDWARE	[HW] TABLET No 4 Samsung	20	[E19] Fugas de información	CVE-2017-18643: Se descubrió un problema en los dispositivos móviles Samsung con el software M(6.x) y N(7.x). Hay divulgación de información de la dirección kbase_context de un nodo de memoria GPU. El ID de Samsung es SVE-2017-8907 (diciembre de 2017)	I	3	60	C	**1**		60	C
138	HARDWARE	[HW] TABLET No 4 Samsung	20	[A6] Abuso de privilegios de acceso	CVE-2018-21087: Se descubrió un problema en los dispositivos móviles Samsung con el software L(5.x), M(6.x) y N(7.x). Hay un desbordamiento de búfer basado en almacenamiento dinámico de vnswap a través de la función de almacenamiento, con la escalada de privilegios resultante. El ID de	I	3	60	C	**1**		60	C

No. De Amenazas y Vulnerabilidades	Activos de Información	Nombre del activo de información	Valoración del Riesgo de los Activos	Amenazas Metodología MAGERIT	Vulnerabilidades	Niveles de aceptación del .	Probabilidad de vulneración	Cálculo del riesgo neto	Criticidad neta	Calificación de Gestión	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Criticidad residual
					Samsung es SVE-2017-10599 (enero de 2018).								
139	HARDWARE	[HW] HCO (Tarjeta Desarrollo Beaglebone) GASES	17	[I5] Avería de origen físico o lógico	Envejecimiento del hardware.	I	4	**68**	**C**	**1**		68	C
140	HARDWARE	[HW] HCO (Tarjeta Desarrollo Beaglebone) GASES	17	[A26] Ataque destructivo	Falta de hardware de repuesto.	I	3	**51**	**C**	**1**		51	C
141	HARDWARE	[HW] HCO (Tarjeta Desarrollo Beaglebone) GASES	17	[A26] Ataque destructivo	Fragilidad del hardware.	I	4	**68**	**C**	**1**		68	C
142	HARDWARE	[HW] HCO (Tarjeta Desarrollo Beaglebone) FRENOMETRO	15	[I5] Avería de origen físico o lógico	Envejecimiento del hardware.	I	4	**60**	**C**	**1**		60	C
143	HARDWARE	[HW] HCO (Tarjeta Desarrollo Beaglebone) FRENOMETRO	15	[A26] Ataque destructivo	Falta de hardware de repuesto.	I	3	**45**	**C**	**1**		45	C
144	HARDWARE	[HW] HCO (Tarjeta Desarrollo Beaglebone) FRENOMETRO	15	[A26] Ataque destructivo	Fragilidad del hardware.	I	4	**60**	**C**	**1**		60	C
145	HARDWARE	[HW] HCO (Tarjeta Desarrollo Beaglebone) LUXOMETRO	17	[I5] Avería de origen físico o lógico	Envejecimiento del hardware.	I	4	**68**	**C**	**1**		68	C
146	HARDWARE	[HW] HCO (Tarjeta Desarrollo Beaglebone) LUXOMETRO	17	[A26] Ataque destructivo	Falta de hardware de repuesto.	I	3	**51**	**C**	**1**		51	C
147	HARDWARE	[HW] HCO (Tarjeta Desarrollo Beaglebone) LUXOMETRO	17	[A26] Ataque destructivo	Fragilidad del hardware.	I	4	**68**	**C**	**1**		68	C
148	SOFTWARE	[SW] APP Pista	17	[E21] Errores de mantenimiento / actualización de programas (software)	Falta procedimiento de actualización.	I	3	**51**	**C**	**1**		51	C
149	SOFTWARE	[SW] APP Pista	17	[E20] Vulnerabilidades de los programas (software)	Uso de versión obsoleta de aplicación.	I	3	**51**	**C**	**1**		51	C
150	SOFTWARE	[SW] APP Pre-revision	15	[E21] Errores de mantenimiento / actualización de programas (software)	Falta procedimiento de actualización.	I	3	45	C	1		45	C

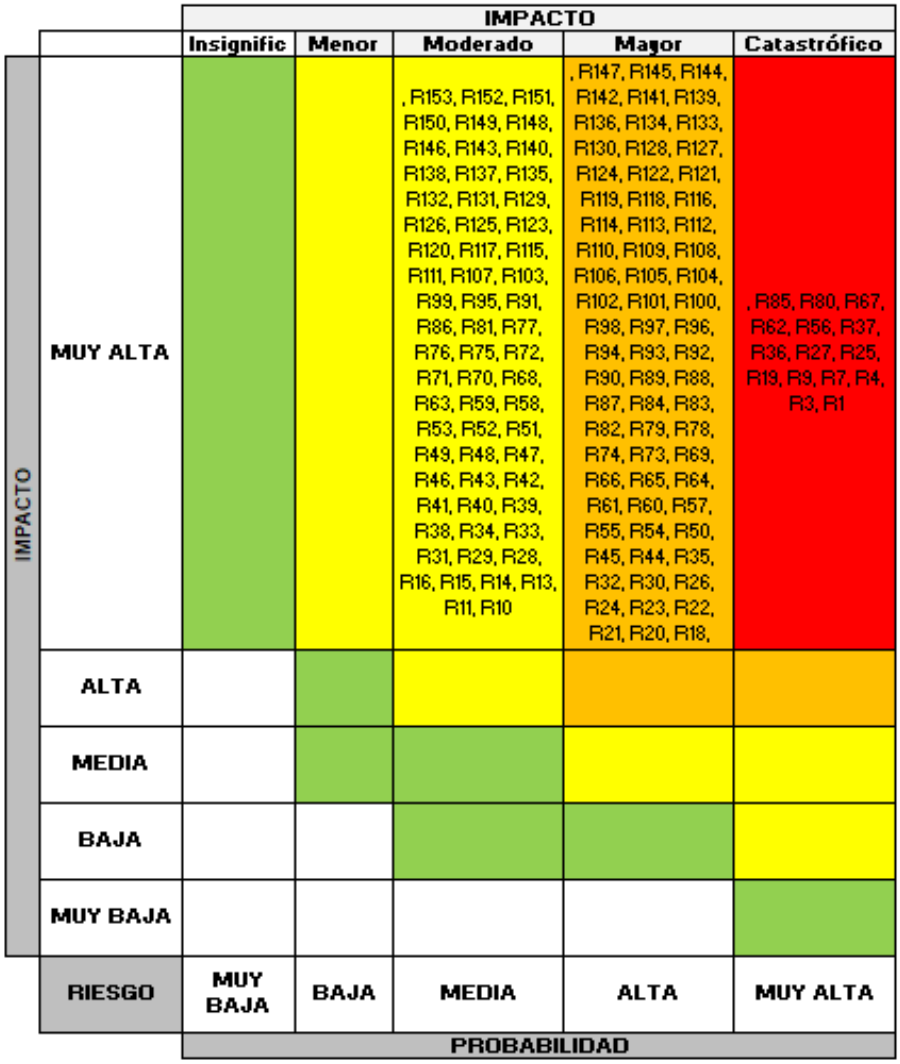
No. De Amenazas y Vulnerabilidades	Activos de Información	Nombre del activo de información	Valoración del Riesgo de los Activos	Amenazas Metodología MAGERIT	Vulnerabilidades	Niveles de aceptación del	Probabilidad de vulneración	Cálculo del riesgo neto	Criticidad neta	Calificación de Gestión	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Criticidad residual
151	SOFTWARE	[SW] APP Pre-revision	15	[E20] Vulnerabilidades de los programas (software)	Uso de versión obsoleta de aplicación.	I	3	45	C	1		45	C
152	SOFTWARE	[SW] APP Servicio	17	[E21] Errores de mantenimiento / actualización de programas (software)	Falta procedimiento de actualización.	I	3	51	C	1		51	C
153	SOFTWARE	[SW] APP Servicio	17	[E20] Vulnerabilidades de los programas (software)	Uso de versión obsoleta de aplicación.	I	3	51	C	1		51	C

Fuente: elaboración propia a partir del instrumento matriz de análisis de riesgos de ciberseguridad.

Para una mejor visualización y comprensión de la identificación de las amenazas de los activos de información, se invita a consultar al Anexo A - Matriz Análisis de Riesgos CDA Motocentro.xlsx en la hoja **APT**, matriz que hace parte integral de este proyecto aplicado.

De acuerdo con la probabilidad y el impacto de los riesgos, a continuación, se visualiza el mapa de calor, a partir del cual se puede identificar que hay 15 riesgos catalogados como de impacto catastrófico, 63 riesgos de impacto mayor y 75 riesgos de impacto Moderado.

Figura 24. Mapa de calor



Fuente: elaboración propia

6.3.3 Plan de tratamiento de riesgos de seguridad de la información.

Luego de identificar los activos, se realizó el análisis y evaluación de los riesgos de estos e identificar y valorar las amenazas, el paso a seguir es establecer los controles que permitan la mitigación de su impacto, en caso de su materialización, es ahí donde comienza a intervenir el plan de tratamiento de los riesgos de seguridad de información, el cual consiste en definir las acciones, sus responsables y la priorización, con el fin de tratarlos o de ser necesario mitigarlos, garantizando el mejoramiento de los niveles de seguridad de la información en el CDA MOTOCENTRO S.A.S..

Para la elaboración del plan de tratamiento de riesgos de los riegos de seguridad de los activos de información del CDA MOTOCENTRO, se sigue utilizando la matriz de análisis de riesgos de ciberseguridad del autor Luis Fernando Zambrano (ver Anexo A hoja APT, columnas desde la P hasta la W), al elaborar la matriz nos permitirá establecer los controles de seguridad de acuerdo con el Anexo A de la ISO 27001:2013 para las diferentes amenazas y vulnerabilidades identificadas sobre los activos de información del área de TI.

De acuerdo con el análisis de riesgos e identificación de posibles amenazas de los activos de información realizado, se diseñó el plan de tratamiento de riesgos de seguridad de la información de MOTOCENTRO S.A.S para mejorar los niveles de seguridad informática de los activos de información del área de TI, el cual se relaciona en la siguiente tabla.

