UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TÍTULO DE TRABAJO DE TITULACIÓN

DISEÑO DE PLAN INTEGRAL DE TRATAMIENTOS DE RIESGOS INFORMÁTICOS EN DATA CENTER GUBERNAMENTAL APLICANDO MAGERIT.

AUTOR

BORBOR TUMBACO, ARIEL STEVEN

COMPONENTE PRÁCTICO DE EXAMEN COMPLEXIVO

Previo a la obtención del grado académico en
INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

TUTOR

ING. MÓNICA JARAMILLO INFANTE, MGT.

Santa Elena, Ecuador

Año 2024

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

Ing. José Sánchez Aquino, Mgt.
DIRECTOR DE LA CARRERA

Ing. Mónica Jaramillo Infante, Mgt.
TUTOR

Ing. Carlos Castillo Yagual, Mgt.
DOCENTE ESPECIALISTA

Ing. Mónica Jaramillo Infante, Mgt.
DOCENTE GUÍA UIC

UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por Ariel Steven Borbor Tumbaco, como requerimiento para la obtención del título de Ingeniero en Tecnologías de la Información.

La Libertad, a los 18 días del mes de junio del año 2024

TUTOR

Ing. Mónica Jaramillo Infante, Mgt

UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Ariel Steven Borbor Tumbaco**

DECLARO QUE:

El trabajo de Titulación, "Diseño de Plan Integral de Tratamientos de Riesgos Informáticos en Data Center Gubernamental aplicando MAGERIT", previo a la obtención del título en Ingeniero en Tecnologías de la Información, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

La Libertad, a los 18 días del mes de junio del año 2024

EL AUTOR

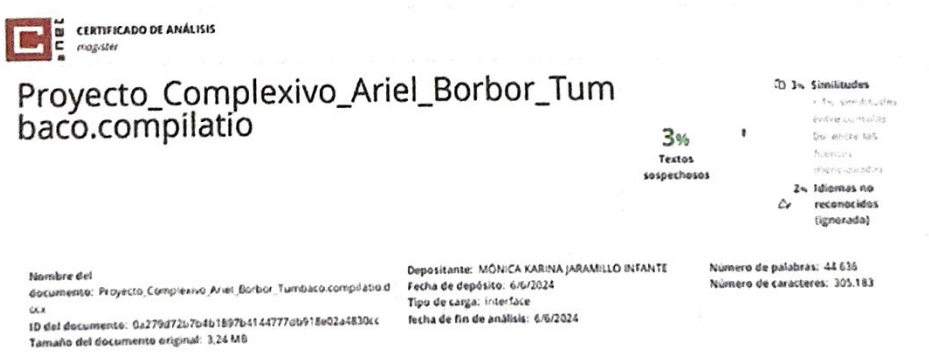
Ariel Steven Borbor Tumbaco

UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado **"Diseño de Plan Integral de Tratamientos de Riesgos Informáticos en Data Center Gubernamental aplicando MAGERIT"**, presentado por el estudiante, Ariel Steven Borbor Tumbaco fue enviado al Sistema Antiplagio, presentando un porcentaje de similitud correspondiente al 3%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.



CERTIFICADO DE ANÁLISIS
magister

Proyecto_Complexivo_Ariel_Borbor_Tumbaco.compilatio

3% Textos sospechosos

3% Similitudes

2% Idiomas no reconocidos (ignorada)

Nombre del documento: Proyecto_Complexivo_Ariel_Borbor_Tumbaco.compilatio.docx
ID del documento: 6a279d72b7b4b1897b4144777a0b918e02a4830cc
Tamaño del documento original: 3,24 MB

Depositante: MÓNICA KARINA JARAMILLO INFANTE
Fecha de depósito: 6/6/2024
Tipo de carga: Interface
fecha de fin de análisis: 6/6/2024

Número de palabras: 44 636
Número de caracteres: 305.183

TUTOR

Ing. Mónica Jaramillo Infante, Mgt.

UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **Ariel Steven Borbor Tumbaco**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales del trabajo de titulación con fines de difusión pública, dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor

Santa Elena, a los 18 días del mes de junio del año 2021

EL AUTOR

Ariel Steven Borbor Tumbaco

AGRADECIMIENTO

Agradezco primero a Dios que me ha dado salud y me ha guiado de manera correcta para finalizar este trabajo. A mis padres y abuelos por brindarme el apoyo incondicional de manera moral y económica durante el transcurso de mi vida universitaria.

Quiero agradecer a mis hermanas y familiares por dame consejos y palabras de aliento mientras realizaba este proceso.

Agradecer a los docentes quienes a partir de sus conocimientos supieron guiarme durante el estudio de esta carrera.

Ariel Steven, Borbor Tumbaco

DEDICATORIA

Este trabajo va dedicado a mis padres y familiares, especialmente a mi abuelo Gonzalo Tumbaco por brindarme su apoyo en los momentos difíciles que pase para cumplir mis metas.

De igual manera a mis amigos y compañeros que estuvieron a lo largo de mi vida estudiantil y por ser fuente de sabiduría en cada tarea que realice.

Ariel Steven, Borbor Tumbaco

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

Resumen

La entidad gubernamental, tiene como fin ofrecer sus servicios a la ciudadanía y comunidad en general, además del personal interno de la institución, en la actualidad cuenta con 47 departamentos y un Data center que respalda los servicios de estos mismos, el cual requiere mejorar su gestión de riesgos informáticos. El enfoque actual, basado en la experiencia del personal sin una guía definida, no es suficiente para enfrentar las amenazas crecientes, lo que aumenta la probabilidad de incidencias y problemas. Se propone diseñar un plan de tratamiento de riesgos informáticos para el centro de datos del GAD Municipal empleando la metodología Magerit como guía fundamental que permitirá analizar los riesgos del Data Center, determinar salvaguardas para prevenir, minimizar, detectar, corregir y aceptar los riesgos, teniendo como fin reducir el impacto de las amenazas a las que está expuesto el centro de cómputo y asegurar la integridad, confidencialidad, disponibilidad y autenticidad de los activos de la información.

Palabras claves: Seguridad de la información, Gestión de riesgos, Magerit, Salvaguardas.

Abstract

The government entity, whose purpose is to offer its services to the citizens and the community in general, in addition to the internal personnel of the institution, currently has 47 departments and a Data center that supports the services of these departments, requires improving its IT risk management. The current approach, based on the experience of the staff without a defined guide, is not sufficient to face the growing threats, which increases the probability of incidents and problems. It is proposed to design an IT risk treatment plan for the data center of the Municipal Government using the Magerit methodology as a fundamental guide that will allow analyzing the risks of the Data Center, determining safeguards to prevent, minimize, detect, correct and accept the risks, with the purpose of reducing the impact of the threats to which the data center is exposed and ensuring the integrity, confidentiality, availability and authenticity of the information assets.

Keywords: Information security, Risk management, Magerit, Safeguards.

Introducción

En un mundo cada vez más digitalizado, la seguridad de la información se ha convertido en un aspecto fundamental para las organizaciones gubernamentales. Los centros de datos albergan información crítica y confidencial, como datos de ciudadanos, registros financieros y documentos gubernamentales sensibles. Proteger estos datos contra amenazas cibernéticas es crucial para garantizar la continuidad de las operaciones gubernamentales, la privacidad de los ciudadanos y la confianza en las instituciones públicas. La seguridad de la información no solo implica la protección contra ataques cibernéticos, sino también la gestión adecuada de riesgos internos y externos que puedan comprometer la infraestructura tecnológica.

El Data Center de la entidad gubernamental no cuenta con un plan de tratamiento de riesgos, el enfoque actual se basa principalmente en la experiencia del responsable del centro de cómputo sin una guía formal, genera un escenario de mayor riesgo. Esta falta de estructura formal aumenta la probabilidad de que los riesgos se materialicen en incidentes y problemas de gravedad considerable.

El presente proyecto tiene como objetivo desarrollar un plan integral de tratamiento de riesgos aplicando la metodología Magerit como guía principal para el análisis y la gestión de los riesgos informáticos de los activos críticos del Data Center, que permitirá identificar, evaluar y tratar los riesgos de manera sistemática, ofreciendo un marco de trabajo que asegure la integridad, confidencialidad, disponibilidad y autenticidad de la información. El trabajo de titulación se estructura en 3 capítulos detallados a continuación:

En el capítulo 1 se describe el contexto y la situación actual de la problemática relacionada a la existencia de amenazas y riesgos en el Data Center. Se presentan los antecedentes que motivan la investigación, se plantean los objetivos generales y específicos que guiarán el desarrollo del estudio, además del alcance de las fases.

En el capítulo 2 se detallan los conceptos que se debe conocer para entender el proyecto, y en el último capítulo se detallan las fases que se siguió para poder realizar el análisis de riesgos con respecto a la metodología aplicada abordando cada etapa hasta el desarrollo del plan de tratamiento de riesgos.

CAPÍTULO I

1. Fundamentación

1.1. Antecedentes

La actual y creciente dependencia de la tecnología de la información en empresas gubernamentales ha ido en aumento dando como resultado un incremento en la cantidad de los activos, datos e información sensible que se almacenan y procesan en dentro de los centros de almacenamiento de datos de estas instituciones y que son importantes para la toma de decisiones. El incremento del volumen de los datos críticos ha traído consigo un aumento de amenazas y vulnerabilidades a los cuales los data centers deben enfrentarse, de manera que la información almacenada se mantenga segura e integra para la continuidad de las operaciones de la empresa [1].

El 8 de abril de 1993 el Gobierno de Sixto Durán Ballén otorgó la cantonización de La Libertad, está organizada por el poder ejecutivo representado por el alcalde y el legislativo conformado por los miembros de concejo cantonal [2]. La entidad gubernamental tiene como fin ofrecer sus servicios a la ciudadanía y comunidad en general, según la información proporcionada por Dirección de Talento Humano, la institución cuenta con 47 departamentos y 711 empleados [3].

Al realizar una entrevista al encargado y responsable del Data Center de la entidad (Anexo 1), se determinó que actualmente existe la incapacidad de la organización para la gestión y trato de riesgos informáticos en el sitio, los procesos que se siguen para tratar los riesgos son de forma empírica tratados solo por el responsable del centro de cómputo, sin una guía que recomiende el proceso o procedimiento adecuado para la minimización, prevención, detección o aceptación del riesgo, causando que en algunos casos el riesgo se concrete y se presente como una incidencia escalando en peores casos hasta un problema.

Los resultados obtenidos con el método de observación en él (Anexo 5), permite identificar posibles amenazas y vulnerabilidades en la seguridad informática, así como comprender mejor el entorno en el que opera. De igual manera nos revela las áreas de preocupación y aspectos que podrían representar riesgos potenciales para la seguridad. Además, de poder identificar la ausencia de procedimientos claros y adecuados para tratar riesgos, teniendo como efecto directo una interrupción de las

funciones operativas de los departamentos que dependen de la continuidad operativa del Data Center de la entidad.

Debido a que recientemente se realizó el cambio de autoridades en la entidad, uno de los problemas es la falta de inversión que se tiene a temas de seguridad informática y seguridad de la información de manera general en la organización como para el mismo Centro de Datos causando que los riesgos no se gestionen de manera adecuada diseñando e implementando un plan de tratamiento de riegos, además de la falta de capacitación y conciencia teniendo como efecto errores u omisiones sobre las mejores prácticas de seguridad informática.

El trabajo realizado en la Universidad Nacional de San Cristóbal de Huamanga cuyo título es "Auditoria para la Evaluar la seguridad física del Data Center del hospital regional del Ayacucho"[4], diseña procedimientos de auditoria con el objetivo de evaluar la seguridad física del Data Center aplicando los marcos de trabajo de control COBIT 5.0 y NTP-ISO/IEC 17799. En donde a partir de los marcos de trabajo antes mencionados se realizó un análisis de riegos logrando identificar las amenazas y riesgos de la seguridad física permitiendo determinar el impacto que abarcaría los riesgos detectados a los activos físicos de la institución. Sin embargo, solo se realizó un análisis de riesgos de seguridad física, dejando la seguridad lógica de un lado lo cual puede resultar en una visión incompleta de seguridad en general de la organización.

En la Universidad Regional Autónoma de los Andes (UNIANDES) se desarrolló el tema "Plan de seguridad informática alineado a la Norma ISO 27001 para fortalecer las seguridades del data center en la cooperativa de ahorro y crédito 1 de julio de la ciudad del Tena"[5], empleando la norma ISO 27001 para la gestión de los proceso internos y la utilización de la metodología MAGERIT para la identificación, evaluación de riesgos e implementación de las políticas de precaución adecuadas para la seguridad informática de la institución.

En el ámbito local resalta el trabajo cuyo título es "Propuesta de un modelo de mejora continua para la gestión de riesgos de la seguridad de la información a una institución educativa privada mediante el ciclo CAP-DO" realizado en la Universidad Estatal Península de Santa Elena, se diseñó de una guía de análisis de

riesgos que se adapte a la institución para la gestión de tomas de decisiones de políticas de seguridad de la información, basada en las metodologías ISO 31000:2018, CRAMM, Magerit y OCTANE [6].

Los trabajos referenciados anteriormente, si bien cada uno realiza su propio análisis y gestión de riesgos, no abordan todos los controles en el plan de mejoras en las entidades respectivas, además de no abordar ambos tipos de seguridad como física y lógica. El actual trabajo propuesto tiene como solución la identificación, evaluación y validación de los activos críticos de la entidad, además del diseño de un plan de tratamiento de los riesgos informáticos de la institución objeto de estudio.

1.2. Descripción del Proyecto

Los riesgos de seguridad informáticos a los que se enfrentan las empresas son de varios tipos, muchas de las amenazas y debilidades nacen a partir de una mala gestión de los activos y recursos tecnológicos [7]. El Data Center es un componente crítico para la operación y el almacenamiento de información sensible, crítica y estratégica, por lo que es esencial garantizar su continuidad operativa [8]. El presente proyecto consiste en analizar los riesgos asociados al Data Center de la entidad gubernamental y diseñar un plan de tratamiento de riesgos efectivo basado en una metodología que permitirán obtener un enfoque estructurado y completo.

El proyecto se basa en el diseño de un plan de tratamiento de riesgos tecnológicos para el Data Center de una entidad gubernamental a partir de un enfoque exhaustivo de identificación, evaluación y gestión de riesgos, empleando la metodología Magerit en su versión 3 [9], como guía fundamental que facilitara la identificación de los activos de la entidad y así dividirlos en diferentes grupos con el objetivo de darles valor y desarrollar los salvaguardas que serán parte del plan anteriormente mencionado.

El plan de tratamiento de riesgos estará destinado al uso del personal que labora en el departamento de sistemas y recursos tecnológicos, donde se encuentra el centro de datos de la entidad gubernamental, debido a que tanto la coordinadora como los demás empleados con experiencia técnica y control sobre la infraestructura tecnológica estarán involucrados en la realización del proyecto.

La versión 3 de la metodología Magerit está estructurado por 3 volúmenes de los cuales 2 son libros y una guía de técnicas. El presente proyecto constara principalmente de las fases de la metodología que se muestran en la siguiente figura.

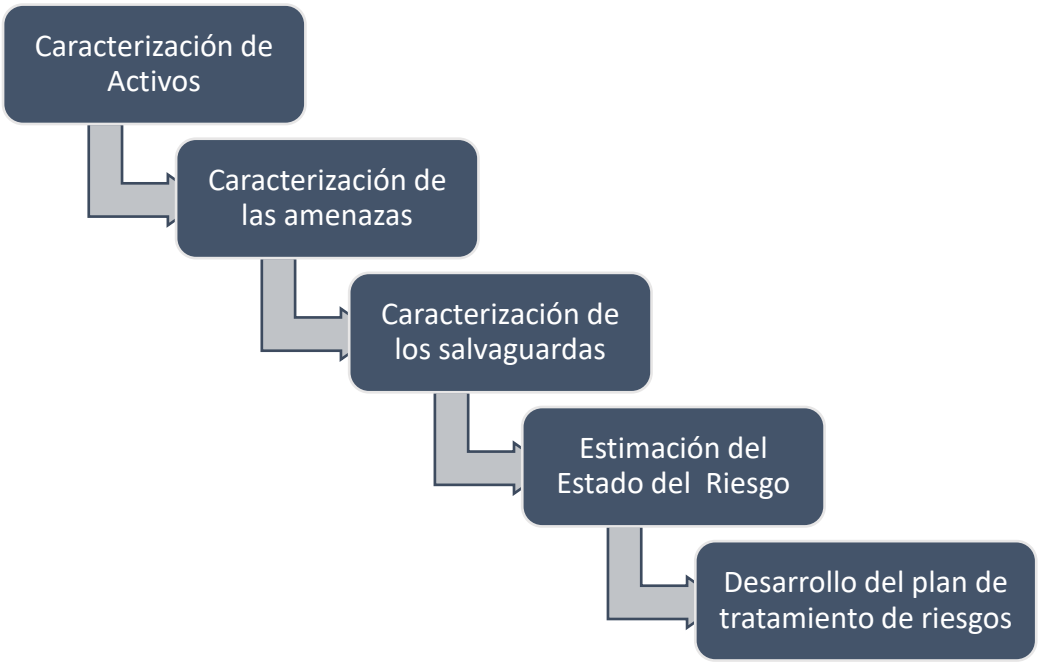


Figura 1: Fases de la Metodología Magerit

- **Fase 1: Caracterización de Activos**

Esta fase tiene la finalidad de identificar, clasificar y analizar los activos claves para la continuidad operativa de la organización.

A partir de esta fase se realizarán las siguientes actividades:

  - Identificación de los Activos
  - Identificación de las dependencias entre activos críticos del Data Center.
  - Valoración de los activos identificados.

- **Fase 2: Caracterización de las Amenazas**

Esta fase tiene como propósito el identificar y comprender en detalle las amenazas a las que están expuestos los activos en el centro de cómputo, como lo estipula el volumen 2 de Magerit.

  - Identificación de Amenazas.

- Valoración de Amenazas.

- **Fase 3: Caracterización de las salvaguardas**

En el desarrollo de esta fase se realizará el proceso de determinar las salvaguardas a partir de la identificación de los activos y sus amenazas. Se realizarán las siguientes actividades:

- Identificación de Salvaguardas.
- Valoración de Salvaguardas.

- **Fase 4: Estimación del Estado del Riesgo**

El objetivo de esta fase es la evaluación de la situación actual de los riesgos identificados en el Data Center. Esta fase es esencial para comprender la magnitud de los riesgos y tomar decisiones informadas sobre cómo abordarlos.

A partir de los ante ya mencionado se realizarán las siguientes actividades:

- Determinar el impacto potencial al que los activos del sistema están expuestos.
- Determinar el riesgo potencial al que los activos del sistema están sometidos.

- **Fase 5: Plan de tratamiento de riesgos**

Con base al análisis de riesgos, se desarrollará el plan de tratamiento de riesgos a partir de las siguientes actividades:

- Definir las salvaguardas para la minimización, prevención, detección y aceptación del riesgo.
- Documentar el plan de detallado que describa las actividades, responsables, eficacia y cualquier información relevante.

Para realizar el análisis de riesgos se utilizará una herramienta proporcionada por la misma metodología:

PILAR: "Procedimiento Informático – Lógico para el Análisis de riesgos", herramienta que soporta el análisis de riesgo siguiendo las fases de caracterización de activos, caracterización de amenazas y evaluación de salvaguardas de la metodología Magerit [10].

Este proyecto contribuirá a la línea de investigación de Tecnología y Sistemas de información (TSI), dado que está relacionado con la sub – línea de investigación: Ingeniería y Gestión de TSI, debido a que el tema aborda aspectos claves de la gestión de la información que son esenciales para la seguridad y gestión de riesgos informáticos [11].

1.3. Objetivos

1.3.1. Objetivo General

Desarrollar un plan integral de tratamiento de riesgos mediante la aplicación de la metodología Magerit como guía principal para prevenir y gestionar los riesgos informáticos de los activos críticos del Data Center de una entidad gubernamental.

1.3.2. Objetivos Específicos

- Recopilar información de la infraestructura del Data Center identificando los activos críticos informáticos expuestos a amenazas y vulnerabilidades mediante técnicas de recolección de información.
- Aplicar los procesos de la metodología Magerit para el análisis y evaluación de los riesgos determinando el impacto de los mismos en la entidad.
- Determinar las salvaguardas apropiadas que serán parte del plan de tratamiento de riesgos para los activos críticos del Data Center.
- Documentar el plan de tratamiento de riesgos, plasmando las actividades adecuadas requeridas para la prevención, minimización, detección y aceptación ante los riesgos informáticos identificados.

1.4. Justificación del Proyecto

El Centro de Datos está considerado como un componente que sin dudas toma un rol estratégico para el buen funcionamiento de una organización basada en sistemas informáticos como parte de sus procesos y servicios. Estas instalaciones están diseñadas para garantizar la disponibilidad, escalabilidad y seguridad de la información permitiendo a las organizaciones a respaldar sus operaciones y brindar sus servicios de manera eficiente [8].

La relevancia social de un plan de tratamiento de riesgos radica en la capacidad de fortalecer la seguridad de los datos y activos críticos del Data Center, asociándolos

a conceptos de la seguridad de la información como son los de integridad, confidencialidad y disponibilidad [12]. A través de un análisis y gestión de riesgos se realiza la determinación de procesos y salvaguardas que estén documentadas de manera adecuada teniendo como beneficiarios a los miembros del departamento de sistemas y demás departamentos que interactúan con los servicios y sistemas asociados al Centro de cómputo, además de la misma entidad gubernamental proyectando una mejor prestación de los servicios y protección de datos digitales [13].

La entidad gubernamental actualmente tiene a su disposición un Centro de Datos que contiene los activos críticos que dan soporte a varios sistemas y servicios dentro de la organización en donde fluye información relevante, esto implica que existen factores de riesgo y están expuestos a diversas amenazas que afectan de manera directa e indirecta a los activos esenciales.

El análisis de riesgos permitirá que se identifiquen y se prioricen con una visión más clara las amenazas y posibles escenarios desfavorables presentes en el entorno tecnológico del Data Center detallando los riesgos asociados a la falta de procedimientos adecuados para tratarlos y la falta de capacitación en seguridad informática, además de evaluar el impacto potencial y la probabilidad de los mismos, puesto que al tener una compresión profunda de los riesgos presentes es esencial al momento de la toma de decisiones sobre los procesos o salvaguardas de cómo abordarlos.

El desarrollo del plan de tratamiento de riesgos permitirá a la organización y al departamento encargado del centro de datos tener una ruta estratégica para prevención, mitigación y aceptación de riesgos informáticos, puesto que se establecerán prioridades claras de los procesos de tratamiento lo que fortalecerá la seguridad de la información, la capacidad para enfrentar posibles incidentes, consiguiendo una mejor continuidad operativa y asegurando la prestación de los servicios en el entorno digital actual de la entidad gubernamental.

Los resultados del análisis de riesgos informáticos servirán como punto de referencia en caso de que se requiera realizar el desarrollo de un futuro plan de seguridad informática que, a diferencia de un plan de tratamiento de riesgo, este

está enfocado en las medidas y políticas necesarias para la prevención de incidentes y problemas en los sistemas digitales de la empresa.

El tema propuesto está asociado a los objetivos que sigue el Plan de Creación de oportunidades y a los siguientes ejes:

Directriz 1: Soporte territorial para la garantía de derechos.

Lineamiento territorial A: Acceso equitativo a servicios y reducción de brechas territoriales [14].

A4: Fortalecer la conectividad y el acceso a las TIC como una vía para mejorar el acceso a otros servicios [14].

Objetivos Eje Social

Objetivo 5: Proteger a las familias, garantizar sus derechos y servicios, erradicar la pobreza y promover la inclusión familiar [14].

Política 5.5: Mejorar la conectividad digital y el acceso a nuevas tecnologías de la población [14].

1.5. Alcance del Proyecto

Este proyecto estará enfocado a los riesgos informáticos que están asociados a los activos críticos afectando a la seguridad y continuidad operativa del Data Center de la entidad gubernamental. La realización de este estudio e investigación permitirá una mejora de los procesos y medidas de tratamiento de riesgos actuales.

El presente proyecto se centra en el diseño de un plan de tratamiento de riesgos como resultado de un análisis y gestión de riegos aplicando la metodología MAGERIT en su versión 3 como guía para la identificación, valoración, evaluación de los riesgos y su impacto potencial en la entidad gubernamental. El plan se enfoca en la prevención, minimización, detección, aceptación y gestión de riegos informáticos priorizando los activos críticos de Data Center estableciendo acciones concretar para reducir la exposición a amenazas y vulnerabilidades, garantizando la continuidad operativa.

Las fases que se llevaran a cabo en este proyecto de describen a continuación:

La fase 1 incluirá la identificación de los activos del centro de cómputo, la cual se llevará a cabo mediante la utilización de metodologías de recolección de información con el fin de comprender la importancia de los activos claves para la continuidad operativa de la entidad gubernamental. Así mismo se identificarán las dependencias entre activos, es decir que cada activo interactúa con otro. Como lo dicta la metodología es la manera en que afecta un activo si este fuese vulnerado a otro activo con el que está relacionado de manera superior o inferior. Se finaliza esta fase con la valorización de los activos identificados en donde se definirá el valor del activo, es decir la importancia que tiene cada activo dentro del Data Center, se establecerá respecto a las dimensiones de confidencialidad, integridad, autenticidad y disponibilidad en base a MAGERIT.

En la fase 2 se realizará la identificación de las amenazas que afecta a cada tipo de activo, esta actividad se realiza en función de la clasificación de los mismos como lo dicta la metodología en activos esenciales, servicios internos, equipamiento, instalación y personal, se utilizará la herramienta PILAR para facilitar esta actividad, ya que cuenta con una biblioteca de amenaza. Así mismo se valorizarán las amenazas identificadas en la actividad anterior, se determinará la influencia en el valor del activo definiendo la probabilidad de que la amenaza se materialice y la degradación en sus niveles con respecto a las dimensiones que se están evaluando.

En la fase 3 a partir de las amenazas identificadas, se determinarán las salvaguardas pertinentes con cada medida efectiva que tiene para la mitigación del riesgo. Se utilizará la herramienta PILAR que sugiere un listado de proceso y medidas adecuadas que se pueden tomar para la minimización de los riesgos que se presentan en cada activo. Estas salvaguardas se tomarán como punto de partida para el diseño del plan de tratamiento de riesgos.

En la fase 4 se estimará el impacto del riesgo al que los activos están expuestos (lo que puede ocurrir), para establecer el grado de daño sobre los activos en el caso que la amenaza se materialice con respecto a las dimensiones que se están evaluando (impacto potencial). Además, se realizará la estimación del impacto una vez que los salvaguardas se hayan implementado (impacto residual), por lo cual se utilizará la

herramienta PILAR que proporcionará los resultados del impacto. Así mismo se estimará el riesgo potencial y residual al que los activos del sistema están sometidos (probablemente ocurra), la herramienta lo calculará de manera automática determinando el riesgo siendo igual a probabilidad de amenaza * magnitud de impacto.

En la fase 5 y una vez finalizado el análisis de riesgos basado en MAGERIT se determinarán a partir de la fase 3 las salvaguardas que serán parte del plan de tratamiento de riesgos. El cual comprenderá de medidas de prevención, minimización, detección y aceptación de los riesgos.

Para finalizar se documentará el plan que describirá las actividades, procedimiento, responsables y recursos necesarios que se necesiten para seguir con las medidas de tratamiento de riesgos adecuadas basándose en las salvaguardas ya identificadas en las fases anteriores.

Es importante resaltar que el proyecto estará enfocado al diseño y planificación del plan de tratamiento de riesgos brindando una guía para el trato de los mismos, sin embargo, este no llegará a implementarse en la entidad gubernamental. Así mismo se recalca que si en un futuro la entidad decide implementar el plan no se asegura que el Data Center este 100% seguro ante riesgos, amenazas e incidentes.

CAPÍTULO II

2. Marco Teórico y Metodología del Proyecto

2.1. Marco Teórico

2.1.1. Información

Se refiere a cualquier dato, conocimiento o contenido digital que tenga valor para una organización o individuo. Estos datos pueden representarse en diferentes tipos y formas, incluyendo documentos, archivos, bases de datos, correos electrónicos, multimedia, entre otros. Además, el contenido puede ser tangible, como archivos físicos o dispositivos de almacenamiento, o intangible, como datos transmitidos a través de redes de comunicación [15].

2.1.2. Seguridad de la información

La seguridad de la información se define como la práctica de proteger los datos y los sistemas de información de amenazas como el acceso sin autorización o la filtración de datos que puedan resultar en la exposición, modificación o eliminación de información confidencial. Esta práctica incluye la aplicación de salvaguardas para garantizar la confidencialidad, integridad y disponibilidad de la información esencial [16].

2.1.3. Seguridad Informática

Se define como seguridad informática al grupo de medidas o prácticas diseñadas para impedir la ejecución de acciones no autorizadas sobre los sistemas informáticos, causando daño a la integridad, confidencialidad y disponibilidad de la información, así como las redes que la procesan, almacenan y transmiten. Disminuyendo el rendimiento de los equipos y la operatividad de los sistemas [17].

2.1.3.1. Principios de la seguridad

La seguridad de la información es un componente importante y esencial en la actual era digital. Existen tres principios que son esenciales para el cumplimiento de la misma [18]. A continuación, se describen los principios:

- **Confidencialidad**

Consiste en garantizar que la información sensible y privilegiada sea accesible únicamente para aquellos usuarios autorizados y que esté protegida contra cualquier acceso no autorizado o divulgación indebida [18].

- **Integridad**

Este principio se centra en garantizar que la información sea precisa, completa y no haya sido alterada de manera no autorizada [18].

- **Disponibilidad**

Se centra en asegurar que los recursos y servicios de tecnología de la información estén disponibles y accesibles cuando sean necesarios por parte de los usuarios autorizados [18].

Además de los tres principios principales se suele tomar en cuenta dos conceptos más.

- **Autenticación**

Se centra en verificar la identidad de los usuarios y sistemas antes de permitirles el acceso a recursos o datos sensibles [19].

- **No repudio**

Se refiere a la imposibilidad de negar la realización de una acción o transacción previamente llevada a cabo [19].

2.1.4. Riesgo Informático

Un riesgo se define como la posibilidad de que ocurra un evento o se materialice una amenaza que pueda causar daño o perjuicio y sus posibles consecuencias [20]. El riesgo informático o tecnológico se refiere a la posibilidad de sufrir daños o pérdidas debido a la vulnerabilidad de los sistemas informáticos [21].

2.1.5. Seguridad Física

La seguridad física consiste en la aplicación de medidas concretas y visibles destinadas a prevenir, mitigar y minimizar amenazas a los equipos informáticos, además de los sistemas e información esencial que están almacenados en los

mismos. Este tipo de seguridad se centra en garantizar la continuidad de las operaciones y la protección de la información crítica [19][20].

2.1.6. Seguridad Lógica

La seguridad lógica se refiere a la protección de la información, sistemas y redes de una organización mediante la aplicación de medidas con el objetivo de garantizar que la información sea accesible solo a los usuarios autorizados y que no exista ningún cambio de las aplicaciones [19].

2.1.7. Análisis y Gestión de Riesgos Informáticos

El análisis de riesgos informático es un proceso que busca identificar y evaluar los posibles riesgos que podrían afectar a la seguridad de los sistemas de la información, incluyendo datos críticos de la organización. Este proceso implica examinar detalladamente los activos, como datos confidenciales, aplicaciones, servicios, redes y hardware, para identificar las posibles fuentes de riesgo a los que están expuestos. Este proceso no solo permite la identificación, además evalúa la probabilidad que una amenaza se materialice y el impacto que esta tendría en la organización [22].

El análisis de riesgos informáticos es un proceso continuo y dinámico que requiere revisión y actualización periódica para mantenerse al día con las nuevas amenazas y vulnerabilidades que surgen en el entorno digital. Al realizar este análisis de manera regular, las organizaciones pueden tomar decisiones informadas sobre cómo asignar recursos para proteger sus activos digitales y garantizar la continuidad de sus operaciones [17].

El análisis de riesgos permite determinar cómo es, cuánto vale y cómo de protegido se encuentra el sistema. En coordinación con los objetivos, estrategia y política de la Organización, las actividades de tratamiento de los riesgos permiten elaborar un plan de seguridad que, implantado y operado, satisfaga los objetivos propuestos con el nivel de riesgo que acepta la Dirección. Al conjunto de estas actividades se le denomina “Proceso de Gestión de Riesgos” [10]. La siguiente figura detalla el recorrido que se realiza al proponer un análisis de riesgos.

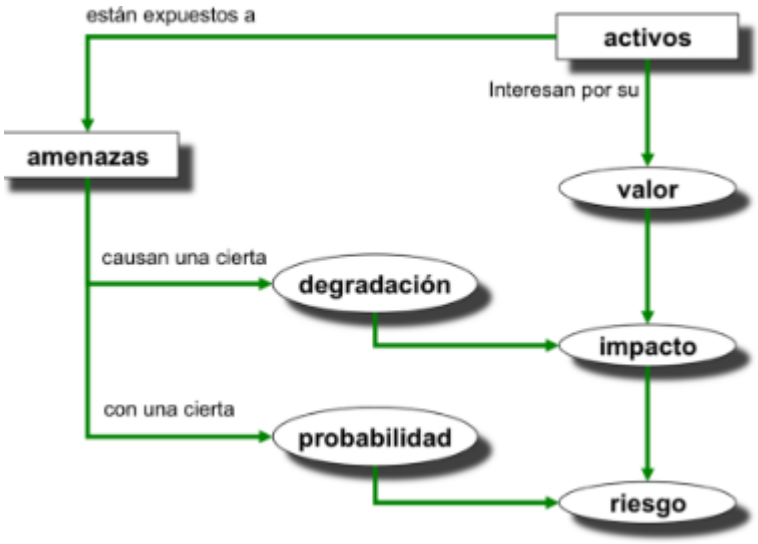


Figura 2: Elementos del análisis de riesgos [10]

La gestión de riesgos informáticos es un proceso que consiste en la identificación, clasificación, manejo y monitoreo de los riesgos vinculados a los activos. Se centra en la aplicación de un conjunto de controles o salvaguardas con el objetivo de disminuir la probabilidad de ocurrencia de las amenazas [22]. En la siguiente figura se denota los procesos que forman parte de la gestión.

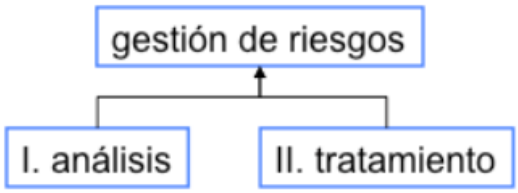


Figura 3: Gestión de Riesgos [10]

2.1.7.1. Análisis Cualitativo

El análisis cualitativo es un enfoque de evaluación de riesgos que se apoya en la percepción subjetiva de cuán grave y probable es un riesgo. En vez de usar datos numéricos, este tipo de análisis emplea descripciones detalladas para detectar y valorar los posibles riesgos. Estos se dividen en niveles de alto, medio o bajo para facilitar la priorización de las acciones de mitigación. A pesar de no ofrecer una medida cuantitativa exacta, el análisis cualitativo es útil para la gestión de riesgos informáticos [23].

2.1.7.2. Análisis Cuantitativo

El análisis cuantitativo en la gestión de riesgos informáticos es un proceso que asigna valores numéricos a los diferentes aspectos del riesgo, como la probabilidad de ocurrencia, la magnitud del impacto y la exposición al riesgo. Este enfoque permite realizar modelizaciones que brindan una comprensión más precisa de la naturaleza y la magnitud del riesgo. A diferencia del cualitativo, para realizar de manera efectiva este análisis se necesita del registro del riesgo, la estimación del tiempo y el plan de gestión de costos o presupuesto [23].

2.1.8. Metodologías para el análisis y gestión de riesgo

2.1.8.1. Magerit

Magerit (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) es una metodología desarrollada por el Consejo Superior de Administración Electrónica del Gobierno de España. Su objetivo principal es minimizar los riesgos asociados con la implementación y uso de las Tecnologías de la Información, especialmente en el ámbito de las Administraciones Públicas [9].

Esta metodología se divide en 3 libros:

- Libro 1. Método. – Este libro se centra en el método de análisis y gestión de riesgos para los sistemas de información. El libro proporciona una visión general de la gestión de riesgos y explica cómo implementarla en el contexto de las tecnologías de la información [9].
- Libro 2. Catálogo de elementos. – Este libro contiene una lista exhaustiva de elementos de la seguridad de la información, se incluyen los tipos de activos, dimensiones de valoración, amenazas y salvaguardas. Facilita el proceso del proyecto con respecto a la identificación y evaluación de los riesgos [9].
- Libro 3: Guía de Técnicas. – Se describen las técnicas que se emplean para llevar a cabo los proyectos de análisis y gestión de riesgos, además de contener ejemplos de tablas, técnicas gráficas y diagramas [9].

2.1.8.1.1. Objetivos de Magerit

La gestión de riesgos de seguridad de la información es un aspecto crítico para cualquier organización en la actualidad, dada la creciente complejidad y sofisticación de las amenazas informáticas. En este sentido, Magerit se presenta como un marco de trabajo integral para abordar los desafíos que traen consigo los riesgos informáticos. A continuación, se presentan los objetivos de la metodología extraídos del libro 1 del volumen 3 [10].

- **Directos**
    - Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos [10].
    - Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC) [10].
    - Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control [10].
- **Indirectos**
    - Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso [10].

2.1.8.1.2. Dimensiones de Seguridad/Valoración

Son las características o atributos que hacen valioso un activo, es un aspecto independiente de otros. Pueden hacerse análisis de riesgos centrados en una única faceta, independientemente de lo que ocurra con otros aspectos. Las dimensiones se utilizan para valorar las consecuencias de la materialización de una amenaza.

- **Disponibilidad**. - Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren [24].
- **Integridad**. - Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada [24].
- **Confidencialidad**. - Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados [24].

- **Autenticidad**. - Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos [24].
- **Trazabilidad**. - Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad [24].

2.1.8.2. Octave

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) es una metodología de evaluación de riesgos desarrollada por el Software Engineering Institute (SEI) en Estados Unidos. El propósito de esta metodología es identificar y abordar los riesgos operacionales, además de las prácticas de seguridad, a lo largo de tres etapas, procesos y actividades, con el fin de desarrollar un análisis detallado de las necesidades de seguridad en una organización. El enfoque se centra en los aspectos de riesgos operativos y prácticas de seguridad, lo cual permite a las organizaciones tomar decisiones pertinentes sobre la protección de la información basándose en riesgos como confidencialidad, integridad o disponibilidad de bienes relacionados con información crítica [25].