Tabla 11. Plan de tratamiento de riesgos

	PLAN DE TRATAMIENTO												
	Indique el control a aplicar a partir de la norma ISO 27001:2013												
No. De Amenazas y Vulnerabilidades	**Transferir**	**Aceptar**	**Eliminar**	**Mitigar**	**DOMINIO**	**OBJETIVO**	**CONTROL**	**Descripción de la aplicación del control**	**Requerimiento Legal**	**Obligación Contractual**	**Requerimiento de**	**Análisis del Riesgo**	**Exclusión**
1				X	DOMINIO_A12	OBJETIVO_A12_6	A12.6.1 Gestión de las 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 medidas apropiadas para tratar el riesgo asociado.	Evaluación de las vulnerabilidades del sistema operativo y hacer la actualización a una nueva versión.				X	
2			X		DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Garantizar el cumplimiento del procedimiento establecido y aplicar el control				X	
3				X	DOMINIO_A9	OBJETIVO_A9_2	A9.2.3 Gestión de derechos de acceso privilegiado --Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	Crear un proceso para realizar revisiones recuentes y periódicas de cuentas privilegiadas para identificar y deshabilitar / eliminar cuentas con privilegios redundantes y / o reducir los privilegios				X	
4			X		DOMINIO_A12	OBJETIVO_A12_2	A12.2.1 Controles contra códigos maliciosos --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.	Establecer política y procedimientos asociados a controles antimalware				X	
5		X			DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Garantizar el cumplimiento del procedimiento establecido y aplicar el control				X	

	PLAN DE TRATAMIENTO												
	Indique el control a aplicar a partir de la norma ISO 27001:2013												
No. De Amenazas y Vulnerabilidades	Transferir	Aceptar	Eliminar	Mitigar	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control	Requerimiento Legal	Obligación Contractual	Requerimiento de	Análisis del Riesgo	Exclusión
6				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de obsolescencia se pueda remplazar				X	
7				X	DOMINIO_A9	OBJETIVO_A9_2	A9.2.5 Revisión de los derechos de acceso de usuarios --Control: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	Se llevará el control de los usuarios a través del directorio activo y se tendrán actualizados los permisos según rol establecido. Garantizar el cumplimiento de la política de control de acceso.				X	
8				X	DOMINIO_A9	OBJETIVO_A9_2	A9.2.5 Revisión de los derechos de acceso de usuarios --Control: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	Se llevará el control de los usuarios a través del directorio activo y se tendrán actualizados los permisos según rol establecido. Garantizar el cumplimiento de la política de control de acceso.				X	
9				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.2 Servicios de suministro --Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	Verificar la capacidad de la UPS vs equipos que requieren continuidad de negocio, de ser necesario cambiar la UPS por una de mayor capacidad, de acuerdo con las necesidades de la organización, garantizando la operación.				X	
10				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.2 Servicios de suministro --Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	Verificar la capacidad de la UPS vs equipos que requieren continuidad de negocio, de ser necesario cambiar la UPS por una de mayor capacidad, de acuerdo con las necesidades de la organización, garantizando la operación.				X	

	PLAN DE TRATAMIENTO												
	Indique el control a aplicar a partir de la norma ISO 27001:2013												
No. De Amenazas y Vulnerabilidades	Transferir	Aceptar	Eliminar	Mitigar	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control	Requerimiento Legal	Obligación Contractual	Requerimiento de	Análisis del Riesgo	Exclusión
11				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de no existir repuestos se pueda remplazar, adicionalmente mejorar la política de mantenimiento estableciendo un contrato para el mantenimiento preventivo y correctivo a todo costo que garantice el funcionamiento ininterrumpido de los equipos.				X	
12				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de avería se pueda remplazar				X	
13				X	DOMINIO_A9	OBJETIVO_A9_4	A9.4.1 Restricción de acceso a la información --Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	Restringir el acceso a la información de los equipos, mediante la política de control de accesos, adicionalmente de acuerdo con la vulnerabilidad identificada, se debe mantener actualizado el software de los dispositivos para que se instalen los parches de seguridad.				X	
14				X	DOMINIO_A12	OBJETIVO_A12_2	A12.2.1 Controles contra códigos maliciosos --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.	Disposición de software antimalware con actualizaciones automáticas y escaneo del sistema diario y en tiempo real. Implementar controles de detección, prevención y recuperación, para proteger contra software malicioso				X	
15				X	DOMINIO_A9	OBJETIVO_A9_2	A9.2.3 Gestión de derechos de acceso privilegiado --Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	Crear un proceso para realizar revisiones recuentes y periódicas de cuentas privilegiadas para identificar y deshabilitar / eliminar cuentas con privilegios redundantes y / o reducir los privilegios				X	

	PLAN DE TRATAMIENTO												
	Indique el control a aplicar a partir de la norma ISO 27001:2013												
No. De Amenazas y Vulnerabilidades	Transferir	Aceptar	Eliminar	Mitigar	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control	Requerimiento Legal	Obligación Contractual	Requerimiento de	Análisis del Riesgo	Exclusión
16				X	DOMINIO_A9	OBJETIVO_A9_2	A9.2.3 Gestión de derechos de acceso privilegiado --Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	Crear un proceso para realizar revisiones recuentes y periódicas de cuentas privilegiadas para identificar y deshabilitar / eliminar cuentas con privilegios redundantes y / o reducir los privilegios				X	
17				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Establecer una política para el mantenimiento y/o actualización del software				X	
18				X	DOMINIO_A9	OBJETIVO_A9_4	A9.4.1 Restricción de acceso a la información --Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	Restringir el acceso a la información de los equipos, mediante la política de control de accesos, adicionalmente de acuerdo con la vulnerabilidad identificada, se debe mantener actualizado el software de los dispositivos para que se instalen los parches de seguridad.				X	
19			X		DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Garantizar el cumplimiento del procedimiento establecido y aplicar el control				X	
20				**X**	DOMINIO_A12	OBJETIVO_A12_1	A12.1.1 Procedimientos de operación documentados --Control: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.	Documentar el procedimiento para el uso de los servidores con el fin de evitar errores por parte de los usuarios, por cuanto se puede dar una fuga de información.				X	
21				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.2 Servicios de suministro --Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	Verificar la capacidad de la UPS vs equipos que requieren continuidad de negocio, de ser necesario cambiar la UPS por una de mayor capacidad, de acuerdo con las necesidades de la organización.				X	

	PLAN DE TRATAMIENTO												
	Indique el control a aplicar a partir de la norma ISO 27001:2013												
No. De Amenazas y Vulnerabilidades	Transferir	Aceptar	Eliminar	Mitigar	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control	Requerimiento Legal	Obligación Contractual	Requerimiento de	Análisis del Riesgo	Exclusión
22				X	DOMINIO_A11	OBJETIVO_A11_1	A11.1.4 Protección contra amenazas externas y ambientales. --Control: Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	Establecer un procedimiento de recuperación de desastres.				X	
23			X		DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Garantizar el cumplimiento del procedimiento establecido y aplicar el control				X	
24				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de obsolescencia se pueda remplazar				X	
25				X	DOMINIO_A9	OBJETIVO_A9_2	A9.2.5 Revisión de los derechos de acceso de usuarios --Control: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	Se llevará el control de los usuarios a través del directorio activo y se tendrán actualizados los permisos según rol establecido. Garantizar el cumplimiento de la política de control de acceso.				X	
26				X	DOMINIO_A9	OBJETIVO_A9_2	A9.2.5 Revisión de los derechos de acceso de usuarios --Control: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	Se llevará el control de los usuarios a través del directorio activo y se tendrán actualizados los permisos según rol establecido. Garantizar el cumplimiento de la política de control de acceso.				X	
27				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.2 Servicios de suministro --Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	Verificar la capacidad de la UPS vs equipos que requieren continuidad de negocio, de ser necesario cambiar la UPS por una de mayor capacidad, de acuerdo con las necesidades de la organización, garantizando la operación.				X	

	PLAN DE TRATAMIENTO												
	Indique el control a aplicar a partir de la norma ISO 27001:2013												
No. De Amenazas y Vulnerabilidades	Transferir	Aceptar	Eliminar	Mitigar	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control	Requerimiento Legal	Obligación Contractual	Requerimiento de	Análisis del Riesgo	Exclusión
28				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.2 Servicios de suministro --Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	Verificar la capacidad de la UPS vs equipos que requieren continuidad de negocio, de ser necesario cambiar la UPS por una de mayor capacidad, de acuerdo con las necesidades de la organización, garantizando la operación.				X	
29				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de no existir repuestos se pueda remplazar, adicionalmente mejorar la política de mantenimiento estableciendo un contrato para el mantenimiento preventivo y correctivo a todo costo que garantice el funcionamiento ininterrumpido de los equipos.				X	
30				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de avería se pueda remplazar				X	
31				X	DOMINIO_A9	OBJETIVO_A9_2	A9.2.3 Gestión de derechos de acceso privilegiado --Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	Crear un proceso para realizar revisiones recuentes y periódicas de cuentas privilegiadas para identificar y deshabilitar / eliminar cuentas con privilegios redundantes y / o reducir los privilegios				X	
32				**X**	DOMINIO_A9	OBJETIVO_A9_1	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.	Se elaborará política de control de acceso a través de ACL. Implementar la autenticación de doble factor (2FA).				X	

	PLAN DE TRATAMIENTO												
	Indique el control a aplicar a partir de la norma ISO 27001:2013												
No. De Amenazas y Vulnerabilidades	Transferir	Aceptar	Eliminar	Mitigar	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control	Requerimiento Legal	Obligación Contractual	Requerimiento de	Análisis del Riesgo	Exclusión
33			X		DOMINIO_A9	OBJETIVO_A9_1	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.	Establecer política de control de acceso donde se incluya el acceso a los backups				X	
34					DOMINIO_A12	OBJETIVO_A12_3	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.	Documentar la política de copias de seguridad.				X	
35				X	DOMINIO_A9	OBJETIVO_A9_2	A9.2.3 Gestión de derechos de acceso privilegiado --Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	Crear un proceso para realizar revisiones recuentes y periódicas de cuentas privilegiadas para identificar y deshabilitar / eliminar cuentas con privilegios redundantes y / o reducir los privilegios				X	
36				X	DOMINIO_A9	OBJETIVO_A9_2	A9.2.5 Revisión de los derechos de acceso de usuarios --Control: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	Se llevará el control de los usuarios a través del directorio activo y se tendrán actualizados los permisos según rol establecido. Garantizar el cumplimiento de la política de control de acceso.				X	
37				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.2 Servicios de suministro --Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	Verificar la capacidad de la UPS vs equipos que requieren continuidad de negocio, de ser necesario cambiar la UPS por una de mayor capacidad, de acuerdo con las necesidades de la organización, garantizando la operación.				X	

	PLAN DE TRATAMIENTO												
	Indique el control a aplicar a partir de la norma ISO 27001:2013												
No. De Amenazas y Vulnerabilidades	Transferir	Aceptar	Eliminar	Mitigar	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control	Requerimiento Legal	Obligación Contractual	Requerimiento de	Análisis del Riesgo	Exclusión
38				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. -- Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de no existir repuestos se pueda remplazar, adicionalmente mejorar la política de mantenimiento estableciendo un contrato para el mantenimiento preventivo y correctivo a todo costo que garantice el funcionamiento ininterrumpido de los equipos.				X	
39				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. -- Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de avería se pueda remplazar				X	
40				X	DOMINIO_A9	OBJETIVO_A9_2	A9.2.3 Gestión de derechos de acceso privilegiado --Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	Crear un proceso para realizar revisiones recuentes y periódicas de cuentas privilegiadas para identificar y deshabilitar / eliminar cuentas con privilegios redundantes y / o reducir los privilegios				X	
41				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. -- Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Establecer una política para el mantenimiento y/o actualización del software				X	
42				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. -- Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Establecer una política para el mantenimiento y/o actualización del software				X	
43			X		DOMINIO_A9	OBJETIVO_A9_1	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.	Se llevará el control de los usuarios a través del directorio activo y se tendrán actualizados los permisos según rol establecido. Garantizar el cumplimiento de la política de control de acceso.				X	

	PLAN DE TRATAMIENTO												
	Indique el control a aplicar a partir de la norma ISO 27001:2013												
No. De Amenazas y Vulnerabilidades	Transferir	Aceptar	Eliminar	Mitigar	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control	Requerimiento Legal	Obligación Contractual	Requerimiento de	Análisis del Riesgo	Exclusión
44				X	DOMINIO_A12	OBJETIVO_A12_2	A12.2.1 Controles contra códigos maliciosos --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.	Disposición de software antimalware con actualizaciones automáticas y escaneo del sistema diario y en tiempo real. Implementar controles de detección, prevención y recuperación, para proteger contra software malicioso				X	
45				X	DOMINIO_A12	OBJETIVO_A12_2	A12.2.1 Controles contra códigos maliciosos --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.	Disposición de software antimalware con actualizaciones automáticas y escaneo del sistema diario y en tiempo real. Implementar controles de detección, prevención y recuperación, para proteger contra software malicioso				X	
46				X	DOMINIO_A9	OBJETIVO_A9_2	A9.2.3 Gestión de derechos de acceso privilegiado --Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	Crear un proceso para realizar revisiones recuentes y periódicas de cuentas privilegiadas para identificar y deshabilitar / eliminar cuentas con privilegios redundantes y / o reducir los privilegios				X	
47			X		DOMINIO_A12	OBJETIVO_A12_2	A12.2.1 Controles contra códigos maliciosos --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.	Establecer política y procedimientos asociados a controles antimalware				X	
48			X		DOMINIO_A9	OBJETIVO_A9_1	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.	Establecer VPN para la conexión segura a la red de la empresa, con el fin que se tenga un cifrado de extremo a extremo.				X	

	PLAN DE TRATAMIENTO												
	Indique el control a aplicar a partir de la norma ISO 27001:2013												
No. De Amenazas y Vulnerabilidades	Transferir	Aceptar	Eliminar	Mitigar	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control	Requerimiento Legal	Obligación Contractual	Requerimiento de	Análisis del Riesgo	Exclusión
49			X		DOMINIO_A9	OBJETIVO_A9_1	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.	Establecer VPN para la conexión segura a la red de la empresa, con el fin que se tenga un cifrado de extremo a extremo.				X	
50				X	DOMINIO_A12	OBJETIVO_A12_2	A12.2.1 Controles contra códigos maliciosos --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.	Disposición de software antimalware con actualizaciones automáticas y escaneo del sistema diario y en tiempo real. Implementar controles de detección, prevención y recuperación, para proteger contra software malicioso				X	
51			X		DOMINIO_A9	OBJETIVO_A9_1	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.	Establecer VPN para la conexión segura a la red de la empresa, con el fin que se tenga un cifrado de extremo a extremo.				X	
52				X	DOMINIO_A12	OBJETIVO_A12_2	A12.2.1 Controles contra códigos maliciosos --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.	Disposición de software antimalware con actualizaciones automáticas y escaneo del sistema diario y en tiempo real. Implementar controles de detección, prevención y recuperación, para proteger contra software malicioso				X	
53				X	DOMINIO_A12	OBJETIVO_A12_2	A12.2.1 Controles contra códigos maliciosos --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.	Disposición de software antimalware con actualizaciones automáticas y escaneo del sistema diario y en tiempo real. Implementar controles de detección, prevención y recuperación, para proteger contra software malicioso				X	

	PLAN DE TRATAMIENTO												
	Indique el control a aplicar a partir de la norma ISO 27001:2013												
No. De Amenazas y Vulnerabilidades	Transferir	Aceptar	Eliminar	Mitigar	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control	Requerimiento Legal	Obligación Contractual	Requerimiento de	Análisis del Riesgo	Exclusión
54			X		DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Garantizar el cumplimiento del procedimiento establecido y aplicar el control				X	
55				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de obsolescencia se pueda remplazar				X	
56				X	DOMINIO_A9	OBJETIVO_A9_2	A9.2.5 Revisión de los derechos de acceso de usuarios --Control: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	Se llevará el control de los usuarios a través del directorio activo y se tendrán actualizados los permisos según rol establecido. Garantizar el cumplimiento de la política de control de acceso.				X	
57				X	DOMINIO_A9	OBJETIVO_A9_2	A9.2.5 Revisión de los derechos de acceso de usuarios --Control: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	Se llevará el control de los usuarios a través del directorio activo y se tendrán actualizados los permisos según rol establecido. Garantizar el cumplimiento de la política de control de acceso.				X	
58				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Establecer una política para el mantenimiento y/o actualización del software				X	
59				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Establecer una política para el mantenimiento y/o actualización del software				X	
60			X		DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Garantizar el cumplimiento del procedimiento establecido y aplicar el control				X	

	PLAN DE TRATAMIENTO												
	Indique el control a aplicar a partir de la norma ISO 27001:2013												
No. De Amenazas y Vulnerabilidades	Transferir	Aceptar	Eliminar	Mitigar	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control	Requerimiento Legal	Obligación Contractual	Requerimiento de	Análisis del Riesgo	Exclusión
61				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de obsolescencia se pueda remplazar				X	
62				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.2 Servicios de suministro --Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	Verificar la capacidad de la UPS vs equipos que requieren continuidad de negocio, de ser necesario cambiar la UPS por una de mayor capacidad, de acuerdo con las necesidades de la organización, garantizando la operación.				X	
63				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de no existir repuestos se pueda remplazar, adicionalmente mejorar la política de mantenimiento estableciendo un contrato para el mantenimiento preventivo y correctivo a todo costo que garantice el funcionamiento ininterrumpido de los equipos.				X	
64				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de avería se pueda remplazar				X	
65			X		DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Garantizar el cumplimiento del procedimiento establecido y aplicar el control				X	
66				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de obsolescencia se pueda remplazar				X	

	PLAN DE TRATAMIENTO												
	Indique el control a aplicar a partir de la norma ISO 27001:2013												
No. De Amenazas y Vulnerabilidades	Transferir	Aceptar	Eliminar	Mitigar	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control	Requerimiento Legal	Obligación Contractual	Requerimiento de	Análisis del Riesgo	Exclusión
67				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.2 Servicios de suministro --Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	Verificar la capacidad de la UPS vs equipos que requieren continuidad de negocio, de ser necesario cambiar la UPS por una de mayor capacidad, de acuerdo con las necesidades de la organización, garantizando la operación.				X	
68				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de no existir repuestos se pueda remplazar, adicionalmente mejorar la política de mantenimiento estableciendo un contrato para el mantenimiento preventivo y correctivo a todo costo que garantice el funcionamiento ininterrumpido de los equipos.				X	
69				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de avería se pueda remplazar				X	
70				X	DOMINIO_A9	OBJETIVO_A9_4	A9.4.1 Restricción de acceso a la información --Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	Restringir el acceso a la información de los equipos, mediante la política de control de accesos, adicionalmente de acuerdo con la vulnerabilidad identificada, se debe mantener actualizado el software de los dispositivos para que se instalen los parches de seguridad.				X	
71				X	DOMINIO_A9	OBJETIVO_A9_2	A9.2.3 Gestión de derechos de acceso privilegiado --Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	Crear un proceso para realizar revisiones recuentes y periódicas de cuentas privilegiadas para identificar y deshabilitar / eliminar cuentas con privilegios redundantes y / o reducir los privilegios				X	

	PLAN DE TRATAMIENTO												
	Indique el control a aplicar a partir de la norma ISO 27001:2013												
No. De Amenazas y Vulnerabilidades	Transferir	Aceptar	Eliminar	Mitigar	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control	Requerimiento Legal	Obligación Contractual	Requerimiento de	Análisis del Riesgo	Exclusión
72				X	DOMINIO_A9	OBJETIVO_A9_4	A9.4.1 Restricción de acceso a la información --Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	Restringir el acceso a la información de los equipos, mediante la política de control de accesos, adicionalmente de acuerdo con la vulnerabilidad identificada, se debe mantener actualizado el software de los dispositivos para que se instalen los parches de seguridad.				X	
73			X		DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. -- Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Garantizar el cumplimiento del procedimiento establecido y aplicar el control				X	
74				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. -- Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de obsolescencia se pueda remplazar				X	
75				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. -- Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Establecer una política para el mantenimiento y/o actualización del software				X	
76				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. -- Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Establecer una política para el mantenimiento y/o actualización del software				X	
77				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. -- Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Establecer una política para el mantenimiento y/o actualización del software				X	
78			X		DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. -- Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Garantizar el cumplimiento del procedimiento establecido y aplicar el control				X	

	PLAN DE TRATAMIENTO												
	Indique el control a aplicar a partir de la norma ISO 27001:2013												
No. De Amenazas y Vulnerabilidades	Transferir	Aceptar	Eliminar	Mitigar	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control	Requerimiento Legal	Obligación Contractual	Requerimiento de	Análisis del Riesgo	Exclusión
79				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de obsolescencia se pueda remplazar				X	
80				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.2 Servicios de suministro --Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	Verificar la capacidad de la UPS vs equipos que requieren continuidad de negocio, de ser necesario cambiar la UPS por una de mayor capacidad, de acuerdo con las necesidades de la organización, garantizando la operación.				X	
81				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de no existir repuestos se pueda remplazar, adicionalmente mejorar la política de mantenimiento estableciendo un contrato para el mantenimiento preventivo y correctivo a todo costo que garantice el funcionamiento ininterrumpido de los equipos.				X	
82				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de avería se pueda remplazar				X	
83			X		DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Garantizar el cumplimiento del procedimiento establecido y aplicar el control				X	
84				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de obsolescencia se pueda remplazar				X	

	PLAN DE TRATAMIENTO												
	Indique el control a aplicar a partir de la norma ISO 27001:2013												
No. De Amenazas y Vulnerabilidades	Transferir	Aceptar	Eliminar	Mitigar	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control	Requerimiento Legal	Obligación Contractual	Requerimiento de	Análisis del Riesgo	Exclusión
85				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.2 Servicios de suministro --Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	Verificar la capacidad de la UPS vs equipos que requieren continuidad de negocio, de ser necesario cambiar la UPS por una de mayor capacidad, de acuerdo con las necesidades de la organización, garantizando la operación.				X	
86				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de no existir repuestos se pueda remplazar, adicionalmente mejorar la política de mantenimiento estableciendo un contrato para el mantenimiento preventivo y correctivo a todo costo que garantice el funcionamiento ininterrumpido de los equipos.				X	
87				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de avería se pueda remplazar				X	
88			X		DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Garantizar el cumplimiento del procedimiento establecido y aplicar el control				X	
89				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de obsolescencia se pueda remplazar				X	
90				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.2 Servicios de suministro --Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	Verificar la capacidad de la UPS vs equipos que requieren continuidad de negocio, de ser necesario cambiar la UPS por una de mayor capacidad, de acuerdo con las necesidades de la organización, garantizando la operación.				X	

	PLAN DE TRATAMIENTO												
	Indique el control a aplicar a partir de la norma ISO 27001:2013												
No. De Amenazas y Vulnerabilidades	Transferir	Aceptar	Eliminar	Mitigar	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control	Requerimiento Legal	Obligación Contractual	Requerimiento de	Análisis del Riesgo	Exclusión
91				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de no existir repuestos se pueda remplazar, adicionalmente mejorar la política de mantenimiento estableciendo un contrato para el mantenimiento preventivo y correctivo a todo costo que garantice el funcionamiento ininterrumpido de los equipos.				X	
92			X		DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Garantizar el cumplimiento del procedimiento establecido y aplicar el control				X	
93				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de obsolescencia se pueda remplazar				X	
94				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.2 Servicios de suministro --Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	Verificar la capacidad de la UPS vs equipos que requieren continuidad de negocio, de ser necesario cambiar la UPS por una de mayor capacidad, de acuerdo con las necesidades de la organización, garantizando la operación.				X	
95				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de no existir repuestos se pueda remplazar, adicionalmente mejorar la política de mantenimiento estableciendo un contrato para el mantenimiento preventivo y correctivo a todo costo que garantice el funcionamiento ininterrumpido de los equipos.				X	