2.1.8.3. CRAMM

CRAMM (CCTA Risk Analysis and Management Method) es una metodología de análisis de riesgos desarrollada por la Agencia Central de Comunicación y Telecomunicación del gobierno británico. El enfoque de esta metodología es identificar activos, evaluar riesgos y seleccionar controles de seguridad. A pesar de que podría necesitar una inversión importante en tiempo y recursos, CRAMM es utilizada extensamente en diversas industrias y situaciones, tanto en el sector público como privado.

La metodología CRAMM incluye tres fases: definición de los objetivos de seguridad, análisis de riesgos con su respectiva identificación y selección de medidas de seguridad. Mediante este proceso, las entidades pueden detectar y reducir los posibles riesgos, lo que a su vez mejora la seguridad de sus sistemas de información [26].

2.1.8.4. COBIT

COBIT (Control Objetive for Information and Related Technologies) es un marco integral de gobernanza y gestión de TI que ayuda a las organizaciones a alcanzar sus objetivos de negocio mediante una gestión efectiva y eficiente de la tecnologías de la información [27]. La metodología proporciona una estructura sistemática de gestión de riesgos que permite un mejor entendimiento de estos mismos y de su impacto en la organización. COBIT se basa en identificar, evaluar y mitigar los riesgos relacionados con los sistemas de información, además de enfatizar en la importancia de los sistemas e incrementar las capacidades de las organizaciones con respecto a los riesgos [28], [29].

2.1.8.5. Comparación entre Metodologías

En la siguiente tabla se presenta una comparación entre las metodologías Magerit, OCTAVE, CRAMM y COBIT, abarcando aspectos clave como su enfoque, ámbito de aplicación y principales características:

Metodología	Enfoque	Ámbito de aplicación	Principales Características
MAGERIT	Gestión de riesgos	Utilizada principalmente por la Administración Pública, pero es aplicable a todos los sectores. Organizaciones que necesitan evaluar y gestionar los riesgos de sus sistemas de información	Desarrollada por el Consejo Superior de Administración Electrónica de España. Basada en identificar activos, amenazas y vulnerabilidades. Metodología detallada con guías prácticas y documentos de soporte.
OCTAVE	Evaluación de riesgos	Organizaciones de cualquier tamaño que	Desarrollada por el CERT de la Universidad Carnegie Mellon.

	de seguridad	buscan mejorar su seguridad de la información.	Enfocada en la autoevaluación y la identificación de riesgos por parte del personal interno. Proporciona una visión estratégica de la seguridad organizacional.
CRAMM	Gestión de riesgos y auditoría	Utilizada en una variedad de industrias y contextos, incluyendo el sector público y privado	Desarrollada por el gobierno del Reino Unido. Estructurada en tres fases: identificación y evaluación de activos, análisis y evaluación de riesgos, y selección e implementación de contramedidas. Utiliza una base de datos de contramedidas específicas.
COBIT	Gobierno y gestión de TI	Organizaciones que buscan alinear sus procesos de TI con los objetivos empresariales	Enfocada en la integridad, disponibilidad y confidencialidad de la información. Define objetivos de control y proporciona métricas y modelos de madurez.

Tabla 1. Comparación de Metodologías

2.1.9. Metodología Magerit V3

2.1.9.1. Activos Informáticos

Un activo se define como cualquier recurso valioso para la organización, sea parte de un sistema o no, se refiere a todo lo que tenga valor y deba ser protegido en un futuro de alguna amenaza. Estos pueden ser información, software (sistemas), hardware y el personal que interactúe con la infraestructura tecnológica [20].

Es un elemento o aspecto de un sistema de información que podría ser objeto de un ataque intencional o accidental, con posibles repercusiones para la organización. Esto abarca una amplia gama de elementos, como información confidencial, datos críticos, servicios operativos, software y hardware, así como recursos administrativos [10].

- **Dependencias**

Magerit cataloga la dependencia como la interrelación y la influencia mutua entre los recursos de un sistema de información. De manera que los activos forman grafos de dependencia donde la seguridad que tenga un activo superior depende de los activos inferiores. La dependencia se refleja de arriba hacia abajo (activos superiores hasta llegar a los inferiores), mientras que la propagación del daño en caso de materializarse se refleja de abajo hacia arriba [10].

- **Valoración**

La valoración se refiere a la importancia que se les da a los recursos tecnológicos, de manera que se les asigna un valor desde la perspectiva de cuánto se lo quiere proteger, es decir que, si el valor de un activo es alto, la importancia y necesidad de protegerlo es mayor. Magerit presenta dos tipos de valoración, la cualitativa que se basa en determinar un valor exacto a cada activo respecto a un orden relativo, y la cuantitativa que determina valores absolutos, además de tener la capacidad de sumarlos [10].

2.1.9.2. Amenazas

Una amenaza se define como a cualquier evento o circunstancia que afecte al sistema, sus activos y su funcionamiento provocando que las dimensiones de la seguridad se afecten de manera directa [22]. Se considera amenaza a una causa

potencial de un incidente que puede causar daños a un sistema de información o a una organización, Magerit cataloga las amenazas en: origen natural, del entorno (de origen industrial), defectos de las aplicaciones, causadas por las personas de forma accidental (errores y fallos no intencionados) y por las personas de forma deliberada (ataques deliberados) [10].

2.1.9.3. Impacto Potencial y Residual

- Potencial

Se denomina impacto potencial a la medida o magnitud del daño que se produce y afecta a las propiedades de la seguridad de la información, se determina una vez conociendo el valor de las dimensiones y la degradación en porcentaje del activo [10].

- Residual

El impacto residual es el valor cuando cierto conjunto de salvaguardas ha sido desplegado de manera que exista una madurez en el estado del impacto potencial dando un cambio en el valor inicial [10].

2.1.9.4. Riesgo Potencial y Residual

- Potencial

Se denomina riesgo potencial al nivel de daño probable que un activo de información enfrentaría en ausencia de salvaguardas o medidas de seguridad. Es una medida de la exposición de un activo a amenazas, sin tener en cuenta las salvaguardas existentes [10].

- Residual

El riesgo residual se refiere al nivel de riesgo que queda después de haber aplicado las salvaguardas o medidas de seguridad. Es decir, es el riesgo que todavía existe después de haber implementado las acciones de mitigación [10].

2.1.9.5. Salvaguardas

Se define como salvaguarda a las actividades, procedimientos o mecanismos que se emplean para reducir el riesgo (activas) e impacto (pasivas) de las amenazas. Las salvaguardas pueden tratar aspectos organizativos, técnicos, físicos o relativos a la

gestión de personal [10] [17]. En PILAR, que es una herramienta que implementa la metodología MAGERIT, las salvaguardas se pueden evaluar por dominio o por activo.

2.1.10. Tratamiento de Riesgos

Es una fase que se encuentra dentro de la gestión de riesgos, se centra en la determinación de estrategias y medidas diseñadas para minimizar, transferir, aceptar o prevenir los riesgos, según su impacto y probabilidad de ocurrencia. En conjunto, estas medidas permiten a las organizaciones a gestionar de manera efectiva los riesgos con la finalidad de proteger los activos asociados a los sistemas de información [10].

2.1.11. EAR/PILAR

Software diseñado para el "Procedimiento Informático – Lógico del Análisis de Riesgos", herramienta que facilita la aplicación de la metodología Magerit siguiendo las fases de caracterización de activos, caracterización de amenazas y evaluación de salvaguardas. Permite identificar activos, evaluar sus amenazas, calcular la probabilidad de impacto y gestionar las medidas como contramedida para los riesgos [10].

2.2. Metodología del Proyecto

2.2.1. Metodología de Investigación

El propósito de la metodología de investigación es proporcionar un enfoque estructurado que exponga los elementos indispensables para llevar a cabo la búsqueda, recopilación de información y la interpretación de la misma, lo cual se considera importante para el desarrollo del presente proyecto [30].

El presente proyecto se clasifica como una investigación exploratoria, debido a que, si bien el tema ha sido abordado anteriormente, es totalmente novedoso en el contexto de la entidad gubernamental [30]. Dado que existe poca información de soluciones previas o de un enfoque predefinido al objeto de estudio por este problema en específico, se necesita de una investigación exploratoria para identificar y desarrollar un marco de tratamiento de riegos que se ajuste a las necesidades de la entidad.

Así mismo, se aplica una investigación diagnostica, debido a que su propósito es la de indagar sobre el problema y la situación actual con la finalidad de entender mejor el problema [4]. Dado que implica una evaluación del estado actual de los procesos de tratamientos de riesgos del Data Center, identificando problemas y vulnerabilidades de la gestión de riesgo. Esta metodología se realizará mediante una observación directa al centro de cómputo y una entrevista al encargado del mismo para detallar si existen los procesos adecuados para el tratamiento de riesgos.

A su vez, se cataloga como una investigación de carácter experimental [30], debido a la manipulación controlada de la variable independiente: el diseño del plan. Aunque el plan solo se diseñará y no se implementará, se sigue un enfoque experimental al utilizar el método MAGERIT para evaluar y gestionar los riesgos informáticos. Además, a través de la herramienta PILAR se realizará una simulación de implementación de las salvaguardas que se identifiquen, dando como resultado datos e información valiosa sobre cuánto disminuye el impacto y el riesgo en el objeto de estudio, proporcionando un marco riguroso para comprender la seguridad de la información en entornos críticos, como los centros de datos gubernamentales.

Se aplicará un enfoque cualitativo [30], debido a que se recopilaran datos mediante técnicas como la observación con el objetivo de recopilar información de manera directa de las operaciones, sistemas, condiciones físicas y lógicas del Data Center. También se realizarán entrevistas con la finalidad de conocer sobre los activos críticos, procedimientos de tratamiento de riesgos actuales, su funcionamiento y los posibles riesgos existentes que pueden afectar al centro de cómputo. Además, la investigación se caracteriza como inductiva [30], porque se centra en la exploración y comprensión de las prácticas específicas de gestión de riesgos presentes en el entorno del Data Center gubernamental, sin partir de teorías preexistentes. En lugar de ello, se busca generar nuevas perspectivas y comprensiones a partir de los datos recopilados, llegando a resultados únicos para el contexto de la problemática.

2.2.2. Técnicas e instrumentos de recolección de información de datos

- **Técnica**

Técnica de observación y entrevistas.

- **Instrumento**

La técnica de observación se empleó en el Data Center de la entidad gubernamental, con el objetivo de recopilar información de manera directa de las operaciones, sistemas, condiciones físicas y lógicas del Data Center.

Las entrevistas estarán dirigidas a los jefes de área del departamento de sistemas y recursos tecnológicos, dándole prioridad al encargado del centro de cómputo, con la finalidad de conocer sobre los procedimientos de tratamiento de riesgos actuales, su funcionamiento y los posibles riesgos existentes que pueden afectar al Data Center.

Las fuentes de referencia bibliográficas permitirán realizar un análisis literario con el fin de entender mejor la problemática que se está evaluando.

- **Población**

La población de la cual se recopilará la información y que a su vez son los beneficiarios directos del proyecto son las autoridades del departamento de sistemas y recursos tecnológicos. En la siguiente tabla se detalla a los involucrados del proyecto.

Informantes	Cantidad
Coordinador/a del Área de sistemas y recursos tecnológicos	1
Analista de seguridad informática / Encargado del Data Center	1
Analista Técnico de base de datos	1
Programador Senior	1
Programador de sistemas	1
Técnico De Hardware	2
Total	7

Tabla 2. Población del Proyecto

Para este proyecto se trabajará con la población completa.

2.2.2.1. Análisis de la recolección de información

En el trascurso de la realización del proyecto se aplicaron dos técnicas de recolección de información con la finalidad de conocer sobre las condiciones físicas, lógicas y sistemas del data center, así como los procesos actuales que siguen para el tratamiento de riegos del sitio, estas fueron la técnica de observación y entrevistas al encargado del centro de cómputo.

La técnica de entrevista al encargado y responsable del Data Center (Anexo 1), permitió obtener información valiosa sobre la situación actual del sitio. Se determinó la incapacidad de la organización y del departamento de sistemas para la gestión y el trato a los riesgos informáticos en seguridad física como lógica, además reveló que no existen procesos o procedimientos documentados para abordar los riesgos de seguridad, lo que pone de manifiesto la necesidad urgente de mejorar las prácticas de seguridad.

Tal cual se ha identificado que el Data Center no cuenta con un inventario de activos debidamente documentado, lo que es esencial para la gestión efectiva de la seguridad de la información. A pesar de la presencia de un responsable del Data Center, se reconoce la ausencia de un área específica dedicada a la seguridad física y lógica. Esto subraya la necesidad de un enfoque más estructurado y especializado en la seguridad de la información.

Las entrevistas realizadas a las autoridades del departamento de sistemas y recursos tecnológicos (Anexo 2), permitieron determinar los posibles riesgos existentes en el entorno del Data Center. Se obtuvo una visión previa de los desafíos y vulnerabilidades potenciales que enfrenta el centro de cómputo, lo que proporcionó una base sólida para la identificación y evaluación de riesgos en el análisis posterior.

La técnica de observación aplicada (Anexo 5), permitió determinar varios aspectos de seguridad que posee y de los que carece el centro de cómputo. Estos hallazgos resaltan que tanto la seguridad física y lógica está expuesta a amenazas en su infraestructura, poniendo en peligro las propiedades de la seguridad de la información almacenada en el Data Center, lo que destaca la importancia de tomar medidas correctivas y preventivas.

2.2.2.2. Beneficiarios del proyecto

Los beneficiarios directos serán los miembros del departamento de sistemas y recursos tecnológicos (7 personas), aunque no se llevará a cabo la implementación del plan, se beneficiarán al contar con un enfoque teórico en el proceso de análisis de riesgos ya que dará como resultados una mejor y profunda comprensión de las amenazas relacionadas con los tipos de activos críticos en la seguridad en el entorno del Data Center. A pesar de la falta de implementación, el diseño del plan tiene un valor preventivo y preparativo al fortalecer la preparación del departamento para futuras decisiones de implementación.

Los beneficiarios indirectos serán los distintos departamentos cuyos sistemas estén soportados por el centro de cómputo de la entidad (47 departamentos y 711 empleados), en este caso se centraría en la conciencia y conocimiento sobre los riesgos que podrían afectar a los sistemas que manejan.

2.2.3. Variable del proyecto

Para el desarrollo de este proyecto investigativo se ha empleado el registro de la cantidad de riesgos identificados con sus respectivas salvaguardas como variable, donde se realiza la estimación de la cantidad identificada antes y después de realizar el proceso de análisis de riesgos.

Variable	Definición conceptual	Indicador	Método de medición
Cantidad de riesgos con sus respectivas salvaguardas	Es la cantidad de riesgos que se han identificados y posteriormente la determinación de sus salvaguardas para tratarlos.	Número Total de riesgos identificados.	(N°) Cantidad en valor numérico.

Tabla 3. Variable del Proyecto

2.2.4. Metodología de Desarrollo

2.2.4.1. Metodología MAGERIT V3

La metodología Magerit está especializada en el proceso de análisis y gestión de riesgos de los sistemas de información, fue desarrollada por el Consejo Superior de Administración Electrónica en España, es de uso público y está destinada a la evaluación y gestión de riesgos para las tecnologías de la información, proporciona un marco sólido y completo relacionado a la seguridad de la información [31]. A continuación, se describen las fases propuestas para el desarrollo del proyecto:

- Fase 1: Caracterización de Activos.
- Fase 2: Caracterización de las Amenazas.
- Fase 3: Categorización de las salvaguardas.
- Fase 4: Estimación del Estado del Riesgo.
- Fase 5: Plan de tratamiento de riesgos

Fase 1: Caracterización de activos. - La finalidad de esta fase es la de identificar, clasificar, evaluar, validar los activos del Data Center de la entidad y que son claves para una efectiva continuidad operativa de los sistemas y servicios. Esta fase conlleva las siguientes actividades:

- Identificación de los Activos
- Identificación de las dependencias entre activos críticos del Data Center.
- Valoración de los activos identificados.

Fase 2: Caracterización de Amenazas. – El objetivo de esta fase es identificar y comprender en detalle las amenazas a las que están expuestos los tipos de activos en el centro de cómputo. Las actividades por seguir son las siguientes:

- Identificación de Amenazas.
- Valoración de Amenazas.

Fase 3: Caracterización de las salvaguardas. – El propósito de esta fase es el de determinar las salvaguardas adecuadas para cada tipo de activos con relación a las amenazas identificadas, lo que conlleva a realizar las siguientes actividades:

- Identificación de Salvaguardas.
- Valoración de Salvaguardas.

Fase 4: Estimación del Estado del Riesgo. - El objetivo de esta fase es la evaluación de la situación actual de los riesgos identificados en el Data Center. Esta fase es esencial para comprender la magnitud de los riesgos y tomar decisiones informadas sobre cómo abordarlos. Esta fase conlleva a realizar las siguientes actividades:

- Determinar el impacto potencial al que los activos del sistema están expuestos.
- Determinar el riesgo potencial al que los activos del sistema están sometidos.

Fase 5: Plan de tratamiento de riesgos. – Finalizado el análisis de riesgos con los resultados obtenidos, se desarrollará el plan de tratamiento de riesgos a partir de las siguientes actividades:

- Definir las salvaguardas para la minimización, prevención, detección y aceptación del riesgo.
- Establecer el plan de acción que incluya actividades, responsables y eficacia de la tarea propuesta.

CAPÍTULO III.

3. PROPUESTA

3.1. Requerimientos

RQ-1	Revisar la documentación de la metodología Magerit V3, el libro 1 (Método) con el objetivo de conocer el proceso de planificación, análisis y gestión de riesgos informáticos.
RQ-2	Recopilar información de la situación actual del Data Center, su infraestructura física, sus servicios funcionales y salvaguardas existentes si ese es el caso.
RQ-3	Instalar la herramienta PILAR para facilitar y garantizar la precisión en el análisis de riesgos. Se hace uso de una licencia de evaluación.
RQ-4	Realizar un inventario de los activos físicos y lógicos informáticos del Data Center.
RQ-5	Identificar y documentar las amenazas potenciales que pueden afectar la seguridad del Data Center.
RQ-6	Se realiza una entrevista al personal que interactúa de forma directa y que se encarga del Data Center para identificar los posibles riesgos existentes.
RQ-7	Determinar el grado de degradación y la probabilidad de ocurrencia de cada riesgo o amenaza sobre cada tipo de activo.
RQ-8	Determinar el impacto potencial de los riesgos identificados en el funcionamiento del Data Center.
RQ-9	Establecer las salvaguardas correspondientes para la minimización, prevención, detección y aceptación del riesgo.

RQ-10	Documentar el plan detallado que describa las actividades, responsables, eficacia y cualquier información relevante.

Tabla 4. Requerimientos

3.1.1. Situación Actual del Data Center

El Gobierno Autónomo Descentralizado de La Libertad (GAD La libertad) tiene a su disposición un Data Center implementado, se ubica en el segundo piso del edificio principal del GAD municipal dentro del departamento de Sistemas y Recursos Tecnológicos. En la siguiente figura se presenta la infraestructura del sitio, con una dimensiones físicas de Ancho: 2.60 m; Alto: 3.00m; Largo: 2.90m con un área total de 7.54m2.

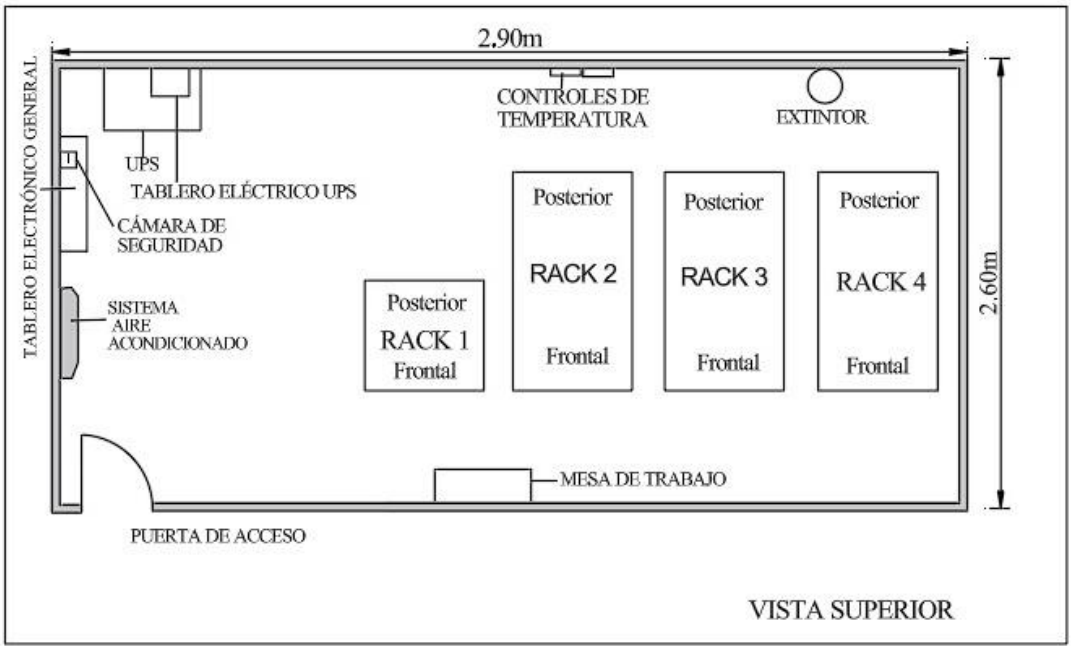


Figura 4: Infraestructura Física - Data Center

A partir de la infraestructura física, se determinó el diagrama de racks representado en la siguiente figura (Figura 5). Este diagrama muestra la distribución física de los racks en el data center, así como la ubicación de los servidores, switches, dispositivos de almacenamiento y otros equipos montados en los racks.

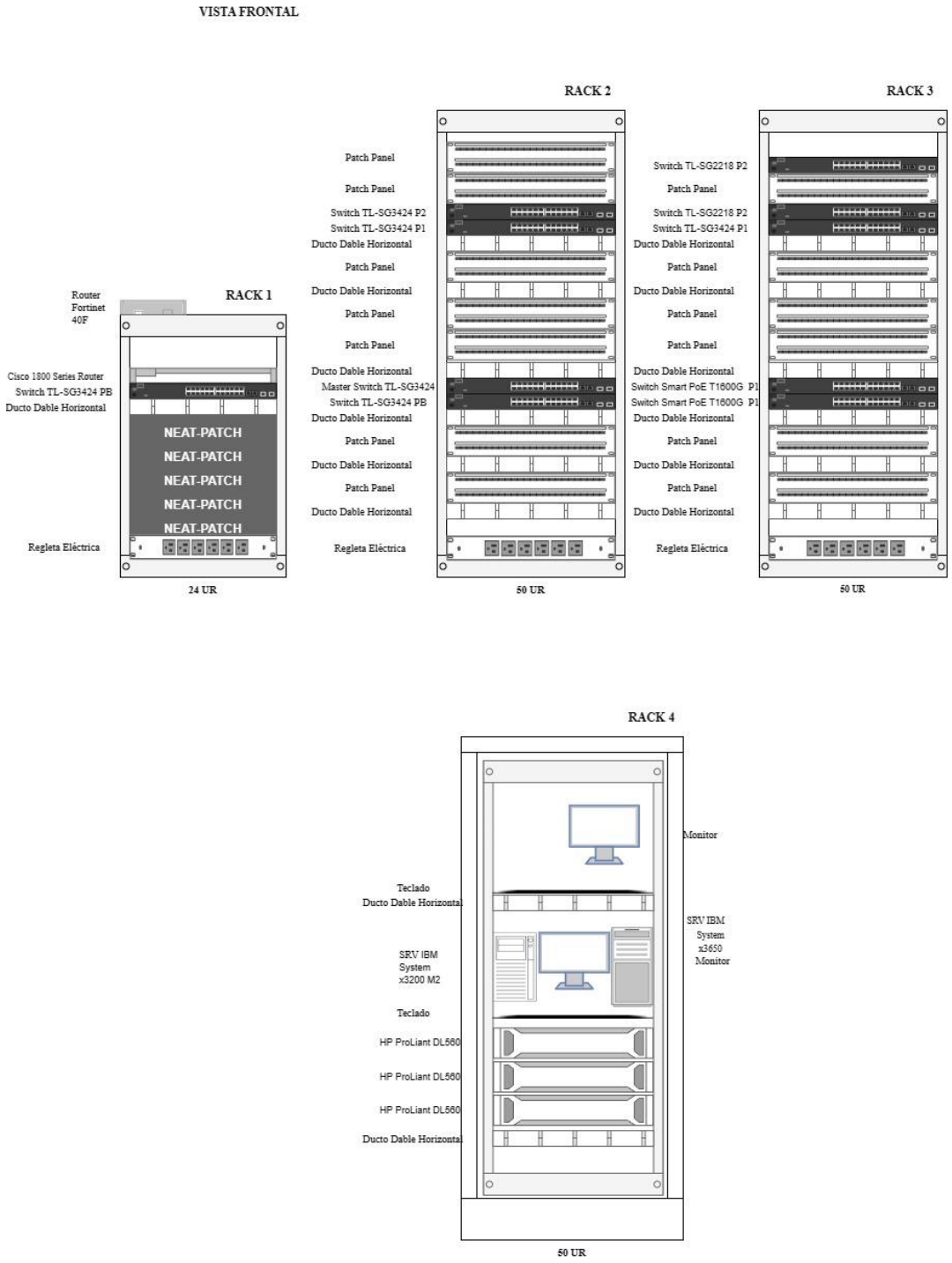


Figura 5: Ubicación Física – Diagrama de Racks

3.1.2. Servicios Funcionales del Data Center Gubernamental

Los servicios funcionales desempeñan un papel crucial en el soporte y la operación eficiente de las infraestructuras tecnológicas que respaldan las actividades de la entidad. Estos servicios no solo garantizan la disponibilidad y la confiabilidad de

los recursos informáticos, sino que también facilitan la prestación de servicios esenciales, promoviendo la transparencia, la eficacia y la seguridad en la gestión de datos de los sistemas. A continuación, se presentan los servicios que soporta el centro de cómputo:

- Alojamiento de servidores y sistemas.
- Virtualización de servidores.
- Almacenamiento de archivos y datos en la nube.
- Backup y recuperación de datos.
- Sistema Financiero/Administrativo.
- Servicios de copias de seguridad y almacenamiento en la nube.
- Servicios de correo electrónico Institucional.
- Servicios de red y conectividad (Internet).
- Servicio de redes inalámbricas.
- Servicios de seguridad informática (firewalls, sistemas de detección de intrusiones).
- Seguridad de la información y gestión de accesos.
- Alojamiento de sitios web y servicios web.
- Gestión de bases de datos.
- Gestión de cambios y versiones de software.

3.1.3. Topología Física

En la siguiente figura (Figura 6), se presenta la topología física del Data Center, donde el acceso a internet y sus servicios son proporcionados por un router Cisco 1800 Series por un enlace de fibra óptica que llega al Master Switch Core TL – SG3424. A este conmutador se encuentran conectados a través de los puestos 10, 11, 13 y 14 el servidor de producción, NAS, de aplicaciones y los servidores virtuales (Promox) respectivamente. Además, a partir de este conmutador se divide la red en tres segmentos por los tres pisos que existen en el edifico de la entidad.

La primera subred está distribuida desde el puerto 15 a un Switch TL – SG3424 este segmento pertenece a la Planta Baja (PB). Este interconecta a dos Switch Smart PoE T1600G – 28, los cuales proveen conectividad a los departamentos tales como: Financiero, Tesorería, Rentas y a los usuarios finales de dicha planta, además de

que se conecta a través del puerto 2 al 20 la red inalámbrica por medio de un Access Point.

La segunda subred de la misma manera está distribuida desde el puerto 16 a un Switch TL – SG3424. Este segmento pertenece al Piso 1 que interconecta a dos Switch Smart PoE T1600G – 28 que proveen conexión a los departamentos de ese piso tales como: Talento humano, Planificación, Sistemas y a los usuarios finales de dicho piso. Igualmente, se tienen un Access Point que provee conexión inalámbrica.

Finalmente, la tercera subred se distribuye desde el puerto 17 a un Switch TL – SG3424, constituye al segmento del Piso 2 de la entidad y el cual interconecta a dos Switch TL - SG2218 que proveen conexión a los departamentos que se encuentran en dicho piso. Como se visualiza en la figura, es una red en topología árbol ya que el master switch es el equipo fundamental para el funcionamiento del Data Center y sus servicios.

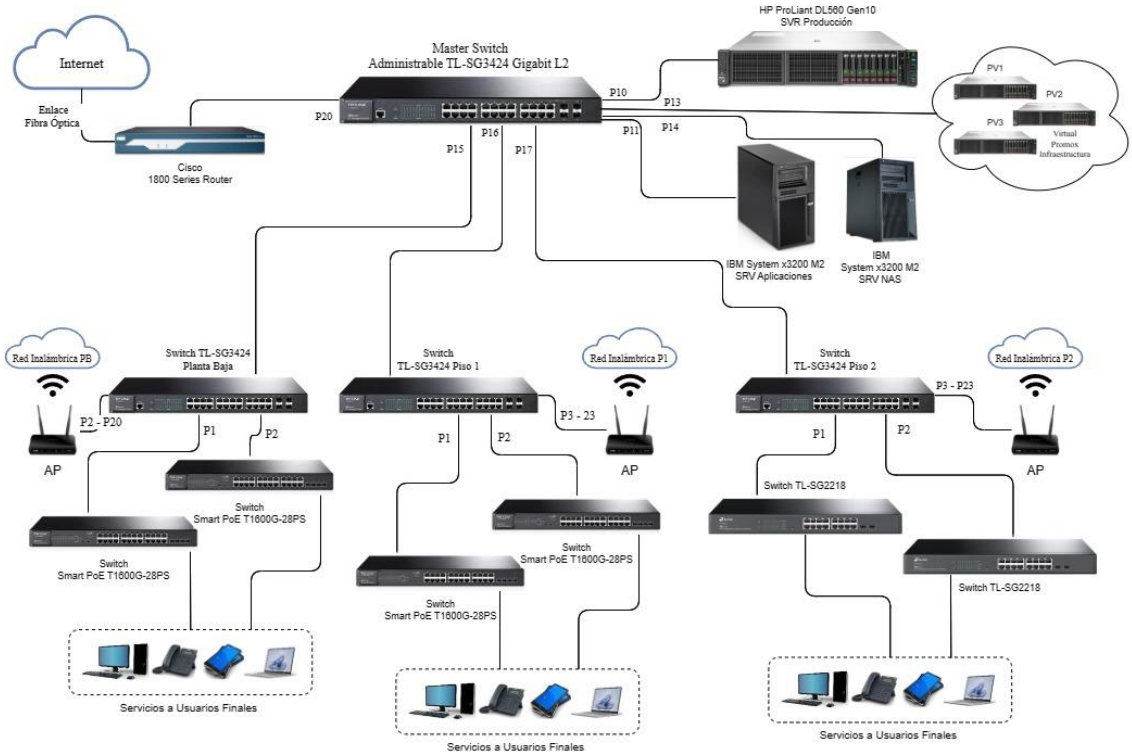


Figura 6: Topología Física - Data Center

3.1.4. Topología Lógica

En la siguiente figura (Figura 7), se observa la topología lógica del centro de cómputo, la cual está constituida por un router Cisco 1800 Series el cual provee internet a la red. Este enlace pasa a través de un firewall en software que verifica y analiza el tráfico en la red, este se conecta al Master Switch Administrable (Core TL – SG3424), a partir de este conmutador se determinan VLAN para cada piso en la entidad gubernamental. La Vlan 1 para la planta baja, Vlan 2 para el piso 1 y Vlan 3 para el piso 2, de los segmentos de VLAN se conecta a tres switch administrables (TL – SG3424) que son los encargados de proveer conexión a 2 switch (Smart PoE T1600G – 28) por cada piso y a los access points respectivamente. Al Master Switch se encuentra la conexión de los servidores físicos y la estructura virtual de servidores de almacenamiento, servidor web, servidor de correo virtualizados mediante Promox.

Como se mencionó en el punto anterior la red se encuentra en una topología Árbol con un enrutamiento e IP estáticas.

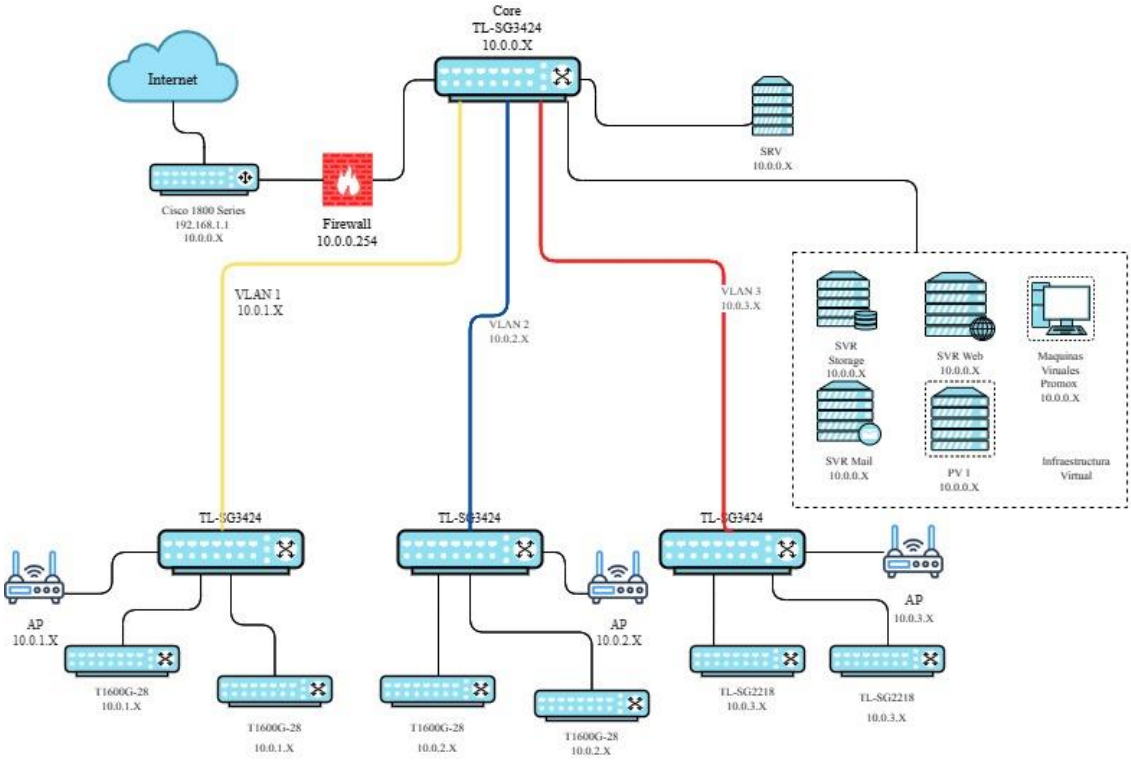


Figura 7: Topología Lógica - Data Center

3.1.5. Salvaguardas Existentes

A través de una visita técnica al Data Center, se determina que existen salvaguardas de activos físicos y lógicos, las cuales son las siguientes:

Físicos

- Para la seguridad física de los equipos, se cuenta con una cámara de vigilancia dentro del mismo, a su vez una cámara que vigila el pasillo del departamento.
- Se cuenta con un sistema de alimentación ininterrumpida, en casos de fallos eléctricos o desconexión del mismo. Este sistema se encarga de garantizar la continuidad de los servicios críticos en el Data Center, proporcionando energía de respaldo para mantener operativos los equipos y sistemas.
- Se cuenta con un sistema de control de temperatura y humedad para garantizar condiciones óptimas de operación de los equipos.
- Se cuenta con dos extintores contra incendios que están colocados en lugares estratégicos.
- Los equipos y cables se encuentran etiquetados para facilitar la gestión o el mantenimiento.

Lógicos

- Se cuenta con un firewall en software implementado en Linux, para proteger la red del Data Center contra accesos no autorizados y ataques maliciosos, filtrando el tráfico no deseado y detectando actividades sospechosas.
- Se cuenta con sistemas de detección de malware y antivirus, para identificar y eliminar cualquier software malicioso que pueda comprometer la seguridad de los sistemas del Data.
- Se cuenta con segregación de entornos de desarrollo, pruebas y producción, para evitar el riesgo de que cambios no autorizados en el código o la configuración afecten a los entornos de producción.
- La red cuenta con una topología en estrella, donde todos los dispositivos están conectados directamente a un nodo, lo que facilita la administración y el monitoreo de la red, así como la identificación y resolución de problemas.

- Se cuenta con dos proveedores de internet en caso de que un proveedor experimente problemas técnicos o cortes de servicio.
- Se cuenta con un sistema de respaldo y recuperación de datos con procedimientos de restauración, para asegurar la disponibilidad y la integridad de los datos en caso de fallo del sistema, error humano o desastre.
- Se realizan las copias de seguridad automáticas y periódicas en Zimbra (Zimbra Backup and Restore) para el correo institucional.
- Se revisa el código fuente (enlaces rotos, botones no funcionales, etc.) y las configuraciones de la página web a diario.

3.2. Desarrollo de la propuesta

3.2.1. Planificación

El objetivo principal del análisis de riesgos en esta etapa es emplear la metodología Magerit para evaluar y comprender los riesgos asociados a los sistemas informáticos del Data Center Gubernamental, identificando activos, amenazas, vulnerabilidades, salvaguardas y el posible impacto de los riesgos.

3.2.2. Análisis de riesgos

Para llevar a cabo el proceso de análisis se hará uso de la herramienta PILAR proporcionada por la metodología antes mencionada y la cual se basa en la misma soportando las fases de caracterización de activo, caracterización de amenazas, categorización de salvaguardas y la estimación del impacto del riesgo. Para el uso de la herramienta se obtuvo una licencia de evaluación.

3.2.2.1. Caracterización de activos

El objetivo de esta fase es identificar y clasificar los activos que hay dentro del Data Center de la institución, determinar su valorización a través de las 4 dimensiones de seguridad que se han establecido y definir la dependencia que existe entre activos.

3.2.2.1.1. Identificación de activos

La primera actividad que se realiza es la identificación de los activos que formarán parte del análisis y gestión de riesgos, los cuales de acuerdo con la metodología

Magerit, cada activo debe tener un nombre y un código de identificación, además de agruparlos en las siguientes categorías:

- Servicios Internos [IS]
- Equipamiento [E]
    - Software (Aplicaciones) [SW]
    - Hardware (Equipos Físicos) [HW]
    - Comunicaciones [COM]
    - Elementos Auxiliares [AUX]
- Soportes de Información [Media]
- Instalaciones [L]
- Personal [P]

Se recopiló la lista de los activos identificado como inventario (Anexo 9), a través de una entrevista al responsable del centro de cómputo, los cuales serán evaluados en la herramienta PILAR, además de ser categorizados previamente como lo dicta la metodología en las categorías antes mencionadas.

Como siguiente paso se ingresan los activos en la herramienta PILAR, con su respectivo nombre y código como lo sugiere el anexo correspondiente. En la siguiente figura se observan los activos ingresados en la correspondiente herramienta con los cuales se trabajará a lo largo del proceso.

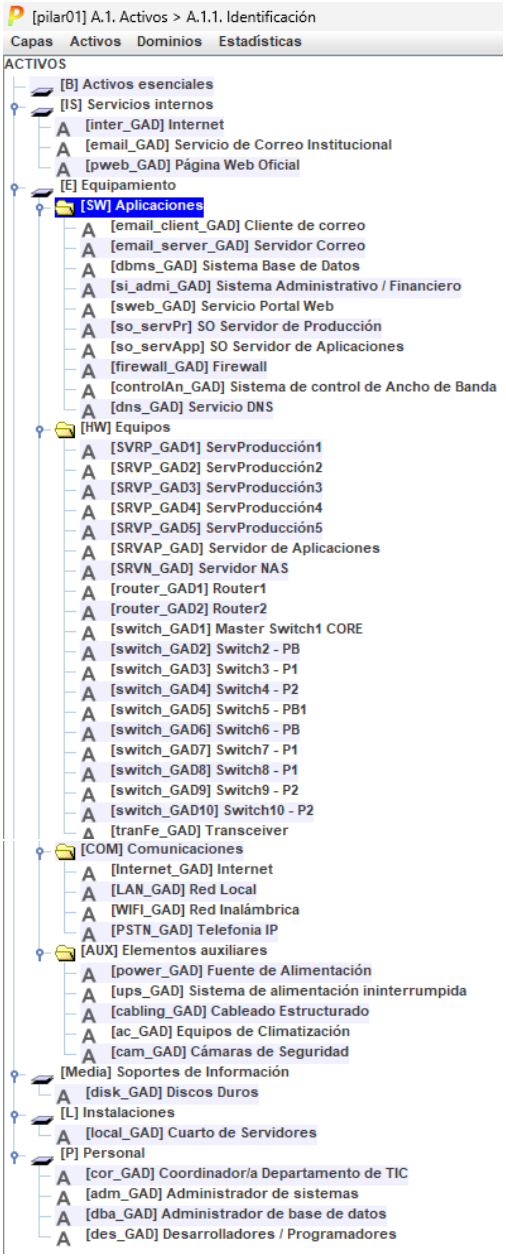


Figura 8: Identificación de Activos PILAR

3.2.2.1.2. Dependencia de Activos

El propósito de esta actividad es proporcionar una visión más completa de la infraestructura de los activos de información, es decir, tener una mejor comprensión de cómo los activos dependen uno de otros, y que un grupo de activos puede ser más significativo que otros. En esta actividad se determinará si existe interacción entre activos, eso quiere decir, que si un activo inferior (Padre) se ve afectado por algún riesgo informático, el activo superior (Hijo) también se verá afectado por el

mismo riesgo. Para realizar la actividad de valoración se deben tomar en cuenta las dependencias que se han determinado.

En la siguiente figura (Figura9) se observan las dependencias entre los activos críticos del Data Center, en donde los servidores se han considerado como activos superiores (Hijo), pero que estos a su vez dependen de los equipos de red, y de la misma manera estos dependen de los activos inferiores (Padre), que en este caso se los considera a los elementos auxiliares. Cabe recalcar que se muestra la dependencia de los activos críticos considerados del centro de cómputo.

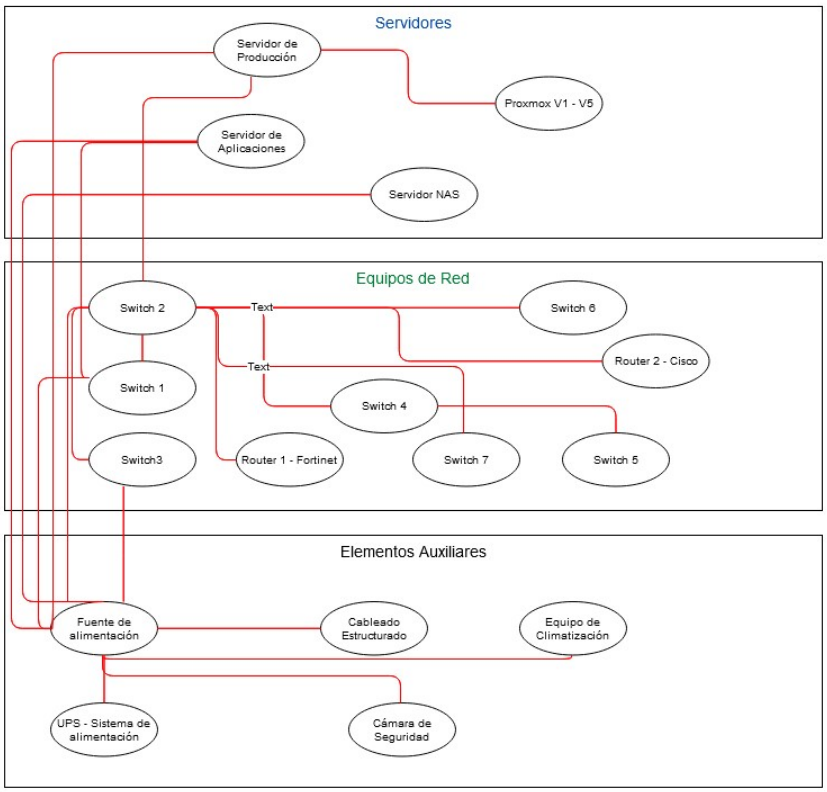


Figura 9: Dependencia de Activos

La herramienta PILAR también nos permite establecer las dependencias entre cada activo. En este caso, como luego se realizará la valoración de activos por activo, se establecen las dependencias antes, en caso de que se realice la valoración por dominios, se puede saltar esta actividad. A continuación, en la figura 10 (Figura10), se muestra la dependencia del activo servidor de aplicaciones como ejemplo, en donde destacan los colores que representa cada nivel, y en la figura 11 (Figura11),

se observa la dependencia de activos, pero de manera más general con la presencia de todos los activos identificados.

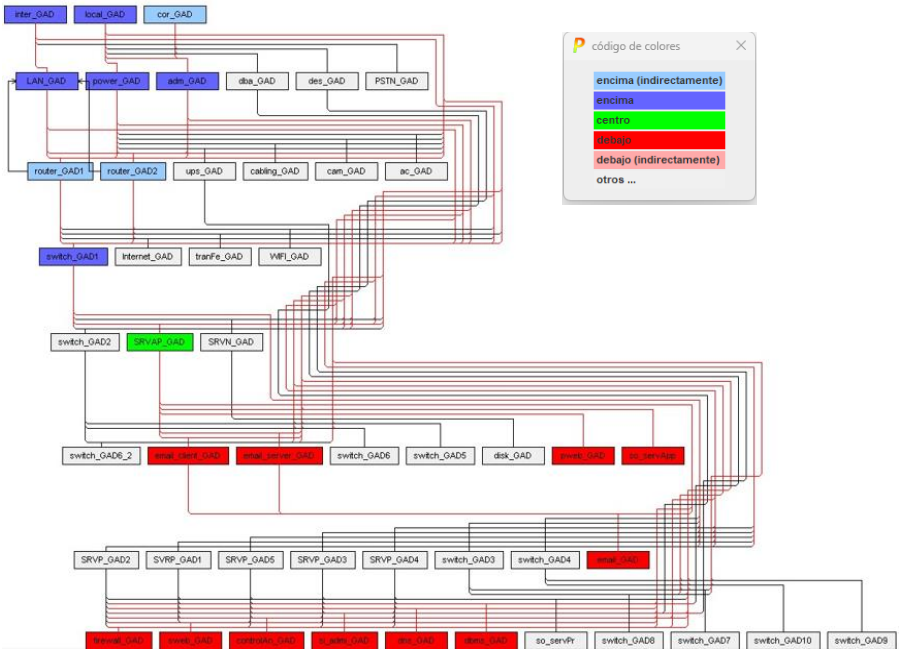


Figura 10: Dependencia de Activo [SRVAP_GAD] Servidor de Aplicaciones

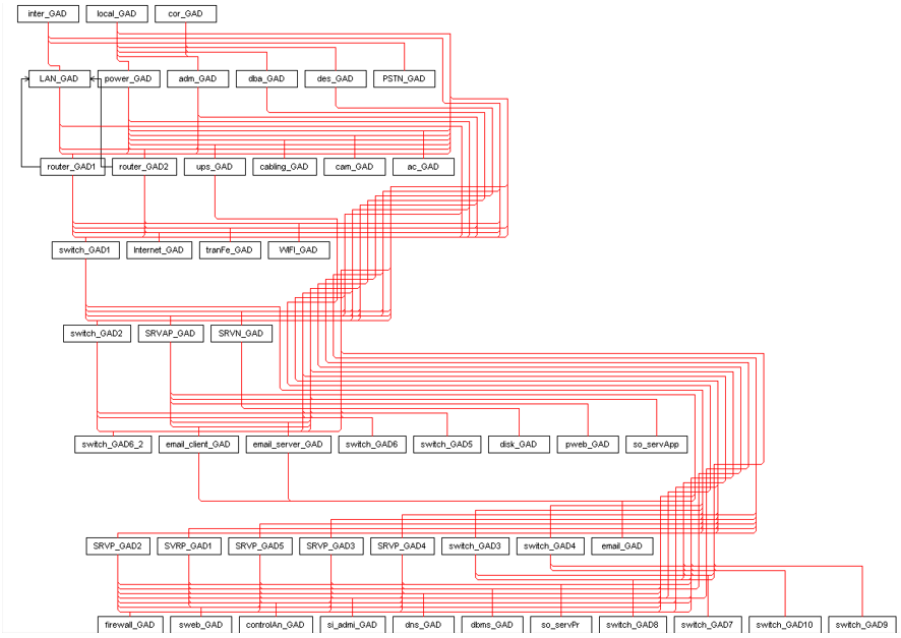


Figura 11: Dependencia de Activos PILAR

3.2.2.1.3. Clasificación de Activos

La clasificación de activos implica identificar y categorizar cada activo dentro de un tipo específico; un activo puede encajar en varias categorías. En la tabla adjunta (Tabla 6), se presenta la clasificación de los mismos conforme a los distintos tipos descritos en el libro 2 "Catálogo de Elementos" de Magerit. Los códigos mostrados en la columna "Tipo de Activo" siguen la jerarquía sugerida por la metodología. En la siguiente figura (Figura 12), se puede observar un ejemplo de la clasificación de un activo y su jerarquía en la herramienta PILAR.

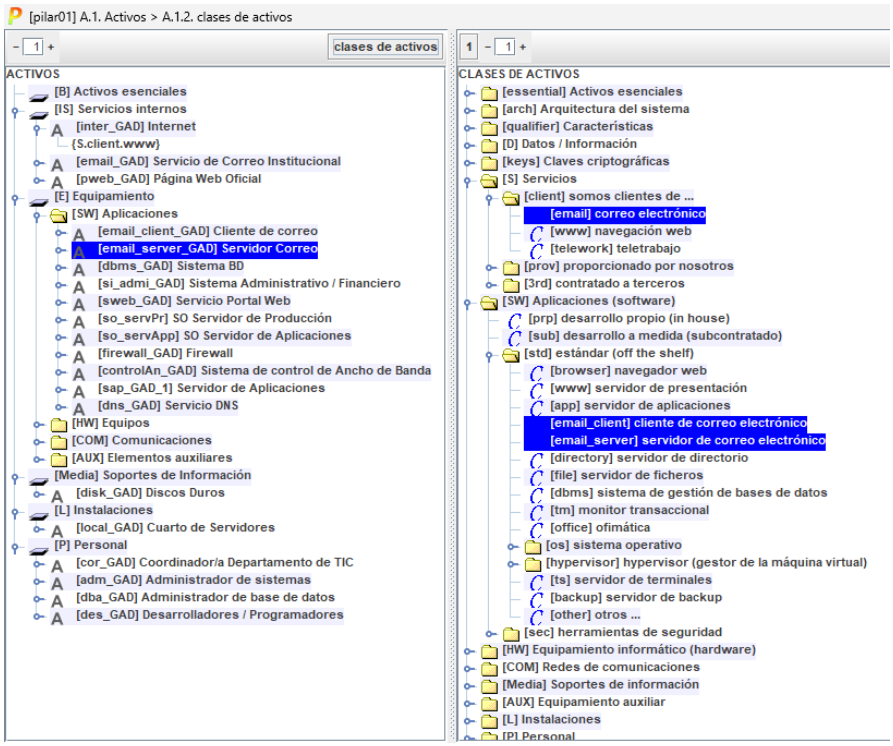


Figura 12: Clasificación de Activos PILAR

En la siguiente tabla, se observa la clasificación de los activos que se identificaron y se están considerando para el proceso de gestión de riesgos de este proyecto. Los recursos deben clasificarse de manera correcta con el objetivo de influir en los demás puntos del análisis, ya que a partir de esta se asignarán las amenazas y salvaguardas.

Nombre y código	Tipo de Activo
Internet [inter_GAD]	[S] [client] [www] navegación web [S] [prov] [www] world wide web
Página Web Oficial [pweb_GAD]	[S] [prov] [ext] usuarios externos [S] [prov] [int] usuarios externos [S] [prov] [www] word wide web
Servicio de correo Institucional [email_GAD]	[D] [conf] datos de configuración [D] [password] credenciales [S] [prov] [email] correo electrónico
Servidor Correo [email_server_GAD] Cliente de correo [email_client_GAD]	[S] [client] [email] correo electrónico [SW] [std] [email_client] cliente de correo electrónico [SW] [std] [email_server] servidor de correo electrónico
Sistema Base de datos [dbms_GAD]	[D] [files] fichero de datos [D] [backup] copias de respaldo [D] [conf] datos de configuración [D] [password] credenciales [D] [auth] datos de validación de credenciales [D] [log] registro de actividad [SW] [std][dbms] sistema de gestión de base de datos
Sistema Administrativo / Financiero [si_admi_GAD]	[D] [files] fichero de datos [D] [backup] copias de respaldo [D] [conf] datos de configuración [D] [password] credenciales [D] [auth] datos de validación de credenciales [S] [int] usuarios internos [SW] [sub] desarrollo a medias (subcontratado)
Servicio Portal Web [sweb_GAD]	[SW] [std] [www] servidor de presentación
SO Servidor de Producción	[SW] [std] [os] Linux

SO Servidor de Aplicaciones	[SW] [std] [os] Linux
Firewall [firewall_GAD]	[SW] [sec] [ids] IDS/IPS (detección/prevención de intrusos) [SW] [sec] [traf] análisis de trafico
Sistema de control de Ancho de Banda [controlAn_GAD]	[SW] [sec] [traf] análisis de tráfico
Servidor de Producción - HP ProLiant DL560 [sp_GAD]	[D] [conf] datos de configuración [D] [log] registro de actividad [SW] [os] [linux] linux [HW] [host] grandes equipos [HW] [backup] equipamiento de respaldo [HW] [data] que almacena datos
Servidor de Aplicaciones [sap_GAD]	[D] [conf] datos de configuración [D] [log] registros de actividad [S] [prov] [int] usuarios internos [SW] [stp] [app] servidor de aplicaciones [SW] [std] [dbms] sistema de gestión de base de datos [SW] [os] [linux] linux [HW] [host] grandes equipos [HW] [data] que almacena datos
ServProduccion1 [sp_GAD1]	[HW] [host] grandes equipos [HW] [vhost] equipos virtuales [HW] [backup] equipo de respaldo [HW] [data] que almacena datos
ServProduccion2 [sp_GAD2]	[HW] [host] grandes equipos [HW] [vhost] equipos virtuales [HW] [backup] equipo de respaldo [HW] [data] que almacena datos
ServProduccion3 [sp_GAD3]	[HW] [host] grandes equipos [HW] [vhost] equipos virtuales [HW] [backup] equipo de respaldo [HW] [data] que almacena datos

ServProduccion4 [sp_GAD4]	[HW] [host] grandes equipos [HW] [vhost] equipos virtuales [HW] [backup] equipo de respaldo [HW] [data] que almacena datos
ServProduccion5 [sp_GAD5]	[HW] [host] grandes equipos [HW] [vhost] equipos virtuales [HW] [backup] equipo de respaldo [HW] [data] que almacena datos
Transceiver [tranFE_GAD]	[HW] [network] [bridge] puente
Servidor NAS – IBM System x3650 [snas_GAD]	[HW] [host] grandes equipos [HW] [backup] equipo de respaldo [HW] [data] que almacena datos [Media] [electronic] [san] almacenamiento en red
Router 1 [router_GAD1]	[HW] [network] [router] encaminador
Router 2 [router_GAD2]	[HW] [network] [router] encaminador
Master Switch 1 Core [switch_GAD1]	[HW] [network] [switch] conmutador
Switch 2 – PB [switch_GAD2]	[HW] [network] [switch] conmutador
Switch 3 – P1 [switch_GAD3]	[HW] [network] [switch] conmutador
Switch 4 – P2 [switch_GAD4]	[HW] [network] [switch] conmutador
Switch 5 [switch_GAD5]	[HW] [network] [switch] conmutador
Switch 6 [switch_GAD6]	[HW] [network] [switch] conmutador
Transceiver [tranFE_GAD]	[HW] [network] [bridge] puente
Red Local [LAN_GAD]	[D] [conf] datos de configuración [HW] [COM] [LAN] red local
Red inalámbrica [WIFI_GAD]	[HW] [COM] [WIFI] wifi
Telefonía IP [PSTN_GAD]	[HW] [COM] [PSTN] red telefónica

Fuente de alimentación [power_GAD]	[HW] [other] otros [AUX] [power] fuente de alimentación [AUX] [supply] suministros esenciales
Sistema de alimentación Ininterrumpida [ups_GAD]	[HW] [other] otros [AUX] [ups] sistema de alimentación ininterrumpida
Cableado Estructurado [cabling_GAD]	[AUX] [cabling] cableado de datos [AUX] [cabling] [wire] cable eléctrico [AUX] [cabling] [fiber] fibra óptica
Equipo de Climatización [ac_GAD]	[AUX] [ac] equipos de climatización
Cámaras de seguridad [cam_GAD]	[HW] [data] que almacena datos [AUX] [other] otros
Discos Duros [disk_GAD]	[D] [backup] copias de respaldo [D] [conf] datos de configuración [Media] [electronic]][disk] discos
Administrador de sistemas [adm_GAD]	[P] [adm] administrador de sistemas
Administrador de base de datos [dba_GAD]	[P] [dba] administrador BBDD
Desarrolladores [des_GAD]	[P] [dev] desarrolladores / programadores

Tabla 5. Caracterización de Activos

3.2.2.1.4. Valoración de Activos

La metodología Magerit propone una escala estándar de diez valores para la evaluación, reservando el cero como valor mínimo (depreciable), lo que significa que su pérdida o daño carece de importancia y no afecta el funcionamiento del Data Center. Por otro lado, un valor de diez representa el máximo (extremo), indicando que la pérdida o daño de dicho activo tendría consecuencias graves para el centro de cómputo. La siguiente figura (Figura 13) ilustra esta escala de valores.

valor		*criterio*
10	extremo	daño extremadamente grave
9	muy alto	daño muy grave
6-8	alto	daño grave
3-5	medio	daño importante
1-2	bajo	daño menor
0	despreciable	irrelevante a efectos prácticos

Figura 13: Criterios de valoración de Activos

Para la correcta valoración de los activos, se evaluarán las cuatro dimensiones de la seguridad que se han establecido: Disponibilidad (D), Integridad (I), Confidencialidad (C) y Autenticidad (A). Cada dimensión se aborda mediante preguntas específicas que requieren respuestas dentro de un rango de valores predefinido por la metodología. Para la disponibilidad, se necesita responder a la pregunta ¿Qué importancia tendría que el activo no estuviera disponible? Para la integridad, se contesta a ¿Qué importancia tendría que los datos fueran modificados fuera de control? Para la confidencialidad, la pregunta es ¿Qué importancia tendría que el dato fuera conocido por personas no autorizadas? Y finalmente para la dimensión de autenticidad, se da respuesta a ¿Qué importancia tendría que quien accede al servicio no sea realmente quien se cree?

En las figuras desde la 14 hasta la 19 se observa la valoración de los activos en sus categorías correspondiente.

ACTIVOS				
[B] Activos esenciales				
[IS] Servicios internos				
[inter_GAD] Internet	[7]	[7]	[5]	[2]
[email_GAD] Servicio de Correo Institucional	[8]	[7]	[6]	[6]
[pweb_GAD] Página Web Oficial	[7]	[8]		[6]

Figura 14: Valoración de activos de servicios internos

activo	[D]	[I]	[C]	[A]
ACTIVOS				
[B] Activos esenciales				
[IS] Servicios internos				
[E] Equipamiento				
[SW] Aplicaciones				
[email_client_GAD] Cliente de correo	[8]	[8]	[9]	[7]
[email_server_GAD] Servidor Correo	[8]	[8]	[8]	[8]
[dbms_GAD] Sistema BD	[8]	[7]	[7]	[8]
[si_admi_GAD] Sistema Administrativo / Financie	[7]	[7]	[7]	[8]
[sweb_GAD] Servicio Portal Web	[8]	[7]	[6]	[6]
[so_servPr] SO Servidor de Producción	[8]			[5]
[so_servApp] SO Servidor de Aplicaciones	[8]			[5]
[firewall_GAD] Firewall	[9]			
[controlAn_GAD] Sistema de control de Ancho de	[5]	[2]	[3]	[3]
[sap_GAD_1] Servidor de Aplicaciones	[7]	[6]	[7]	[7]
[dns_GAD] Servicio DNS	[7]	[7]	[7]	[7]
[HW] Equipos				
[COM] Comunicaciones				

Figura 15: Valoración de activos de aplicaciones (SW)

[HW] Equipos				
[SVRP_GAD1] ServProducción1	[8]	[8]	[7]	[7]
[SRVP_GAD2] ServProducción2	[8]	[8]	[7]	[7]
[SRVP_GAD3] ServProducción3	[8]	[8]	[7]	[7]
[SRVP_GAD4] ServProducción4	[8]	[8]	[7]	[7]
[SRVP_GAD5] ServProducción5	[8]	[8]	[7]	[7]
[SRVAP_GAD] Servidor de Aplicaciones	[8]	[7]	[7]	[7]
[SRVN_GAD] Servidor NAS	[7]	[8]	[8]	[8]
[router_GAD1] Router1	[8]	[7]	[8]	[7]
[router_GAD2] Router2	[8]	[7]	[8]	[7]
[switch_GAD1] Master Switch1 CORE	[8]	[6]	[6]	[7]
[switch_GAD2] Switch2 - PB	[8]	[5]	[6]	[7]
[switch_GAD3] Switch3 - P1	[8]	[5]	[6]	[7]
[switch_GAD4] Switch4 - P2	[8]	[5]	[6]	[7]
[switch_GAD5] Switch5 - PB1	[8]	[5]	[6]	[7]
[switch_GAD6] Switch6 - PB	[8]	[5]	[6]	[7]
[switch_GAD7] Switch7 - P1	[8]	[5]	[6]	[7]
[switch_GAD8] Switch8 - P1	[8]	[5]	[6]	[7]
[switch_GAD9] Switch9 - P2	[8]	[5]	[6]	[7]
[switch_GAD10] Switch10 - P2	[8]	[5]	[6]	[7]
[tranFe_GAD] Transceiver	[8]	[5]	[5]	[5]

Figura 16: Valoración de activos de equipos (HW)

activo	[D]	[I]	[C]	[A]
ACTIVOS				
[B] Activos esenciales				
[IS] Servicios internos				
[E] Equipamiento				
[SW] Aplicaciones				
[HW] Equipos				
[COM] Comunicaciones				
[Internet_GAD] Internet	[8]	[7]	[5]	[3]
[LAN_GAD] Red Local	[8]	[7]	[8]	[3]
[WIFI_GAD] Red Inalámbrica	[7]	[7]	[7]	[3]
[PSTN_GAD] Telefonia IP	[7]	[7]	[7]	[2]

Figura 17: Valoración de activos de Comunicaciones

activo	[D]	[I]	[C]	[A]
ACTIVOS				
[B] Activos esenciales				
[IS] Servicios internos				
[E] Equipamiento				
[SW] Aplicaciones				
[HW] Equipos				
[COM] Comunicaciones				
[AUX] Elementos auxiliares				
[power_GAD] Fuente de Alimentación	[7]			
[ups_GAD] Sistema de alimentación ininter	[8]			
[cabling_GAD] Cableado Estructurado	[7]			
[ac_GAD] Equipos de Climatización	[7]			
[cam_GAD] Cámaras de Seguridad	[7]	[4]	[4]	[3]

Figura 18: Valoración de activos Elementos Auxiliares

activo	[D]	[I]	[C]	[A]
ACTIVOS				
[B] Activos esenciales				
[IS] Servicios internos				
[E] Equipamiento				
[Media] Soportes de Información				
[disk_GAD] Discos Duros	[6]	[7]	[7]	[5]
[L] Instalaciones				
[local_GAD] Cuarto de Servidores	[8]	[8]	[7]	[8]
[P] Personal				
[cor_GAD] Coordinador/a Departamento de TIC	[7]		[4]	
[adm_GAD] Administrador de sistemas	[8]		[8]	
[dba_GAD] Administrador de base de datos	[7]		[5]	
[des_GAD] Desarrolladores / Programadores	[7]		[5]	

Figura 19: Valoración de Activos - Media - Instalaciones - Personal

3.2.2.2. Caracterización de amenazas

Se prosigue con la siguiente fase, la cual tiene como propósito identificar, analizar y comprender las amenazas que podrían afectar a cada tipo de activo dentro del objeto de estudio. Esta fase permite comprender de mejor manera los riesgos a los que se enfrenta el Data Center de la entidad, facilitando la futura determinación de salvaguardas.

3.2.2.2.1. Identificación de amenazas

Para la actividad de identificar las amenazas, estas se determinan por cada categoría o tipo de activo en los que se ha clasificado en la fase anterior. A través de la herramienta PILAR se ha realizado la selección de las amenazas, dado que cada una está asociada a un tipo de activo en particular, por lo que para la selección se está utilizando la información proporcionada por la misma herramienta, es decir, se utiliza la biblioteca de amenazas que viene incluida con el software de apoyo (PILAR), las amenazas están clasificadas en grupos:

- [N] Desastres Naturales
- [I] De origen industrial
- [E] Errores y fallos no intencionados
- [A] Ataques Deliberados

En la siguiente figura (Figura 20), se puede observar el listado de amenazas que la herramienta proporciona para el activo Página Web Oficial con código [pweb_GAD] que se está clasificado dentro de Servicios Internos, en este caso primero se realizó la asignación automática y luego se realiza de manera manual.

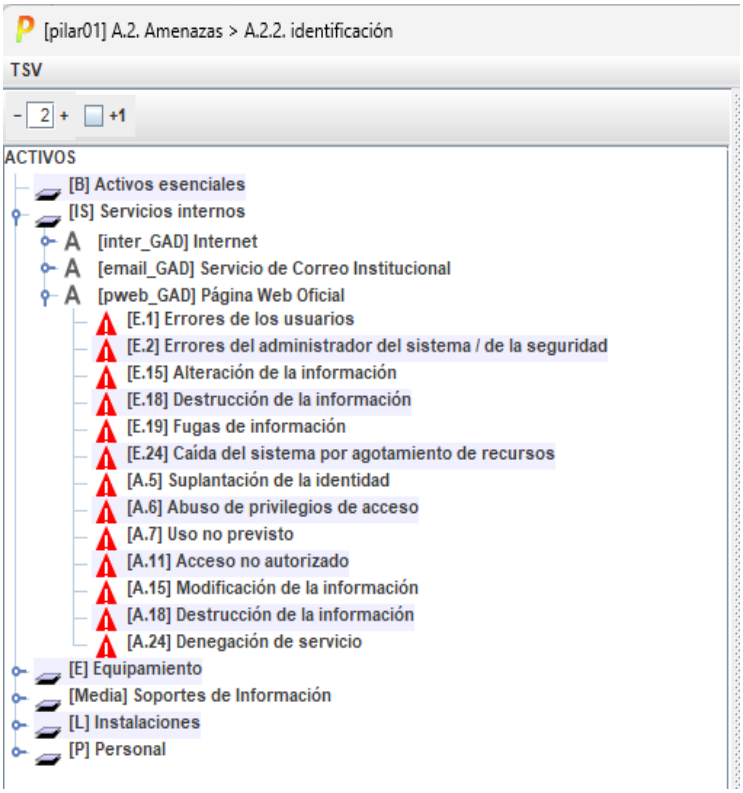


Figura 20: Identificación de amenazas PILAR (pweb_GAD)

3.2.2.2.2. Valoración de amenazas

La valoración de las amenazas se realizó determinando la degradación por porcentajes (cuán perjudicado resultaría el valor del activo) y la probabilidad o frecuencia (cuán probable es que se materialice la amenaza) con respecto a las dimensiones establecidas que se están evaluando. Determinar el grado de degradación y la probabilidad o frecuencia de ocurrencia de cada riesgo o amenaza sobre cada tipo de activo tiene como propósito conocer el impacto y riego potencial

que posee cada una sobre cada activo identificado. En la Tabla 6 y 7 se establecen los valores de evaluación.

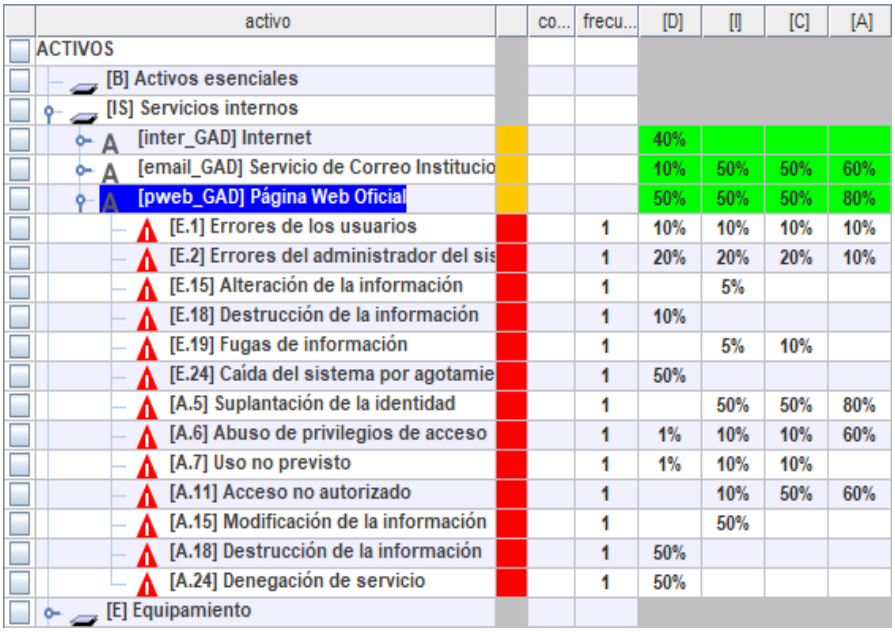
Detalle		
T	Total	96% - 100%
MA	Muy Alta	66 % – 95%
A	Alta	26% – 65%
M	Media	6% – 25%
B	Baja	0% – 5%

Tabla 6. Degradación del valor

			Detalle
MA	100	A Diario	Casi seguro
A	10	Mensualmente	Muy Alto
M	1	Una vez al año	Posible
B	1/10	Cada varios años	Poco Probable
MB	1/100	Siglos	Muy Raro

Tabla 7. Probabilidad de ocurrencia

Los resultados de la valoración se presentan en el anexo correspondiente (Anexo 11), detallando el grado de degradación y la probabilidad de ocurrencia. En la siguiente figura (Figura 21), se observan los valores de las amenazas, tomando como ejemplo el activo de servicios internos, Página Web Oficial con código [pweb_GAD].



activo		co...	frecu...	[D]	[I]	[C]	[A]
ACTIVOS							
[B] Activos esenciales							
[IS] Servicios internos							
[inter_GAD] Internet				40%			
[email_GAD] Servicio de Correo Institucio				10%	50%	50%	60%
[pweb_GAD] Página Web Oficial				50%	50%	50%	80%
[E.1] Errores de los usuarios			1	10%	10%	10%	10%
[E.2] Errores del administrador del sis			1	20%	20%	20%	10%
[E.15] Alteración de la información			1		5%		
[E.18] Destrucción de la información			1	10%			
[E.19] Fugas de información			1		5%	10%	
[E.24] Caída del sistema por agotamie			1	50%			
[A.5] Suplantación de la identidad			1		50%	50%	80%
[A.6] Abuso de privilegios de acceso			1	1%	10%	10%	60%
[A.7] Uso no previsto			1	1%	10%	10%	
[A.11] Acceso no autorizado			1		10%	50%	60%
[A.15] Modificación de la información			1		50%		
[A.18] Destrucción de la información			1	50%			
[A.24] Denegación de servicio			1	50%			
[E] Equipamiento							

Figura 21: Valoración de amenazas

3.2.2.2.3. Identificación de los riesgos

Una vez realizado el proceso inicial de identificación de amenazas, se procede a reconocer los posibles riesgos existentes asociados a estas mismas. Este paso se llevó a cabo mediante entrevistas al personal que interactúa de forma directa y que se encarga del Data Center Gubernamental. Estas entrevistas ofrecieron una oportunidad para explorar a fondo las posibles vulnerabilidades o deficiencias en la infraestructura y los sistemas, basándose en la información recopilada previamente mediante el método de observación. De esta manera, se estableció un panorama claro y detallado de los riesgos potenciales que podrían afectar la operatividad y seguridad del data center, los cuales pueden observarse en la siguiente tabla.

N°	**Riesgo (Amenaza)**
Sección: Riesgos de Seguridad física	
1	Intrusión no autorizada en las instalaciones.
2	Fallos en los sistemas de seguridad (cámaras, alarmas, controles de acceso).
3	Robo de equipos y hardware.

4	Acceso no autorizado a áreas restringidas (Fallo en la seguridad de las cerraduras y sistemas de acceso.).
5	Pérdida de datos físicos (documentos impresos, discos duros).
6	Fallos en los sistemas de detección de intrusos.
7	Deficiencias en la protección perimetral del Data Center.
8	Fallos en los sistemas de vigilancia y monitorización.
9	Vandalismo.
10	Uso no Previsto.
Sección: Riesgos de Seguridad Lógica	
11	Malware y virus informáticos.
12	Phishing y ataques de ingeniería social.
13	Fuga de información confidencial.
14	Acceso no autorizado a sistemas y bases de datos.
15	Ataques de denegación de servicio (DDoS).
16	Fallos en los sistemas de autenticación y autorización.
17	Ataques de ransomware.
18	Interrupciones en los sistemas de almacenamiento.
19	Ataques de inyección de código SQL.
20	Configuraciones incorrectas de firewalls y reglas de seguridad.
21	Desbordamiento de búfer en aplicaciones.
22	Fallos en la gestión de privilegios de usuarios.
Sección: Riesgos de Infraestructura	
23	Fuego (Fallos en los sistemas de detección y extinción de incendios).
24	Daños por Agua (Inundación o filtración de agua).

25	Pérdida de energía eléctrica.
26	Sobrecargas eléctricas y cortes de energía.
27	Fallos en la transmisión de datos.
28	Fallos en el suministro de energía de respaldo (UPS, generadores).
29	Problemas de refrigeración y sobrecalentamiento de equipos.
30	Caída del sistema por agotamiento de recursos.
31	Fallos en la conectividad de red.
32	Pérdida de conectividad de Internet.
33	Problemas de cableado estructurado.
34	Fallo en los sistemas de almacenamiento y respaldo de datos.
35	Fallo de los servidores (Físicos y Virtualizados).
36	Fallos en los dispositivos de red (routers, switches, etc.).
37	Errores en la configuración de redes.
38	Errores de configuración de los servidores
39	Manipulación inadecuada del hardware.
40	Errores de mantenimiento y actualización.
Sección: Riesgos de Gestión de Datos	
41	Pérdida de datos debido a fallos en los sistemas de almacenamiento.
42	Corrupción de datos e información.
43	Alteración de datos e información.
44	Acceso no autorizado a datos sensibles.
45	Fallos en los procesos de respaldo y recuperación de datos.
46	Pérdida de integridad de los datos debido a errores en la entrada o procesamiento.

47	Pérdida de datos debido a errores humanos.
48	Fugas de información.
49	Manipulación de los registros logs.
Sección: Riesgos de Operación (Gestión de Personal)	
50	Indisponibilidad. cambiar
51	Asignación inadecuada de roles y responsabilidades.
52	Phishing y ataques de ingeniería social.
53	Falta de conciencia sobre seguridad informática.
54	Acceso no autorizado a sistemas y datos.

Tabla 8. Posibles riesgos existentes

3.2.2.3. Caracterización de Salvaguardas

A partir de las amenazas y riegos identificados, se determinan las salvaguardas pertinentes o controles. Esta fase permite comprender lo que se necesita para la protección de los activos críticos del Data Center, las salvaguardas se centran en la reducción de la probabilidad y del impacto. Durante el desarrollo, se emplea el catálogo de salvaguardas que proporciona la metodología MAGERIT en el libro 2 y se los toma como salvaguardas propias basadas en la ISO 27001/2013.