	PLAN DE TRATAMIENTO												
	Indique el control a aplicar a partir de la norma ISO 27001:2013												
No. De Amenazas y Vulnerabilidades	Transferir	Aceptar	Eliminar	Mitigar	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control	Requerimiento Legal	Obligación Contractual	Requerimiento de	Análisis del Riesgo	Exclusión
96			X		DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Garantizar el cumplimiento del procedimiento establecido y aplicar el control				X	
97				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de obsolescencia se pueda remplazar				X	
98				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.2 Servicios de suministro --Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	Verificar la capacidad de la UPS vs equipos que requieren continuidad de negocio, de ser necesario cambiar la UPS por una de mayor capacidad, de acuerdo con las necesidades de la organización, garantizando la operación.				X	
99				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de no existir repuestos se pueda remplazar, adicionalmente mejorar la política de mantenimiento estableciendo un contrato para el mantenimiento preventivo y correctivo a todo costo que garantice el funcionamiento ininterrumpido de los equipos.				X	
100			X		DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Garantizar el cumplimiento del procedimiento establecido y aplicar el control				X	
101				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de obsolescencia se pueda remplazar				X	

	PLAN DE TRATAMIENTO												
	Indique el control a aplicar a partir de la norma ISO 27001:2013												
No. De Amenazas y Vulnerabilidades	Transferir	Aceptar	Eliminar	Mitigar	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control	Requerimiento Legal	Obligación Contractual	Requerimiento de	Análisis del Riesgo	Exclusión
102				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.2 Servicios de suministro --Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	Verificar la capacidad de la UPS vs equipos que requieren continuidad de negocio, de ser necesario cambiar la UPS por una de mayor capacidad, de acuerdo con las necesidades de la organización, garantizando la operación.				X	
103				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de no existir repuestos se pueda remplazar, adicionalmente mejorar la política de mantenimiento estableciendo un contrato para el mantenimiento preventivo y correctivo a todo costo que garantice el funcionamiento ininterrumpido de los equipos.				X	
104			X		DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Garantizar el cumplimiento del procedimiento establecido y aplicar el control				X	
105				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de obsolescencia se pueda remplazar				X	
106				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.2 Servicios de suministro --Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	Verificar la capacidad de la UPS vs equipos que requieren continuidad de negocio, de ser necesario cambiar la UPS por una de mayor capacidad, de acuerdo con las necesidades de la organización, garantizando la operación.				X	

	PLAN DE TRATAMIENTO												
	Indique el control a aplicar a partir de la norma ISO 27001:2013												
No. De Amenazas y Vulnerabilidades	Transferir	Aceptar	Eliminar	Mitigar	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control	Requerimiento Legal	Obligación Contractual	Requerimiento de	Análisis del Riesgo	Exclusión
107				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de no existir repuestos se pueda remplazar, adicionalmente mejorar la política de mantenimiento estableciendo un contrato para el mantenimiento preventivo y correctivo a todo costo que garantice el funcionamiento ininterrumpido de los equipos.				X	
108			X		DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Garantizar el cumplimiento del procedimiento establecido y aplicar el control				X	
109				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de obsolescencia se pueda remplazar				X	
110				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.2 Servicios de suministro --Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	Verificar la capacidad de la UPS vs equipos que requieren continuidad de negocio, de ser necesario cambiar la UPS por una de mayor capacidad, de acuerdo con las necesidades de la organización, garantizando la operación.				X	
111				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de no existir repuestos se pueda remplazar, adicionalmente mejorar la política de mantenimiento estableciendo un contrato para el mantenimiento preventivo y correctivo a todo costo que garantice el funcionamiento ininterrumpido de los equipos.				X	

	PLAN DE TRATAMIENTO												
	Indique el control a aplicar a partir de la norma ISO 27001:2013												
No. De Amenazas y Vulnerabilidades	Transferir	Aceptar	Eliminar	Mitigar	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control	Requerimiento Legal	Obligación Contractual	Requerimiento de	Análisis del Riesgo	Exclusión
112			X		DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Garantizar el cumplimiento del procedimiento establecido y aplicar el control				X	
113				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de obsolescencia se pueda remplazar				X	
114				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.2 Servicios de suministro --Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	Verificar la capacidad de la UPS vs equipos que requieren continuidad de negocio, de ser necesario cambiar la UPS por una de mayor capacidad, de acuerdo con las necesidades de la organización, garantizando la operación.				X	
115				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de no existir repuestos se pueda remplazar, adicionalmente mejorar la política de mantenimiento estableciendo un contrato para el mantenimiento preventivo y correctivo a todo costo que garantice el funcionamiento ininterrumpido de los equipos.				X	
116				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de obsolescencia se pueda remplazar				X	

	PLAN DE TRATAMIENTO												
	Indique el control a aplicar a partir de la norma ISO 27001:2013												
No. De Amenazas y Vulnerabilidades	Transferir	Aceptar	Eliminar	Mitigar	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control	Requerimiento Legal	Obligación Contractual	Requerimiento de	Análisis del Riesgo	Exclusión
117				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. -- Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de no existir repuestos se pueda remplazar, adicionalmente mejorar la política de mantenimiento estableciendo un contrato para el mantenimiento preventivo y correctivo a todo costo que garantice el funcionamiento ininterrumpido de los equipos.				X	
118			X		DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. -- Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Garantizar el cumplimiento del procedimiento establecido y aplicar el control				X	
119				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. -- Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de obsolescencia se pueda remplazar				X	
120				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. -- Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de no existir repuestos se pueda remplazar, adicionalmente mejorar la política de mantenimiento estableciendo un contrato para el mantenimiento preventivo y correctivo a todo costo que garantice el funcionamiento ininterrumpido de los equipos.				X	
121			X		DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. -- Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Garantizar el cumplimiento del procedimiento establecido y aplicar el control				X	
122				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. -- Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de obsolescencia se pueda remplazar				X	

	PLAN DE TRATAMIENTO												
	Indique el control a aplicar a partir de la norma ISO 27001:2013												
No. De Amenazas y Vulnerabilidades	Transferir	Aceptar	Eliminar	Mitigar	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control	Requerimiento Legal	Obligación Contractual	Requerimiento de	Análisis del Riesgo	Exclusión
123				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de no existir repuestos se pueda remplazar, adicionalmente mejorar la política de mantenimiento estableciendo un contrato para el mantenimiento preventivo y correctivo a todo costo que garantice el funcionamiento ininterrumpido de los equipos.				X	
124				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de avería se pueda remplazar				X	
125				X	DOMINIO_A9	OBJETIVO_A9_4	A9.4.1 Restricción de acceso a la información --Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	Restringir el acceso a la información de los equipos, mediante la política de control de accesos, adicionalmente de acuerdo con la vulnerabilidad identificada, se debe mantener actualizado el software de los dispositivos para que se instalen los parches de seguridad.				X	
126				X	DOMINIO_A9	OBJETIVO_A9_2	A9.2.3 Gestión de derechos de acceso privilegiado --Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	Crear un proceso para realizar revisiones recuentes y periódicas de cuentas privilegiadas para identificar y deshabilitar / eliminar cuentas con privilegios redundantes y / o reducir los privilegios				X	
127			X		DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Garantizar el cumplimiento del procedimiento establecido y aplicar el control				X	
128				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de obsolescencia se pueda remplazar				X	

	PLAN DE TRATAMIENTO												
	Indique el control a aplicar a partir de la norma ISO 27001:2013												
No. De Amenazas y Vulnerabilidades	Transferir	Aceptar	Eliminar	Mitigar	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control	Requerimiento Legal	Obligación Contractual	Requerimiento de	Análisis del Riesgo	Exclusión
129				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de no existir repuestos se pueda remplazar, adicionalmente mejorar la política de mantenimiento estableciendo un contrato para el mantenimiento preventivo y correctivo a todo costo que garantice el funcionamiento ininterrumpido de los equipos.				X	
130				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de avería se pueda remplazar				X	
131				X	DOMINIO_A9	OBJETIVO_A9_4	A9.4.1 Restricción de acceso a la información --Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	Restringir el acceso a la información de los equipos, mediante la política de control de accesos, adicionalmente de acuerdo con la vulnerabilidad identificada, se debe mantener actualizado el software de los dispositivos para que se instalen los parches de seguridad.				X	
132				X	DOMINIO_A9	OBJETIVO_A9_2	A9.2.3 Gestión de derechos de acceso privilegiado --Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	Crear un proceso para realizar revisiones recuentes y periódicas de cuentas privilegiadas para identificar y deshabilitar / eliminar cuentas con privilegios redundantes y / o reducir los privilegios				X	
133			X		DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Garantizar el cumplimiento del procedimiento establecido y aplicar el control				X	
134				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de obsolescencia se pueda remplazar				X	

	PLAN DE TRATAMIENTO												
	Indique el control a aplicar a partir de la norma ISO 27001:2013												
No. De Amenazas y Vulnerabilidades	Transferir	Aceptar	Eliminar	Mitigar	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control	Requerimiento Legal	Obligación Contractual	Requerimiento de	Análisis del Riesgo	Exclusión
135				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de no existir repuestos se pueda remplazar, adicionalmente mejorar la política de mantenimiento estableciendo un contrato para el mantenimiento preventivo y correctivo a todo costo que garantice el funcionamiento ininterrumpido de los equipos.				X	
136				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de avería se pueda remplazar				X	
137				X	DOMINIO_A9	OBJETIVO_A9_4	A9.4.1 Restricción de acceso a la información --Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	Restringir el acceso a la información de los equipos, mediante la política de control de accesos, adicionalmente de acuerdo con la vulnerabilidad identificada, se debe mantener actualizado el software de los dispositivos para que se instalen los parches de seguridad.				X	
138				X	DOMINIO_A9	OBJETIVO_A9_2	A9.2.3 Gestión de derechos de acceso privilegiado --Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	Crear un proceso para realizar revisiones recuentes y periódicas de cuentas privilegiadas para identificar y deshabilitar / eliminar cuentas con privilegios redundantes y / o reducir los privilegios				X	
139				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de obsolescencia se pueda remplazar				X	

	PLAN DE TRATAMIENTO												
	Indique el control a aplicar a partir de la norma ISO 27001:2013												
No. De Amenazas y Vulnerabilidades	Transferir	Aceptar	Eliminar	Mitigar	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control	Requerimiento Legal	Obligación Contractual	Requerimiento de	Análisis del Riesgo	Exclusión
140				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. -- Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de no existir repuestos se pueda remplazar, adicionalmente mejorar la política de mantenimiento estableciendo un contrato para el mantenimiento preventivo y correctivo a todo costo que garantice el funcionamiento ininterrumpido de los equipos.				X	
141				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. -- Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de avería se pueda remplazar				X	
142				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. -- Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de obsolescencia se pueda remplazar				X	
143				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. -- Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de no existir repuestos se pueda remplazar, adicionalmente mejorar la política de mantenimiento estableciendo un contrato para el mantenimiento preventivo y correctivo a todo costo que garantice el funcionamiento ininterrumpido de los equipos.				X	
144				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. -- Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de avería se pueda remplazar				X	
145				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. -- Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de obsolescencia se pueda remplazar				X	

	PLAN DE TRATAMIENTO												
	Indique el control a aplicar a partir de la norma ISO 27001:2013												
No. De Amenazas y Vulnerabilidades	Transferir	Aceptar	Eliminar	Mitigar	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control	Requerimiento Legal	Obligación Contractual	Requerimiento de	Análisis del Riesgo	Exclusión
146				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. -- Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de no existir repuestos se pueda remplazar, adicionalmente mejorar la política de mantenimiento estableciendo un contrato para el mantenimiento preventivo y correctivo a todo costo que garantice el funcionamiento ininterrumpido de los equipos.				X	
147				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. -- Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar los equipos con el fin que en caso de avería se pueda remplazar				X	
148				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. -- Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Establecer una política para el mantenimiento y/o actualización del software				X	
149				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. -- Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Establecer una política para el mantenimiento y/o actualización del software				X	
150				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. -- Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Establecer una política para el mantenimiento y/o actualización del software				X	
151				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. -- Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Establecer una política para el mantenimiento y/o actualización del software				X	
152				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. -- Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Establecer una política para el mantenimiento y/o actualización del software				X	

	PLAN DE TRATAMIENTO												
	Indique el control a aplicar a partir de la norma ISO 27001:2013												
No. De Amenazas y Vulnerabilidades	Transferir	Aceptar	Eliminar	Mitigar	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control	Requerimiento Legal	Obligación Contractual	Requerimiento de	Análisis del Riesgo	Exclusión
153				X	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. -- Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Establecer una política para el mantenimiento y/o actualización del software				X	

Fuente: elaboración propia a partir del instrumento matriz de análisis de riesgos de ciberseguridad.