Para el correcto entendimiento de la fase se toman en cuenta las siguientes tablas:

Abreviaturas	**Aspecto (asp)**
G	Para Gestión
T	Para Técnico
F	Para Seguridad Física
P	Para Gestión de persona

Tabla 9. Aspectos de Salvaguardas

Abreviaturas	Tipo de protección (tdp)
PR	Preventivo
IM	Minimización
EL	Eliminatorios
DC	Detección
AC	Aceptación
CR	Correctivos
AW	De concienciación

Tabla 10. Tipos de Salvaguardas

Factor	Nivel	Significado / Madurez	Significado/ Estado
0%	L0	Inexistente	Inexistente
10%	L1	Inicial / ad hoc	Iniciado
50%	L2	Reproducible pero intuitivo	Parcialmente realizado
80%	L3	Proceso definido	En funcionamiento
90%	L4	Gestionado y medible	Monitorizado
100%	L5	Optimizado	Mejor Continua

Tabla 11. Eficacia, Madurez y Estado de las salvaguardas

Valor (recom)	Significado
8	Ser tratadas de manera inmediata (máxima prioridad)
6 – 7	Ser tratadas de manera inmediata
4 – 5	Ser tratadas a mediano plazo (nivel de criticidad medio)
2 - 3	Ser tratadas a mediano plazo (nivel de criticidad bajo)

Tabla 12. Valor de la salvaguarda

3.2.2.3.1. Identificación de salvaguardas

Una vez realizada la caracterización de amenazas o riesgos, se procede a identificar las salvaguardas que en una fase posterior serán parte del plan de tratamiento de riesgos. A partir del catálogo de salvaguardas que posee la herramienta PILAR, se

eligieron los controles que más se adapten a la entidad de estudio. A continuación, se enlistan las salvaguardas elegidas para el desarrollo del proyecto.

- **Protecciones Generales**
    - Control de acceso lógico
    - Gestión de privilegios
    - Acceso Remoto
    - Monitorización y mantenimiento remoto
    - Segregación de tareas
    - Gestión de incidencias
    - Herramienta de monitorización de trafico
- **Identificación y autenticación**
    - Identificación de usuarios.
    - Gestión de identificación de usuarios
    - Cuentas especiales administración
    - Biometría
- **Protección de la información**
    - Aseguramiento de la integridad.
    - Protección de la confidencialidad
    - Cifrado de Información
    - Copia de seguridad de datos.
- **Protección de los servicios**
    - Aseguramiento de la disponibilidad.
    - Aceptación y puesta en operación.
    - Se aplican perfiles de seguridad
    - Operación
    - Gestión de cambios (mejoras y sustituciones).
    - Actualizaciones y Parches.
    - Protección de servicios y aplicaciones web.
    - Protección del correo electrónico.
    - Protección del servicio de nombres de dominio
    - Voz sobre IP
- **Protección de las aplicaciones**

    - Copias de Seguridad.
    - Se aplican perfiles de seguridad.
    - Operación/Producción
    - Cambios (Actualización y mantenimiento).
- **Protección de los equipos**
    - Se aplican perfiles de seguridad.
    - Aseguramiento de la disponibilidad.
    - Correcta Instalación
    - Operación
    - Cambios (Actualización y mantenimiento).
    - Protección de los dispositivos de red
    - Máquinas Virtuales
- **Protección de las comunicaciones**
    - Aseguramiento de disponibilidad.
    - Autenticación del canal
    - Protección de la integridad de los datos intercambiados.
    - Control de acceso a la red
    - Cambios (Actualizaciones y mantenimiento)
    - Operación
    - Internet.
    - Seguridad Wireless (WiFi).
    - Segregación de red en dominios
- **Protección de los soportes de información**
    - Aseguramiento de disponibilidad.
    - Limpieza de contenidos.
    - Destrucción de soportes.
- **Protección de los elementos auxiliares**
    - Aseguramiento de disponibilidad.
    - Correcta instalación.
    - Suministro eléctrico.
    - Climatización.
    - Protección de cableado.

- **Protección de las instalaciones**
    - Control de acceso físico.
    - Aseguramiento de disponibilidad de recursos.
- **Salvaguardas de gestión de personal**
    - Formación y concienciación.
    - Aseguramiento de la disponibilidad
- **Herramientas de seguridad**
    - Herramienta contra código dañino
    - IDP/IPS: Herramienta de detección/prevención de intrusos
    - Monitorización de la integridad de los ficheros
    - Herramienta de monitorización de tráfico

3.2.2.3.2. Valoración de salvaguardas

De la misma manera, se realiza la valoración de salvaguardas priorizando los valores propuestos (Tabla. 12), que establecen su importancia y la prioridad de tratamiento. También se evalúa la eficacia de los controles elegidos, determinando el valor de la situación actual (current) y objetivo (target), utilizando los valores de la tabla de eficacia de salvaguardada (Tabla 11).

A continuación, en la siguiente figura se observa el proceso realizado en la herramienta PILAR, como ejemplo el grupo de salvaguardas de [IA] identificación y autenticación.

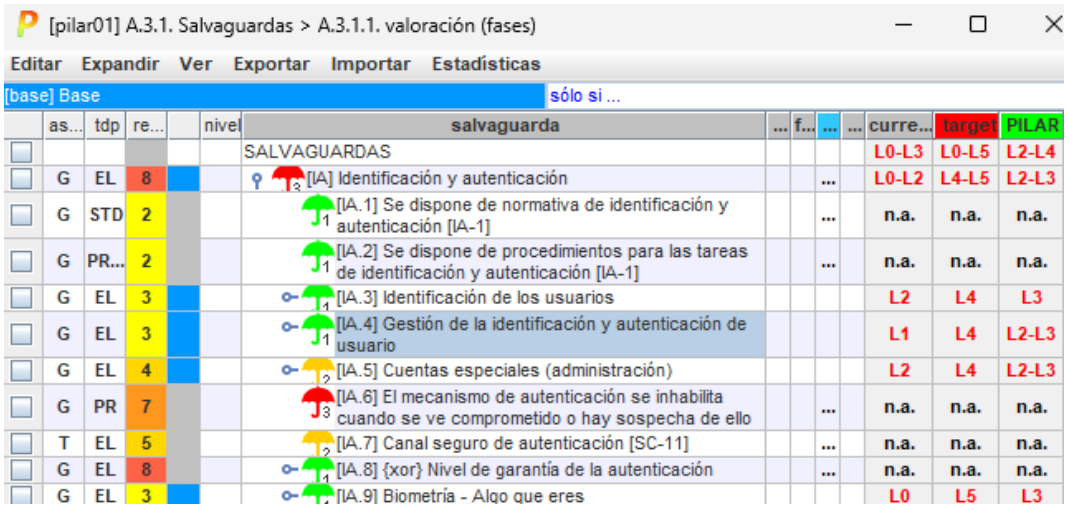


Figura 22: Valorización y Eficacia de las salvaguardas

Desde la Tabla 14 hasta la 23, se presentan los grupos de salvaguardas una vez realizado el proceso de valoración.

asp	tdp	reco	Salvaguarda	curr	targ	PILAR
G	PR	5	[H] Protección Generales	L1	L5	L2 – L3
G	PR – IM	5	[H.AC] Control de acceso lógico	L1	L4	L2 – L3
T	PR	3	[AC.1] Gestión de Privilegios	L2	L4	L2 – L3
T	IM	4	[AC.5] Acceso remoto	L2	L4	L2 – L3
T	PR	3	[AC.6] Monitorización y mantenimiento remoto	L1	L4	L2 – L3
G	PR	3	[H.ST] Segregación de tareas	L1	L4	L2 – L3
G	PR - CR	5	[H.IR] Gestión de incidencias	L1	L5	L2 – L3
G	PR - DC	4	[S.www] Herramienta de monitorización de trafico	L0	L4	L2 – L3

Tabla 13. Valorización salvaguardas - Protección Generales

asp	tdp	reco	Salvaguarda	curr	targ	PILAR
G	PR	7	[D] Protección de la información	L1 – L2	L4 – L5	L2 – L4
G	PR	4	[D.I] Aseguramiento de la integridad	L1	L4	L3
G	PR	4	[D.5] Protección de la confidencialidad	L2	L5	L2 – L3
G	PR	4	[D.C] Cifrado de información	L1	L2	L2 – L3
G	PR - RC	7	[D.backup] Copia de seguridad de datos	L2	L4	L2 – L4

Tabla 14. Valorización salvaguardas - Protección de la información

asp	tdp	reco	Salvaguarda	curr	targ	PILAR
G	PR	5	[S] Protección de los servicios	L1	L5	L2 – L3
G	PR - DC	2	[S.A] Aseguramiento de la disponibilidad	L1	L4	L2 – L3
G	PR	3	[S.start] Aceptación y puesta en operación	L1	L4	L2 – L3
T	PR	5	[S.SC] Se aplican perfiles de seguridad	L2	L4	L3
G	PR	4	[S.op] Operación	L0	L4	L2 – L3

G	CR	3	[S.CM] Gestión de cambios	L1	L5	L2 – L3
G	PR – IM	4	[S.www] Protección de servicios y aplicaciones web	L1	L4	L2 – L3
G	PR - IM	3	[S.email] Protección del correo electrónico	L1	L4	L2 – L3
T	PR	3	[S.dns] Protección del servicio de nombres de dominio	L2	L5	L2 – L3
T	PR	3	[S.voip] Voz sobre IP	L3	L5	L2 – L3

Tabla 15. Valorización salvaguardas - Protección de los servicios

asp	tdp	reco	Salvaguarda	curr	targ	PILAR
G	PR	5	[SW] Protección de las aplicaciones informáticas	L0-L2	L4	L2 – L3
G	PR	4	[SW.backup] Copias de Seguridad	L2	L4	L2 – L3
T	PR - IM	5	[SW.SC] Se aplican perfiles de seguridad	L2	L4	L3
G	PR	4	[SW.op] Operación/Producción	L2	L4	L2 – L3
G	CR	3	[SW.CM] Cambios (Actualización y mantenimiento)	L0	L4	L2 – L3

Tabla 16. Valorización salvaguardas - Protección de las aplicaciones

asp	tdp	reco	Salvaguarda	curr	targ	PILAR
G	PR	5	[HW] Protección de los equipos informáticos	L0	L3 – L4	L2 – L3
T	PR	4	[HW.SC] Se aplican perfiles de seguridad	L1	L3	L3
T	IM	4	[HW.cont] Aseguramiento de la disponibilidad	L0	L4	L3
G	PR	5	[HW.7] Correcta Instalación	L2	L4	L3
G	PR	3	[HW.op] Operación – Manual del correcto uso	L0	L3	L2 – L3
G	CR	3	[HW.CM] Gestión de cambios	L0	L4	L2
G	PR	4	[HW.12] Protección de los dispositivos de red	L2	L4	L3
G	PR	4	[HW.14] Máquinas virtuales	L2	L5	L2 – L3
G	PR	3	[HW.pabx] Protección de la centralita telefónica (PABX)	L1	L3	L3

Tabla 17. Valorización salvaguardas - Protección de los equipos

asp	tdp	reco	Salvaguarda	curr	targ	PILAR
G	PR	8	[COM] Protección de las comunicaciones	L0 – L1	L3 – L4	L2 – L4
T	PR	8	[COM.SC] Se aplican perfiles de seguridad	L2	L5	L3 – L5
G	PR	5	[COM.cont] Aseguramiento de disponibilidad	L0	L4	L2 – L3
T	PR	4	[COM.aut] Autenticación del canal	L2	L4	L3
T	PR	4	[COM.I] Protección de la integridad de los datos intercambiados	L1	L3	L2 – L3
T	PR	4	[COM.13] Control de Acceso a la red	L2	L5	L2 – L4
G	PR	3	[COM.CM] Cambios (Actualizaciones y mantenimiento)	L1	L3	L2 – L3
T	CR	3	[COM.op] Operación – Manual del correcto uso	L0	L3	L3
G	IM	4	[COM.internet] Internet	L1	L3	L2 – L3
G	PR - IM	7	[COM.wifi] Seguridad Wireless (WiFi)	L1	L4	L2 – L4
T	PR	5	[COM.DS] Segregación de red en dominios	L3	L4	L2 – L3

Tabla 18. Valorización salvaguardas - Protección de las comunicaciones

asp	tdp	reco	Salvaguarda	curr	targ	PILAR
G	PR	5	[M - MP] Protección de los soportes de información	L0	L3 – L5	L2 – L3
G	IM	5	[M.cont] Aseguramiento de disponibilidad	L1	L4	L3
G	EL	4	[MP.clean] Limpieza de contenidos	L0	L3	L2 – L3
G	EL	4	[MP.end] Destrucción de soportes	L0	L4	L2- L3

Tabla 19. Valorización salvaguardas - Protección de Media

asp	tdp	reco	Salvaguarda	curr	targ	PILAR
G	PR	5	[AUX] Protección de elementos auxiliares	L0 – L3	L3 – L5	L2 – L3
G	IM	5	[AUX.cont] Aseguramiento de disponibilidad	L0	L3	L3
F	DC	4	[AUX.start] Correcta instalación	L2	L3	L3

F	PR	4	[AUX.power] Suministro eléctrico	L3	L5	L2 - L3
F	PR	4	[AUX.AC] Climatización	L3	L5	L2 – L3
F	PR	5	[AUX.wires] Protección de cableado	L3	L5	L2 – L3

Tabla 20. Valorización salvaguardas - Protección de elementos auxiliares

asp	tdp	reco	Salvaguarda	curr	targ	PILAR
F	PR	4	[L] Protección de las instalaciones	L1 – L2	L3	L2 – L3
F	CR	4	[L.5] Protección frente a desastres	L2	L5	L2 – L3
F	PR	4	[L.AC] Control de acceso físico	L0	L3	L2 – L3
F	PR	2	[L.A] Aseguramiento de disponibilidad de recursos	L1	L3	L2

Tabla 21. Valoración salvaguardas - Protección de las instalaciones

asp	tdp	reco	Salvaguarda	curr	targ	PILAR
P	PR	5	[P - PS] Gestión del Personal	L0 – L2	L0 – L5	L2 – L3
P	AW – CR	2	[P.AT] Formación y concienciación	L0	L5	L2
P	PR	3	[P.cont] Aseguramiento de la disponibilidad	L2	L3	L2 – L3

Tabla 22. Valoración salvaguardas - Gestión del personal

asp	tdp	reco	Salvaguarda	curr	targ	PILAR
T	PR	7	[tools] Herramientas de seguridad	L0 – L2	L0 – L5	L2 – L3
T	PR	7	[tools.AV] Herramienta contra código dañino	L1	L3	L2
T	DC - PR	5	[tools.IDS] Herramienta de detección/prevención de intrusos	L0	L5	L2
T	DC	5	[tools.FIM] Monitorización de la integridad de ficheros	L1	L3	L2 – L3
T	DC	4	[tools.traffic] Herramienta de monitorización de trafico	L3	L5	L2 – L3

Tabla 23. Valoración salvaguardas - Herramientas de seguridad

Una vez valoradas las salvaguardas PILAR pasa a aplicarlas con respecto al concepto de tratamiento de riesgos como se observa en la siguiente Figura

Figura 23: Aplicación de las salvaguardas

3.2.2.4. Estimación del Estado del Riesgo

Esta fase tiene como propósito evaluar la situación actual de las amenazas o riesgos identificados en el Data Center, se basa en la ponderación de la probabilidad de que ocurran las amenazas y la evaluación del impacto potencial en caso de materializarse, teniendo en cuenta la eficacia de las salvaguardas implementadas.

3.2.2.4.1. Estimación del impacto potencial

A continuación, se presentan los valores del impacto potencial de los activos identificados, teniendo como referencia la siguiente tabla de niveles (Tabla. 24).

Impacto		
Nivel	**Criterio**	**Siglas**
10	Extremadamente Alto	MA
9	Muy Alto	
8	Muy Alto (-)	
7	Alto	A
6	Alto (-)	
5	Medio (+)	M
4	Medio	
3	Medio (-)	
2	Bajo (+)	B
1	Bajo	
0	Despreciable	MB

Tabla 24. Niveles de impacto

A través de la siguiente formula se calcula el valor de impacto:

$$\text{Impacto} = \text{Valor del Activo} * \text{Degradacion del valor sobre el activo evaluado}$$

Al calcular el valor representativo del impacto, se genera una matriz (Tabla 25), que proporciona una representación visual y organizada de la magnitud del impacto que un riesgo podría tener en el Data Center. Para el cálculo del impacto se utilizó el valor del activo acumulado (Anexo 10).

Impacto		Degradación										
		Baja		Media		Alta			Muy Alta		Total	
		0%	10%	11%	25%	26%	50%	65%	66%	94%	95%	100%
Valor	10	0	1	2	3	4	5	6	7	8	9	10
	9	0	1	2	3	4	5	5	6	7	8	9
	8	0	1	2	2	3	4	4	6	6	7	8
	7	0	1	1	2	3	4	4	5	6	6	7
	6	0	1	1	2	2	3	4	4	5	5	6
	5	0	0	1	1	2	2	2	3	3	4	5
	3	0	0	1	1	1	2	2	2	2	3	3
	2	0	0	0	1	1	1	1	1	2	2	2
	1	0	0	0	0	0	1	1	1	1	1	1
	0	0	0	0	0	0	0	0	0	0	0	0

Tabla 25. Matriz de Impacto

A partir de la magnitud del impacto se llega a las siguientes conclusiones:

- Los activos que están sombreados de color rosa representan el nivel de impacto alto y muy alto en las dimensiones de disponibilidad e integridad, en el caso de que se llegue a concretar el impacto de sus amenazas, podrían afectar de manera directa al Data Center. Estos activos son los servidores, equipos de red (switch, router) y el centro de cómputo por las dependencias de todos los equipos y aplicaciones que existen dentro.
- Los activos sombreados de color amarillo representan un nivel alto, pero no tan alto como los de color rosa, este nivel de impacto sigue siendo susceptible a la materialización de las amenazas, afectando a las cuatro dimensiones de la seguridad de la información que se están evaluando. Los activos que están dentro de este nivel son los de Aplicaciones y Comunicaciones.
- Los activos sombreados de color celestes representan un nivel medio en el impacto de las amenazas en caso de que se materialicen, afectando a la

dimensión de integridad de los quipos de red y la disponibilidad en el personal.

Activo	D	I	C	A
[IS] Servicios Internos	7	8	8	9
[inter_GAD] Internet	6	4	2	
[email_GAD] Servicio de Correo Institucional	7	8	8	9
[pweb_GAD] Página Web Oficial	7	7	7	8
[SW] Aplicaciones	8	7	7	7
[email_client_GAD] Cliente de correo	7	6	7	
[email_GAD] Servidor de Correo	7	6	6	
[dbms_GAD] Sistema BD	8	7	7	7
[si_admi_GAD] Sistema Administrativo/ Financiero	7	7	7	7
[sweb_GAD] Servicio Portal Web	7	6	6	
[sp_servPr] SO Servidor de Producción	7		7	
[sp_servApp] SO Servidor de Aplicaciones	7		7	
[firewall_GAD] Firewall	8	6	6	
[dns_GAD] Servicio DNS	7	6	6	
[HW] Equipos	8	8	8	
[SRVP_GAD1] ServProduccion	8	8	8	
[SRVP_GAD2] ServProduccion 2	8	8	8	
[SRVP_GAD3] ServProduccion 3	8	8	8	
[SRVP_GAD4] ServProduccion 4	8	8	8	
[SRVP_GAD5] ServProduccion 5	8	8	8	
[SRVAP_GAD] Servidor de Aplicaciones	8	8	8	
[SRVN_GAD] Servidor NAS	8	7	8	
[router_GAD1] Router 1	8	5	7	
[router_GAD2] Router 2	8	5	7	
[switch_GAD1] Master Switch CORE	8	7	7	
[switch_GAD2] Switch 2 – PB	8	7	7	
[switch_GAD3] Switch 3 – P1	8	5	7	
[switch_GAD4] Switch 4 – P2	8	5	7	
[switch_GAD5] Switch 5 – PB1	8	5	7	
[switch_GAD6] Switch 6 – PB2	8	5	7	
[switch_GAD7] Switch 7 – P1	8	5	7	
[switch_GAD7] Switch 8 – P1	8	5	7	
[switch_GAD7] Switch 9 – P2	8	5	7	
[switch_GAD7] Switch 10– P2	8	5	7	
[transFe] Transceiver	8	7	7	
[COM] Comunicaciones	7	6	7	8
[Internet_GAD] Internet	7	6	7	7
[LAN_GAD] Red Local	7	6	7	8
[WIFI_GAD] Red Inalámbrica	7	6	7	7
[PSTN_GAD] Telefonía IP	6	5	6	
[AUX] Elementos Auxiliares	8	5	6	
[power_GAD] Fuente de Alimentación	8	5	6	

[ups_GAD] Sistema de alimentación ininterrumpida	8			
[cabling_GAD] Cableado Estructurado	8	5	6	
[ac_GAD] Equipos de Climatización	5			
[cam_GAD] Cámaras de Seguridad	8	5	6	
[Media] Media soporte de información	8	5	7	
[disk_GAD] Discos Duros	8	5	7	
[L] Instalaciones	8		6	
[local_GAD] Cuarto de Servidores	8		6	
[P] Personal	6		7	
[cor_GAD] Coordinador/a Departamento de TIC	4			
[adm_GAD] Administrador de sistemas	6	7	7	
[dba_GAD] Administrador de base de datos	6	7	6	
[des_GAD] Desarrolladores / Programadores	6	7	5	

Tabla 26. Impacto Potencial

3.2.2.4.2. Estimación del impacto 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 posible impacto que se denomina residual [10]. En esta fase se realiza el análisis de los valores de impacto teniendo en cuenta las salvaguardas identificadas en la fase anterior. En las siguientes figuras, con la ayuda de la herramienta PILAR, se observa cómo el valor disminuye una vez realizada la simulación de la implementación de las salvaguardas.

A través de la siguiente formula se calcula el valor de impacto:

$$\text{Impacto residual} = \text{Valor del Activo} * \text{Degradacion residual del valor del activo evaluado}$$

Activo	D	I	C	A
[IS] Servicios Internos	3	3	3	4
[inter_GAD] Internet	2	0	0	
[email_GAD] Servicio de Correo Institucional	1	3	3	4
[pweb_GAD] Página Web Oficial	3	2	2	3
[SW] Aplicaciones	3	2	3	3
[email_client_GAD] Cliente de correo	3	2	3	
[email_GAD] Servidor de Correo	3	2	2	
[dbms_GAD] Sistema BD	3	2	2	3
[si_admi_GAD] Sistema Administrativo/ Financiero	3	2	2	3
[sweb_GAD] Servicio Portal Web	3	2	2	
[sp_servPr] SO Servidor de Producción	3		3	

[sp_servApp] SO Servidor de Aplicaciones	3		3	
[firewall_GAD] Firewall	3	2	2	
[dns_GAD] Servicio DNS	2	2	2	
[HW] Equipos	4	4	4	0
[SRVP_GAD1] ServProduccion_1	4	4	4	
[SRVP_GAD2] ServProduccion 2	4	4	4	
[SRVP_GAD3] ServProduccion 3	4	4	4	
[SRVP_GAD4] ServProduccion 4	4	4	4	
[SRVP_GAD5] ServProduccion 5	4	4	4	
[SRVAP_GAD] Servidor de Aplicaciones	4	3	4	
[SRVN_GAD] Servidor NAS	3	1	4	
[router_GAD1] Router 1	4	1	4	
[router_GAD2] Router 2	4	1	3	
[switch_GAD1] Master Switch CORE	4	1	3	
[switch_GAD2] Switch 2 – PB	4	2	3	
[switch_GAD3] Switch 3 – P1	4	2	3	
[switch_GAD4] Switch 4 – P2	4	0	3	
[switch_GAD5] Switch 5 – PB1	4	0	3	
[switch_GAD6] Switch 6 – PB2	4	0	3	
[switch_GAD7] Switch 7 – P1	4	1	3	
[switch_GAD7] Switch 8 – P1	4	1	3	
[switch_GAD7] Switch 9 – P2	4	1	3	
[switch_GAD7] Switch 10– P2	4	1	3	
[transFe] Transceiver	4	2	3	
[COM] Comunicaciones	2	0	2	3
[Internet_GAD] Internet	2	0	2	2
[LAN_GAD] Red Local	2	0	2	3
[WIFI_GAD] Red Inalámbrica	2	0	2	2
[PSTN_GAD] Telefonía IP	1	0	0	
[AUX] Elementos Auxiliares	4	0	2	0
[power_GAD] Fuente de Alimentación	4			
[ups_GAD] Sistema de alimentación ininterrumpida	3			
[cabling_GAD] Cableado Estructurado	2	0	2	
[ac_GAD] Equipos de Climatización	1			
[cam_GAD] Cámaras de Seguridad	3	0	2	
[Media] Media soporte de información	2	1	2	
[disk_GAD] Discos Duros	2	1	2	
[L] Instalaciones	2	0	1	0
[local_GAD] Cuarto de Servidores	2		1	
[P] Personal	2	3	3	
[cor_GAD] Coordinador/a Departamento de TIC	2		0	
[adm_GAD] Administrador de sistemas	2	3	3	
[dba_GAD] Administrador de base de datos	2	3	2	
[des_GAD] Desarrolladores / Programadores	2	3	1	

Tabla 27. Impacto Residual

La comparación se visualiza en el anexo correspondiente (Anexo 12), que se hace con los valores de impacto existentes actuales y los valores luego de la implementación de salvaguardas, se concluye que luego de las salvaguardas que recomienda PILAR y que se seleccionó de manera manual del catálogo, el impacto en los activos disminuyo un 40% aproximadamente.

3.2.2.4.3. Estimación del riesgo potencial

Una vez se haya calculado el impacto, se determina el riesgo potencial, donde Magerit denomina riesgo a la medida del daño probable sobre un sistema, conociendo el impacto de las amenazas sobre los activos [10]. El riesgo potencial proporciona una medida clave al combinar la probabilidad de ocurrencia de las amenazas con su posible impacto.

Para determinar el riesgo se utiliza la siguiente formula:

$$\text{Riesgo} = \text{Probabilidad de Amenaza} * \text{Magnitud del Daño (Impacto)}$$

Riesgo	
Nivel	**Criterio**
6	Muy Critico
5	Critico
4	Muy Alto
3	Alto
2	Medio
1	Bajo
0	Despreciable

Tabla 28. Niveles de Criticidad

Al calcular el valor representativo del riesgo, se genera una matriz que proporcionará una visión clara de la probabilidad de un riesgo y su impacto potencial en el Data Center. A continuación, se presenta dicha matriz permitiendo una evaluación más precisa de la magnitud del riesgo.

Riesgo		Probabilidad					
		MB	B	M	A	MA	MA+
Impacto	Muy Alto	2	3	4	5	6	6
	Alto	2	3	4	4	5	6
	Medio	1	2	3	3	4	5
	Bajo	0	1	2	2	2	4
	Despreciable	0	0	1	1	2	3

Tabla 29. Matriz de riesgo.

La siguiente tabla (Tabla 30), demuestran el valor del riesgo calculado con ayuda de la herramienta PILAR, teniendo en cuenta los niveles de criticidad (Tabla 28), con lo que se determina el valor del riesgo a cada activo.

Activo	D	I	C	A
[IS] Servicios Internos	5,1	5,7	5,7	6,0
[inter_GAD] Internet	3,5	3,3	2,1	
[email_GAD] Servicio de Correo Institucional	4,4	5,7	5,7	5,0
[pweb_GAD] Página Web Oficial	5,1	5,1	5,1	5,5
[SW] Aplicaciones	5,7	5,3	5,3	5,3
[email_client_GAD] Cliente de correo	5,1	4,4	5,0	
[email_GAD] Servidor de Correo	5,1	4,4	4,4	
[dbms_GAD] Sistema BD	5,4	5,3	5,3	4,4
[si_admi_GAD] Sistema Administrativo/ Financiero	4,7	5,3	5,3	5,3
[sweb_GAD] Servicio Portal Web	5,1	4,4	4,4	
[sp_servPr] SO Servidor de Producción	5,1		5,1	
[sp_servApp] SO Servidor de Aplicaciones	5,1		5,1	
[firewall_GAD] Firewall	5,7	4,4	4,4	
[dns_GAD] Servicio DNS	5,1	4,4	4,4	
[HW] Equipos	5,7	5,7	5,7	
[SRVP_GAD1] ServProduccion	5,7	5,7	5,7	
[SRVP_GAD2] ServProduccion 2	5,7	5,7	5,7	
[SRVP_GAD3] ServProduccion 3	5,7	5,7	5,7	
[SRVP_GAD4] ServProduccion 4	5,7	5,7	5,7	
[SRVP_GAD5] ServProduccion 5	5,7	5,7	5,7	
[SRVAP_GAD] Servidor de Aplicaciones	5,7	5,7	5,7	
[SRVN_GAD] Servidor NAS	5,7	3,9	5,7	
[router_GAD1] Router 1	5,7	3,9	5,7	
[router_GAD2] Router 2	5,7	3,9	5,0	
[switch_GAD1] Master Switch CORE	5,7	3,9	5,0	
[switch_GAD2] Switch 2 – PB	5,7	5,0	5,0	

[switch_GAD3] Switch 3 – P1	5,7	5,0	5,0	
[switch_GAD4] Switch 4 – P2	5,7	3,9	5,1	
[switch_GAD5] Switch 5 – PB1	5,7	3,9	5,1	
[switch_GAD6] Switch 6 – PB2	5,7	3,9	5,1	
[switch_GAD7] Switch 7 – P1	5,7	3,9	5,1	
[switch_GAD7] Switch 8 – P1	5,7	3,9	5,1	
[switch_GAD7] Switch 9 – P2	5,7	3,9	5,1	
[switch_GAD7] Switch 10– P2	5,7	3,9	5,1	
[transFe] Transceiver	5,7	5,1	5,1	
[COM] Comunicaciones	5,1	4,4	5,1	5,7
[Internet_GAD] Internet	5,0	4,4	5,1	5,1
[LAN_GAD] Red Local	5,0	4,4	5,1	5,7
[WIFI_GAD] Red Inalámbrica	5,0	4,4	5,1	5,1
[PSTN_GAD] Telefonía IP	4,5	3,8	3,8	
[AUX] Elementos Auxiliares	5,7	3,9	4,5	
[power_GAD] Fuente de Alimentación	5,0			
[ups_GAD] Sistema de alimentación ininterrumpida	5,7			
[cabling_GAD] Cableado Estructurado	5,3	3,9	4,5	
[ac_GAD] Equipos de Climatización	3,9			
[cam_GAD] Cámaras de Seguridad	5,3	3,9	4,5	
[Media] Media soporte de información	5,6	3,9	5,1	
[disk_GAD] Discos Duros	5,6	3,9	5,1	
[L] Instalaciones	5,5		3,7	
[local_GAD] Cuarto de Servidores	5,5		3,7	
[P] Personal	4,2	5,1	5,1	
[cor_GAD] Coordinador/a Departamento de TIC	3,3		0,7	
[adm_GAD] Administrador de sistemas	4,2	5,1	5,1	
[dba_GAD] Administrador de base de datos	4,2	5,1	4,5	
[des_GAD] Desarrolladores / Programadores	4,2	5,1	3,8	

Tabla 30. Riesgo Potencial

3.2.2.4.4. Estimación del riesgo residual

De la misma manera se realiza el cálculo del riesgo residual, la herramienta PILAR simula que las salvaguardas identificadas fueron implementadas en el objeto de estudio, dando como resultado la disminución de los valores de riesgos en los activos que se están valorando dentro del Data Center. A continuación, en la siguiente tabla se observa la valorización del riego residual.

Para determinar el riesgo residual se utiliza la siguiente formula:

$$\text{Riesgo residual} = \text{Impacto Residual} * \text{Probabilidad Residual}$$

Activo	D	I	C	A
[IS] Servicios Internos	1,7	1,9	1,9	2,4
[inter_GAD] Internet	0,8	0,6	0,4	
[email_GAD] Servicio de Correo Institucional	0,9	1,9	1,9	2,4
[pweb_GAD] Página Web Oficial	1,7	1,6	1,5	1,7
[SW] Aplicaciones	1,6	1,4	1,8	1,7
[email_client_GAD] Cliente de correo	1,3	0,8	0,9	
[email_GAD] Servidor de Correo	1,3	0,9	0,9	
[dbms_GAD] Sistema BD	1,6	1,2	1,2	0,8
[si_admi_GAD] Sistema Administrativo/ Financiero	0,9	1,2	1,2	1,2
[sweb_GAD] Servicio Portal Web	1,3	0,8	0,8	
[sp_servPr] SO Servidor de Producción	1,3		0,9	
[sp_servApp] SO Servidor de Aplicaciones	1,3		0,9	
[firewall_GAD] Firewall	1,8	0,8	0,8	
[dns_GAD] Servicio DNS	1,3	0,8	0,8	
[HW] Equipos	2,4	2,6	2,6	
[SRVP_GAD1] ServProduccion 1	2,4	2,1	2,6	
[SRVP_GAD2] ServProduccion 2	2,4	2,6	2,6	
[SRVP_GAD3] ServProduccion 3	2,4	2,6	2,6	
[SRVP_GAD4] ServProduccion 4	2,4	2,6	2,6	
[SRVP_GAD5] ServProduccion 5	2,4	2,6	2,6	
[SRVAP_GAD] Servidor de Aplicaciones	2,4	2,1	2,6	
[SRVN_GAD] Servidor NAS	2,1	2,1	1,9	
[router_GAD1] Router 1	2,4	0,8	2,6	
[router_GAD2] Router 2	2,4	0,8	2,0	
[switch_GAD1] Master Switch CORE	2,4	0,8	2,0	
[switch_GAD2] Switch 2 – PB	2,4	1,7	2,0	
[switch_GAD3] Switch 3 – P1	2,4	1,7	2,0	
[switch_GAD4] Switch 4 – P2	2,4	0,8	2,0	
[switch_GAD5] Switch 5 – PB1	2,4	0,8	2,0	
[switch_GAD6] Switch 6 – PB2	2,4	0,8	2,0	
[switch_GAD7] Switch 7 – P1	2,4	0,8	2,0	
[switch_GAD7] Switch 8 – P1	2,4	0,8	2,0	
[switch_GAD7] Switch 9 – P2	2,4	0,8	2,0	
[switch_GAD7] Switch 10– P2	2,4	0,8	2,0	
[transFe] Transceiver	2,1	1,7	2,0	
[COM] Comunicaciones	2,6	1,7	2,7	2,5
[Internet_GAD] Internet	2,6	1,7	2,7	2,4
[LAN_GAD] Red Local	2,6	1,7	2,5	1,7
[WIFI_GAD] Red Inalámbrica	2,6	1,7	2,5	2,5
[PSTN_GAD] Telefonía IP	2,0	0,9	2,1	
[AUX] Elementos Auxiliares	2,2	0,8	1,3	
[power_GAD] Fuente de Alimentación	2,0			
[ups_GAD] Sistema de alimentación ininterrumpida	2,2			
[cabling_GAD] Cableado Estructurado	1,8	0,8	1,0	

[ac_GAD] Equipos de Climatización	0,9			
[cam_GAD] Cámaras de Seguridad	2,0	0,8	1,3	
[Media] Media soporte de información	1,6	0,8	2,0	
[disk_GAD] Discos Duros	1,6	0,8	2,0	
[L] Instalaciones	1,6		0,8	
[local_GAD] Cuarto de Servidores	0,7		0,8	
[P] Personal	0,9	1,9	1,9	
[cor_GAD] Coordinador/a Departamento de TIC	0,9		0,1	
[adm_GAD] Administrador de sistemas	0,9	1,9	1.9	
[dba_GAD] Administrador de base de datos	0,9	1,9	1,4	
[des_GAD] Desarrolladores / Programadores	1,2	1,9	1,2	

Tabla 31. Riesgo Residual

La comparación se visualiza en el anexo correspondiente (Anexo 12), que se hace con los valores de riesgo existentes actuales y los valores luego de la implementación de salvaguardas, se concluye que luego de las salvaguardas que recomienda PILAR y que se seleccionó de manera manual del catálogo, el riesgo en los activos disminuyo un 30% en la escala utilizada y un 50% aproximadamente en una escala de 10.

3.2.2.5. Interpretación de resultados del análisis de riesgos

A través de la herramienta PILAR se ha obtenido resultados del análisis, observados en los siguientes gráficos:

La siguiente figura (Figura 24) muestra las dimensiones de seguridad que se evaluaron y cómo estas afectan a cada activo identificado, donde se concluye que la dimensión de disponibilidad e integridad son las que más se ve afectada en la mayoría de los activos.

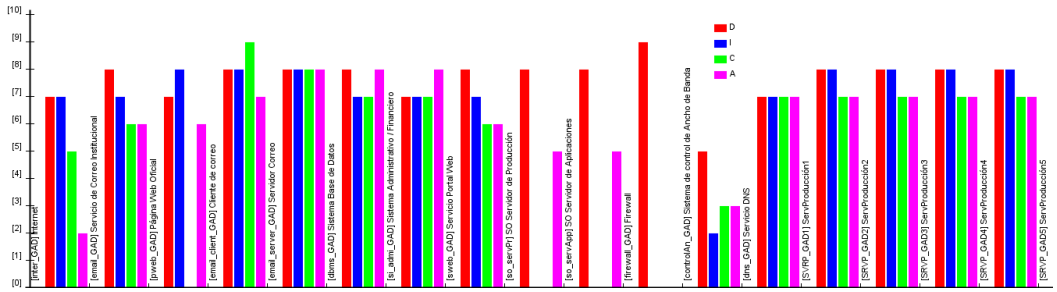


Figura 24: Valor de Activo por Dimensión

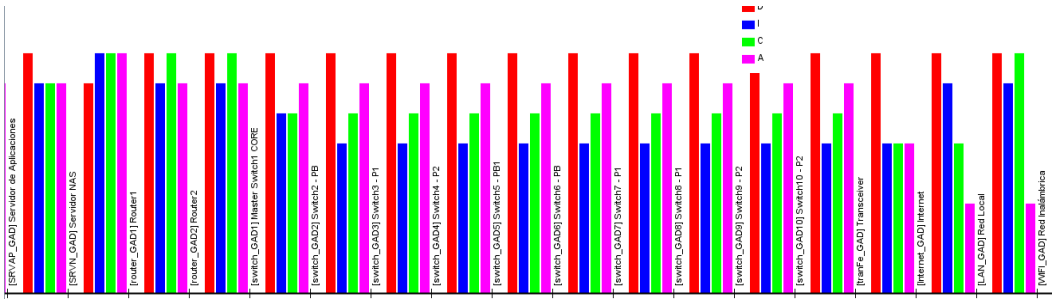


Figura 25: Valor de Activo por Dimensión 2

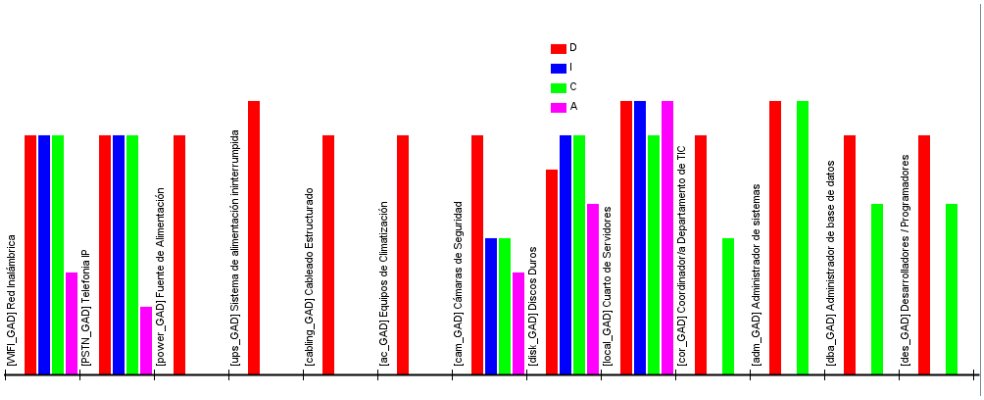


Figura 26: Valor de Activo por Dimensión 3

En las figuras 27 y 28 (Figura 27), se observa el resultado de las fases de activos, amenazas y salvaguardas, se muestra el impacto y riesgo al que están expuestos cada activo evaluado en la situación actual. Los activos con los niveles más altos en ambos casos son los servidores principales, los cuales participan en la continuidad operativa de los servicios que brinda el sitio y los equipos de red. Se denota también la disminución de los valores una vez implementadas las salvaguardas escogidas para el tratamiento de riesgos.