Para una mejor visualización y comprensión del plan de tratamiento de los riesgos de la seguridad de la información de los activos de información, se invita a consultar al Anexo A - Matriz Análisis de Riesgos CDA Motocentro.xlsx en la hoja **APT**, matriz que hace parte integral de este proyecto aplicado.

7 CONCLUSIONES

Se realizó el análisis de la infraestructura tecnológica de la empresa CDA MOTOCENTRO S.A.S. y se hizo la identificación de 76 activos de información en el área de TI, logrando su tipificación de acuerdo con lo planteado por la metodología MAGERIT V3 así: i. [K] Claves Criptográficas: dos (2), ii. [S] Servicio: dos (2), iii. [SW] Software: cuarenta (40) y iv. [HW] Hardware: treinta y dos (32), en ese mismo sentido se logró la clasificación de estos según el impacto a nivel de seguridad de la información, donde 10 activos tienen impacto leve, 58 importante y 8 grave.

Una vez identificados y tipificados los activos de información, se estableció la matriz con el análisis y evaluación de los riesgos de seguridad de los activos de información del área de TI de MOTOCENTRO S.A.S., que de acuerdo con las dimensiones que propone la metodología MAGERIT V3 para la valoración de riesgos, se identificaron 5 riesgos con nivel Moderado y 148 con nivel Inaceptable, según su valoración de probabilidad e impacto. Así mismo, se identificó el nivel de riesgo en los 76 activos de información de TI donde 2 activos tienen nivel bajo, 9 nivel medio, 36 nivel alto y 29 nivel extremo, según el impacto en la confidencialidad, integridad y disponibilidad de la información.

Con el análisis y la evaluación de los riesgos de seguridad de los activos de información del área de TI de MOTOCENTRO S.A.S. se lograron identificar 153 posibles vulnerabilidades de los activos de información, de las cuales luego de su valoración de probabilidad e impacto se tienen 5 con nivel de Riesgo Moderado y 148 con nivel de riesgo Inaceptable, frente a lo cual se diseñó el plan de tratamiento de riesgos de seguridad de la información, el cual contiene cada uno de los controles del anexo A de la norma ISO/IEC 27001 que se deben aplicar para cada una de las 153 vulnerabilidades identificadas, logrando mejorar los niveles de seguridad informática de los activos de información del área de TI.

De acuerdo con las anteriores conclusiones, se logró cumplir con lo planteado tanto en el objetivo general como en los objetivos específicos del presente proyecto aplicado.

8 RECOMENDACIONES

Para que un plan de tratamiento de riesgos sea exitoso se debe tener presente las siguientes recomendaciones:

- Identificar y valorar los activos de información: se debe realizar un inventario y clasificación de los activos de información que hacen parte de la organización, como estrategia con respecto a la seguridad de estos, de conformidad con lo planteado en la norma ISO/IEC 27001:2013 y la metodología MAGERIT V. 3.0.

- Realizar análisis y puntuación del riesgo: lo más recomendable es tener un inventario de los riesgos con su respectiva valoración, donde se pueda visualizar que tan crítico es el riesgo de cada uno de los activos de información (extremo, alto, medio, bajo), esto se logra con la valoración cualitativa y cuantitativa de los activos.

- Promover la capacitación del personal de CDA MOTOCENTRO S.A.S sobre el uso adecuado de los datos, las TICs y la normatividad legal vigente relacionada directamente con los estándares de seguridad como lo es la norma ISO/IEC 27001:2013, mitigando de esta manera las debilidades en los sistemas de información que se utilizan en el día a día de la empresa, con el fin de aumentar la seguridad de la información que garantice la integridad, confidencialidad y disponibilidad de la misma y manteniendo un estricto control de sus activos impidiendo su perdida y manipulación.

- Se sugiere a la empresa realizar una validación de los niveles de riesgo según la clasificación y valoración de los activos de información, basándose en la metodología de análisis y gestión de riesgos MAGERIT V3.0, para que de esta manera sea más sencilla la identificación de las amenazas y

vulnerabilidades permitiendo establecer controles que sean eficaces y que generen confianza al momento de proteger la información.

- Llevar a cabo el plan de tratamiento de riesgos de seguridad de la información, aplicando los diferentes controles definidos para cada una de las posibles vulnerabilidades con el fin de mejorar la seguridad de los activos de información.

BIBLIOGRAFÍA

ALEMÁN, Helena; RODRÍGUEZ, Claudia “Metodologías Para el Análisis de Riesgos en los SGSI”. Journal specializingin engineering, Vol.; 9. No 1. {En linea} {29 de enero de 2019} disponible en (http://hemeroteca.unad.edu.co/index.php/publicaciones-einvestigacion/article/view/1435/1874)

ANDRADE, Diego. Análisis de los conceptos, elementos y técnicas de la gestión de riesgo orientado a las pymes del sector de las telecomunicaciones basado en magerit v3. 2021, 136 p. Monografía (Especialización en Seguridad Informática). UNAD. Escuela de Ciencias Básicas, Tecnología e Ingeniería - ECBTI disponible en: (https://repository.unad.edu.co/handle/10596/43373)

BOJACÁ, Edgar. Diseño de un Sistema de Gestión de Seguridad Informática basado en la norma ISO/IEC 27001- 27002 para el área administrativa y de historias clínicas del Hospital San Francisco de Gachetá. 2016, 204p. Monografía (Especialización en Seguridad Informática). Universidad Nacional Abierta y a Distancia UNAD. Escuela de Ciencias Básicas, Tecnología e Ingeniería - ECBTI disponible en (https://repository.unad.edu.co/handle/10596/12685)

CASTILLO, Anthony. Modelo para la gestión del riesgo en TI como apoyo a las entidades públicas dedicadas a promover la ciencia, cultura, tecnología e innovación tecnológica de la ciudad de Cali. 2022, 169p. Proyecto aplicado (Especialización en Seguridad Informática). Universidad Nacional Abierta y a Distancia UNAD. Escuela de Ciencias Básicas, Tecnología e Ingeniería - ECBTI disponible en (https://repository.unad.edu.co/handle/10596/51651)

CRIOLLO, Irmaena. Etapa de planificación de un sistema de gestión de seguridad de la información para el área de tecnología de la IPS Garper Médica SAS basado en la norma ISO/IEC 27001:2013.2021, 182p. Proyecto aplicado (Especialización

en Seguridad Informática). Universidad Nacional Abierta y a Distancia UNAD. Escuela de Ciencias Básicas, Tecnología e Ingeniería - ECBTI disponible en (https://repository.unad.edu.co/handle/10596/48702)

ESET ®. Security Report Latinoamérica 2020 {en línea} {13 de abril de 2022} disponible en (https://www.welivesecurity.com/wp-content/uploads/2020/08/ESET-Security-Report-LATAM_2020.pdf)

FERRUZOLA, Enrique; DUCHIMAZA, Johanna; RAMOS, Johanna, ALEJANDRO, Maria. Plan de contingencia para los equipos y sistemas informáticos utilizando la metodología Magerit. Revista Científica y Tecnológica UPSE, 6 (1), 34-41. DOI: 10.26423/rctu. v6i1.429 {en línea} {20 de mayo de 2022} disponible en: (https://incyt.upse.edu.ec/ciencia/revistas/index.php/rctu/article/view/429/362)

GOMEZ, Alvaro. B-secure pasión por la seguridad. Vulnerabilidades en el producto MySQL de Oracle {en línea} {30 de noviembre de 2022} disponible en: (https://www.b-secure.co/alertas-seguridad/vulnerabilidades-en-el-producto-mysql-de-oracle)

INCIBE. ¡Fácil y sencillo! Análisis de riesgos en 6 pasos {en línea} {26 de mayo de 2022} disponible en (https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo)

INCIBE. Protección de la información. España. {en línea} {17 de abril de 2022} disponible en https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion-de-la-informacion.pdf

INCIBE. Vulnerabilidad en Cobian Backup (CVE-2017-11318) {en línea} {9 de diciembre de 2022} disponible en (https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2017-11318)

INCIBE. Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? {en línea} {17 de abril de 2022} disponible en (https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian)

ISO27000.COM. Serie "27000" {en línea} {10 de marzo de 2022} disponible en (https://www.iso27000.es/iso27000.html)

ISOTOOLS EXCELLENCE. Sistemas de Gestión de Riesgos y Seguridad {en línea} {12 de marzo de 2022} disponible en (https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/)

MENDOZA, Denis. Diseño de un sistema de gestión de seguridad de la información basado en la Norma ISO/IEC 27001 para la Secretaría de Educación Departamental del Norte de Santander. 2019, 234p. Proyecto aplicado (Especialización en Seguridad Informática). Universidad Nacional Abierta y a Distancia UNAD. Escuela de Ciencias Básicas, Tecnología e Ingeniería - ECBTI disponible en https://repository.unad.edu.co/handle/10596/30723

MINTIC. Controles de seguridad y privacidad de la información {en línea} {23 de mayo de 2022} disponible en (https://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf)

MINTIC. Guía para la Gestión y Clasificación de Activos de Información. {en línea} {23 de mayo de 2022} disponible en (https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf)

MOLINA, Sandra; QUINTERO, Jack. Diseño de un sistema de gestión de seguridad de la información (SGSI) para la empresa Bonos y Descuentos S.A.S, a partir de la norma ISO 27001:2013. 2021, 136p. Proyecto aplicado (Especialización en

Seguridad Informática). Universidad Nacional Abierta y a Distancia UNAD. Escuela de Ciencias Básicas, Tecnología e Ingeniería - ECBTI disponible en. https://repository.unad.edu.co/handle/10596/48928

OIDOR, Juan. Diseño de un Sistema de Gestión de Seguridad de la Información - SGSI bajo la norma ISO/IEC 27001:2013 para la empresa “en Línea Financiera” de la ciudad de Cali – Colombia. 2016, 143p. Proyecto aplicado (Especialización en Seguridad Informática). Universidad Nacional Abierta y a Distancia UNAD. Escuela de Ciencias Básicas, Tecnología e Ingeniería - ECBTI disponible en https://repository.unad.edu.co/handle/10596/11907

OÑATE, Adriana. Propuesta de Políticas de Seguridad de la Información para proteger los activos de información en las organizaciones. 2021, 79p. Monografía (Especialización en Seguridad Informática). Universidad Nacional Abierta y a Distancia UNAD. Escuela de Ciencias Básicas, Tecnología e Ingeniería - ECBTI disponible en https://repository.unad.edu.co/handle/10596/41984

ORTIZ, Amparo. Análisis de riesgos basado en la Norma Magerit v3 de la red WLAN de las Instituciones de Educación Superior del Tolima. 2021, 120p. Monografía (Especialización en Seguridad Informática). Universidad Nacional Abierta y a Distancia UNAD. Escuela de Ciencias Básicas, Tecnología e Ingeniería - ECBTI disponible en https://repository.unad.edu.co/handle/10596/41960