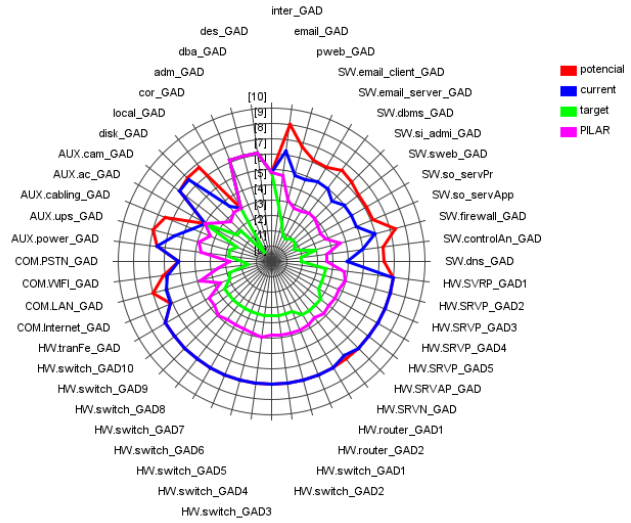


Figura 27: Identificación del Impacto por Activo

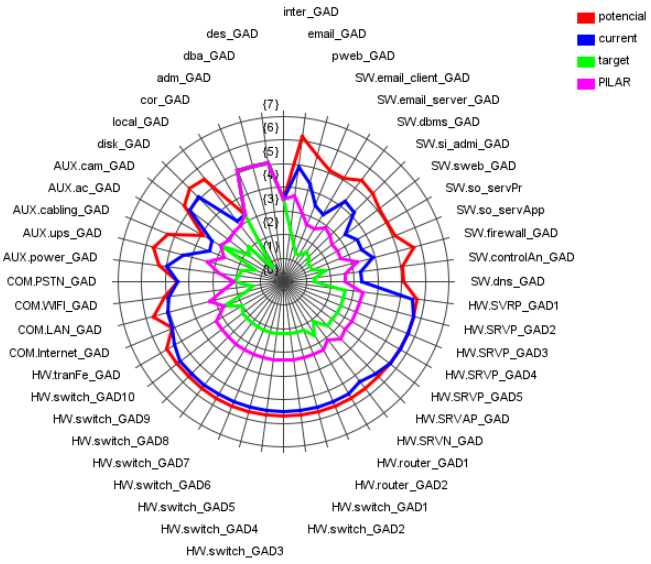


Figura 28: Identificación del riesgo por Activo

Finalmente, en la siguiente figura (Figura 29) se observa la estimación en porcentaje de los tipos de protección de las salvaguardas que se han incluido en el plan de tratamiento de riesgos, además de mostrar una comparativa entre los niveles actuales y los objetivos de las diferentes medidas de protección. La línea azul pertenece al nivel objetivo (target), la verde al nivel actual (current) y la roja al nivel recomendado por PILAR. En la figura se visualiza que el tipo de protección que predomina en las salvaguardas son las actividades de prevención, minimización y

detección siendo las que más se van a encontrar a los largo de todo el plan sin dejar de lado las de corrección, concienciación y aceptación.

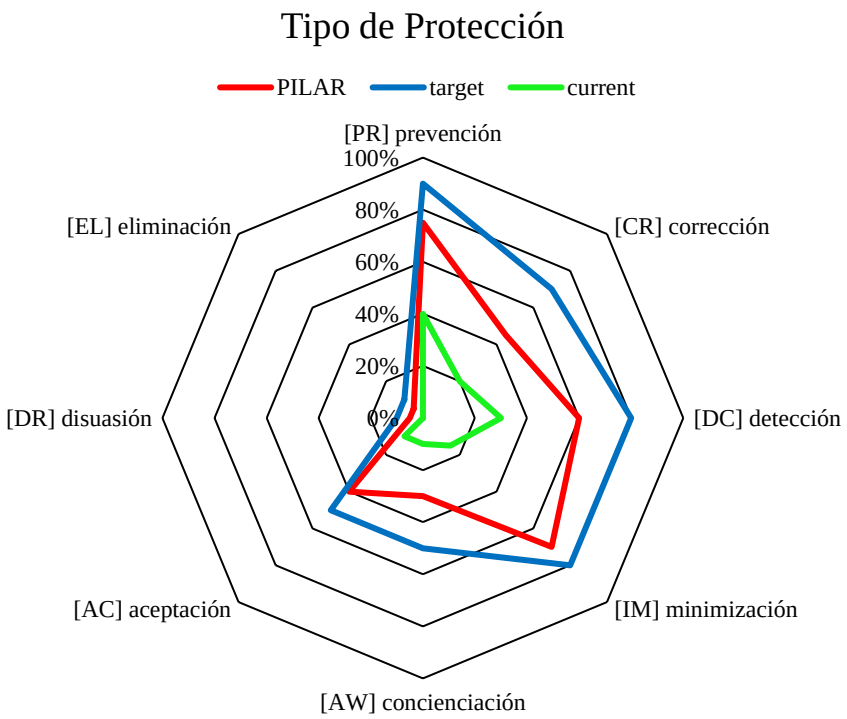


Figura 29: Tipos de protección incluidos en el Plan

3.2.3. Gestión de Riesgo

3.2.3.1. Plan de Tratamiento de riesgos

Una vez determinadas las amenazas a las que están expuestos los diferentes tipos de activos del Data Center, se realiza el plan de tratamiento de riesgos en donde se detallarán las actividades o tareas de prevención, minimización, detección y corrección con respecto a las salvaguardas; de igual manera, se plantea a los responsables de cumplir con aquellas actividades que forman parte del plan propuesto (Anexo 14).

3.2.3.2. Alcance

Con base en el alcance del proyecto, el plan de tratamiento de riesgos propuesto se enfoca en actividades de prevención, minimización, detección, corrección y aceptación de los riesgos o amenazas. Las actividades que se proponen están basadas en las salvaguardas del catálogo de elementos de Magerit, dichas actividades están diseñadas para la protección de las dimensiones valoradas en el

análisis de riesgos asociados a cada tipo de activos identificados en el Data Center de la entidad objeto de estudio.

3.2.3.3. Objetivo del Plan

Salvaguardar la disponibilidad, integridad, confidencialidad y autenticidad de los activos de información del Data Center de la institución mediante un plan de tratamiento de riesgos informáticos, que contribuirá a la continuidad operativa y fortalecerá la postura de seguridad.

3.2.4. Resultados

El proceso de planificación, análisis y gestión de riesgos para la entidad gubernamental tiene como resultado lo siguiente:

- El análisis realizado reveló que las dimensiones de disponibilidad e integridad son las que más se verán afectadas en la mayoría de los activos.
- El impacto y riesgo con los niveles más altos en ambos casos son los servidores principales, los mismos que participan en la continuidad operativa de los servicios que brinda el sitio y los equipos de red.
- La implementación de las salvaguardas a través de una simulación que permite PILAR dio como resultado que el impacto y el riesgo en los activos disminuyen un 36% y 55% respectivamente.
- El inventario de activos informáticos realizado para el análisis de riesgos proporciona una visión detallada de los recursos con los que el Data Center cuenta, además de que este mismo puede ser utilizado en un futuro para gestionar activos, planificar la capacidad, priorizar inversiones y cumplir con la normativa.
- El análisis de riesgos realizado puede ser utilizado como base sólida para la toma de decisiones estratégicas, permitiendo al encargado del departamento asignar recursos de manera efectiva y priorizar acciones.
- El análisis de riesgos sirve como punto de referencia para la realización futura de una gestión de incidentes o problemas informáticos.

3.2.4.1. Resultados de la variable

Variable: Cantidad de riesgos con sus respectivas salvaguardas antes y después de realizar el análisis de riesgos.

Para poder establecer el número de riesgos o amenazas que ya contaban con una salvaguarda se realizaron entrevistas a los jefes de áreas del departamento encargado del centro de cómputo, de los cual se detalla los controles y posibles amenazas existentes en los apartados **3.1.2.** y **3.2.2.2.3.** respectivamente. A continuación, se presenta una tabla que indica esta cantidad por tipo de activo.

VARIABLE					
Tipo de Activo	**Cantidad de Riesgos Antes del Análisis**	**Cantidad de Riesgos con su respectivo Salvaguarda (Antes)**	**Salvaguardas Antes del Análisis**	**Salvaguardas Después del Análisis**	**Cantidad de Riesgos con su respectivo Salvaguarda (Después)**
[IS]	16	8	10	26	16
[SW]	22	10	11	21	22
[HW]	19	9	8	15	19
[COM]	19	10	10	17	19
[AUX]	10	4	4	11	10
[MEDIA]	21	9	9	20	21
[L]	9	4	4	7	9
[P]	10	0	1	6	10
TOTAL	**126**	**50**	**57**	**123**	**126**

Tabla 32. Resultados Variable

Como resultados de la tabla anterior (Tabla 32), se puede destacar que:

- Después del análisis de riesgos, el número total de salvaguardas implementadas aumentó de 57 a 123. Esto indica que la existe una proporción 1 a 2, dado que los salvaguardas se duplicaron.
- Los activos de tipo [IS] y [HW] tienen la mayor cantidad de salvaguardas determinadas después del análisis de riesgos, esto indica que estos tipos de activos son considerados de mayor riesgo.
- Los activos de tipo [P] tenían 1 salvaguardas antes del análisis y solo 6 después del análisis, esto sugiere que estos riesgos se consideran de menor prioridad.
- Finalmente, existe un aumento significativo en la cantidad de riesgos con salvaguardas después del análisis, esto sugiere que el proceso de análisis de riesgos ha sido efectivo para identificar y abordar las vulnerabilidades en los activos. El aumento de 50 a 126 indica que se han implementado nuevas salvaguardas y se han mejorado las existentes para mitigar los riesgos identificados durante el análisis.

CONCLUSIONES

- Se logró un inventario detallado de los activos críticos del Data Center, incluyendo su clasificación tales como: servicios internos, software, hardware, redes de comunicación, equipamiento auxiliar, soportes de información, instalaciones y personal, además de su respectiva valoración que permitió determinar que los activos: servicio de correo institucional, sistema BD, sistema administrativo/financiero, servidores, routers y red local son de mayor importancia para la continuidad funcional del centro de cómputo.

- La aplicación de los procesos de la metodología Magerit ha permitido un análisis y evaluación única de los riesgos informáticos del Data Center de la entidad, lo que ha llevado a determinar de forma clara el impacto potencial de estos, donde los activos que tuvieron el nivel mayor de impacto en las dimensiones de disponibilidad e integridad fueron: los servidores, equipos de red (switch, router) y el centro de cómputo por las dependencias de todos los recursos que existen dentro. Así como también las aplicaciones (SW) y las comunicaciones (COM) se encuentran en un nivel de impacto inferior, pero afectando mayormente a tres de las cuatro dimensiones.

- El catálogo de elementos ha sido fundamental para determinar las salvaguardas apropiadas que forman parte del plan de tratamiento de riesgos para los activos críticos del Data Center. Identificando de manera precisa los activos críticos y las medidas de seguridad asociadas necesarias para protegerlos. Esto ha permitido una selección más eficiente y específica de las salvaguardas, asegurando que el plan de tratamiento de riesgos esté alineado con las amenazas específicas que enfrenta el Data Center.

- El proceso de documentar el plan de tratamiento de riesgos ha sido fundamental para establecer un enfoque claro y estructurado en la gestión de los riesgos informáticos identificados en el Data Center. Al plasmar las actividades adecuadas para la prevención, minimización, detección y

aceptación de los riesgos, se ha proporcionado una guía detallada que, si bien no garantiza la seguridad completa de los activos, proporciona una base sólida para proteger la infraestructura.

- PILAR ha demostrado ser una herramienta útil para la evaluación de riesgos y la gestión de la seguridad informática en el Data Center de la entidad gubernamental. Al proporcionar un marco estructurado y completo, ha facilitado la identificación de activos críticos, amenazas, así como la determinación de medidas de seguridad apropiadas. Además, dado el caso que se requiera realizar un nuevo análisis o modificar el actual debido a cambios en el centro de cómputo, la herramienta permite la edición del archivo dando nuevos resultados.

RECOMENDACIONES

- Actualizar periódicamente el plan de tratamiento de riesgos (salvaguardas, responsables, actividades) para adaptarse a los cambios en el entorno operativo del Data Center, nuevos activos, las amenazas emergentes y las nuevas vulnerabilidades que puedan surgir.

- Tomar en cuenta el análisis de riesgos como base para el diseño futuro de la gestión de incidencias o problemas. Esta documentación será esencial para proporcionar información crucial que permitirá evaluar y validar la efectividad de la gestión de riesgos durante auditorías futuras.

- Complementar el análisis y gestión de riesgos con otras metodologías enfocadas a la seguridad informática o seguridad de la información como: las normas ISO 27001 e ISO 27005 que ofrecen directrices adicionales sobre la gestión de la seguridad de la información, además de controles para mitigar el riesgo, la metodología OCTAVE que también puede ser útil para la evaluación de amenazas. Obteniendo una visión más completa y robusta aumentando el porcentaje de protección de los activos del Data Center.

- Si bien el plan actual elaborado con la metodología Magerit se considera robusto, se recomienda la inclusión de la metodología CAP-DO para enriquecer aún más la gestión de riesgos de esta investigación. Esta ofrece un ciclo continuo de mejoras a través de sus fases de Check, Analyze, Plan y Do. La integración de CAP-DO permitirá una gestión más adaptable de los riesgos, facilitando la identificación temprana de nuevas amenazas y proporcionando un marco para la implementación, monitoreo y ajuste continuo de las estrategias del plan de tratamiento de riesgos.

REFERENCIAS

[1] C. Merido Bada y R. Cañizares Sales, *Auditoría de sistemas de gestión de seguridad de la información*, FC Editorial. Madrid, España, 2014.

[2] H. Villón, "GESTIÓN DEL TALENTO HUMANO DEL GADM DEL CANTÓN LA LIBERTAD", La Libertad, 2022. Consultado: el 4 de agosto de 2023. [En línea]. Disponible en: https://repositorio.upse.edu.ec/bitstream/46000/8217/4/UPSE-MTH-2022-0037.pdf

[3] "La Libertad". Consultado: el 6 de agosto de 2023. [En línea]. Disponible en: https://lalibertad.gob.ec/?menu=31

[4] A. Vilca, "AUDITORÍA PARA EVALUAR LA SEGURIDAD FÍSICA DEL DATA", UNIVERSIDAD NACIONAL DE SAN CRISTÓBAL DE HUAMANGA FACULTAD DE INGENIERÍA DE MINAS, GEOLOGÍA Y CIVIL ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS, Ayacucho, 2019.

[5] Á. Maliza, "PLAN DE SEGURIDAD INFORMÁTICA ALINEADO A LA NORMA ISO 27001 PARA FORTALECER LAS SEGURIDADES DEL DATA CENTER EN LA COOPERATIVA DE AHORRO Y CREDITO 1 DE JULIO DE LA CIUDAD DEL TENA", UNIVERSIDAD REGIONAL AUTONOMA DE LOS ANDES, Puyo, 2021.

[6] J. Rodríguez, "PROPUESTA DE UN MODELO DE MEJORA CONTINUA PARA LA GESTIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN A UNA INSTITUCIÓN EDUCATIVA PRIVADA MEDIANTE EL CICLO CAP-DO", UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA, Santa Elena, 2023.

[7] E. J. S. Chinchilla y J. S. Allende, "Riesgos de ciberseguridad en las Empresas", *Tecnología y desarrollo*, vol. 15, núm. 0, dic. 2017, Consultado: el 9 de agosto de 2023. [En línea]. Disponible en: https://revistas.uax.es/index.php/tec_des/article/view/1174

[8] G. Pacio, *Data Centers hoy*, Alfaimega Group. 2014.

[9] Consejo Superior de Administración Electrónica, “PAe - MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información”. Consultado: el 27 de septiembre de 2023. [En línea]. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XZojom5FxPY

[10] Consejo Superior de Administración Electrónica, *MAGERIT - versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método*. 2016. Consultado: el 10 de agosto de 2023. [En línea]. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XZojom5FxPY

[11] R. R.-F.-S.-0. N. 03-2021, “Resolución RCF-FST-SO-09 No. 03-2021”, pp. 1998–2005.

[12] V. Jácome, “PLAN DE SEGURIDAD PARA LA GESTIÓN DE RIESGOS EN EL DATACENTER DE LA FACULTAD DE INGENIERA EN CIENCIAS APLICADAS CON LA METODOLOGÍA MAGERIT V3.0”, UNIVERSIDAD TÉCNICA DEL NORTE, Ibarra, 2019.

[13] ISO/IEC 27000, “Sistema de Gestión de la Seguridad de la Información”, 2018. [En línea]. Disponible en: www.iso.org

[14] Secretaría General de Planificación, “Plan de Creación de Oportunidades 2021 - 2025”, 2021. Consultado: el 12 de octubre de 2023. [En línea]. Disponible en: https://www.planificacion.gob.ec/wp-content/uploads/2021/09/Plan-de-Creacio%CC%81n-de-Oportunidades-2021-2025-Aprobado.pdf

[15] K. Josep Altamirano-de-la-Borda, “La seguridad de la información en la administración pública”, 2021.

[16] S. Garre Gui, “Introducción a la seguridad de la información”, 2018.

[17] A. Gómez Vieites, *Enciclopedia de la seguridad informática*, Segunda Edición. RA-MA Editorial, 2014.

[18] E. Chicano Tejada, *Gestión de incidentes de seguridad informática. IFCT0109,* Segunda Edición. IC Editorial, 2023.

[19] J. Costas, *Gestión de la seguridad informática en la empresa*. Madrid: RA-MA Editorial, 2021.

[20] G. Escrivá Gascó, *Seguridad informática* . Madrid: Macmillan Iberia, S.A., 2013. Consultado: el 30 de abril de 2024. [En línea]. Disponible en: https://elibro.net/es/ereader/uteq/43260

[21] G. Baca Urbina, *Introducción a la seguridad informática*, Primera. México: Grupo Editorial Patria, 2016. Consultado: el 20 de mayo de 2024. [En línea]. Disponible en: https://elibro.net/es/ereader/utnorte/40458?page=1

[22] E. Chicano Tejada, *Auditoría de seguridad informática. IFCT0109,* Segunda Edición. Málaga: IC Editorial, 2023. Consultado: el 30 de abril de 2024. [En línea]. Disponible en: https://elibro.net/es/lc/espoch/titulos/232692

[23] A. Azofeifa, "ANÁLISIS CUALITATIVO Y CUANTITATIVO DE LOS RIESGOS", may 2021.

[24] Consejo Superior de Administración Electrónica, "Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro II : Catálogo de elementos", 2016, Consultado: el 19 de mayo de 2024. [En línea]. Disponible en: http://administracionelectronica.gob.es/

[25] A. E. Pacheco, F. Luis, I. S. Santamaría, J. Hover, y G. Chacón, "Aplicar la Metodología OCTAVE de Identificación de Amenazas y Vulnerabilidades en una Entidad Bancaria", 2021.

[26] E. Crespo Martínez y G. Cordero Torres, "ESTUDIO COMPARATIVO ENTRE LAS METODOLOGÍAS CRAMM Y MAGERIT PARA LA GESTIÓN DE RIESGO DE TI EN LAS MPYMES", 2015. Consultado: el 18 de mayo de 2024. [En línea]. Disponible en: https://revistas.uazuay.edu.ec/index.php/udaakadem/article/view/129/126

[27] R. Gómez, D. Hernán Pérez, Y. Donoso, y A. Herrera, "Metodología y gobierno de la gestión de riesgos de tecnologías de la información

Methodology and Governance of the IT Risk Management", pp. 109–118, 2010.

[28] ISACA, "COBIT 5 for Risk", Rolling Meadows, Illinois, EE.UU., 2013.

[29] ISACA, "Marco de Riesgo de TI", 2009, Consultado: el 30 de mayo de 2024. [En línea]. Disponible en: www.isaca.org

[30] R. Hernández Sampieri, C. Fernández Collado, y P. Baptista Lucio, *Metodología de la Investigación*. México, 1998.

[31] D. Bernal, "Implementación de la gestión de riesgos TI para una empresa dental en la Ciudad de Lima – 2021", UNIVERSIDAD TECNOLOGICA DEL PERU, Lima, 2020. Consultado: el 10 de agosto de 2023. [En línea]. Disponible en: https://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/4430/Didier_Bernal_Trabajo_de_Suficiencia_Profesional_Titulo_Profesional_2021.pdf?sequence=1&isAllowed=y

[32] Hewlett Packard Enterprise Development LP, "HPE ProLiant DL560 Gen10 server", HPE Store US. Consultado: el 13 de noviembre de 2023. [En línea]. Disponible en: https://buy.hpe.com/us/en/compute/rack-servers/proliant-dl500-servers/proliant-dl560-server/hpe-proliant-dl560-gen10-server/p/1010026837?q=1010026837:relevance:facet_processorspd:2.1%2BGHz&text=1010026837&textSearch=

[33] IBM Support, "IBM System x3200", Overview - IBM System x3200. Consultado: el 13 de noviembre de 2023. [En línea]. Disponible en: https://www.ibm.com/support/pages/overview-ibm-system-x3200

[34] TP-LINK, "TL-SG3424", Switches Administrables. Consultado: el 13 de noviembre de 2023. [En línea]. Disponible en: https://www.tp-link.com/ar/business-networking/managed-switch/tl-sg3424/#specifications

[35] TP-Link, "T1600G-52TS (TL-SG2452)", Switches Inteligentes. Consultado: el 13 de noviembre de 2023. [En línea]. Disponible en: https://www.tp-link.com/ec/business-networking/smart-switch/t1600g-52ts/#specifications

[36] TP-Link, “TL-SG2218”, Switch inteligente. Consultado: el 13 de noviembre de 2023. [En línea]. Disponible en: https://www.tp-link.com/ar/business-networking/smart-switch/tl-sg2218/#specifications

[37] Cisco, “Cisco 1841 Router (Modular)”, Cisco 1800 Series Integrated Services Routers. Consultado: el 14 de noviembre de 2023. [En línea]. Disponible en: https://www.cisco.com/c/en/us/products/collateral/routers/1800-series-integrated-services-routers-isr/product_data_sheet0900aecd8016a59b.html

ANEXOS

Anexo 1: Recopilación de la Información de los procedimientos actuales

UNIVERSIDAD ESTATAL PENINSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

Realizado por:	Borbor Tumbaco Ariel
Fecha:	14/05/2024
Entrevistado:	Encargado del Data Center: Ing. Luis Chalen Rodríguez
Metodología	Entrevista
Objetivo de la fase:	Recopilar información de los procedimientos de tratamiento de los riesgos.

Preguntas

- **¿Cuál es el soporte del Data Center de la Entidad? ¿Su funcionamiento son las 24 horas del día, los 7 días de la semana y los 365 días del año?**

El soporte que realiza es a las demás áreas de la entidad gubernamental, prestando servicios de correo, de internet, de almacenamiento de datos, de backup y recuperación de datos, de conectividad y la administración de usuarios. El data center está gestionado cumplir con dicho funcionamiento las 25 horas 5 días por semana.

- **¿Conoce Ud. si se ha realizado un análisis y gestión de riesgos al Data Center de la entidad?**

No se ha realizado, ni revisado ninguna propuesta acerca de un análisis y gestión de riesgos para el Data Center.

- **¿Existen procesos o procedimientos formales para el tratamiento de los riesgos de seguridad física?**

No, no existen documentos que plasmen las políticas, medidas o procedimientos que se deben tomar para la presencia de riesgos de seguridad física, aun así, si se toma las medidas necesarias para prevenir los mismos en el momento que se presentan.

- **¿Existen procesos o procedimientos formales para el tratamiento de los riesgos de seguridad lógica?**

No, no existen documentos que plasmen las políticas, medidas o procedimientos que se deben tomar para la presencia de riesgos de seguridad lógica, aun así, si se toma las medidas necesarias para prevenir los mismos en el momento que se presentan.

- **¿El centro de datos cuenta con un inventario de activos debidamente documentado?**

No, no existen documentos que plasmen un inventario de activos de la data center.

- **¿Existe una persona responsable del Centro de Datos?**

Si, actualmente la persona responsable del Data Center es mi persona (Ing. Luis Chalen), yo me encargo del acceso al mismo y de los cambios que se realizan o realizarán.

- **El departamento ¿Cuenta con un área específica para la seguridad física y lógica del Data Center?**

No, ningún área relacionada al departamento de Sistemas y recursos tecnológicos se encarga de la seguridad del centro de datos, todo los que se refiere a la seguridad de la información del Data Center deber ser cubierto por mi puesto.

- **¿Considera Ud. que las medidas de respuesta ante la presencia de riesgo son importantes para la continuidad operacional de la entidad?**

Si, las medidas de respuesta ante la presencia de riesgos son muy importante para la continuidad operacional de la institución y sus usuarios.

- **¿Qué cree Ud. que aportaría a la organización el desarrollo de un análisis y gestión de riesgos al Data Center?**

Aportaría una mejor identificación de amenazas y vulnerabilidades, mejora de seguridad, una reducción de riesgos, una mayor continuidad operativa de la organización.

- **¿Qué cree Ud. que aportaría a la organización el desarrollo de un plan de tratamiento de los riesgos informáticos del Data Center?**

Aportaría a la institución a disminuir los daños a los sistemas, datos y activos críticos, a su aumentando la protección de datos e información privada, garantiza una mejora continua en el tema de seguridad.

Anexo 2: Entrevista para el análisis de riesgos dirigida a la coordinadora de departamento de Sistemas y recursos tecnológicos.

UNIVERSIDAD ESTATAL PENINSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

Realizado por:	Borbor Tumbaco Ariel
Fecha:	14/05/2024
Entrevistado/a:	Coordinadora: Ing. Sandra Suárez Severino
Metodología:	Entrevista
Objetivo de la fase:	Determinar los posibles riesgos o amenazas existentes que afecta el funcionamiento del Data Center

Pregunta	**Respuesta**
Sección: Incendios	
¿El Data Center tiene instalados sistemas de detección contra incendios?	No
¿En los últimos meses se ha presentado alguna posibilidad de incendio?	No se ha presentado.
¿Se dispone de equipos de extinción de incendios adecuados en el Data Center?	Si, uno dentro del mismo y otro fuera.

Si la respuesta anterior es Si, ¿Los equipos de extinción de incendios están ubicados en lugares estratégicos del Data Center?	Si.
¿Dentro del Data Center se almacenan materiales inflamables?	Si.
¿Se han identificado las áreas críticas del Data Center más vulnerables a un incendio?	No.
¿Se ha proporcionado capacitación al personal sobre cómo actuar en caso de un incendio?	Si, pero poca capacitación.
¿Se llevan a cabo simulacros de incendio periódicos para practicar los procedimientos de emergencia?	Si, cada 3 meses.
¿Se cuenta con sistemas de respaldo para proteger los datos en caso de un incendio?	Si.
¿Existe la posibilidad de que fallos en las instalaciones eléctricas puedan desencadenar un incendio en el Data Center?	Si, aunque no se han presentado hasta el momento.
¿Se han realizado inspecciones regulares de las instalaciones eléctricas para identificar posibles fallos o sobrecargas?	Si.
¿Las instalaciones eléctricas se encuentran diseñadas y mantenidas de manera que minimicen el riesgo de chispas o cortocircuitos que podrían iniciar un incendio?	Si, están diseñadas de manera que la probabilidad de que suceda
¿Existen señalizaciones tanto dentro de Data Center como en el departamento de No fumar, etc.?	Dentro no existen, pero en el departamento sí.
¿Están adecuadamente aterrizados los racks que contienen los servidores en el Data Center?	Si.
¿El sitio cuenta con salidas de emergencia? ¿Con cuentas cuenta?	No cuenta con ninguna.
Sección: Daños por Agua	

¿El centro de datos está ubicado en un lugar que reduzca las posibilidades de inundaciones o daños por agua?	Si.
¿Hay un sistema de drenaje para desviar el agua lejos del Data Center?	En el data center no, pero en el piso superior sí.
¿Existen barreras físicas para proteger el Data Center de inundaciones?	Si, el data center se encuentra en un segundo piso.
¿En los últimos meses se han presentado problemas por lluvias que afecten al funcionamiento del Data Center?	No, y no se ha presentado en ningún momento.
¿Se crean lagunas, desagües o se presenta algún vestigio de agua cerca del centro de datos?	No.
¿El sistema de tuberías pasa cerca del Data Center?	No.
¿La altura de los tomacorrientes es la adecuada para prevenir cortos por contacto con el agua?	Si, los tomacorriente están a la altura adecuada.
¿Se ha proporcionado capacitación al personal sobre cómo responder de manera efectiva en caso de una emergencia relacionada con el agua, como una inundación repentina?	Si se ha proporcionada pero la capacitación no es la adecuada.
¿Se han implementado barreras físicas adicionales, como selladores de juntas, para prevenir filtraciones de agua en las paredes?	Hasta el momento no ha sido necesario ese tipo de barreras.
¿El Data Center cuenta con un techo falso instalado como medida preventiva para proteger la infraestructura sensible contra posibles daños por agua?	No el sitio no cuenta con un techo falso y no cuenta con un piso falso.
Sección: Gestión del Personal	
¿Se han establecido roles y responsabilidades claras para el personal del Data Center?	Si, solo los que interactúan con el data center.

¿Se proporciona capacitación regular al personal sobre procedimientos de seguridad y operación del Data Center?	No.
¿Se han identificado y capacitado a empleados sustitutos o suplentes para asumir responsabilidades críticas en ausencia	Si, se capacita a los están mas preparados para asumir el puesto.
¿Se han implementado tecnologías y herramientas que permitan al personal acceder y administrar los sistemas de forma remota en caso de necesidad?	Si, los servidores y demás quipos de redes se pueden manejar de forma remota.
¿En caso de vacaciones o ausencia del personal encargado del centro de datos, este queda sin supervisión o lo remplaza otra persona del departamento?	Si, lo reemplaza la persona mejor capacitada.

Anexo 3: Entrevista para el análisis de riesgos dirigida al Encargado del Data Center.

UNIVERSIDAD ESTATAL PENINSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

Realizado por:	Borbor Tumbaco Ariel
Fecha:	14/05/2024
Entrevistado/a:	Encargado del Data Center: Ing. Luis Chalen Rodríguez
Metodología:	Entrevista
Objetivo de la fase:	Determinar los posibles riesgos o amenazas existentes que afecta el funcionamiento del Data Center

Pregunta	**Respuesta**
Sección: Infraestructura de redes (Comunicaciones)	
¿Cuánto tiempo llevan en funcionamiento los equipos de comunicaciones de red (routers, switches, etc.)?	Los equipos llevan 1 año como máximo.
¿Se han experimentado interrupciones de la conectividad de red debido a fallos en los equipos de red?	Si, pero a pequeña escala.

¿Se ha detectado pérdida de paquetes de datos en la red como resultado de fallos en los dispositivos de red?	Si.
¿Se ha producido degradación en la calidad de servicio (QoS) debido a fallos en los dispositivos de red?	Si, pero solo un poco.
¿Los routers y switches del Data Center utilizan protocolos de enrutamiento redundantes para aumentar la disponibilidad de la red?	No, el enrutamiento de los equipos es estático y es tipo árbol.
¿Se utilizan equipos de red de marcas reconocidas y con reputación en la industria para garantizar la fiabilidad y estabilidad de la red?	Si, IBM y Cisco.
¿Los routers y switches del Data Center están equipados con capacidades de gestión remota para facilitar la monitorización y administración de la red?	Si.
¿Los routers y switches del Data Center están configurados con listas de control de acceso (ACL) para controlar el tráfico de red y limitar el acceso a recursos específicos?	Si.
¿Los equipos de red del Data Center están equipados con interfaces de administración seguras, como SSH o HTTPS, para proteger el acceso a la configuración del dispositivo?	Si.
¿Se utilizan cables de fibra óptica para conexiones de red de alta velocidad y mayor seguridad contra interferencias externas?	Si, se utilizan cable de fibra óptica.
¿Se utiliza cableado de par trenzado blindado (STP) en áreas con alta interferencia electromagnética para garantizar una transmisión de datos más estable?	Si.
¿Los routers y switches están instalados en armarios o racks diseñados para protegerlos contra el polvo y otros contaminantes ambientales?	Si, están instalados en racks.
¿Se han experimentado sobrecargas en los servidores y caídas de servicios provocadas por ataques de denegación de servicio (DDoS) en el Data Center?	No, hasta el momento.
¿Se realiza el cifrado de datos sensibles para proteger la confidencialidad durante la transmisión a través de la red?	Si.

¿Se lleva a cabo algún procedimiento de balanceo de carga para distribuir equitativamente el tráfico entre múltiples enlaces?	No.
¿Se realizan análisis de tráfico para identificar patrones anómalos que puedan indicar posibles actividades maliciosas en la red?	No.
Sección: Identificación y autenticación	
¿Se han experimentado intentos de acceso no autorizado a sistemas y servicios del Data Center debido a fallos en los mecanismos de autenticación?	No, hasta el momento.
¿Se ha registrado un aumento en los incidentes de phishing o suplantación de identidad como consecuencia de fallos en los mecanismos de autenticación?	No, pero si existe el phishing a través de correo electrónicos.
¿Existen restricciones claras sobre el acceso a los sistemas críticos del Data Center y se han revisado recientemente?	Si.
¿El personal autorizado cuenta con credenciales de identificación que le permita el ingreso al centro de datos?	No.
¿Existe un sistema biométrico para la identificación de usuarios que entran al centro de datos?	No.
¿Se realiza el mantenimientos a las puestas de ingreso al Data Center?	Si, cada 3 meses.
¿Quién es la persona responsable del acceso al sitio?	Ing. Luis Chalen
¿Se lleva un registro detallado de todas las personas que ingresan y salen del Data Center?	No.
¿Se han implementado medidas de protección contra intrusiones físicas, como alarmas y cámaras de seguridad, en el Data Center?	Si, están las cámaras y alarmas.
¿Se han detectado intentos de acceso no autorizado a las instalaciones del Data Center en el pasado?	No.
¿Se ha capacitado al personal para reconocer y reportar actividades sospechosas relacionadas con el acceso físico al Data Center?	Si.
¿Se han reportado casos de phishing u otras técnicas de ingeniería social dirigidas a obtener credenciales de usuario?	No, hasta el momento.
Sección: Protección de la Información	

¿Se utilizan técnicas de encriptación para proteger la confidencialidad de la información sensible almacenada en el Data Center?	Si.
¿Se realizan copias de seguridad regulares de los archivos y datos críticos almacenados en el Data Center?	Si.
¿Se han establecido políticas de retención de datos para garantizar la eliminación segura y oportuna de la información obsoleta o no necesaria?	No.
¿Se utilizan sistemas de prevención de pérdida de datos (DLP) para evitar la filtración de información confidencial fuera del Data Center?	No.
¿Se ha implementado un proceso de cifrado de extremo a extremo para proteger la seguridad de la información durante su transmisión y almacenamiento?	No.
¿Se proporciona formación y concienciación en seguridad a los empleados para promover prácticas seguras en el manejo y protección de la información?	Si.
¿Se han establecido mecanismos de control de versiones para garantizar la integridad y autenticidad de los archivos y datos almacenados?	Si.
¿Existe un plan de respaldo y recuperación de datos?	Si.
¿Se realizan pruebas regulares de recuperación de datos para garantizar la eficacia del plan de respaldo y recuperación ante desastres en la protección de la información crítica?	No
Sección: Equipos Informáticos (Servidores)	
¿Se ha experimentado alguna falla significativa en los servidores en el último año?	No.
¿Qué tipo de servidores se utilizan predominantemente en el Data Center (por ejemplo, servidores de rack, blade, o torre)?	Servidores de Rack.
¿Cuál es el sistema operativo principal utilizado en los servidores del Data Center (por ejemplo, Windows Server, Linux, Unix)?	El S.O es Linux (centOS)
¿Los servidores de virtualización están configurados con medidas de seguridad como aislamiento de redes y control de acceso basado en roles?	Si.

¿Se han implementado medidas de redundancia para garantizar la disponibilidad de los servidores en caso de falla?	Si.
¿Cuántos servidores físicos están actualmente en funcionamiento en el Data Center?	3 servidores físicos.
¿Qué porcentaje de los servidores están virtualizados en comparación con los servidores físicos?	Un 65% están virtualizados.
¿Se ha realizado alguna actualización importante de hardware en los servidores recientemente?	No.
¿Se lleva un registro de las intervenciones de mantenimiento realizadas en los servidores, como actualizaciones de firmware o reemplazos de componentes?	Si.
¿Se realizan copias de seguridad periódicas de los datos almacenados en los servidores?	Si.
¿Se han experimentado problemas de rendimiento en los servidores debido a la sobrecarga de recursos?	No, hasta el momento.
Sección: Suministro eléctrico	
¿El Gad cuenta con su propia planta de energía eléctrica en caso de cortes de energía?	No.
¿Se cuenta con sistemas de alimentación ininterrumpida (UPS) para garantizar la disponibilidad de energía en caso de cortes de energía?	Si, se cuenta con un UPS.
¿El UPS cuenta con un tablero ByPass?	Si. Automático y switch.
¿Qué cantidad de equipos soporta el UPS?	30
¿En alguna ocasión han existido sabotaje en la energía eléctrica que han ocasionado problemas al Data Center?	No, hasta el momento.
¿Se realiza un mantenimiento regular de los sistemas eléctricos para asegurar su funcionamiento óptimo y reducir el riesgo de fallos?	Si, cada 3 meses.
¿Los equipos informáticos están conectados de manera correcta?	Si.

¿Se cuenta con iluminación de emergencia en caso de cortes de energía repentinos?	No.
¿Se han identificado y corregido posibles puntos de falla en el sistema eléctrico, como conexiones sueltas o cables desgastados?	Si.
¿El cableado eléctrico se encuentra ubicado debajo de un piso falso?	No, está por arriba de los equipos.
Sección: Climatización	
¿El Data Center cuenta con un sistema de climatización para regular la temperatura de los quipos?	Si, cuenta con 2 aires acondicionados.
¿Se verifica regularmente que los sistemas de aire acondicionado estén funcionando correctamente?	Si, se los verifica diariamente.
¿Existen dentro del Data Center indicadores que indiquen a que temperatura se encuentra el sitio?	Si.
¿Se mantienen las puertas del Data Center cerradas para evitar la entrada de aire caliente?	Si, siempre.
¿Se han colocado sensores de temperatura en diferentes áreas del Data Center para identificar zonas con problemas de sobrecalentamiento?	No.
¿Se realizan ajustes manuales en los sistemas de climatización según sea necesario?	Si, cuando es necesario.
¿Se utilizan ventiladores adicionales para mejorar la circulación del aire frío?	No.
¿Los equipos informáticos han sufrido de sobrecalentamiento?	No hasta el momento.
¿El sistema de climatización está instalado bajo normas?	No.

Anexo 4: Entrevista para el análisis de riesgos dirigida al Analista Técnico de Base de Datos del departamento de Sistemas y Recursos tecnológicos.

UNIVERSIDAD ESTATAL PENINSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

Realizado por:	Borbor Tumbaco Ariel
Fecha:	14/05/2024
Entrevistado/a:	Analista Técnico de Base de Datos: Ing. John Reyes Lindao
Metodología:	Entrevista
Objetivo de la fase:	Determinar los posibles riesgos o amenazas existentes que afecta el funcionamiento del Data Center

Pregunta	**Respuesta**
¿La base de datos se encuentra alojada en un entorno físico o en la nube?	En un entorno físico.
¿Qué sistema de gestión de bases de datos (SGBD) se utiliza?	Oracle Database 11g
¿Se realizan copias de seguridad de la base de datos de manera regular?	Si.
¿Se implementan medidas de seguridad como el cifrado de datos en la base de datos?	Si.
¿Se utilizan firewalls o sistemas de detección de intrusos para proteger la base de datos	No.
¿Se han experimentado problemas de rendimiento en la base de datos debido a la sobrecarga de consultas?	Hasta el momento no.
¿Se lleva un registro de los usuarios que tienen acceso a la base de datos y sus privilegios?	Si.
¿La base de datos almacena información sensible o crítica para la organización?	Si,
¿Se han experimentado incidentes de pérdida de datos en la base de datos en el pasado?	Incidentes graves no.

¿Se realiza un monitoreo constante del rendimiento y la disponibilidad de la base de datos?	Si.
¿La base de datos ha experimentado alguna violación de seguridad en el pasado?	No hasta el momento.
¿Se han encontrado inconsistencias o errores en la integridad de los datos almacenados en la base de datos?	No.
¿La base de datos se integra con otros sistemas o aplicaciones dentro de la infraestructura tecnológica?	Si, con el sistema Financiero y Administrativo.
¿Se han identificado cuellos de botella en la infraestructura de red que podrían afectar el rendimiento de la base de datos?	No hasta el momento.
¿Se han detectado problemas de escalabilidad que podrían afectar el crecimiento futuro de la base de datos?	No.

Anexo 5: Entrevista para el análisis de riesgos dirigida al Programador de Sistemas del departamento de Sistemas y Recursos tecnológicos.

UNIVERSIDAD ESTATAL PENINSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

Realizado por:	Borbor Tumbaco Ariel
Fecha:	14/05/2024
Entrevistado/a:	Programador de Sistemas: Ing. Denisse Morocho Tigrero
Metodología:	Entrevista
Objetivo de la fase:	Determinar los posibles riesgos o amenazas existentes que afecta el funcionamiento del Data Center

Pregunta	**Respuesta**
Sección: Fallas en los sistemas	

¿Los sistemas implementados cuentan con medidas de seguridad robustas?	Si, con controles de acceso, encriptación de clave y un inicio de sesión seguro.
¿Cuántas fallas significativas ha experimentado el sistema en el último año?	Fallas significativas ninguna, pero si fallas de mínima gravedad.
¿Cuál es el tiempo promedio de resolución de las fallas del sistema?	Si el problema es complejo se soluciona en 4 o 6 hojas y si es aún más complejo se toma el tiempo de uno o más días.
¿El personal que interactúa con el sistema es capacitado cada que este se actualiza o se implementa uno nuevo?	Si, el personal que interactúa tiene la debida capacitación.
¿Existen manuales de usuarios de los sistemas implementados?	No.
¿Las fallas en los sistemas han causado interrupciones significativas en las operaciones de la institución?	No hasta el momento.
¿Se cuenta con personal de soporte técnico disponible las 24 horas para responder a las fallas del sistema?	Si, en este caso durante las horas de trabajo.
¿Existe un proceso de gestión de parches para mantener los sistemas actualizados?	No.
¿Se realizan copias de seguridad periódicas de los datos almacenados en los sistemas?	Si.
¿Se han identificado y mitigado vulnerabilidades conocidas en los sistemas?	No.
¿Los sistemas implementados son originales de la institución o son sistemas contratados?	Son originales y dedicados para la entidad.
¿El equipo informático cumple con los requisitos mínimos para soportar los sistemas?	Si.

Sección: Errores de configuración	
¿Se ha experimentado alguna vez una interrupción del servicio debido a una configuración incorrecta en los sistemas?	No.
¿Se ha observado alguna vez que los sistemas no funcionen correctamente después de realizar cambios en la configuración?	Si.
¿Se han producido pérdidas de datos como consecuencia de configuraciones incorrectas en los sistemas de respaldo?	No.
¿Cuáles son los errores más comunes que se presentan en los equipos que alojan los sistemas?	Errores de red, errores de inicio y registro de datos.
¿Cada cuánto tiempo se revisa las configuraciones de los sistemas, aplicaciones y base de datos?	Cada 3 meses.
¿Se disponen de documentos que tengan plasmados la configuración de los sistemas en los equipos?	No todos.
¿Se dispone de una gestión de incidentes en caso de errores graves de configuración?	No.

Anexo 6: Recopilación de la Información aplicando el método de Observación

UNIVERSIDAD ESTATAL PENINSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

Realizado por:	Borbor Tumbaco Ariel
Fecha	14/05/2024
Metodología	Observación
Objetivo de la fase:	Recopilar información de manera directa de las operaciones, sistemas, condiciones físicas y lógicas del Data Center.

Resultados

Operaciones y Sistemas

- La monitorización y mantenimiento del sitio están controladas por el encargado de Data Center (Ing. Luis Chalen).
- La supervisión del rendimiento, la detección de problemas y la aplicación de actualizaciones y parches de seguridad.
- Los sistemas que están bajo el soporte del centro de datos son el sistema financiero y el sistema administrativo.

Físicos

- El acceso controlado al centro de datos no cuenta con un sistema de seguridad biométrica o con credenciales para los usuarios autorizados.
- La ubicación del centro de datos está en las oficinas del departamento de sistemas y recursos tecnológicos
- Existe una cámara en la entrada del centro de datos, pero no está vigilada por personal dentro del mismo centro de datos.
- No cuenta con guardias de seguridad por motivo que se encuentra dentro de otro departamento.
- Los equipos informáticos cuentan con un sistema de alimentación ininterrumpida (UPS).
- Cuenta con un sistema de control de temperatura y humedad para garantizar condiciones óptimas de operación de los equipos.
- El centro de datos cuenta con 2 extintores contra incendios colocados en áreas estratégicas.
- No cuenta con sistemas de detección de intrusiones físicas de personal no autorizado.
- La entrada del centro de datos no cuenta con una puerta de seguridad adecuada para la protección de los activos.

- Cuenta con un sistema de ventilación y refrigeración que controla la temperatura de los equipos informáticos.

Lógicos

- No cuenta con un firewall en hardware, sin embargo, si con un firewall en software implementado en Linux.
- No cuenta con una gestión de incidentes, cambios y problemas.
- La red posee una topología estrella.
- No tiene configuración de VLANs en sus equipos.
- Cuenta con configuraciones de almacenamiento en NAS (Network Attached Storage).
- No cuenta con la implementación de RAID es la configuración de los servidores.
- Los sistemas operativos que manejan los servidores son en su mayoría de distribución LINUX (CentOS).
- El entorno de virtualización que se usan en los servidores es Proxmox Virtual Environment.

Anexo 7: Fichas de recolección de información de activos

[IS] Servicios Internos

Servicio [IS]	
Nombre:	
Descripción:	
Estado	Activo ( ) Inactivo ( )
Responsable:	

Equipamiento

[SW] Aplicaciones

Aplicaciones [SW]	
Nombre:	
Descripción:	
Estado:	
Función:	
Responsable:	
Ubicación:	

[HW] Hardware

Equipos [HW]		
Nombre:		
Descripción:		
Detalle	Memoria RAM	
	Disco Duro	
	Sistema Operativo	
	Estado	Activo ( ) Inactivo ( )
Función:		
Responsable:		
Ubicación:		

[COM] Comunicaciones

Redes de comunicación [COM]	
Nombre:	
Descripción:	
Función:	

Responsable:	
Ubicación:	

[AUX] Elementos Auxiliares

Elementos Auxiliares [AUX]	
Nombre:	
Descripción:	
Función:	
Responsable:	
Ubicación:	

[L] Instalaciones

Instalaciones [L]	
Nombre:	
Descripción:	
Función:	
Responsable:	
Ubicación:	

[P] Personal

Personal [P]	
Nombre:	
Descripción:	
Función:	

Anexo 8: Ficha Técnica Servidores, Switch y Router

HP ProLiant DL560 Gen10 Server Producción	
Producto / Características	Descripción
Modelo:	ProLiant DL560
Memoria:	512 GB
Fuente de alimentación:	205W
Controlador de red:	Optional FlexibleLOM
Tipo de memoria:	HPE DDR4 Smart Memory
Ranuras de memoria:	48 DIMM slots como máximo
Tipo de fuente de	4 HPE Flexible Slot Power Supplies
Procesador:	Intel® Xeon® Scalable 8268
Velocidad del procesador:	2.9 GHz
Controlador de	HPE Smart Array S100i
Sistema Operativo:	Proxmox
Estado:	Activo
Función:	Servidor de producción (Virtualización)
Ubicación:	Rack - Data Center
Ranuras de expansión:	8 como máximo
Responsable:	Ing. Luis Chalen

Tabla 33. Información Técnica - HP Proliant DL560 [32]

IBM System x3200 M2	
Producto / Características	Descripción
Modelo:	X3200 M2
Memoria:	16 GB
Fuente de alimentación:	400W
Controlador de red:	Controlador Gigabit Ethernet integrado
Tipo de memoria:	DDR3 SDRAM DIMM memory
Ranuras de memoria:	5 DIMM slots como máximo

Almacenamiento:	SATA 4.5TB (6 x 750GB) SAS 1.8TB (6 x
Tipo de fuente de	Redundant Dual Power Supply
Procesador:	Intel® Xeon® X3210
Velocidad del procesador:	2.13 GHz
Controlador de	3.5-inch hot-swap
Sistema Operativo:	Centos 7
Estado:	Activo
Función:	Servidor de Aplicaciones
Ubicación:	Rack 3 - Data Center
Ranuras de expansión:	8 como máximo
Responsable:	Ing. Luis Chalen

Tabla 34. Información Técnica - IBM System x3200 M2 [33]

IBM System x3650	
Producto / Características	Descripción
Modelo:	x3650 T 7980
Memoria:	16 GB
Fuente de alimentación:	600W
Controlador de red:	Controlador Gigabit Ethernet integrado
Tipo de memoria:	DDR2 SDRAM DIMM memory
Ranuras de memoria:	5 DIMM slots como máximo
Almacenamiento:	SATA 4.5TB (6 x 750GB) SAS 1.8TB (6 x
Tipo de fuente de	Hot swap redundant power supplies
Procesador:	Intel® Xeon®
Velocidad del procesador:	3.2 GHz
Controlador de	Two 146.8 GB 10 000 rpm Ultra320 SCSI HDs
Sistema Operativo:	Centos 7
Estado:	Activo
Función:	Servidor NAS

Ubicación:	Rack 3- Data Center
Ranuras de expansión:	8 como máximo
Responsable:	Ing. Luis Chalen

Switch Administrable TL-SG3424 Gigabit L2 - 24 P	
Producto / Características	Descripción
Modelo:	TL-SG3424 SFP
Estándares y protocolos:	IEEE 802.3i, IEEE 802.3u, IEEE 802.3ab, IEEE802.3z, IEEE 802.3ad, IEEE 802.3x, IEEE 802.1d, IEEE 802.1s, IEEE 802.1w, IEEE 802.1q, IEEE 802.1x, IEEE 802.1p
Interface:	24 Puertos RJ45 10/100/1000Mbps (Negociación automática/Auto MDI/MDIX) 4 ranuras Combo SFP 100/1000Mbps 1 puerto de consola
Medios de red:	10BASE-T: UTP categoría 3, 4, 5 cables (100m máximo) 100BASE-TX / 1000Base-T: UTP categoría 5, 5e o superior de cable (100 metros como máximo) 1000BASE-X: MMF, SMF
Fuente de alimentación:	100~240VAC, 50/60Hz
Consumo de Poder:	Máximo: 23.3W (220V/50Hz)
Ancho de banda / plano	48Gbps
Tasa de reenvío de paquetes:	35.7Mpps

Procesador:	Intel® Xeon®
Tabla de direcciones MAC:	8K
VLAN:	Soporta hasta 4K VLAN simultáneamente (de 4K VLAN IDs) Puerto/MAC/VLAN basado en protocolo-GARP/GVRP
Requisitos del sistema:	Microsoft® Windows® 98SE, NT, 2000, XP, Vista™ or Windows 7, MAC® OS, NetWare®, UNIX® or Linux.
Estado:	Activo
Función:	Encaminador
Ubicación:	Rack 2- Data Center
Responsable:	Ing. Luis Chalen

Tabla 35. Información Técnica - Switch Administrable TL-SG3424 [34]

Switch Smart PoE T1600G-28PS SFP JetStream – 24 P	
Producto / Características	Descripción
Modelo:	T1600G-28PS (TL-SG2424P)
Estándares y protocolos:	IEEE 802.3i, IEEE 802.3u, IEEE 802.3ab, IEEE802.3z, IEEE 802.3ad, IEEE 802.3x, IEEE 802.1d, IEEE 802.1s, IEEE 802.1w, IEEE 802.1q, IEEE 802.1p, IEEE 802.1x
Interface:	24 Puertos RJ 45 10/100 / 1000Mbps (Auto Negociación/Auto MDI/MDIX) 4 Gigabit SFP Slots
Medios de red:	10BASE-T: UTP categoría 3, 4, 5 cable (máximo 100m)

	100BASE-TX/1000Base-T: UTP categoría 5, 5e or above cable (máximo 100m) 1000BASE-X: MMF, SMF
Fuente de alimentación:	100~240VAC, 50/60Hz
Consumo de Poder:	Máximo (PoE on): 264.8W (220V/50Hz)
Ancho de banda	56Gbps
Tasa de reenvío de paquetes:	41.7Mpps
Tabla de direcciones MAC:	16k
VLAN:	Admite hasta 4K VLAN simultáneamente (fuera de 4K VLAN ID)
Requisitos del sistema:	Microsoft® Windows® XP, Vista™ o Windows 7, Windows 8, MAC® OS, NetWare®, UNIX® o Linux.
Estado:	Activo
Función:	Encaminador
Ubicación:	Rack 2- Data Center
Responsable:	Ing. Luis Chalen

Tabla 36. Información Técnica - Switch Smart PoE TL-SG2424P [35]

Switch Inteligente (TL-SG2218) SFP JetStream – 16 P	
Producto / Características	Descripción
Modelo:	T TL-SG2218
Interface:	• Puertos RJ45 de 16 × 10/100/1000 Mbps • 2 ranuras Gigabit SFP
Fuente de alimentación:	100~240VAC, 50/60Hz
Consumo de Poder:	12.3 W (220 V/50 Hz)
Ancho de banda	36 Gbps
Tasa de reenvío de paquetes:	26.8 Mpps

Tabla de direcciones MAC:	8k
VLAN:	• Grupo de VLAN - Grupos máximos de VLAN 4K • VLAN etiquetada 802.1q • MAC VLAN: 12 entradas - QinQ basado en puertos - QinQ selectivo • VLAN de voz
Requisitos del sistema:	Microsoft® Windows® 98SE, NT, 2000, XP, Vista™ or Windows 7/8/10/11, MAC® OS, NetWare®, UNIX® or Linux.
Estado:	Activo
Función:	Encaminador
Ubicación:	Rack 1 - Data Center
Responsable:	Ing. Luis Chalen

Tabla 37. Información Técnica - Switch Inteligente (TL-SG2218) [36]

Cisco 1800 Series Router	
Producto / Características	Descripción
Modelo:	Cisco 1841
Aplicaciones de destino	Secure data
Factor de forma:	Desktop, 1-rack-unit (1RU) height (4.75 cm high with rubber feet)
DRAM:	DRAM de módulo de memoria dual en línea (DIMM) síncrono
Capacidad de memoria RAM	• Default: 256 MB

	• Máximo: 384 MB
Flash Memory:	External compact Flash
Flash Memory Capacity:	• Default: 64 MB • Máximo: 128 MB
Modular Slots-Total	Dos
Soporte de cifrado en software y hardware de forma predeterminada:	DES, 3DES, AES 128, AES 192, AES 256
Voltaje de entrada de CA:	100 a 240 VAC
Potencia de salida:	50W
Estado:	Activo
Función:	Router
Ubicación:	Rack 1 - Data Center
Responsable:	Ing. Luis Chalen

Tabla 38. Información Técnica - Cisco 1841 Router [37]

Anexo 9: Inventario de activos

Activos Del Data Center GAD		
[S] Servicios Internos		
Código	**Nombre**	**Detalle**
inter_GAD	Internet	CNT (Telconet) Fibra óptica - Servicio de 60 Megas
email_GAD	Servicio de Correo Institucional	Zimbra (Virtualizado – Linux CentOs)
pweb_GAD	Página Web Oficial	Página Web del GAD Municipal
[SW] Software		
email_client_GAD	Cliente de correo	Zimbra
email_server_GAD	Servidor Correo	Promox (Virtualizado – Linux CentOs)
dbms_GAD	Sistema BD	Oracle Database
si_admi_GAD	Sistema Administrativo	Java – Oracle – Virtualizado
sweb_GAD	Servicio Portal Web	PHP – JavaScript's – HTML – CSS – Bootstrap
so_servPr	SO Servidor de Producción	VMWare (Virtualización) – Linux – 64 bits – Versión 6
so_servApp	SO Servidor de Aplicaciones	CentOS – Linux – 64 bits – Versión 7

firewall_GAD	Firewall	ShoreWall – Linux – CentOs – Versión 5.2.8
controlAn_GAD	Sistema de control de Ancho de Banda	Squid – Linux – CentOS
dns_GAD	Servicio DNS	Dynamix Client
[HW] Hardware		
SRVP_GAD1	ServProducción1	HP ProLiant DL560 Gen10 Server (Promox V1)
SRVP _GAD2	ServProducción2	HP ProLiant DL560 Gen10 Server (Promox V2)
SRVP _GAD3	ServProducción3	HP ProLiant DL560 Gen10 Server (Promox V3)
SRVP _GAD4	ServProducción4	HP ProLiant DL560 Gen10 Server (Promox V4)
SRVP _GAD5	ServProducción5	HP ProLiant DL560 Gen10 Server (Promox V5)
SRVAP _GAD	Servidor de Aplicaciones	IBM System x3200 M2 (Aplicaciones)
snas_GAD	Servidor NAS	IBM System x3650 (NAS)
router_GAD1	Router1	Fortinet FortiGate 40F (Internet)
router_GAD2	Router2	Cisco 1800 Series Router (Internet)
switch_GAD1	Master Switch1 CORE	Switch Administrable TL-SG3424 Gigabit L2 SFP JetStream - 24 P

switch_GAD2	Switch2 – PB	Switch Administrable TL-SG3424 Gigabit L2 SFP JetStream - 24 P
switch_GAD3	Switch3 – P1	Switch Administrable TL-SG3424 Gigabit L2 SFP JetStream - 24 P
switch_GAD4	Switch4 – P2	Switch Administrable TL-SG3424 Gigabit L2 SFP JetStream - 24 P
switch_GAD5	Switch5 – PB1	Switch Smart PoE T1600G-28PS (TL-SG2424P) JetStream 24 P
switch_GAD6	Switch6 – PB2	Switch Smart PoE T1600G-28PS (TL-SG2424P) JetStream 24 P
switch_GAD7	Switch7 – P1	Switch Smart PoE T1600G-28PS (TL-SG2424P) JetStream 24 P
switch_GAD8	Switch8 – P1	Switch Smart PoE T1600G-28PS (TL-SG2424P) JetStream 24
switch_GAD9	Switch9 – P2	Switch Inteligente (TL-SG2218) SFP JetStream – 16 P
switch_GAD10	Switch10 – P2	Switch Inteligente (TL-SG2218) SFP JetStream – 16 P
tranFe_GAD	Transceiver	TP Link Transceiver MC111CS
[COM] Redes de Comunicaciones		
Internet_GAD	Internet	CNT (Telconet) Fibra óptica - Servicio de 60 Megas
LAN_GAD	Red Local	Topología Árbol - IPs Estáticas – Capacidad de transmisión 1 Gbit/s

WIFI_GAD	Red Inalámbrica	Red inalámbrica - Capacidad de transmisión 1 Gbit/s
[AUX] Equipamiento Auxiliar		
power_GAD	Fuente de Alimentación	Regleta de alimentación para switch y routers.
ups_GAD	Sistema de alimentación ininterrumpida	UPS COMPUTER POWER SERIES VTN – 10 KVA
cabling_GAD	Cableado Estructurado	Fibra Óptica / Cable Eléctrico
ac_GAD	Equipos de Climatización	
cam_GAD	Cámaras de Seguridad	Hikvision DS-2CD2147G2(SU)
[MEDIA] Soportes de información		
disk_GAD	Disco Duros	Dispositivo de almacenamiento – Soporte de información
[L] Instalaciones		
local_GAD	Cuarto de Servidores	Ancho: 2.60 m; Alto: 3.00m; Largo: 2.90m
[P] Personal		
cor_GAD	Coordinador/a Departamento de TIC	Encargado del departamento de sistemas y recursos tecnológicos.

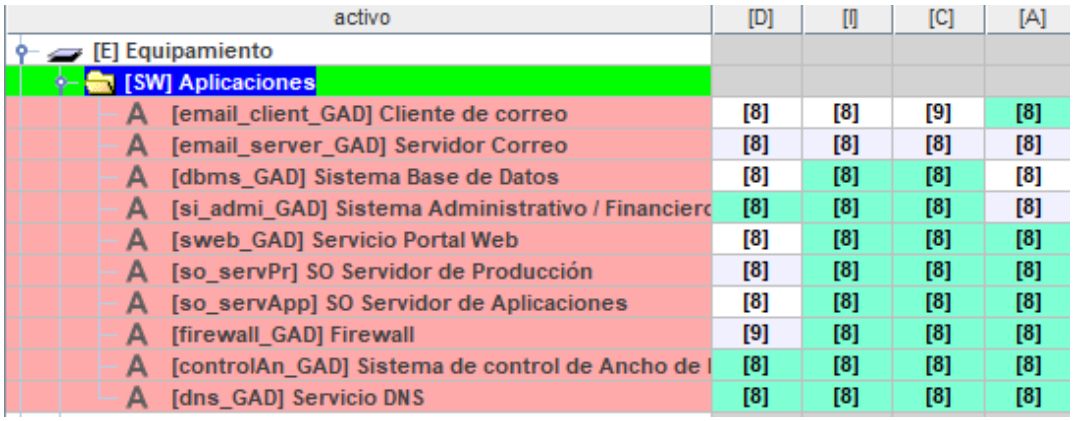
adm_GAD	Administrador de sistemas	Encargado del centro de cómputo de la Institución.
dba_GAD	Administrador de base de datos	Encargado de la administración de la base de datos.
des_GAD	Desarrolladores / Programadores	Encargados de la programación y desarrollo de sistemas.
te_GAD	Técnico Informático	Encargado de la electrónica y soporte al usuario.

Tabla 39. Inventario de Activos

Anexo 10: Valores Acumulados de Activos

activo	[D]	[I]	[C]	[A]
ACTIVOS				
[B] Activos esenciales				
[IS] Servicios internos				
[inter_GAD] Internet	[7]	[7]	[5]	[2]
[email_GAD] Servicio de Correo Institucional	[8]	[9]	[9]	[9]
[pweb_GAD] Página Web Oficial	[8]	[8]	[8]	[8]

Figura 30: Valor Acumulado - IS



activo	[D]	[I]	[C]	[A]
[E] Equipamiento				
[SW] Aplicaciones				
[email_client_GAD] Cliente de correo	[8]	[8]	[9]	[8]
[email_server_GAD] Servidor Correo	[8]	[8]	[8]	[8]
[dbms_GAD] Sistema Base de Datos	[8]	[8]	[8]	[8]
[si_admi_GAD] Sistema Administrativo / Financier	[8]	[8]	[8]	[8]
[sweb_GAD] Servicio Portal Web	[8]	[8]	[8]	[8]
[so_servPr] SO Servidor de Producción	[8]	[8]	[8]	[8]
[so_servApp] SO Servidor de Aplicaciones	[8]	[8]	[8]	[8]
[firewall_GAD] Firewall	[9]	[8]	[8]	[8]
[controlAn_GAD] Sistema de control de Ancho de	[8]	[8]	[8]	[8]
[dns_GAD] Servicio DNS	[8]	[8]	[8]	[8]

Figura 31: Valor Acumulado - SW

activo	[D]	[I]	[C]	[A]
[E] Equipamiento				
[SW] Aplicaciones				
[HW] Equipos				
[SVRP_GAD1] ServProducción1	[8]	[8]	[8]	[8]
[SRVP_GAD2] ServProducción2	[8]	[8]	[8]	[8]
[SRVP_GAD3] ServProducción3	[8]	[8]	[8]	[8]
[SRVP_GAD4] ServProducción4	[8]	[8]	[8]	[8]
[SRVP_GAD5] ServProducción5	[8]	[8]	[8]	[8]
[SRVAP_GAD] Servidor de Aplicaciones	[8]	[8]	[8]	[8]
[SRVN_GAD] Servidor NAS	[8]	[8]	[8]	[8]
[router_GAD1] Router1	[8]	[8]	[8]	[8]
[router_GAD2] Router2	[8]	[8]	[8]	[8]
[switch_GAD1] Master Switch1 CORE	[8]	[8]	[8]	[8]
[switch_GAD2] Switch2 - PB	[8]	[8]	[8]	[8]
[switch_GAD3] Switch3 - P1	[8]	[8]	[8]	[8]
[switch_GAD4] Switch4 - P2	[8]	[8]	[8]	[8]
[switch_GAD5] Switch5 - PB1	[8]	[8]	[8]	[8]
[switch_GAD6] Switch6 - PB	[8]	[8]	[8]	[8]
[switch_GAD7] Switch7 - P1	[8]	[8]	[8]	[8]
[switch_GAD8] Switch8 - P1	[8]	[8]	[8]	[8]
[switch_GAD9] Switch9 - P2	[8]	[8]	[8]	[8]
[switch_GAD10] Switch10 - P2	[8]	[8]	[8]	[8]
[tranFe_GAD] Transceiver	[8]	[8]	[8]	[8]

Figura 32: Valor Acumulado - HW

activo	[D]	[I]	[C]	[A]
[IS] Servicios internos				
[E] Equipamiento				
[SW] Aplicaciones				
[HW] Equipos				
[COM] Comunicaciones				
[Internet_GAD] Internet	[8]	[8]	[8]	[8]
[LAN_GAD] Red Local	[8]	[8]	[8]	[8]
[WIFI_GAD] Red Inalámbrica	[8]	[8]	[8]	[8]
[PSTN_GAD] Telefonia IP	[7]	[7]	[7]	[2]
[AUX] Elementos auxiliares				
[power_GAD] Fuente de Alimentación	[8]	[8]	[7]	[8]
[ups_GAD] Sistema de alimentación ininterrumpid	[8]	[8]	[7]	[8]
[cabling_GAD] Cableado Estructurado	[8]	[8]	[7]	[8]
[ac_GAD] Equipos de Climatización	[8]	[8]	[7]	[8]
[cam_GAD] Cámaras de Seguridad	[8]	[8]	[7]	[8]
[Media] Soportes de Información				
[disk_GAD] Discos Duros	[8]	[8]	[8]	[8]
[L] Instalaciones				
[local_GAD] Cuarto de Servidores	[8]	[8]	[7]	[8]
[P] Personal				
[cor_GAD] Coordinador/a Departamento de TIC	[7]		[4]	
[adm_GAD] Administrador de sistemas	[8]	[8]	[8]	[8]
[dba_GAD] Administrador de base de datos	[8]	[8]	[7]	[8]
[des_GAD] Desarrolladores / Programadores	[8]	[8]	[7]	[8]

Figura 33: Valor Acumulado - COM - AUX - Media - L - P

Anexo 11: Identificación y Valoración de Amenazas

Valorización de las amenazas activo [inter_GAD] Internet

Amenazas	Prob	[D]	[I]	[C]	[A]
[I.8] Fallo de servicios de comunicaciones	0,1	40%			
[E.1] Errores de usuarios	1	10%	10%	10%	
[E.24] Caída del sistema por agotamiento de recursos	0,1	20%			

Valorización de las amenazas activo [email_GAD] Servicio Correo Institucional

Amenazas	Prob	[D]	[I]	[C]	[A]
[E.1] Errores de los usuarios	1	10%	10%	10%	10%
[E.2] Errores del administrador del sistema	1	10%	20%	20%	10%
[E.4] Errores de configuración	1	5%			
[E.15] Alteración de la información	1	1%	50%	50%	
[E.19] Fugas de información	0,01	1%	40%	20%	
[E.24] Caída del sistema por agotamiento de recursos	0,1	50%			
[A.5] Suplantación de identidad	0,1	5%		20%	60%
[A.7] Uso no previsto	1	10%	10%		
[A.8] Difusión de software dañino	0,01	10%	20%	40%	
[A.11] Acceso no autorizado	1		10%	50%	100%
[A.24] Denegación de servicios	0,1				
[A.30] Ingeniería Social	1		5%	40%	10%

Valorización de las amenazas activo [pweb_GAD] Página Web Oficial

Amenazas	Prob	[D]	[I]	[C]	[A]
[E.1] Errores de los usuarios	1	10%	10%	10%	10%
[E.2] Errores del administrador del sistema	1	20%	20%	20%	10%
[E.15] Alteración de la información	1		5%		
[E.18] Destrucción de información	1	10%			
[E.19] Fugas de información	1		5%	10%	
[E.24] Caída del sistema por agotamiento de recursos	1	50%			
[A.5] Suplantación de identidad	1		50%	50%	80%
[A.6] Abuso de privilegios de acceso	1	1%	10%	10%	60%
[A.7] Uso no privilegiado	1	1%	10%	10%	
[A.11] Acceso no autorizado	1		10%	50%	60%
[A.11] Modificación de información	1		50%		
[A.18] Destrucción de información	1	50%			
[A.24] Denegación de servicios	0,1	50%			

Valorización de las amenazas activo [email_client_GAD] Cliente de Correo

Amenazas	Prob	[D]	[I]	[C]	[A]
[I.5.1] Averías de origen lógico	1	50%			
[E.8] Difusión de software dañino	1	10%	10%	10%	
[E.20] Vulnerabilidades de los programas	1	1%	20%	20%	
[E.21] Errores de mantenimiento / actualizaciones	1	1%	10%	20%	
[A.8] Difusión de software dañino	0,1	20%	20%	20%	
[A.22] Manipulación de programas	0,1	50%	20%	20%	

Valorización de las amenazas activo [email_server_GAD] Servidor de correo

Amenazas	Prob	[D]	[I]	[C]	[A]
[I.5.1] Averías de origen lógico	1	50%			
[E.8] Difusión de software dañino	1	10%	10%	10%	
[E.20] Vulnerabilidades de los programas	1	1%	20%	20%	
[E.21] Errores de mantenimiento / actualizaciones	1	1%	10%	20%	
[A.8] Difusión de software dañino	0,1	60%	20%	20%	
[A.22] Manipulación de programas	0,1	50%	20%	20%	

Valorización de las amenazas activo [dbms_GAD] Sistema Gestor de Base de datos

Amenazas	Prob	[D]	[I]	[C]	[A]
[I.5.1] Averías de origen lógico	1	50%			
[E.3] Errores de monitorización	1		40%		
[E.4] Errores de configuración	1	20%			
[E.8] Difusión de software dañino	0,1	10%	10%	10%	
[E.15] Alteración de la información	1		60%	60%	
[E.18] Destrucción de la información	1	70%	60%	60%	
[E.19] Fugas de información	1			10%	
[E.20] Vulnerabilidades de los programas	0,1	1%	20%	20%	
[E.21] Errores de mantenimiento / actualizaciones	1	1%	10%	50%	
[A.3] Manipulación de los registros de actividad	1		50%		
[A.4] Manipulación de los ficheros de configuración	0,1	10%	10%	10%	10%
[A.5] Suplantación de identidad	0,1		10%	50%	60%
[A.6] Abuso de privilegios de acceso	0,1	1%	10%	50%	
[A.8] Difusión de software dañino	0.1	20%	20%	20%	
[A.11] Acceso no autorizado	1		10%	50%	
[A.22] Manipulación de programas	0,1	50%	30%	20%	

Valorización de las amenazas activo [si_admi_GAD] Sistema Administrativo/ Financiero

Amenazas	Prob	[D]	[I]	[C]	[A]
[I.5.1] Averías de origen lógico	0,1	50%			

[E.1] Errores de usuarios	1	10%	10%		
[E.4] Errores de configuración	1	10%	5%		
[E.8] Difusión de software dañino	0,1	10%	10%	10%	
[E.15] Alteración de la información	1		60%	60%	1%
[E.18] Destrucción de la información	1	30%	60%	60%	
[E.19] Fugas de información	0,1			10%	
[E.20] Vulnerabilidades de los programas	1	1%	20%	20%	
[E.21] Errores de mantenimiento / actualizaciones	1	1%	10%	50%	
[A.4] Manipulación de los ficheros de configuración	0,1	10%	10%	10%	
[A.5] Suplantación de identidad	1		30%	30%	60%
[A.6] Abuso de privilegios de acceso	0,1	1%	10%	10%	20%
[A.7] Uso no previsto	1	1%	10%	10%	
[A.8] Difusión de software dañino	0.1	20%	20%	20%	
[A.11] Acceso no autorizado	1		10%	50%	60%
[A.24] Denegación de servicios	0,1	50			

Valorización de las amenazas activo [sweb_GAD] Servicio Portal Web

Amenazas	Prob	[D]	[I]	[C]	[A]
[I.5.1] Averías de origen lógico	1	50%			
[E.8] Difusión de software dañino	1	10%	10%	10%	
[E.20] Vulnerabilidades de los programas	1	1%	20%	20%	
[E.21] Errores de mantenimiento / actualización	1	1%	10%	20%	
[A.8] Difusión de software dañino	0,1	60%	20%	20%	
[A.22] Manipulación de programas	0,1	50%	20%	20%	

Valorización de las amenazas activo [so_servPr] SO Servidor de Producción

Amenazas	Prob	[D]	[I]	[C]	[A]
[I.5.1] Averías de origen lógico	1	50%			
[E.8] Difusión de software dañino	1	10%		10%	
[E.20] Vulnerabilidades de los programas	1	1%		20%	
[E.21] Errores de mantenimiento / actualización	1	1%		50%	
[A.8] Difusión de software dañino	0,1	60%		20%	
[A.22] Manipulación de programas	0,1	50%		20%	

Valorización de las amenazas activo [so_servApp] SO Servidor de Aplicaciones

Amenazas	Prob	[D]	[I]	[C]	[A]
[I.5.1] Averías de origen lógico	1	50%			
[E.8] Difusión de software dañino	1	10%		10%	
[E.20] Vulnerabilidades de los programas	1	1%		20%	
[E.21] Errores de mantenimiento / actualización	1	1%		50%	
[A.8] Difusión de software dañino	0,1	60%		20%	
[A.22] Manipulación de programas	0,1	50%		20%	

Valorización de las amenazas activo [firewall_GAD] Firewall

Amenazas	Prob	[D]	[I]	[C]	[A]
[I.5.1] Averías de origen lógico	1	50%			
[E.8] Difusión de software dañino	1	10%	10%	10%	
[E.20] Vulnerabilidades de los programas	1	1%	20%	20%	
[E.21] Errores de mantenimiento / actualización	1	1%	10%	20%	
[A.8] Difusión de software dañino	0,1	60%	20%	20%	
[A.22] Manipulación de programas	0,1	50%	20%	20%	