ORTIZ, Roger; PRADA, German. Diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) para el área de Tecnologías de la Información y la Comunicación del Hospital San Vicente de Paúl de Fresno. 2022, 98p. Proyecto aplicado (Especialización en Seguridad Informática). Universidad Nacional Abierta y a Distancia UNAD. Escuela de Ciencias Básicas, Tecnología e Ingeniería - ECBTI disponible en https://repository.unad.edu.co/handle/10596/51482

PAREDES, Adriana. ANÁLISIS DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN UTILIZANDO LA METODOLOGÍA MAGERIT EN LA INSTITUCIÓN

EDUCATIVA DOMINGO SAVIO EN LA CIUDAD DE FLORENCIA – CAQUETÁ. {en línea} {17 de marzo de 2022} disponible en (https://repository.unad.edu.co/bitstream/handle/10596/19646/1078748025.pdf?sequence=1&isAllowed=y)

PORTAL ADMINISTRACIÓN ELECTRÓNICA. MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I: Método. Libro II: Catálogo de Elementos. Libro III: Guía de Técnicas {en línea} {10 de marzo de 2022} disponible en (https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html)

QUINTANA, Juan. EVALUACIÓN DEL NIVEL DEL RIESGO EN SEGURIDAD DE LA INFORMACIÓN PARA LAS SECRETARIAS DE PLANEACIÓN E INFRAESTRUCTURA DE LA ALCALDÍA DE TUNJA A TRAVÉS DE LA METODOLOGÍA STRIDE / DREAD. {en línea} {6 de mayo de 2022} disponible en (https://repository.usta.edu.co/bitstream/handle/11634/30829/2018juanquintana.pdf?sequence=1&isAllowed=y)

ROJAS, Hernán. APLICACION DE LA METODOLOGÍA MAGERIT PARA EL ANÁLISIS DE RIESGOS DE LOS SISTEMAS DE CONTROL EN LA ESTACIÓN TENAY DEL OLEODUCTO {en línea} {14 de abril de 2022} disponible en (https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/27758/1/1075211684.pdf)

SAAVEDRA, Jorge. DISEÑO DE UN PLAN DE GESTIÓN DE RIESGOS Y VULNERABILIDADES DEL CASO DE ESTUDIO DE LA EMPRESA QWERTY S.A., BASADOS EN LOS ESTÁNDAR NTC-ISO/IEC 27001 Y NTC-ISO/IEC 27032 {en línea} {13 de abril de 2022} disponible en

(https://repository.unad.edu.co/bitstream/handle/10596/36866/jsaavedraag.pdf?sequence=3)

SUÁREZ, John. Diseño de la fase de planeación para el sistema de gestión de seguridad de la información a partir de la norma ISO/IEC 27001:2013 para la empresa grupo confeccionistas. 2021, 138p. Proyecto aplicado (Especialización en Seguridad Informática). Universidad Nacional Abierta y a Distancia UNAD. Escuela de Ciencias Básicas, Tecnología e Ingeniería - ECBTI disponible en. https://repository.unad.edu.co/handle/10596/48930

TARAZONA, Cesar. Amenazas informáticas y seguridad de la información. {en línea} {30 de noviembre de 2022} disponible en (https://infolibros.org/pdfview/10137-amenazas-informaticas-y-seguridad-de-la-informacion-articulo-cesar-h-tarazona-t/)

THE MITRE CORPORATION'S – CVE. Anydesk: Security Vulnerabilities {en línea} {9 de diciembre de 2022} disponible en (https://www.cvedetails.com/vulnerability-list/vendor_id-16953/product_id-40173/Anydesk-Anydesk.html)

THE MITRE CORPORATION'S – CVE. Google Android 6.0.1: Security Vulnerabilities {en línea} {6 de diciembre de noviembre de 2022} disponible en (https://www.cvedetails.com/vulnerability-list/vendor_id-1224/product_id-19997/version_id-498228/opginf-1/Google-Android-6.0.1.html)

THE MITRE CORPORATION'S – CVE. Google Android 6.0: Security Vulnerabilities {en línea} {6 de diciembre de 2022} disponible en (https://www.cvedetails.com/vulnerability-list/vendor_id-1224/product_id-19997/version_id-498231/Google-Android-6.0.html)

THE MITRE CORPORATION'S – CVE. Oracle-MySql 5.7.17: Security Vulnerabilities {en línea} {30 de noviembre de 2022} disponible en

(https://www.cvedetails.com/vulnerability-list/vendor_id-93/product_id-21801/version_id-565154/Oracle-Mysql-5.7.17.html)

THE MITRE CORPORATION'S – CVE [sitio web]. Vm Virtualbox : Security Vulnerabilities {en línea} {30 de noviembre de 2022} disponible en (https://www.cvedetails.com/vulnerability-list/vendor_id-93/product_id-20406/Oracle-Vm-Virtualbox.html)

TORRES, Kerwin. Diseño del sistema de seguridad basado en el análisis de vulnerabilidades identificadas en la Empresa Nostradamus S.A.S. 2021, 96p. Proyecto aplicado (Especialización en Seguridad Informática). Universidad Nacional Abierta y a Distancia UNAD. Escuela de Ciencias Básicas, Tecnología e Ingeniería - ECBTI disponible en https://repository.unad.edu.co/handle/10596/47871

VALENCIA, Alba. Análisis de los riesgos de seguridad de la información del sistema de gestión documental de la Alcaldía Municipal de Ibagué. 2022, 151p. Proyecto aplicado (Especialización en Seguridad Informática). Universidad Nacional Abierta y a Distancia UNAD. Escuela de Ciencias Básicas, Tecnología e Ingeniería - ECBTI disponible en https://repository.unad.edu.co/handle/10596/51504

VARÓN, Juan. Estudio de análisis y gestión de riesgo al sistema de información de la empresa Agesagro S.A.S utilizando la metodología Magerit. 2017, 87p. Monografía (Especialización en Seguridad Informática). Universidad Nacional Abierta y a Distancia UNAD. Escuela de Ciencias Básicas, Tecnología e Ingeniería - ECBTI disponible en https://repository.unad.edu.co/handle/10596/11915

WELIVESECURITY ™ BY ESET ®. MAGERIT: metodología práctica para gestionar riesgos {en línea} {20 de marzo de 2022} disponible en (https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/)

ZAMBRANO, Luis. Diseño de un sistema de seguridad de la información para la Cooperativa Multiactiva de Centrales Eléctricas de Nariño basado en la norma ISO 27001:2013. 2021, 150p. Proyecto aplicado (Especialización en Seguridad Informática). Universidad Nacional Abierta y a Distancia UNAD. Escuela de Ciencias Básicas, Tecnología e Ingeniería - ECBTI disponible en https://repository.unad.edu.co/handle/10596/39349

ANEXOS

Anexo A – Resumen Analítico Especializado

Anexo B - Resumen Ejecutivo de los resultados del Análisis de Riesgos

Anexo C - Matriz Análisis de Riesgos CDA MOTOCENTRO.

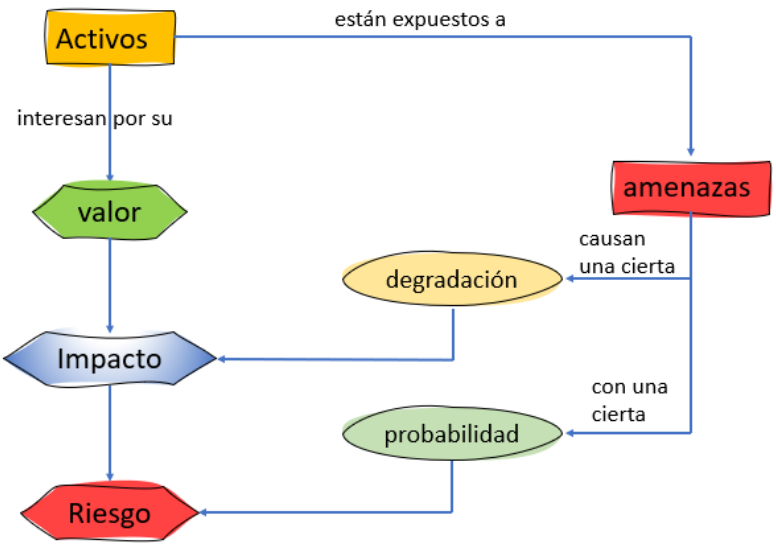
RESUMEN ANALÍTICO ESPECIALIZADO – RAE

TEMA:	Diseño del plan de tratamientos de riesgos informáticos del área de TI para un CDA. El tema del presente proyecto se enmarca dentro del campo de proyectos tecnológicos, en el área de seguridad de la información.
TÍTULO:	Tratamiento de riesgos informáticos del área de TI de la empresa Centro de Diagnóstico Automotor MOTOCENTRO S.A.S.
AUTOR (ES):	Omar Rosas Aldana
FUENTE BIBLIOGRÁFICA:	Se referencian 38 fuentes bibliográficas, entre las más destacadas se tienen: ISOTOOLS EXCELLENCE. Sistemas de Gestión de Riesgos y Seguridad {en línea} {12 de marzo de 2022} disponible en (https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/) MINTIC. Guía para la Gestión y Clasificación de Activos de Información. {en línea} {23 de mayo de 2022} disponible en (https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf) MINTIC [sitio web]. Controles de seguridad y privacidad de la información {en línea} {23 de mayo de 2022} disponible en (https://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf) PORTAL ADMINISTRACIÓN ELECTRÓNICA. MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I: Método. Libro II: Catálogo de Elementos. Libro III: Guía de Técnicas {en línea} {10 de marzo de 2022} disponible en (https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html)
AÑO:	2023
RESUMEN:	El presente proyecto contextualiza la importancia que hoy en día se le debe dar a la seguridad de los activos de información de cualquier organización, indistintamente de su naturaleza y tamaño, en vista de que a medida que crece el uso de la tecnología, en la misma proporción o mayor es el crecimiento de los ataques cibernéticos, en ese sentido toda organización debe plantear dentro de sus principales estrategias corporativas la de establecer un plan de tratamiento de riesgos de seguridad que garantice la mitigación de los ataques cibernéticos y mejore la seguridad en sus activos de información.

	Ahora bien, este proyecto está orientado hacia la identificación de los activos de información del área de TI de la empresa CENTRO DE DIAGNOSTICO AUTOMOTOR MOTOCENTRO S.A.S., con un resultado de 76 activos de información tipificados de conformidad con los tipos de activos que plantea la metodología MAGERIT V3, entre los cuales están Claves Criptográficas, Servicio, Software y Hardware. Luego de la identificación y tipificación, el proyecto se enfoca en establecer la matriz de análisis y evaluación de los riesgos de seguridad de los activos de información de la empresa, aplicando la metodología mencionada anteriormente, se identifican los riesgos que tienen nivel Moderado e Inaceptable, de acuerdo con las dimensiones de la metodología aplicada, así mismo, según el impacto en la confidencialidad, integridad y disponibilidad de la información se establece los riesgos de seguridad que tienen nivel bajo, medio, alto y extremo. Por último, en el presente proyecto se identifican las posibles vulnerabilidades de los activos de información del área de TI y se diseña el plan de tratamiento de riesgos de seguridad de la información aplicando los controles propuestos en el Anexo A de la norma ISO/IEC 27001 con el objetivo de mejorar los niveles de seguridad de los activos de información mitigando los riesgos a los que pueden estar expuestos estos.
PALABRAS CLAVES:	Activos de información, ISO 27001, MAGERIT, Plan de tratamiento de riesgos, Seguridad de la Información.
CONTENIDOS:	Definición del problema Justificación Objetivos Marco Referencial Diseño Metodológico Desarrollo de los objetivos Conclusiones Recomendaciones Bibliografía
DESCRIPCIÓN DEL PROBLEMA:	El CDA MOTOCENTRO S.A.S, es un organismo de inspección tipo A, acreditado por ONAC, bajo la norma técnica colombiana NTC ISO IEC 17200, en Revisión Técnico-Mecánica y de Emisiones Contaminantes en vehículos automotores Motocicletas 2T Motocicletas 4T.