Valorización de las amenazas activo [dns_GAD] Servicio DNS

Amenazas	Prob	[D]	[I]	[C]	[A]
[I.5.1] Averías de origen lógico	1	50%			
[E.8] Difusión de software dañino	1	10%	10%	10%	
[E.20] Vulnerabilidades de los programas	1	1%	20%	20%	
[E.21] Errores de mantenimiento / actualización	1	1%	10%	20%	
[A.8] Difusión de software dañino	0,1	60%	20%	20%	
[A.22] Manipulación de programas	0,1	50%	20%	20%	
[A.24] Denegación de servicio	0,1	50%			

Valorización de las amenazas activo [SRVP_GAD] Servidor de Producción - HP ProLiant DL560 Gen10 Server (Promox)

Amenazas	Prob	[D]	[I]	[C]	[A]
[N.1] Fuego	0,1	100%			
[N.2] Daños por agua	0,1	50%			
[I.1] Fuego	0,5	100%			
[I.2] Daños por agua	0,5	50%			
[I.5.2] Avería de origen físico	1	50%			
[I.6] Corte de suministro eléctrico	1	100%			
[I.7] Condiciones inadecuadas de temperatura	1	100%			
[E.4] Errores de configuración					
[E.15] Alteración de la información					
[E.18] Destrucción de la información					
[E.23] Errores de mantenimiento / actualización	1	10%	10%	50%	
[E.24] Caída del sistema por agotamiento de recursos	1	50%			
[E.25] Pérdida de equipos	1	100%		100%	
[A.4] Manipulación de los ficheros de configuración	0,1	10%	10%	10%	
[A.6] Abuso de privilegios de acceso	1	10%	100%	100%	
[A.7] Uso no previsto	1	10%	10%	100%	
[A.11] Acceso no autorizado	1	10%	100%	100%	
[A.23] Manipulación de hardware	0,5	50%		50%	
[A.24] Denegación de servicios	1	100%			
[A.25] Robo de equipos	0,5	100%		100%	
[A.26] Ataque destructivo	0,5	100%			

Valorización de las amenazas activo [SRVAP_GAD] Servidor de Aplicaciones - IBM System x3200 M2 (Aplicaciones)

Amenazas	Prob	[D]	[I]	[C]	[A]
[N.1] Fuego	0,1	100%			
[N.2] Daños por agua	0,1	50%			
[I.1] Fuego	0,5	100%			
[I.2] Daños por agua	0,5	50%			
[I.5.2] Avería de origen físico	1	50%			
[I.6] Corte de suministro eléctrico	1	100%			
[I.7] Condiciones inadecuadas de temperatura	1	100%			
[E.4] Errores de configuración					
[E.15] Alteración de la información					
[E.18] Destrucción de la información					
[E.23] Errores de mantenimiento / actualización	1	10%	10%	50%	
[E.24] Caída del sistema por agotamiento de recursos	10	50%			
[E.25] Pérdida de equipos	1	100%		100%	
[A.4] Manipulación de los ficheros de configuración	1	10%	10%	10%	
[A.6] Abuso de privilegios de acceso	1	10%	100%	100%	
[A.7] Uso no previsto	1	10%	10%	100%	
[A.11] Acceso no autorizado	1	10%	100%	100%	
[A.23] Manipulación de hardware	0,5	50%			
[A.24] Denegación de servicios	1	100%			
[A.25] Robo de equipos	0,5	100%		100%	
[A.26] Ataque destructivo	1	100%			

Valorización de las amenazas activo [SRVN_GAD] Servidor NAS - IBM System x3650 (NAS)

Amenazas	Prob	[D]	[I]	[C]	[A]
[N.1] Fuego	0,1	100%			
[N.2] Daños por agua	0,1	50%			
[I.1] Fuego	0,5	100%			
[I.2] Daños por agua	0,5	50%			
[I.5.2] Avería de origen físico	1	50%			
[I.6] Corte de suministro eléctrico	1	100%			
[I.7] Condiciones inadecuadas de temperatura	1	100%			
[I.10] Degradación de los soportes de almacenamiento					
[E.15] Alteración de la información					
[E.18] Destrucción de la información					
[E.23] Errores de mantenimiento / actualización	1	10%	10%	50%	
[E.24] Caída del sistema por agotamiento de recursos	1	50%			
[E.25] Pérdida de equipos	1	100%		100%	
[A.4] Manipulación de los ficheros de configuración	0,1	10%	10%	10%	
[A.7] Uso no previsto	1	10%	10%	50%	
[A.11] Acceso no autorizado	1	10%	100%	50%	
[A.15] Modificación de la información					
[A.23] Manipulación de hardware	0,5	50%			
[A.24] Denegación de servicios	1	100%			
[A.25] Robo de equipos	0,5	100%		100%	
[A.26] Ataque destructivo	1	100%			

Valorización de las amenazas activo [router_GAD1] Router1 - Fortinet FortiGate 40F (Internet)

Amenazas	Prob	[D]	[I]	[C]	[A]
[N.1] Fuego	0,1	100%			
[N.2] Daños por agua	0,1	50%			
[I.1] Fuego	0,5	100%			
[I.2] Daños por agua	0,5	50%			
[I.5.2] Avería de origen físico	1	50%			
[I.6] Corte de suministro eléctrico	1	100%			
[I.7] Condiciones inadecuadas de temperatura	1	100%			
[E.4] Errores de configuración					
[E.23] Errores de mantenimiento / actualización	1	10%	10%	50%	
[E.24] Caída del sistema por agotamiento de recursos	10	50%			
[E.25] Pérdida de equipos	1	100%		50%	
[A.4] Manipulación de los ficheros de configuración	1	10%	10%	10%	
[A.7] Uso no previsto	1	10%	10%	100%	
[A.11] Acceso no autorizado	1	10%	10%	100%	
[A.23] Manipulación de hardware	0,5	50%			
[A.24] Denegación de servicios	0,5	100%			
[A.25] Robo de equipos	0,5	50%		100%	
[A.26] Ataque destructivo	1	100%			

Valorización de las amenazas activo [router_GAD2] Router2 - Cisco 1800 Series Router

Amenazas	Prob	[D]	[I]	[C]	[A]
[N.1] Fuego	0,1	100%			
[N.2] Daños por agua	0,1	50%			
[I.1] Fuego	0,5	100%			
[I.2] Daños por agua	0,5	50%			
[I.5.2] Avería de origen físico	1	50%			
[I.6] Corte de suministro eléctrico	1	100%			
[I.7] Condiciones inadecuadas de temperatura	1	100%			
[E.23] Errores de mantenimiento / actualización	1	10%	10%	50%	
[E.24] Caída del sistema por agotamiento de recursos	1	50%			
[E.25] Pérdida de equipos	1	100%		50%	
[A.4] Manipulación de los ficheros de configuración	0,1	10%	10%	10%	
[A.7] Uso no previsto	1	10%	10%	100%	
[A.11] Acceso no autorizado	1	10%	10%	100%	
[A.23] Manipulación de hardware	0,5	50%		20%	
[A.24] Denegación de servicios	0,5	100%			
[A.25] Robo de equipos	1	50%		100%	
[A.26] Ataque destructivo	0,1	100%			

Valorización de las amenazas activo [switch_GAD1] Switch Administrable TL TL-SG3424 Gigabit L2 SFP JetStream - 24 P

Amenazas	Prob	[D]	[I]	[C]	[A]
[N.1] Fuego	0,1	100%			

[N.2] Daños por agua	0,1	50%			
[I.1] Fuego	0,5	100%			
[I.2] Daños por agua	0,5	50%			
[I.5.2] Avería de origen físico	1	50%			
[I.6] Corte de suministro eléctrico	1	100%			
[I.7] Condiciones inadecuadas de temperatura	1	100%			
[E.23] Errores de mantenimiento / actualización	1	10%	10%	50%	
[E.24] Caída del sistema por agotamiento de recursos	1	50%			
[E.25] Pérdida de equipos	1	20%		100%	
[A.4] Manipulación de los ficheros de configuración	0,1	10%	10%	10%	
[A.6] Abuso de privilegios de acceso	1	10%	100%	100%	
[A.7] Uso no previsto	1	10%	10%	100%	
[A.11] Acceso no autorizado	0,5	10%	10%	100%	
[A.23] Manipulación de hardware	0,5	50%		20%	
[A.24] Denegación de servicios	1	100%			
[A.25] Robo de equipos	0,1	50%		100%	
[A.26] Ataque destructivo	0,1	100%			

Valorización de las amenazas activo [switch_GAD5] Switch Smart PoE T1600G-28PS (TL-SG2424P) JetStream 24 P

Amenazas	Prob	[D]	[I]	[C]	[A]
[N.1] Fuego	0,1	100%			
[N.2] Daños por agua	0,1	50%			
[I.1] Fuego	0,5	100%			
[I.2] Daños por agua	0,5	50%			
[I.5.2] Avería de origen físico	1	50%			
[I.6] Corte de suministro eléctrico	1	100%			
[I.7] Condiciones inadecuadas de temperatura	1	100%			
[E.23] Errores de mantenimiento / actualización	1	10%	10%	50%	
[E.24] Caída del sistema por agotamiento de recursos	1	50%			
[E.25] Pérdida de equipos	1	20%		50%	
[A.4] Manipulación de los ficheros de configuración	0,1	10%	10%	10%	
[A.7] Uso no previsto	1	10%	50%	10%	
[A.11] Acceso no autorizado	1	10%	10%	50%	
[A.23] Manipulación de hardware	0,5	100%		20%	
[A.24] Denegación de servicios	0,5	100%			
[A.25] Robo de equipos	1	20%		100%	
[A.26] Ataque destructivo	0,1	100%			

Valorización de las amenazas activo [switch_GAD9] Switch Inteligente (TL-SG2218) SFP JetStream – 16 P

Amenazas	Prob	[D]	[I]	[C]	[A]
[N.1] Fuego	0,1	100%			
[N.2] Daños por agua	0,1	50%			
[I.1] Fuego	0,5	100%			
[I.2] Daños por agua	0,5	50%			
[I.5.2] Avería de origen físico	1	50%			
[I.6] Corte de suministro eléctrico	1	100%			
[I.7] Condiciones inadecuadas de temperatura	1	100%			
[E.23] Errores de mantenimiento / actualización	1	10%	10%	50%	

[E.24] Caída del sistema por agotamiento de recursos	1	50%			
[E.25] Pérdida de equipos	1	20%		50%	
[A.4] Manipulación de los ficheros de configuración	0,1	10%	10%	10%	
[A.7] Uso no previsto	1	10%	50%	10%	
[A.11] Acceso no autorizado	1	10%	10%	50%	
[A.23] Manipulación de hardware	0,5	50%		20%	
[A.24] Denegación de servicios	0,5	100%			
[A.25] Robo de equipos	1	20%		50%	
[A.26] Ataque destructivo	0,1	100%			

Valorización de las amenazas activo [tranFe_GAD] Transceiver

Amenazas	Prob	[D]	[I]	[C]	[A]
[N.1] Fuego	0,1	100%			
[N.2] Daños por agua	0,1	50%			
[I.1] Fuego	0,5	100%			
[I.2] Daños por agua	0,5	50%			
[I.5.2] Avería de origen físico	1	50%			
[I.6] Corte de suministro eléctrico	1	100%			
[I.7] Condiciones inadecuadas de temperatura	1	100%			
[E.23] Errores de mantenimiento / actualización	1	10%	10%	50%	
[E.24] Caída del sistema por agotamiento de recursos	1	50%			
[E.25] Pérdida de equipos	1	20%		50%	
[A.7] Uso no previsto	1	10%	50%	10%	
[A.11] Acceso no autorizado	1	10%	10%	50%	
[A.23] Manipulación de hardware	0,5	50%		20%	
[A.25] Robo de equipos	0,5	20%		50%	

Valorización de las amenazas activo [internet_GAD] Internet

Amenazas	Prob	[D]	[I]	[C]	[A]
[I.8] Fallo de servicios de comunicaciones	1	50%			
[E.2] Errores del administrador del sistema	1	20%	20%	20%	
[E.9] Errores de [re-]encaminamiento	1			10%	
[E.10] Errores de secuencia	1		10%		
[E.24] Caída del sistema por agotamiento de recursos	0,1	50%			
[A.4] Manipulación de los ficheros de configuración	0,1	50%			
[A.7] Uso no previsto	1	10%	10%	10%	
[A.10] Alteración de secuencia	1		10%		
[A.11] Acceso no autorizado	1		10	50%	50%
[A.12] Análisis de trafico	1			2%	
[A.24.1] Saturación de los canales de información	1	20%		10%	

Valorización de las amenazas activo [LAN_GAD] Red Local

Amenazas	Prob	[D]	[I]	[C]	[A]
[I.8] Fallo de servicios de comunicaciones	1	50%			
[E.2] Errores del administrador del sistema	1	20%	20%	20%	

[E.9] Errores de [re-]encaminamiento	1			10%	
[E.10] Errores de secuencia	1		10%		
[E.15] Alteración de la información	0,1		1%		
[E.19] Fugas de información	0,1			10%	
[E.24] Caída del sistema por agotamiento de recursos	1	50%			
[A.4] Manipulación de los ficheros de configuración	0,1	50%			
[A.7] Uso no previsto	1	10%	10%	10%	
[A.11] Acceso no autorizado	1		10	50%	50%
[A.12] Análisis de trafico	1			2%	
[A.14] Interceptación de información	0,1			10%	
[A.15] Modificación de la información	0,1		10%		
[A.18] Destrucción de la información	1	50%			
[A.24] Denegación de servicios	0,1	50%			
[A.24.1] Saturación de los canales de información	1	20%		10%	

Valorización de las amenazas activo [WIFI_GAD] Red Inalámbrica

Amenazas	Prob	[D]	[I]	[C]	[A]
[I.8] Fallo de servicios de comunicaciones	1	50%			
[E.2] Errores del administrador del sistema	1	20%	20%	20%	
[E.9] Errores de [re-]encaminamiento	1			10%	
[E.15] Alteración de la información	0,1		1%		
[E.19] Fugas de información	0,1			10%	
[E.24] Caída del sistema por agotamiento de recursos	0,1	50%			
[A.5] Suplantación de identidad	1				
[A.7] Uso no previsto	1	10%	10%	10%	
[A.11] Acceso no autorizado	1		10%	50%	50%
[A.12] Análisis de trafico	1			2%	
[A.24] Denegación de servicios	0,1	50%			
[A.24.1] Saturación de los canales de información	1	20%		10%	

Valorización de las amenazas activo [PSTN_GAD] Telefonía IP

Amenazas	Prob	[D]	[I]	[C]	[A]
[I.8] Fallo de servicios de comunicaciones	1	50%			
[E.2] Errores del administrador del sistema	1	20%	20%	20%	
[E.9] Errores de [re-]encaminamiento	1			10%	
[E.24] Caída del sistema por agotamiento de recursos	0,1	50%			
[A.5] Suplantación de identidad	1				
[A.7] Uso no previsto	1	10%	10%	10%	
[A.12] Análisis de trafico	1			2%	

Valorización de las amenazas activo [power_GAD] Fuente de alimentación

Amenazas	Prob	[D]	[I]	[C]	[A]
[N.1] Fuego	0,1	70%			
[N.2] Daños por agua	0,1	50%			

[I.1] Fuego	0,5	70%			
[I.2] Daños por agua	0,5	50%			
[I.7] Condiciones inadecuadas de temperatura	1	20%			
[E.23] Errores de mantenimiento / actualización	1	10%			
[A.7] Uso no previsto	1	50%			
[A.23] Manipulación de hardware	1	50%			
[A.25] Robo de equipos	0,5	90%			
[A.26] Ataque destructivo	0,1	90%			

Valorización de las amenazas activo [ups_GAD] Sistema de alimentación ininterrumpida

Amenazas	Prob	[D]	[I]	[C]	[A]
[N.1] Fuego	0,1	1%			
[N.2] Daños por agua	0,1	1%			
[I.1] Fuego	0,5	1%			
[I.2] Daños por agua	0,5	1%			
[I.3]Contaminación medioambiental	0,1	1%			
[I.7] Condiciones inadecuadas de temperatura	1	1%			
[E.23] Errores de mantenimiento / actualización	1	1%			
[A.7] Uso no previsto	1	1%			
[A.23] Manipulación de hardware	1	1%			
[A.25] Robo de equipos	0,5	1%			
[A.26] Ataque destructivo	0,1	1%			

Valorización de las amenazas activo [cabling_GAD] Cableado Estructurado

Amenazas	Prob	[D]	[I]	[C]	[A]
[N.1] Fuego	0,1	70%			
[N.2] Daños por agua	0,1	50%			
[I.1] Fuego	0,5	70%			
[I.2] Daños por agua	0,5	50%			
[I.7] Condiciones inadecuadas de temperatura	1	20%			
[E.23] Errores de mantenimiento / actualización	0,1	10%			
[A.7] Uso no previsto	1	50%	1%	1%	
[A.11] Acceso no autorizado	1		10%	50%	
[A.23] Manipulación de hardware	1	50%		50%	
[A.25] Robo de equipos	0,8	70%			
[A.26] Ataque destructivo	0,1	60%			

Valorización de las amenazas activo [ac_GAD] Equipo de climatización

Amenazas	Prob	[D]	[I]	[C]	[A]
[N.1] Fuego	0,1	10%			
[N.2] Daños por agua	0,1	10%			
[I.1] Fuego	0,5	10%			
[I.2] Daños por agua	0,5	10%			
[I.6] Corte de suministro eléctrico	0,1	10%			
[I.7] Condiciones inadecuadas de temperatura	0,01	1%			
[I.9] Interrupción de otros servicios	1	10%			

[E.23] Errores de mantenimiento / actualización	1	10%			
[A.7] Uso no previsto	1	10%			
[A.23] Manipulación de hardware	1	10%			
[A.25] Robo de equipos	0,5	10%			
[A.26] Ataque destructivo	0,1	10%			

Valorización de las amenazas activo [cam_GAD] Cámaras de seguridad

Amenazas	Prob	[D]	[I]	[C]	[A]
[N.1] Fuego	0,1	70%			
[N.2] Daños por agua	0,1	50%			
[I.1] Fuego	0,5	70%			
[I.2] Daños por agua	0,5	50%			
[I.6] Corte de suministro eléctrico	1	60%			
[E.23] Errores de mantenimiento / actualización	1	10%			
[A.7] Uso no previsto	1	50%	10%	20%	
[A.23] Manipulación de hardware	1	50%		50%	
[A.25] Robo de equipos	0,5	60%		10%	
[A.26] Ataque destructivo	1	60%			

Valorización de las amenazas activo [disk_GAD] Discos Duros

Amenazas	Prob	[D]	[I]	[C]	[A]
[N.1] Fuego	0,1	80%			
[N.2] Daños por agua	0,1	50%			
[I.1] Fuego	0,5	80%			
[I.2] Daños por agua	0,5	50%			
[I.5.2] Avería de origen físico	1	50%			
[I.7] Condiciones inadecuadas de temperatura	1	60%			
[I.10] Degradación de los soportes de almacenamiento	1	60%			
[E.4] Errores de configuración	1		1%		
[E.15] Alteración de la información	1		1%		
[E.18] Destrucción de la información	1	70%			
[E.19] Fugas de información	1			10%	
[E.23] Errores de mantenimiento / actualización	0,1	20%	10%	50%	
[E.25] Pérdida de equipos	1	10%		50%	
[A.4] Manipulación de ficheros de configuración	1		10%	10%	
[A.7] Uso no previsto	1	1%		1%	
[A.11] Acceso no autorizado	1		1%	50%	
[A.15] Modificación de la información	1		50%		
[A.18] Destrucción de la información	1	70%			
[A.23] Manipulación de hardware	0,1	50%		50%	
[A.25] Robo de equipos	0,1	90%		20%	
[A.26] Ataque destructivo	0,1	10%			

Valorización de las amenazas activo [local_GAD] Cuarto de Servidores

Amenazas	Prob	[D]	[I]	[C]	[A]
[N.1] Fuego	0,1	70%			

[N.2] Daños por agua	0,1	50%			
[I.1] Fuego	0,5	70%			
[I.2] Daños por agua	0,5	50%			
[E.25] Pérdida de equipos					
[A.6] Abuso de privilegios de acceso					
[A.7] Uso no previsto	1	50%	10%	20%	
[A.25] Robo de equipos	0,5	60%		10%	
[A.26] Ataque destructivo	1	60%			

Valorización de las amenazas activo [cor_GAD] Coordinadora del Departamento de sistemas

Amenazas	Prob	[D]	[I]	[C]	[A]
[E.18] Destrucción de la información	1	1%			
[E.19] Fugas de información	0,1			1%	
[A.18] Destrucción de la información	1	10%			
[A.19] Revelación de información	0,1			1%	
[A.28] Indisponibilidad del personal	0,5	10%			
[A.29] Extorsión	0,9	10%		1%	
[A.30] Ingeniería social	0,5	10%		1%	

Valorización de las amenazas activo [adm_GAD] Administrador de sistemas

Amenazas	Prob	[D]	[I]	[C]	[A]
[E.18] Destrucción de la información	1	1%			
[E.19] Fugas de información	1			10%	
[E.28] Indisponibilidad del personal	1	10%			
[A.18] Destrucción de la información	1	10%			
[A.19] Revelación de información	1			50%	
[A.28] Indisponibilidad del personal	0,5	20%			
[A.29] Extorsión	0,9	50%		50%	
[A.30] Ingeniería social	0,5	50%		50%	

Valorización de las amenazas activo [dba_GAD] Administrador de base de datos

Amenazas	Prob	[D]	[I]	[C]	[A]
[E.18] Destrucción de la información	1	1%			
[E.19] Fugas de información	1			10%	
[E.28] Indisponibilidad del personal	1	10%			
[A.18] Destrucción de la información	1	10%			
[A.19] Revelación de información	10			50%	
[A.28] Indisponibilidad del personal	0,5	20%			
[A.29] Extorsión	0,9	1%		50%	
[A.30] Ingeniería social	0,5	1%		50%	

Valorización de las amenazas activo [des_GAD] Desarrolladores / Programadores

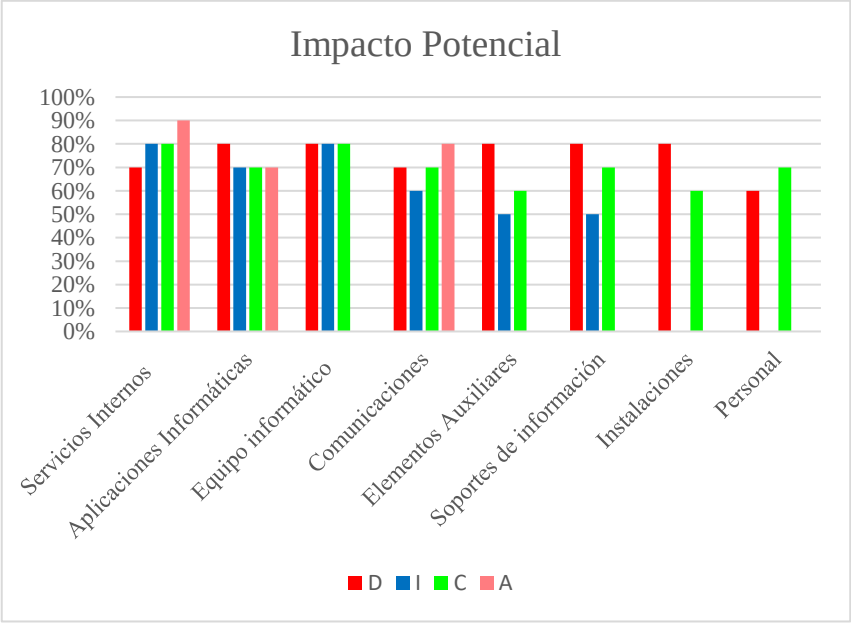
Amenazas	Prob	[D]	[I]	[C]	[A]
[E.18] Destrucción de la información	1	1%			
[E.19] Fugas de información	1			10%	
[E.28] Indisponibilidad del personal	1	10%			
[A.18] Destrucción de la información	1	10%			
[A.19] Revelación de información	10			20%	
[A.28] Indisponibilidad del personal	0,5	20%			
[A.29] Extorsión	0,1	1%		20%	
[A.30] Ingeniería social	0,5	1%		20%	

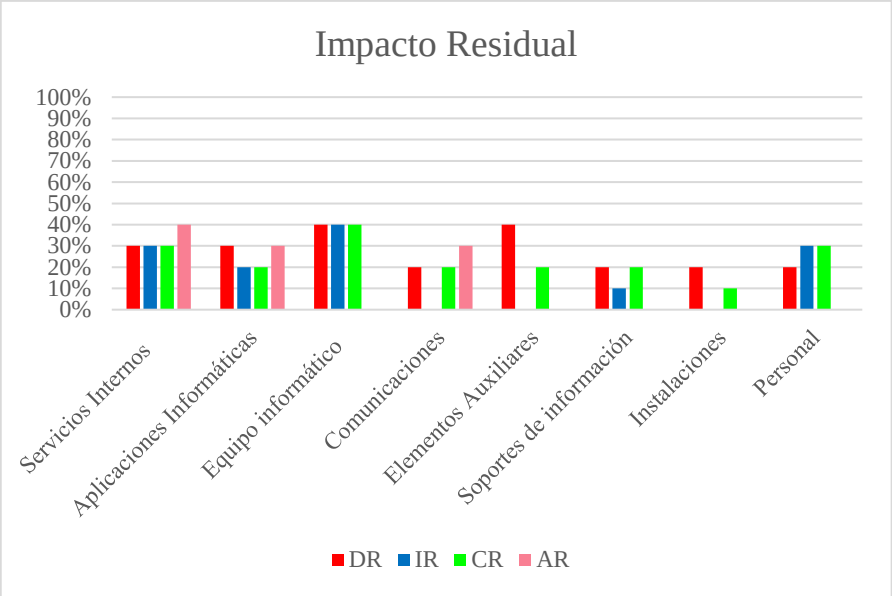
Anexo 12. Mejora de la seguridad: Disminución de los valores de impacto y riesgo

Indicador: Impacto Potencial y Residual

A continuación, se presentan los resultados de los valores de impacto y riesgo, con el objetivo de realizar el cálculo de cuanto mejoro la seguridad o en otras palabras cuanto disminuyo el impacto y riesgo.

Sin Salvaguardas								
Principios de la seguridad	Activos							
	[IS]	[SW]	[HW]	[COM]	[AUX]	[MEDIA]	[L]	[P]
D	7	8	8	8	8	8	8	6
I	8	7	8	6	5	5	0	7
C	8	7	8	7	6	7	6	7
A	9	7	0	8	0	6	0	0
Salvaguardas Implementadas								
DR	3	3	4	2	4	2	2	2
IR	3	2	4	0	0	1	0	3
CR	3	2	4	2	2	2	1	3
AR	4	3	0	3	0	0	0	0



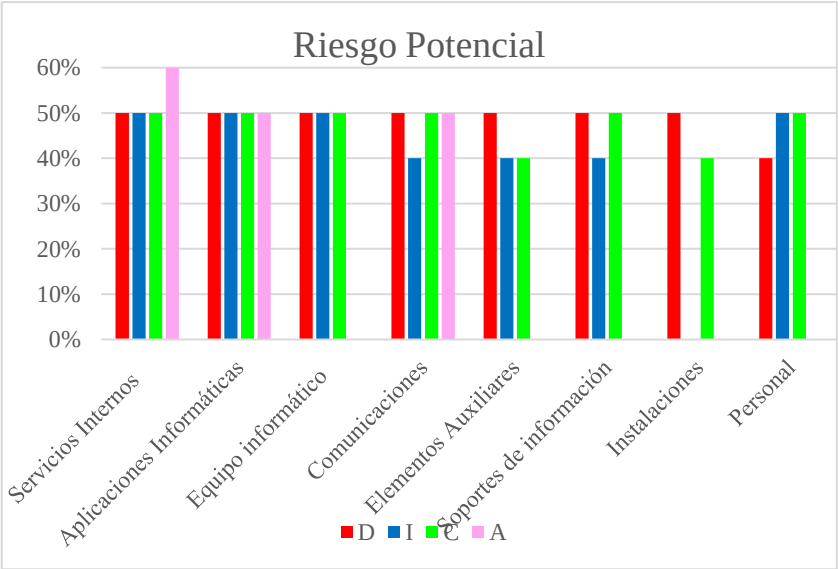


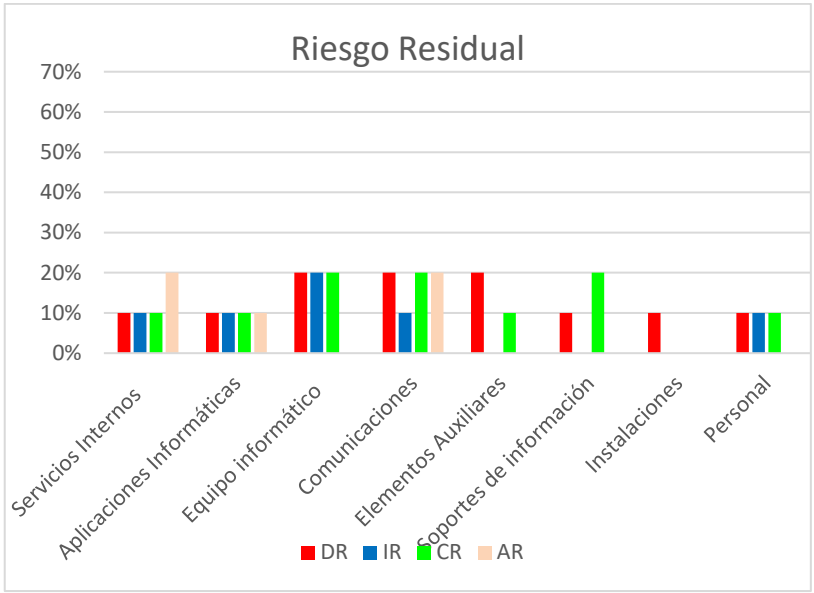
Interpretación:

En las figuras anteriores se observa el impacto potencial y residual en porcentajes de cada dimensión de seguridad valorada (Disponibilidad, Integridad, Confidencialidad y Autenticidad), para realizar el cálculo de la disminución del impacto se toma como referencia los valores del mismo que nos proporciona la herramienta PILAR, los cuales puedes ser observados en la fase de Estimación del Estado del riesgo. Al realizar un cálculo promedial se llegó al resultado que luego de la implementación de las salvaguardas respectivas el valor del impacto disminuyo un 40% aproximadamente.

Indicador: Riesgo Potencial y Residual

Sin Salvaguardas								
Principios de la seguridad	Activos							
	[IS]	[SW]	[HW]	[COM]	[AUX]	[MEDIA]	[L]	[P]
D	5	5	5	5	5	5	5	4
I	5	5	5	4	4	4	0	5
C	5	5	5	5	4	5	4	5
A	6	5	0	5	0	0	0	0
Salvaguardas Implementadas								
DR	1	1	2	2	2	1	1	1
IR	1	1	2	1	0	0	0	1
CR	1	1	2	2	1	2	0	1
AR	2	1	0	2	0	0	0	0





Interpretación:

De la misma manera con respecto a las figuras anteriores corresponden a la estimación del ambos tipo de riesgos, en donde se realiza el cálculo dando como resultado que el riesgo disminuye un 30% en la escala utilizada y un 50% aproximadamente en una escala de 10.

Anexo 13. Carta Aval de apertura de realización del trabajo de titulación

La Libertad
ALCALDÍA

DIRECCIÓN DE TALENTO HUMANO

La Libertad, 13 de mayo del 2024
Oficio Nº 162-DTH-GADMCLL-2024

José Sánchez Aquino, Mgtr.
Director de la Carrera de Tecnología de la Información
Facultad de Sistemas y Telecomunicaciones.
Universidad Estatal Península de Santa Elena
Presente.-

De mi consideración:

Reciba un cordial saludo, en atención al Oficio No. UPSE-CTI-115-2024-OF de fecha 07 de abril de 2024, solicitando la emisión de Carta Aval para que el estudiante Sr. ARIEL STEVEN BORBOR TUMBACO, realice su trabajo de titulación con el tema "DISEÑO DE PLAN INTEGRAL DE TRATAMIENTOS DE RIESGO INFORMÁTICOS EN DATA CENTER GUBERNAMENTAL APLICANDO MAGERT".

Por lo antes descrito se concede al Sr. ARIEL STEVEN BORBOR TUMBACO la apertura para realizar el trabajo de titulación en el área correspondiente.

Particular que comunico a usted para los fines a seguir.

Atentamente.

Abg. Estefanía Moreno Ponce
Directora de Talento Humano
GAD Municipal del cantón La Libertad

C.c. Archivo.-
jrm.-

Anexo 14. Plan de Tratamiento de Riesgos

PLAN

DE

TRATAMIENTO DE

RIESGOS INFORMÁTICOS

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CARRERA DE TECNOLOGÍAS DE LA INFORMACION

Realizado por: Ariel Steven Borbor Tumbaco

Introducción

Alcance del Plan

El plan de tratamiento de riesgos propuesto se enfoca en actividades de prevención, minimización, detección, corrección y aceptación de los riesgos o amenazas. Las actividades que se proponen están basadas en las salvaguardas del catálogo de elementos de Magerit, dichas actividades están diseñadas para la protección de las dimensiones valoradas en el análisis de riesgos asociados a cada tipo de activos identificados en el Data Center de la entidad objeto de estudio.

Objetivo del Plan

Salvaguardar la disponibilidad, integridad, confidencialidad y autenticidad de los activos de información del Data Center de la institución mediante un plan de tratamiento de riesgos informáticos, que contribuirá a la continuidad operativa y fortalecerá la postura de seguridad.

Estrategias – Tipo de protección

El plan presentado tiene medidas de protección categorizados en los siguientes tipos:

- PR – Prevención
- IM – Minimización
- CR – Corrección
- AW – Concienciación
- DC – Detección
- AC – Aceptación

A partir del catálogo de salvaguardas que posee la herramienta PILAR, se eligieron los controles que más se adataron a la entidad de estudio. A continuación, se enlistan las salvaguardas elegidas que contiene el plan establecido.

- **Protecciones Generales**
    - Control de acceso lógico
    - Gestión de privilegios
    - Acceso Remoto
    - Monitorización y mantenimiento remoto
    - Segregación de tareas
    - Gestión de incidencias

    - Herramienta de monitorización de trafico
- **Identificación y autenticación**
    - Identificación de usuarios.
    - Gestión de identificación de usuarios
    - Cuentas especiales administración
    - Biometría
- **Protección de la información**
    - Aseguramiento de la integridad.
    - Protección de la confidencialidad
    - Cifrado de Información
    - Copia de seguridad de datos.
- **Protección de los servicios**
    - Aseguramiento de la disponibilidad.
    - Aceptación y puesta en operación.
    - Se aplican perfiles de seguridad
    - Operación
    - Gestión de cambios (mejoras y sustituciones).
    - Actualizaciones y Parches.
    - Protección de servicios y aplicaciones web.
    - Protección del correo electrónico.
    - Protección del servicio de nombres de dominio
- **Protección de las aplicaciones**
    - Copias de Seguridad.
    - Se aplican perfiles de seguridad.
    - Operación/Producción
    - Cambios (Actualización y mantenimiento).
- **Protección de los equipos**
    - Se aplican perfiles de seguridad.
    - Aseguramiento de la disponibilidad.
    - Correcta Instalación
    - Operación
    - Cambios (Actualización y mantenimiento).