	Debe cumplir entre otras normas con la NTC 5385, NUMERAL 4.16 donde se habla de los requisitos de hardware y software, así como de los requisitos de seguridad de la información, aunque el organismo cuenta con un sistema de gestión enfocado en el cumplimiento de la NTC ISO IEC 17200; este no es lo suficientemente robusto para controlar los riesgos de seguridad de la información. El CDA MOTOCENTRO S.A.S cuenta con una política de seguridad de la información, procedimientos de mantenimiento de equipos de cómputo, instructivos para la realización y restauración de copias de seguridad, bitácoras de fallos, sin embargo, no se ha tenido en cuenta en la identificación de los riesgos asociados a la seguridad de la información, tampoco se cuenta con un inventario completo y actualizado de todos los activos informáticos. De esta manera al no tener definidos los riesgos ni los activos, el CDA MOTOCENTRO S.A.S no cuenta con los controles necesarios para hacer frente a las amenazas que puedan surgir y poner en riesgo la seguridad de la información, lo cual conlleva un gran problema para la organización al ser un organismo de inspección acreditado, que debe tener planes de contingencia y de continuidad de la prestación de sus servicios. De conformidad con lo descrito anteriormente, se plantea la siguiente formulación del problema así: ¿Cómo el plan de tratamiento de riesgos de seguridad de la información de CDA MOTOCENTRO S.A.S., permitirá mejorar la seguridad de sus activos de información del área de TI?
OBJETIVO GENERAL:	Proponer el plan de tratamiento de los riesgos informáticos en la empresa CDA MOTOCENTRO SAS, para mejorar la seguridad de los activos de información del área de TI, de conformidad con la metodología MAGERIT V3.
OBJETIVOS ESPECÍFICOS:	Analizar la infraestructura tecnológica de MOTOCENTRO S.A.S. para establecer los activos de información del área de TI de la empresa, de conformidad con los tipos de activos que se plantean en la metodología MAGERIT V3. Establecer la matriz del análisis y la evaluación de los riesgos de seguridad de los activos de información del área de TI de MOTOCENTRO S.A.S. para catalogarlos de acuerdo con su nivel de riesgo y de conformidad con las dimensiones de valoración propuestas en la metodología MAGERIT V3. Diseñar el plan de tratamiento de riesgos de seguridad de la información de MOTOCENTRO S.A.S para mejorar los niveles de seguridad informática de los

	activos de información del área de TI, evitando se materialicen los riegos o minimizando su impacto, en caso de su materialización.
METODOLOGÍA:	**TIPO DE INVESTIGACIÓN** El tipo de investigación a emplear en el presente proyecto será orientado hacia la investigación aplicada tecnológica, porque se basa en metodologías, normas y técnicas para realizar el análisis y gestión del riesgo con el objetivo de abordar el problema específico de la empresa CDA MOTOCENTRO S.A.S. que se centra en el tratamiento de los riesgos informáticos de sus activos de información. **METODOLOGÍA DE DESARROLLO** El presente proyecto aplicado está basado en la metodología MAGERIT V:3.0 para el análisis y gestión de riesgos relacionados con la seguridad de la información, la cual plantea las siguientes etapas o pasos a seguir como buenas prácticas para el análisis de riesgos: • Identificar los activos más importantes para la organización. • Establecer a qué amenazas se exponen aquellos activos. • Establecer las salvaguardas con las que se dispone y que tan eficaces son frente al riesgo identificado. • “Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.” • “Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.” La siguiente ilustración permite un recorrido inicial por los diferentes pasos que plantea la metodología. Figura 1: Pasos y elementos del análisis de riesgos

<table>
<tr><td></td><td> 

Fuente: elaboración propia</td></tr>
<tr><td>REFERENTES TEÓRICOS Y CONCEPTUALES:</td><td>MAGERIT: es una metodología enfocada al análisis y gestión de los riesgos de seguridad de la información, la cual fue creada por el Consejo Superior de Administración Electrónica de España , esta metodología brinda el método y las técnicas que permiten establecer el impacto que puede llegar a tener la seguridad de la información en una organización, debido a las vulnerabilidades que pueden existir en sus activos de información, las cuales son utilizadas por personas malintencionadas para realizar intentos de ataques cibernéticos; en ese sentido MAGERIT permite implementar medidas de control mediante un plan de tratamiento que garantice la mitigación de los riesgos.

ISO 27001: Es una norma internacional creada por la Organización Internacional de Normalización (ISO), y su función es de evitar que se generen incidentes relacionados con la Seguridad de la Información, independientemente si un incidente es leve o grave, éste representa un recurso económico para las empresas, en tal sentido al disminuir los incidentes se optimizan los recursos de las organizaciones.

Seguridad de la Información: es la unión de todas las técnicas y procedimientos que se deben tener a nivel de recurso humano como técnico, con el objetivo de salvaguardar los tres pilares fundamentales de la información, independientemente del medio en que se encuentre, los cuales que son:

• Confidencialidad: garantizando que el acceso a los datos y su modificación sea realizado por las personas autorizadas para tal fin.</td></tr>
</table>

	• **Integridad**: certificar que los datos no han sido manipulados por terceros de forma malintencionada, lo que garantiza que la información y sus procedimientos son exactos y completos. • **Disponibilidad**: la información deberá estar accesible en todo momento que se requiera por los usuarios autorizados. **Activo de información:** es todo aquello que guarda relación con el tratamiento de la información y que posee un valor para la empresa, independiente de su medio de almacenamiento que puede ser físico o magnético, por ejemplo, los registros físicos, sistemas de información, bases de datos entre otros. **Administración del Riesgo**: La gestión de riesgos es un enfoque estructurado para manejar la incertidumbre relativa a una amenaza a través de una secuencia de actividades humanas que incluyen la identificación, el análisis y la evaluación de riesgo, para luego establecer las estrategias de su tratamiento utilizando recursos gerenciales.
RESULTADOS:	Se identificaron y tipificaron los activos más críticos en el área de TI y su importancia para la Empresa. Se estableció la matriz con el análisis y evaluación de los riesgos de seguridad de los activos de información del área de TI de la empresa. Se diseñó el plan para el tratamiento de los riesgos de los activos de información identificados acorde con las necesidades de la empresa. Se propuso controles para los riesgos evidenciados. Concientización de los directivos y empleados del CDA sobre el uso adecuado de los datos, las TICs y la normatividad legal vigente relacionada directamente con los estándares de seguridad como lo es la norma ISO/IEC 27001:2013, mitigando de esta manera las debilidades en los sistemas de información que se utilizan en el día a día de la empresa, con el fin de aumentar la seguridad de la información que garantice la integridad, confidencialidad y disponibilidad de la misma y manteniendo un estricto control de sus activos impidiendo su perdida y manipulación. Así mismo, con el proyecto se dio el primer paso para que a mediano plazo la empresa implemente un Sistema de Gestión de seguridad de la información.

CONCLUSIONES:	Se realizó el análisis de la infraestructura tecnológica de la empresa CDA MOTOCENTRO S.A.S. y se hizo la identificación de 76 activos de información en el área de TI, logrando su tipificación de acuerdo con lo planteado por la metodología MAGERIT V3 así: i. [K] Claves Criptográficas: dos (2), ii. [S] Servicio: dos (2), iii. [SW] Software: cuarenta (40) y iv. [HW] Hardware: treinta y dos (32), en ese mismo sentido se logró la clasificación de estos según el impacto a nivel de seguridad de la información, donde 10 activos tienen impacto leve, 58 importante y 8 grave. Una vez identificados y tipificados los activos de información, se estableció la matriz con el análisis y evaluación de los riesgos de seguridad de los activos de información del área de TI de MOTOCENTRO S.A.S., que de acuerdo con las dimensiones que propone la metodología MAGERIT V3 para la valoración de riesgos, se identificaron 5 riesgos con nivel Moderado y 148 con nivel Inaceptable, según su valoración de probabilidad e impacto. Así mismo, se identificó el nivel de riesgo en los 76 activos de información de TI donde 2 activos tienen nivel bajo, 9 nivel medio, 36 nivel alto y 29 nivel extremo, según el impacto en la confidencialidad, integridad y disponibilidad de la información. Con el análisis y la evaluación de los riesgos de seguridad de los activos de información del área de TI de MOTOCENTRO S.A.S. se lograron identificar 153 posibles vulnerabilidades de los activos de información, de las cuales luego de su valoración de probabilidad e impacto se tienen 5 con nivel de Riesgo Moderado y 148 con nivel de riesgo Inaceptable, frente a lo cual se diseñó el plan de tratamiento de riesgos de seguridad de la información, el cual contiene cada uno de los controles del anexo A de la norma ISO/IEC 27001 que se deben aplicar para cada una de las 153 vulnerabilidades identificadas, logrando mejorar los niveles de seguridad informática de los activos de información del área de TI.

Universidad Nacional Abierta y a Distancia
Resumen Ejecutivo del Análisis de Riesgos

Clasificación general y Número de activos

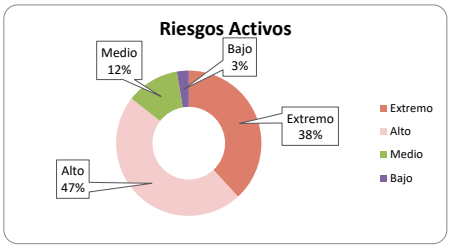
Tipo de activo	Cantidad
Tipo Dato	0
Tipo Claves Criptograficas	2
Tipo Servicio	2
Tipo Software	40
Tipo Hardware	32
Tipo Comunicaciones	0
Tipo Soporte de Información	0
Tipo Equipamento Auxiliar	0
Tipo Instalaciones	0
Tipo Personal	0
Total de Activos	**76**

Clasificación según impacto a la seguridad	
Leve	10
Importante	58
Grave	8
Resumen de nivel de riesgo en los activos	
Extremo	29
Alto	36
Medio	9
Bajo	2
Ubicación	
Fisica	8
Electrónica	68

Clasificación de activos según su valor

Número de activos de clientes o terceros que deben protegerse	59
Activos de información expuestos en internet	49
Activos de información que deben ser restringidos a un número limitado de empleados	72
Número de activos de información que deben ser restringidos a personas externas	74
Activos de información que pueden ser alterados o comprometidos para fraudes o corrupción	70
Número de activos de información que son muy críticos para las operaciones internas	73
Número de activos de información que son muy críticos para el servicio hacia terceros	51

Nivel de Riesgo	
Aceptable	0
Moderado	5
Inaceptable	145

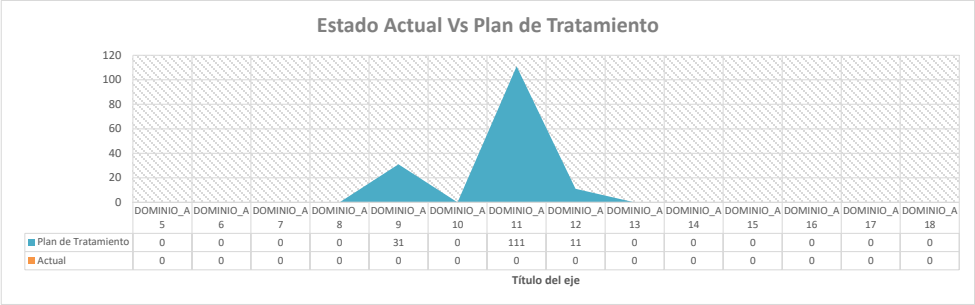


APETITO POR EL RIESGO Y ZONAS DE ADMISIBILIDAD

IMPACTO		Insignificante	Menor	Moderado	Mayor	Catastrófico
IMPACTO	MUY ALTA			, R153, R152, R151, R150, R149, R148, R146, R143, R140, R138, R137, R135, R132, R131, R129, R126, R125, R123, R120, R117, R115, R111, R107, R103, R99, R95, R91, R86, R81, R77, R76, R75, R72, R71, R70, R68, R63, R59, R58, R53, R52, R51, R49, R48, R47, R46, R43, R42, R41, R40, R39, R38, R34, R33, R31, R29, R28, R16, R15, R14, R13, R11, R10	, R147, R145, R144, R142, R141, R139, R136, R134, R133, R130, R128, R127, R124, R122, R121, R119, R118, R116, R114, R113, R112, R110, R109, R108, R106, R105, R104, R102, R101, R100, R98, R97, R96, R94, R93, R92, R90, R89, R88, R87, R84, R83, R82, R79, R78, R74, R73, R69, R66, R65, R64, R61, R60, R57, R55, R54, R50, R45, R44, R35, R32, R30, R26, R24, R23, R22, R21, R20, R18, R17, R12, R8, R6, R5, R2	, R85, R80, R67, R62, R56, R37, R36, R27, R25, R19, R9, R7, R4, R3, R1
	ALTA					
	MEDIA					
	BAJA					
	MUY BAJA					
	RIESGO	MUY BAJA	BAJA	MEDIA	ALTA	MUY ALTA
		PROBABILIDAD				

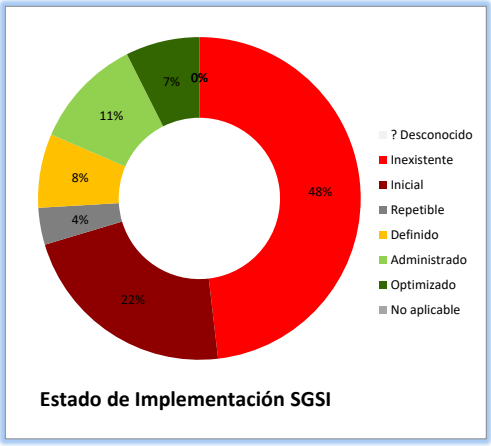
Cunplimieto Norma ISO 27001:2013

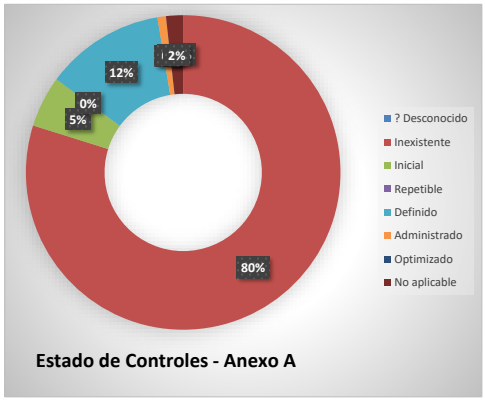
		C Actual	C Plan de T
DOMINIO_A5	Políticas De La Seguridad De La Información	0	0
DOMINIO_A6	Organización De La Seguridad De La Información	0	0
DOMINIO_A7	Seguridad De Los Recursos Humanos	0	0
DOMINIO_A8	Gestión De Activos	0	0
DOMINIO_A9	Control De Acceso	0	31
DOMINIO_A10	Criptografía	0	0
DOMINIO_A11	Seguridad Física Y Del Entorno	0	111
DOMINIO_A12	Seguridad De Las Operaciones	0	11
DOMINIO_A13	Seguridad De Las Comunicaciones	0	0
DOMINIO_A14	Adquisición, Desarrollo Y Mantenimiento De Sistemas	0	0
DOMINIO_A15	Relaciones Con Los Proveedores	0	0
DOMINIO_A16	Gestión De Incidentes De Seguridad De La Información	0	0
DOMINIO_A17	Aspectos De Seguridad De La Información De La Gestión De Continuidad De Negocio	0	0
DOMINIO_A18	Cumplimiento	0	0



Metricas Relacionadas con la Implementación del SGSI

Estado	Significado	Proporción de requerimientos SGSI	Proporción de Controles de Seguridad de la Información
? Desconocido	No ha sido verificado	**0%**	**0%**
Inexistente	No se lleva a cabo el control de seguridad en los sistemas de información.	**48%**	**80%**
Inicial	Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de la buena suerte y de tener personal de la alta calidad.	**22%**	**5%**
Repetible	La medida de seguridad se realiza de un modo totalmente informal (con procedimientos propios, informales). La responsabilidad es individual. No hay formación.	**4%**	**0%**
Definido	El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el Responsable de Seguridad ni el Comité de Dirección.	**7%**	**12%**
Administrado	El control se lleva a cabo de acuerdo a un procedimiento documentado, aprobado y formalizado.	**11%**	**1%**
Optimizado	El control se aplica de acuerdo a un procedimiento documentado, aprobado y formalizado, y su eficacia se mide periódicamente mediante indicadores.	**7%**	**0%**
No aplicable	A fin de certificar un SGSI ,todos los requerimientos principales de ISO/IEC 27001 son obligatorios. De otro modo, pueden ser ignorados por la Administración.	**0%**	**2%**
	Total	100%	100%





Resumen de Valoración de los activos en escala C.C Eficiente

Nombre	Riesgo	Confidencialidad	Integridad	Disponibilidad	Valor
[SW] Windows 7 Professional	EXTREMO	9	9	9	9
[SW] Antivirus Avast	EXTREMO	9	9	9	9
[HW] Equipo WorkStation Servidor HP	EXTREMO	9	9	9	9
[SW] Cobianbackup	EXTREMO	9	9	9	9
[SW] Linux Server virtualizado	EXTREMO	9	9	9	9
[SW] VirtualBox	EXTREMO	9	9	9	9
[HW] Switch TP-Link TL-SG1016D	ALTO	5	5	9	6
[HW] Router Archer C2	EXTREMO	9	9	9	9
[HW] DVR DAHUA 8ch	EXTREMO	9	9	9	9
[SW] Base de datos Mysql 5.7.17	ALTO	5	5	9	6
[SW] RTMyEC (INDUCAPK)	EXTREMO	9	9	9	9
[SW] AnyDesk	ALTO	5	5	9	6
[SW] TeamViewer	EXTREMO	9	9	9	9
[HW] Telefono AT&T	EXTREMO	9	9	9	9
[SW] Windows 10 Profesional 21H2	EXTREMO	9	9	9	9
[SW] Office professional plus 2016	ALTO	6	6	6	6
[HW] Equipo de computo ARGOM	EXTREMO	9	9	9	9
[SW] AudiWeb-FirmaFur	ALTO	9	9	3	7
[SW] SmartPSS	ALTO	9	9	3	7
[SW] RTMyEC (INDUCAPK)	ALTO	9	9	3	7
[HW] IMPRESORA 1 Samsung	ALTO	9	3	9	7
[HW] TABLET No 3 Samsung	ALTO	6	6	9	7
[SW] Android 6.0.1	ALTO	3	9	9	7
[K] Firma Digital	ALTO	3	9	9	7
[HW] Telefono AT&T	ALTO	3	9	9	7
[SW] Windows 10 Profesional 21H2	EXTREMO	9	9	9	9
[SW] Office professional plus 2016	EXTREMO	9	9	9	9
[HW] Equipo de computo ARGOM	EXTREMO	9	9	9	9
[SW] AudiWeb	EXTREMO	9	9	9	9
[S] hq.runt.com.co	EXTREMO	9	9	6	8
[SW] Supergiros	EXTREMO	9	9	9	9
[SW] AnyDesk	EXTREMO	9	9	9	9
[SW] RTMyEC (INDUCAPK)	ALTO	9	9	3	7
[SW] AnyDesk	EXTREMO	9	9	9	9
[SW] SmartPSS	EXTREMO	9	9	9	9
[HW] IMPRESORA 3 Canon	EXTREMO	9	9	9	9
[K] Firma Digital	EXTREMO	9	9	9	9
[HW] Telefono AT&T Base	EXTREMO	9	9	9	9
[SW] Windows 10 Profesional 21H2	ALTO	6	6	6	6
[SW] Office professional plus 2016	ALTO	6	6	6	6
[HW] Equipo de computo JANUS - Administrativo	BAJO	3	3	3	3
[SW] AudiWeb	ALTO	6	6	6	6
[S] hq.runt.com.co	ALTO	6	9	3	6
[SW] Supergiros	EXTREMO	9	9	6	8
[SW] AnyDesk	ALTO	6	6	9	7
[SW] RTMyEC (INDUCAPK)	ALTO	9	9	3	7
[SW] AnyDesk	ALTO	6	6	6	6
[SW] SmartPSS	ALTO	6	6	6	6
[HW] IMPRESORA 2 Samsung	BAJO	3	3	3	3
[HW] FRENOMETRO	ALTO	6	6	6	6
[HW] ALINEADOR DE LUCES	ALTO	6	9	3	6
[HW] SONOMETRO	EXTREMO	9	9	6	8
[HW] ANALIZADOR4T	ALTO	6	6	9	7
[HW] ANALIZADOR2T	MEDIO	3	9	3	5
[HW] TERMOHIGROMETRO	ALTO	6	6	6	6
[HW] TERMOHIGROMETRO RESPALDO	ALTO	6	9	3	6
[HW] PROFUNDIMETRO PF 011	EXTREMO	9	9	6	8
[HW] PROFUNDIMETRO PF 012	ALTO	6	6	9	7
[HW] MANOMETRO	MEDIO	3	9	3	5
[HW] CUENTA REVOLUCIONES	MEDIO	3	9	3	5
[HW] TABLET No 1 Samsung	ALTO	6	6	6	6
[HW] TABLET No 2 Samsung	ALTO	6	9	3	6
[HW] TABLET No 4 Samsung	EXTREMO	9	9	6	8
[HW] HCO (Tarjeta Desarrollo Beaglebone) GASES	ALTO	6	6	9	7
[HW] HCO (Tarjeta Desarrollo Beaglebone) FRENOMETRO	MEDIO	3	9	3	5
[HW] HCO (Tarjeta Desarrollo Beaglebone) LUXOMETRO	ALTO	6	6	9	7
[SW] LINUX ubuntu	MEDIO	3	9	3	5
[SW] LINUX ubuntu	ALTO	6	6	9	7
[SW] LINUX ubuntu	MEDIO	3	9	3	5
[SW] Android 6.0.1	ALTO	6	6	9	7
[SW] Android 6.0.1	MEDIO	3	9	3	5
[SW] Android 10	ALTO	6	6	9	7
[HW] Telefono AT&T	MEDIO	3	9	3	5
[SW] APP Pista	ALTO	6	6	9	7
[SW] APP Pre-revision	MEDIO	3	9	3	5
[SW] APP Servicio	ALTO	6	6	9	7