    - Protección de los dispositivos de red
    - Máquinas Virtuales
- **Protección de las comunicaciones**
    - Aseguramiento de disponibilidad.
    - Autenticación del canal
    - Protección de la integridad de los datos intercambiados.
    - Control de acceso a la red
    - Cambios (Actualizaciones y mantenimiento)
    - Internet.
    - Seguridad Wireless (WiFi).
    - Segregación de red en dominios
- **Protección de los soportes de información**
    - Aseguramiento de disponibilidad.
    - Limpieza de contenidos.
    - Destrucción de soportes.
- **Protección de los elementos auxiliares**
    - Aseguramiento de disponibilidad.
    - Correcta instalación.
    - Suministro eléctrico.
    - Climatización.
    - Protección de cableado.
- **Protección de las instalaciones**
    - Control de acceso físico.
    - Aseguramiento de disponibilidad de recursos.
- **Salvaguardas de gestión de personal**
    - Formación y concienciación.
    - Aseguramiento de la disponibilidad
- **Herramientas de seguridad**
    - Herramienta contra código dañino
    - IDP/IPS: Herramienta de detección/prevención de intrusos
    - Monitorización de la integridad de los ficheros
    - Herramienta de monitorización de tráfico

Acciones de Tratamiento del Riesgo

Servicios Internos [IS]

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgos - Servicios Internos
Fecha	01/06/2024		
Activos Involucrados: Internet			
Riesgo – Amenaza: [I.8] Fallo del servicio de comunicaciones			

Salvaguarda	Actividades propuestas:	TDP	Eficacia
Aseguramiento de la disponibilidad	Ajustar los parámetros de congestión y el tamaño del búfer para optimizar el rendimiento.	PR	L3
	Establecer múltiples enlaces de comunicación con diferentes proveedores de servicios de Internet (ISP) para asegurar la disponibilidad continua en caso de fallo de un proveedor.	PR	L3
	Configurar balanceo de carga para distribuir el tráfico entre los enlaces redundantes y garantizar un cambio automático en caso de fallo.	PR	L3
	Configurar políticas de calidad del servicio (QoS) para priorizar el tráfico crítico y asegurar que el servicio interno de internet tenga suficiente ancho de banda y baja latencia.	PR	L3
	Verificar la configuración de servidores DNS, implementar servidores DNS redundantes y monitorear la resolución de nombres.	PR	L3
	Configurar un protocolo VRRP (Virtual Router Redundancy Protocol), con el fin de proporcionar redundancia de enrutadores de la red local para garantizar la continuidad del servicio en caso de fallo del equipo principal.	PR	L4

Responsable: Analista de seguridad informática / Encargado del Data Center

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgos - Servicios Internos
Fecha	01/06/2024		
Activos Involucrados: Internet			
Riesgo – Amenaza: [E.1] Errores de Usuarios			

Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Aseguramiento de la disponibilidad	Revisar y configurar detalladamente las opciones del servicio de internet para prevenir configuraciones propensas a errores de usuarios.	PR	L3
	Ajustar los parámetros de congestión y el tamaño del búfer para optimizar el rendimiento.	PR	L3
	Divide la red en segmentos y utiliza VLANs para aislar el tráfico y reducir la posibilidad de colisiones y pérdida de paquetes.	PR	L3
	Implementa políticas de calidad de servicio (QoS) para priorizar el tráfico crítico, como voz o video, sobre otros tipos de tráfico.	PR	L3
	Examinar y optimizar las rutas de red para minimizar el número de saltos y reducir la latencia.	PR	L3
Protección de Servicios	Establecer un control estricto de acceso y autenticación para minimizar la posibilidad de errores de usuarios que puedan afectar el servicio interno de Internet. (IDS)	IM	L3
	Utilizar herramientas de monitoreo para supervisar el rendimiento de la red, la utilización de recursos y la seguridad.	DC	L3
Responsable: Analista de seguridad informática / Encargado del Data Center			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgos - Servicios Internos
Fecha	01/06/2024		
Activos Involucrados: Internet			
Riesgo – Amenaza: [E.24] Caída del sistema por agotamiento de recursos			

Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Aseguramiento de Disponibilidad	Optimizar las configuraciones del sistema de Internet para asegurar un uso eficiente de los recursos y prevenir agotamientos innecesarios.	PR	L2
	Tener un enlace de datos de internet alterno o de respaldo, de tal forma que no afecte las operaciones del servicio en la entidad.	PR	L3
	Implementar balanceadores de carga para distribuir el tráfico de red de manera equitativa entre múltiples servidores, evitando la sobrecarga de un solo recurso.	PR	L3
Gestión de Cambios	Mantener todos los sistemas actualizados con los últimos parches y actualizaciones de software para mejorar el rendimiento y la estabilidad.	PR	L3
	Diseñar un plan de cambios que cumpla con las condiciones en caso de que el recurso sufra una caída por agotamiento.	CR	L3
Responsable: Analista de seguridad informática / Encargado del Data Center -			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgos - Servicios Internos
Fecha	01/06/2024		
Activos Involucrados: Servicio Correo Institucional			
Riesgo – Amenaza: [E.1] Errores de Usuarios			

Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Aseguramiento de la disponibilidad	Realizar revisiones regulares de la configuración del servicio de correo electrónico.	PR	L2
	Asegurar que el servidor de correo institucional esté en línea y sea accesible.	CR	L3
	Verificar la configuración de los servidores de correo saliente (SMTP) e entrante (IMAP o POP). Asegurarse de que no haya cuotas de almacenamiento excedidas.	PR	L3
	Revisar y restablecer las credenciales si es necesario. Asegurarse de que los servidores de correo estén configurados con protocolos de seguridad adecuados (SSL/TLS).	PR	L3
Actualizaciones y Parches	Mantener actualizados todos los componentes del sistema de correo electrónico, incluyendo tanto el software del servidor como el cliente de los usuarios.	PR	L3
Protección de Servicios	Implementar herramientas de monitoreo de seguridad para supervisar la actividad de los usuarios y detectar comportamientos inusuales o potencialmente peligrosos, como el envío masivo de correos electrónicos o el acceso desde ubicaciones geográficas inesperadas.	DC	L4
Responsable: Analista de seguridad informática / Encargado del Data Center			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgos - Servicios Internos
Fecha	01/06/2024		
Activos Involucrados: Servicio Correo Institucional			
Riesgo – Amenaza: [E.4] Errores de configuración			

Salvaguarda	Actividades propuestas:	TDP	Eficacia
Copia de seguridad de Datos	Realizar respaldos diarios automáticos de los datos de configuración del servicio de correo electrónico.	PR	L3
Aseguramiento de la disponibilidad	Realizar revisiones periódicas de las configuraciones del servicio identificando errores.	IM	L3
	Verificar la configuración del servidor SMTP proporcionada por el proveedor de correo institucional. Asegurarse de usar el puerto correcto y las credenciales adecuadas.	PR	L3
	Verificar la configuración del servidor IMAP/POP proporcionada por el proveedor. Asegurarse de usar el puerto correcto y seleccionar el protocolo adecuado.	PR	L3
	Asegurar que las opciones de seguridad (SSL/TLS) estén configuradas según las recomendaciones del proveedor. Verificar que los certificados sean válidos.	PR	L3
Responsable: Analista de seguridad informática / Encargado del Data Center			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgos - Servicios Internos
Fecha	01/06/2024		
Activos Involucrados: Servicio Correo Institucional			
Riesgo – Amenaza: [E.15] Alteración de la información			

Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Protección de la Integridad	Establecer políticas de retención de datos para mantener un registro histórico de los correos electrónicos y evitar la eliminación accidental o maliciosa de mensajes importantes.	PR	L3
	Implementar un sistema de autenticación adicional, como el envío de códigos a través de mensajes de texto o el uso de aplicaciones de autenticación (Zimbra 2FA).	IM	L4
	Configurar firmas DKIM (DomainKeys Identified Mail) para autenticar los mensajes salientes y garantizar que no hayan sido alterados durante el tránsito.	PR	L4
Protección de la Confidencialidad	Aplicar cifrado a los datos sensibles en Zimbra para prevenir la alteración de la información (cifrado S/MIME de extremo a extremo).	IM	L4
	Aplicar el protocolo APOP para cifrar la contraseña del usuario durante la sesión POP con el fin de no ser capturadas por sniffer.	IM	L3
Copia de seguridad (backups)	Realizar respaldos diarios automáticos de los datos de configuración del servicio de correo electrónico.	PR	L3
	Configurar copias de seguridad automáticas y periódicas en Zimbra (Zimbra Backup and Restore (ZBR), para corregir la alteración de la información	PR	L4

	mediante la restauración de datos en caso de incidentes.		
	Verificar la integridad de las copias de seguridad, asegurando que los datos almacenados sean consistentes y no hayan sido alterados.	PR	L4
Cuentas Especiales	Identificar todas las cuentas especiales utilizadas en el servicio de correo institucional, como las cuentas de administrador, de servicio o de respaldo.	IM	L3
	Segregar estas cuentas especiales de las cuentas de usuario regulares para limitar su acceso y protegerlas de posibles compromisos.	IM	L3
Protección del correo electrónico	Establecer requisitos de complejidad para las contraseñas, incluyendo longitud mínima, combinación de caracteres, cambio periódico de contraseñas.	PR	L2
	Configurar sistemas de detección de correo electrónico fraudulento (SPF, DKIM, DMARC) para prevenir el envío de correos electrónicos falsificados o modificados.	IM	L3
Responsable: Analista de seguridad informática / Encargado del Data Center			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgos - Servicios Internos
Fecha	01/06/2024		
Activos Involucrados: Servicio Correo Institucional			
Riesgo – Amenaza: [E.19] Fugas de la información			

Salvaguarda	Actividades propuestas:	TDP	Eficacia
Identificación de Usuarios	Implementar un sistema de autenticación adicional, como el envío de códigos a través de mensajes de texto o el uso de aplicaciones de autenticación (Zimbra 2FA).	IM	L4
Perfiles de Seguridad	Implementar un sistema de control de acceso basado en perfiles que otorgue a los usuarios acceso únicamente a los recursos y funciones necesarios para realizar sus tareas laborales en el servicio de correo.	IM	L4
	Desarrollar perfiles de usuario que especifiquen los niveles de acceso y los privilegios asociados para cada tipo de usuario del servicio de correo institucional, basados en las funciones y responsabilidades del usuario.	PR	L3
	Establecer un proceso regular para revisar y actualizar los perfiles de seguridad de los usuarios a medida que cambian sus roles o responsabilidades dentro de la organización.	CR	L4
Protección del correo electrónico	Aplicar un filtro de seguridad para la restricción de correo entrante, saliente y revisión de archivos adjuntos.	IM	L3
	Aplicar cifrado a los datos sensibles en Zimbra para prevenir la fuga de la información (cifrado S/MIME de extremo a extremo).	PR	L3

	Instalar antivirus y filtros anti-spam en los dispositivos de seguridad del servicio de correo electrónico.	IM	L3
Aceptación y puesta en operación	Realizar pruebas de penetración periódicas y evaluaciones de seguridad en el servicio de correo institucional para identificar posibles vulnerabilidades y garantizar que los controles de seguridad sean efectivos y estén actualizados.	AC	L3
Responsable: Analista de seguridad informática / Encargado del Data Center			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgos - Servicios Internos
Fecha	01/06/2024		
Activos Involucrados: Servicio Correo Institucional			
Riesgo – Amenaza: [E.24] Caída del sistema por agotamiento de recursos			
Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Aseguramiento de Disponibilidad	Optimizar las configuraciones del sistema de correo electrónico para asegurar un uso eficiente de los recursos y prevenir agotamientos innecesarios.	PR	L3
	Establecer un sistema de monitoreo constante de los recursos del sistema, como uso de CPU, memoria y almacenamiento. Generando informes cuando se detecten umbrales críticos.	CR	L3
	Realiza análisis periódicos de la capacidad del servidor de correo para anticipar y planificar el crecimiento futuro de la carga de trabajo.	IM	L3
	Implementar balanceadores de carga para distribuir la carga de trabajo de manera equitativa entre varios servidores de correo.	IM	L3

Gestión de Cambios (mejoras y sustituciones)	Diseñar un plan de cambios que cumpla con las condiciones en caso de que el recurso sufra una caída por agotamiento.	CR	L4
	Mantener actualizado el software del servidor de correo y aplicar parches de seguridad de manera regular.	CR	L3
Responsable: Analista de seguridad informática - Coordinador/a del Área de sistemas y recursos tecnológicos			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgos - Servicios Internos
Fecha	01/06/2024		
Activos Involucrados: Servicio Correo Institucional			
Riesgo – Amenaza: [A.5] Suplantación de Identidad, [A.7] Uso no Previsto, [A.11] Acceso no autorizado			
Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Identificación de los Usuarios	Asignar permisos y accesos solo a aquellos usuarios que necesiten tener acceso al servicio de correo electrónico.	PR	L3
	Evitar otorgar privilegios innecesarios para reducir la superficie de un ataque potencial.	PR	L3
Perfiles de Seguridad	Implementar un sistema de control de acceso basado en perfiles que otorgue a los usuarios acceso únicamente a los recursos y funciones necesarios para realizar sus tareas laborales en el servicio de correo.	IM	L4
Cuentas Especiales	Identificar todas las cuentas especiales utilizadas en el servicio de correo institucional, como las cuentas de administrador, de servicio o de respaldo.	IM	L3

Segregación de Tareas	Segregar estas cuentas especiales de las cuentas de usuario regulares para limitar su acceso y protegerlas de posibles compromisos.	IM	L3
Autenticación de los usuarios	Implementar un sistema de autenticación adicional, como el envío de códigos a través de mensajes de texto o el uso de aplicaciones de autenticación (Zimbra 2FA).	IM	L4
Responsable: Analista de seguridad informática, Coordinador/a del Área de sistemas y recursos tecnológicos			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgos - Servicios Internos
Fecha	01/06/2024		
Activos Involucrados: Servicio Página Web Oficial			
Riesgo – Amenaza: [E.1] Errores de Usuarios			
Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Aceptación y Puesta en operación.	Revisar el código fuente (enlaces rotos, botones no funcionales, etc.) y las configuraciones de la página web.	PR	L2
	Implementar validaciones en los formularios para prevenir que los usuarios ingresen información incorrecta, reduciendo así los errores de entrada de datos.	PR	L3
Actualizaciones y Parches.	Mantener actualizadas las tecnologías usadas en el desarrollo del sitio web a su versión más estable y compatible.	PR	L3

Protección de los servicios y aplicaciones web.	Diseñar la interfaz de la página web para que sea fácil de usar y comprender, reduciendo así la posibilidad de errores por parte de los usuarios.	PR	L3
	Estructurar los formularios de manera clara y lógica, con instrucciones y ejemplos visibles para los usuarios.	IM	L3
Responsable: Programador Senior - Programador de sistemas			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgos - Servicios
Fecha	01/06/2024		
Activos Involucrados: Servicio Página Web Oficial			
Riesgo – Amenaza: [E.2] Errores del administrador del sistema			
Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Aseguramiento de la disponibilidad	Instalar un certificado SSL/TLS de una autoridad de certificación confiable para garantizar que las comunicaciones sean seguras y autenticadas.	PR	L4
	Utilizar configuraciones recomendadas para SSL/TLS que equilibren seguridad y rendimiento, tales como la habilitación de HTTP/2 y el uso de suites de cifrado modernas.	PR	L3
	Configurar los servidores web para que utilicen HTTPS en lugar de HTTP. Esto incluye la actualización de las configuraciones del servidor para redirigir todo el tráfico HTTP a HTTPS.	PR	L4
Aceptación y Puesta en operación.	Poner a prueba los cambios del servicio de página web antes de ponerlos en producción.	AC	L2
	Realizar copias de seguridad periódicas de servicio de página web con el objetivo que si ocurre un error	IM	L3

	del administrador se vuelva a la última versión funcionales.		
	Aplicar el principio de menor privilegio, asignando solo los privilegios necesarios a los administradores para minimizar el impacto de posibles errores.	IM	L2
Perfiles de Seguridad	Implementar un sistema de control de acceso basado en perfiles que otorgue a los usuarios acceso únicamente a los recursos y funciones necesarios para realizar sus tareas laborales en el servicio de correo	IM	L4
Operación	Implementar herramientas y procedimientos de recuperación ante desastres que permitan restaurar el sistema rápidamente a un estado funcional después de un error.	CR	L4
Actualizaciones y Parches	Comprobar que las tecnologías usadas en el desarrollo del servicio aun sean compatibles y funcionales.	PR	L3
	Mantener el software del servidor web y las aplicaciones siempre actualizados con los últimos parches de seguridad para corregir vulnerabilidades conocidas.	PR	L3
Gestión de Incidentes	Desarrollar planes de respuesta a incidentes que incluyan pasos claros para identificar, corregir y documentar errores del administrador del sistema.	CR	L4
Responsable: Programador Senior - Programador de sistemas – Analista de seguridad informática			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgos - Servicios Internos
Fecha	01/06/2024		
Activos Involucrados: Servicio Página Web Oficial			
Riesgo – Amenaza: [E.15] Alteración de la información – [E.18] Destrucción de la información			

Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Copia de seguridad de Datos	Establecer un programa de copias de seguridad periódicas que incluya la base de datos como los archivos del sitio.	PR	L3
	Utilizar soluciones de almacenamiento en la nube o servidores externos para asegurar la redundancia de las copias de seguridad.	IM	L3
	Verificar la integridad de las copias de seguridad, asegurando que los datos almacenados sean consistentes y no hayan sido alterados.	PR	L3
Cifrado de Información	Implementar un protocolo de cifrado SSL/TLS para la transferencia de datos entre los usuarios y el servidor web.	PR	L3
	Aplicar algoritmos de cifrados robustos para la protección de la información almacenada en la base de datos.	PR	L3
Responsable: Programador Senior - Programador de sistemas – Analista de seguridad informática			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgos - Servicios Internos
Fecha	01/06/2024		
Activos Involucrados: Servicio Página Web Oficial			
Riesgo – Amenaza: [E.19] Fugas de la información			

Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**

Aceptación y puesta en operación	Documentar los posibles riesgos de fugas de información y desarrollar estrategias para gestionarlos, incluyendo la aceptación informada de ciertos riesgos residuales cuando no se puedan eliminar por completo.	AC	L3
Protección de servicios y aplicaciones web	Implementar mecanismos de monitoreo y registro de logs para detectar y rastrear posibles fugas de información.	CR	L3
	Implementar protocolos seguros para la transmisión de sesiones (HTTPS).	PR	L4
	Implementar mecanismo de expiración de sesiones inactivas y gestión adecuadas de cookies.	PR	L4
	Adoptar prácticas de desarrollo seguro, como la revisión de código, pruebas de seguridad y el uso de herramientas de análisis de vulnerabilidades durante el desarrollo de la página web.	PR	L4
Gestión de incidencias	Desarrollar un plan de respuesta a incidentes de seguridad, incluyendo procedimientos específicos para tratar con fugas de información.	CR	L4
Responsable: Programador Senior - Programador de sistemas – Analista de seguridad informática			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgos - Servicios Internos
Fecha	01/06/2024		
Activos Involucrados: Servicio Página Web Oficial			
Riesgo – Amenaza: [E.24] Caída del sistema por agotamiento de recursos			
Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
	Implementación de Sistema de Cluster para garantizar la disponibilidad del Servicio de Página Web.	PR	L4

Aseguramiento de Disponibilidad	Aplicar servicios de CND (Content Delivery Network) para reducir la carga en el servidor principal.	PR	L4
	Configurar redirecciones automáticas a servidores alternativos o páginas de mantenimiento durante períodos de interrupción.	IM	L4
	Implementar sistemas de almacenamiento en caché eficientes para reducir la carga en el servidor y mejorar los tiempos de carga.	IM	L3
Gestión de Cambios	Implementar mecanismos de monitoreo y registro de logs para detectar y rastrear posibles fugas de información.	CR	L4
Responsable: Programador de sistemas – Analista de seguridad informática			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgos - Servicios Internos
Fecha	01/06/2024		
Activos Involucrados: Servicio Página Web Oficial			
Riesgo – Amenaza: [A.5] Suplantación de Identidad			
Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Identificación de los Usuarios	Asignar permisos y accesos solo a aquellos usuarios que necesiten tener acceso al servicio del sistema web.	PR	L2
Autenticación de los usuarios	Implementar un sistema de autenticación adicional, como el envío de códigos a través de mensajes de texto o el uso de aplicaciones de autenticación para el ingreso al sistema web (2FA).	PR	L3
Responsable: Programador Senior - Programador de sistemas – Analista de seguridad informática			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgos - Servicios Internos
Fecha	01/06/2024		
Activos Involucrados: Servicio Página Web Oficial			
Riesgo – Amenaza: [A.15] Alteración de la información – [A.18] Destrucción de la información			
Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Copia de seguridad de Datos	Establecer un programa de copias de seguridad periódicas que incluya la base de datos como los archivos del sitio.	PR	L3
	Utilizar soluciones de almacenamiento en la nube o servidores externos para asegurar la redundancia de las copias de seguridad.	IM	L3
	Verificar la integridad de las copias de seguridad, asegurando que los datos almacenados sean consistentes y no hayan sido alterados.	PR	L3
Cifrado de Información	Implementar un protocolo de cifrado SSL/TLS para la transferencia de datos entre los usuarios y el servidor web.	PR	L3
	Aplicar algoritmos de cifrados robustos para la protección de la información almacenada en la base de datos.	PR	L3
Responsable: Programador Senior - Programador de sistemas – Analista de seguridad informática			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgos - Servicios Internos
Fecha	01/06/2024		
Activos Involucrados: Servicio Página Web Oficial			
Riesgo – Amenaza: [A.6] Abuso de Privilegio de Acceso - **[**A.11] Acceso no autorizado - [A.18] Destrucción de la Información			

Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Identificación de los Usuarios	Implementar un sólido sistema de autenticación que requiera identificación de usuarios de dos pasos.	PR	L4
Protección de servicios y aplicaciones web	Aplicar sistema de detección de intrusos para identificar patrones sospechosos de acceso.	DC	L4
	Utilizar firewalls de aplicaciones web (WAF) para detectar y prevenir ataques.	PR	L4
	Implementar mecanismo de expiración de sesiones inactivas y gestión adecuadas de cookies.	PR	L4
Responsable: Programador de sistemas – Analista de seguridad informática			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgos - Servicios Internos
Fecha	01/06/2024		
Activos Involucrados: Servicio Página Web Oficial			
Riesgo – Amenaza: [A.24] Denegación de servicios			

Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Protección de servicios y aplicaciones web	Implementar firewall (WAF) y sistemas de prevención contra DDoS.	IM	L4
	Aplicar servicios de CND (Content Delivery Network) para reducir la carga en el servidor principal.	PR	L4

Aseguramiento de disponibilidad	Implementación de Sistema de Cluster para garantizar la disponibilidad del Servicio de Página Web.	PR	L3
Responsable: Programador de sistemas – Analista de seguridad informática			

Aplicaciones [SW]

Realizado por:	Borbor Tumbaco	**Nombre del Reporte:**	Plan De Tratamiento de Riesgo – Aplicaciones
Fecha	01/06/2024		
Activos Involucrados: Cliente de Correo (Zimbra)**,** Servidor de correo electrónico (Virtualizado)			
Riesgo – Amenaza: [I.5.1] Averías de origen lógico			
Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Copias de Seguridad	Realizar respaldos periódicos automáticos de los datos del cliente de correo.	PR	L3
	Utilizar sistema de almacenamiento con redundancia y tolerancia a fallos para evitar perdida de datos.	PR	L3
Aseguramiento del Cliente de Correo Electrónico	Implementar monitoreo constante del servicio de correo para detectar posibles interrupciones.	PR	L3
	Diseñar un plan de contingencias para restablecer el servicio de manera rápida en caso de interrupciones.	CR	L3
Responsable: Analista de seguridad informática			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgo – Aplicaciones
Fecha	01/06/2024		

Activos Involucrados: Cliente de Correo (Zimbra), Servidor de correo electrónico (Virtualizado)

Riesgo – Amenaza: [E.8] Difusión de software dañino

Salvaguarda	Actividades propuestas:	TDP	Eficacia
Copias de Seguridad	Realizar respaldos diarios automáticos de los datos de configuración del servicio de correo electrónico.	PR	L3
	Configurar copias de seguridad automáticas y periódicas en Zimbra para corregir la alteración de la información mediante la restauración de datos en caso de incidentes.	PR	L3
	Verificar la integridad de las copias de seguridad, asegurando que los datos almacenados sean consistentes y no hayan sido alterados.	PR	L3
Se aplican perfiles de seguridad	Implementar un sistema de control de acceso basado en perfiles que otorgue a los usuarios acceso únicamente a los recursos y funciones necesarios para realizar sus tareas laborales en el servicio web.	PR	L3
Protección de las aplicaciones	Aplicar un sistema antivirus original y actualizado que se aloje en el servidor de correo.	PR - IM	L4
	Implementar un firewall en el entorno del data center puede ayudar a filtrar el tráfico de red	PR – IM	L4
	Aplicar cifrado a los datos sensibles en Zimbra para prevenir la alteración de la información (cifrado S/MIME de extremo a extremo).	IM	L4

Responsable: Analista de seguridad informática

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgo – Aplicaciones
Fecha	01/06/2024		

Activos Involucrados: Cliente de Correo (Zimbra), Servidor de correo electrónico (Virtualizado)

Riesgo – Amenaza: [E.20] Vulnerabilidades de los programas

Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Herramienta de detección/prevención de intrusos	Implementar un firewall y sistemas de detección de intrusiones para monitorear y bloquear intento de infiltración.	IM	L4
Cambios (Actualización y mantenimiento)	Aplicar las actualizaciones más recientes que solucionan la mayoría de las vulnerabilidades, además de los parches de seguridad para el cliente de correo.	CR	L2

Responsable: Analista de seguridad informática

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgo – Aplicaciones
Fecha	01/06/2024		

Activos Involucrados: Cliente de Correo (Zimbra), Servidor de correo electrónico (Virtualizado)

Riesgo – Amenaza: [E.21] Errores de mantenimiento / actualizaciones

Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Copias de Seguridad	Implementar un sistema de respaldo y recuperación para la restauración del sistema en caso de fallos durante el proceso de actualización y mantenimiento.	IM	L3
	Realizar una revisión de las configuraciones del antes y después de cada actualización o mantenimiento.	PR	L2

Cambios (Actualización y mantenimiento)	Implementar un procedimiento de rollback, en caso de querer deshacer los cambios de configuración incorrectas.	IM	L3
Responsable: Analista de seguridad informática			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgo – Aplicaciones
Fecha	01/06/2024		
Activos Involucrados: Cliente de Correo (Zimbra), Servidor de correo electrónico (Virtualizado)			
Riesgo – Amenaza: [A.8] Difusión de software dañino			
Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Copias de Seguridad	Realizar respaldos diarios automáticos de los datos de configuración del servicio de correo electrónico.	PR	L3
	Configurar copias de seguridad automáticas y periódicas en Zimbra para corregir la alteración de la información mediante la restauración de datos en caso de incidentes.	PR	L3
	Verificar la integridad de las copias de seguridad, asegurando que los datos almacenados sean consistentes y no hayan sido alterados.	PR	L3
Protección de las aplicaciones	Contar con un sistema antivirus original y actualizado que se aloje en el servidor de correo.	PR - IM	L4
	Implementar un firewall y sistemas de detección de intrusiones para monitorear y bloquear intento de infiltración.	DC	L4

	Aplicar cifrado a los datos sensibles en Zimbra para prevenir la alteración de la información (cifrado S/MIME de extremo a extremo).	IM	L4
	Aplicar un filtro de seguridad para la restricción de correo entrante, saliente y revisión de archivos adjuntos.	IM	L4
Aceptación y puesta en operación	Implementar mecanismos de monitoreo continuo para detectar comportamientos anómalos en el servidor.	CR	L4
Responsable: Analista de seguridad informática			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgo – Aplicaciones
Fecha	01/06/2024		
Activos Involucrados: Sistema de Base de Datos (BD)			
Riesgo – Amenaza: [I.5.1] Averías de origen lógico			
Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Aseguramiento de disponibilidad	Revisar el código que interactúa con la base de datos, la validación de entrada, uso correcto de las consultas y la gestión adecuada de transacciones.	PR – IM	L4
Copias de Seguridad	Realizar respaldos diarios automáticos de los datos de configuración del servicio de base de datos.	PR	L3
	Verificar la integridad de las copias de seguridad, asegurando que los datos almacenados sean consistentes y no hayan sido alterados.	PR	L4

Protección de las aplicaciones	Implementar un firewall y sistemas de detección de intrusiones para monitorear y bloquear intento de infiltración.	DC	L4
	Aplicar cifrado a los datos sensibles en Oracle Database para prevenir la alteración de la información.	IM	L4
	Aplicar un filtro de seguridad para la restricción de correo entrante, saliente y revisión de archivos adjuntos.	IM	L4
Responsable: Analista Técnico de base de datos, Programador de sistemas			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgo – Aplicaciones
Fecha	01/06/2024		
Activos Involucrados: Sistema de Base de Datos (BD)			
Riesgo – Amenaza: [E.8] Difusión de software dañino			
Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Protección de las aplicaciones	Contar con un sistema antivirus original y actualizado que se aloje en el servidor de base de datos.	PR - IM	L4
	Implementar un firewall y sistemas de detección de intrusiones para monitorear y bloquear intento de infiltración. (Oracle Audit Vault and Database Firewall)	DC	L4
	Aplicar un filtro de seguridad para la restricción de archivos sospechosos.	IM	L3
Aceptación y puesta en operación	Implementar mecanismos de monitoreo continuo para detectar comportamientos anómalos en el servidor.	CR	L4
Responsable: Analista Técnico de base de datos, Programador de sistemas			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgo – Aplicaciones
Fecha	01/06/2024		

Activos Involucrados: Sistema de Base de Datos (BD)

Riesgo – Amenaza: [E.15] Alteración de la información - [E.18] Destrucción de la información - [E.19] Fugas de información

Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Identificación de usuarios	Aplicar el sistema de identificación de usuarios en Oracle Database "Oracle Unified Directory" (OUD) para la limitación de acceso a datos sensibles.	PR – IM	L4
Protección de la integridad	Implementar el sistema de aseguramiento de integridad "Oracle Data Integrity" para garantizar la exactitud y fiabilidad de la información almacenada.	PR	L4
Protección de la confidencialidad (Cifrado)	Utilizar el sistema de datos trasparente (TPE) integrado con Oracle Database para el cifrado de datos sensibles de la base de datos.	PR – IM	L4
Aseguramiento de la disponibilidad	Implementar sistemas de monitoreo continuo para detectar cualquier intento de alteración de la información en tiempo real. Oracle Enterprise Manager (OEM).	CR	L4
Copias de Seguridad (backup)	Realizar copias de seguridad de los datos mediante Oracle Database Backup Cloud Service, para prevenir la alteración de datos en el sistema.	PR	L4
	Integrar el sistema de Oracle Recovery Manager (RMAN) para asegurar las copias de seguridad y restaurar de forma segura.	PR	L4

Responsable: Analista Técnico de base de datos, Programador de sistemas

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgo – Aplicaciones
Fecha	01/06/2024		
Activos Involucrados: Sistema de Base de Datos (BD)			
Riesgo – Amenaza: [E.20] Vulnerabilidades de los programas			
Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Herramientas de seguridad	Implementar un firewall y sistemas de detección de intrusiones para monitorear y bloquear intento de infiltración (DAM).	IM	L4
Cambios (Actualización y mantenimiento)	Aplicar las actualizaciones más recientes que solucionan la mayoría de las vulnerabilidades, además de los parches de seguridad para la base de datos.	CR	L3
Responsable: Analista Técnico de base de datos, Programador de sistemas			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgo – Aplicaciones
Fecha	01/06/2024		
Activos Involucrados: Sistema de Base de Datos (BD)			
Riesgo – Amenaza: [E.21] Errores de mantenimiento / actualizaciones			
Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Copias de Seguridad (backup)	Implementar un sistema de respaldo y recuperación para la restauración del sistema en caso de fallos durante el proceso de actualización y mantenimiento.	IM	L3
Operación / Producción	Controlar y verificar la integridad del código ejecutable que este enlazado a la base de datos.	IM	L3
Cambios (Actualización y mantenimiento)	Implementar un procedimiento de rollback, en caso de querer deshacer los cambios de configuración incorrectas.	PR	L3

Monitorización Continua	Realizar una revisión de las configuraciones del antes y después de cada actualización o mantenimiento.	PR	L3
Responsable: Analista Técnico de base de datos, Programador de sistemas			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgo – Aplicaciones
Fecha	01/06/2024		
Activos Involucrados: Sistema de Base de Datos (BD)			
Riesgo – Amenaza: [A.3] Manipulación de los registros de actividad [Log] – [A.4] manipulación de los ficheros de configuración.			

Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Identificación de usuario	Aplicar el sistema de identificación de usuarios en Oracle Database "Oracle Unified Directory" (OUD) para la limitación de acceso a datos sensibles.	PR – IM	L4
Acceso Remoto	Utilizar autenticación multifactor (MFA) para todas las conexiones remotas.	PR	L3
	Emplear certificados digitales o claves SSH para asegurar las conexiones.	PR	L3
	Implementar roles y privilegios de manera que los usuarios que deban acceder a la BD tengan el mínimo acceso requerido para realizar sus funciones.	IM	L4
	Determinar que al pasar un periodo de inactividad, se termine automáticamente la sesión SSH	IM	L3
Copia de seguridad	Realizar copias de seguridad de los logs de la base de datos mediante Oracle Recovery Manager (RMAN).	PR	L4
Protección de la integridad	Implementar el sistema de aseguramiento de integridad "Oracle Data Integrity" para garantizar la exactitud y fiabilidad de los logs.	IM	L4

Protección de la confidencialidad	Utilizar el sistema de datos trasparente (TPE) integrado con Oracle Database para el cifrado de los logs.	IM	L3
Responsable: Analista Técnico de base de datos, Programador de sistemas			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgo – Aplicaciones
Fecha	01/06/2024		
Activos Involucrados: Sistema de Base de Datos (BD)			
Riesgo – Amenaza: [A.5] Suplantación de identidad			
Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Identificación de los usuarios	Aplicar el sistema de identificación de usuarios en Oracle Database "Oracle Unified Directory" (OUD) para la limitación de acceso a datos sensibles.	PR – IM	L4
Protección de servicios y aplicaciones web	Implementar sistemas de monitoreo continuo para detectar cualquier intento de alteración de la información en tiempo real. Oracle Enterprise Manager (OEM).	CR	L4
Responsable: Administrador del sistema, Administrador de Base de Datos			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgo – Aplicaciones
Fecha	01/06/2024		
Activos Involucrados: Sistema de Base de Datos (BD)			
Riesgo – Amenaza: [A.6] Abuso de privilegios de acceso			
Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**

Identificación de usuarios	Aplicar el sistema de identificación de usuarios en Oracle Database "Oracle Unified Directory" (OUD) para la limitación de acceso a datos sensibles.	PR – IM	L4
Protección de servicios y aplicaciones web	Definir una ruta de confianza para la aplicación basada en la sesión iniciada, el objeto, los comandos y las consultas SQL.	PR	L3
Se aplican perfiles de seguridad	Aplicar la opción Oracle Label Security, para restringir el acceso de los usuarios a los datos en función de la clasificación de la organización.	PR	L4
Responsable: Analista Técnico de base de datos, Programador de sistemas			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgo – Aplicaciones
Fecha	01/06/2024		
Activos Involucrados: Sistema de Base de Datos (BD)			
Riesgo – Amenaza: [A.8] Difusión de software dañino			
Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Aseguramiento de la disponibilidad	Implementar sistemas de respaldo y recuperación para asegurar la disponibilidad.	PR	L3
Protección de servicios y aplicaciones web	Aplicar practicas seguras de codificación para evitar la inyección de códigos.	PR	L3
	Escanear archivos adjuntos y scripts antes de ser cargados en la base de datos.	PR	L3
	Limitar los privilegios de carga de archivos a usuarios autorizados.	PR	L3

Responsable: Analista Técnico de base de datos, Programador de sistemas

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgo – Aplicaciones
Fecha	01/06/2024		
Activos Involucrados: Sistema de Base de Datos (BD)			
Riesgo – Amenaza: [A.15] Alteración de la información - [A.18] Destrucción de la información - [A.19] Fugas de información			

Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Identificación de usuarios	Asignar permisos y accesos solo a aquellos usuarios que necesiten tener acceso al servicio del sistema de base de datos.	PR – IM	L3
	Implementar un sistema de autenticación adicional, como el envío de códigos a través de mensajes de texto o el uso de aplicaciones de autenticación para el ingreso al sistema administrativo (2FA).	IM	L4
Aseguramiento de la integridad	Implementar el sistema de aseguramiento de integridad “Oracle Data Integrity” para garantizar la exactitud y fiabilidad de la información almacenada.	PR	L4
	Implementar el sistema de Oracle Data Loss Prevention (DLP), para para prevenir la fuga de información confidencial y proteger los datos sensibles almacenados en la base de datos de Oracle.	PR	L4
Cifrado de información	Utilizar el sistema de datos trasparente (TPE) integrado con Oracle Database para el cifrado de datos sensibles de la base de datos.	PR – IM	L4

Aseguramiento de la disponibilidad	Implementar sistemas de monitoreo continuo para detectar cualquier intento de alteración de la información en tiempo real. Oracle Enterprise Manager (OEM).	CR	L4
Copias de Seguridad de Datos	Realizar copias de seguridad de los datos mediante Oracle Database Backup Cloud Service, para prevenir la alteración de datos en el sistema.	PR	L4
	Integrar el sistema de Oracle Recovery Manager (RMAN) para asegurar las copias de seguridad y restaurar de forma segura.	PR	L4
Responsable: Analista Técnico de base de datos, Programador de sistemas			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgo – Aplicaciones
Fecha	01/06/2024		
Activos Involucrados: Sistema Administrativo / Financiero			
Riesgo – Amenaza: [I.5.1] Averías de origen lógico			
Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Aseguramiento de disponibilidad	Revisar el código que interactúa con la base de datos, la validación de entrada, uso correcto de las consultas y la gestión adecuada de transacciones.	PR – IM	L3
Copias de Seguridad	Realizar respaldos diarios automáticos de los datos de configuración del servicio de base de datos.	PR	L3
Protección de la integridad	Verificar la integridad de las copias de seguridad, asegurando que los datos almacenados sean consistentes y no hayan sido alterados.	PR	L3

Protección de la Confidencialidad	Aplicar cifrado a los datos sensibles en Oracle Database para prevenir la alteración de la información.	IM	L4
Protección de las aplicaciones	Implementar un firewall y sistemas de detección de intrusiones para monitorear y bloquear intento de infiltración.	DC	L4
	Aplicar un filtro de seguridad para la restricción de correo entrante, saliente y revisión de archivos adjuntos.	IM	L4
Responsable: Analista Técnico de base de datos, Programador de sistemas, Analista de seguridad informática			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgo – Aplicaciones
Fecha	01/06/2024		
Activos Involucrados: Sistema Administrativo / Financiero			
Riesgo – Amenaza: [A.8] Difusión de software dañino			
Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Copias de Seguridad	Realizar respaldos diarios automáticos de los datos de configuración del sistemas administrativo.	PR	L3
Protección de las aplicaciones Herramientas de Chequeo	Contar con un sistema antivirus original y actualizado que se aloje en el servidor de correo.	PR - IM	L4
	Implementar un firewall y sistemas de detección de intrusiones para monitorear y bloquear intento de infiltración. (Oracle Audit Vault and Database Firewall)	DC	L4

	Aplicar un filtro de seguridad para la restricción de archivos sospechosos.	IM	L4
Aceptación y puesta en operación	Implementar mecanismos de monitoreo continuo para detectar comportamientos anómalos en el servidor.	CR	L4
Responsable: Analista Técnico de base de datos, Programador de sistemas, Analista de seguridad informática			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgo – Aplicaciones
Fecha	01/06/2024		
Activos Involucrados: Sistema Administrativo / Financiero			
Riesgo – Amenaza: [E.15] Alteración de la información - [E.18] Destrucción de la información - [E.19] Fugas de información			
Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Identificación de usuarios	Asignar permisos y accesos solo a aquellos usuarios que necesiten tener acceso al servicio del sistema web.	PR – IM	L3
	Implementar un sistema de autenticación adicional, como el envío de códigos a través de mensajes de texto o el uso de aplicaciones de autenticación para el ingreso al sistema administrativo (2FA).	IM	L4
Protección de la integridad	Implementar el sistema de aseguramiento de integridad “Oracle Data Integrity” para garantizar la exactitud y fiabilidad de la información almacenada.	PR	L4
	Implementar el sistema de Oracle Data Loss Prevention (DLP), para para prevenir la fuga de	PR	L4

	información confidencial y proteger los datos sensibles almacenados en la base de datos de Oracle.		
Cifrado de información	Utilizar el sistema de datos trasparente (TPE) integrado con Oracle Database para el cifrado de datos sensibles de la base de datos.	PR – IM	L4
Aseguramiento de la disponibilidad	Implementar sistemas de monitoreo continuo para detectar cualquier intento de alteración de la información en tiempo real. Oracle Enterprise Manager (OEM).	CR	L4
Copias de Seguridad de Datos	Realizar copias de seguridad de los datos mediante Oracle Database Backup Cloud Service, para prevenir la alteración de datos en el sistema.	PR	L4
	Integrar el sistema de Oracle Recovery Manager (RMAN) para asegurar las copias de seguridad y restaurar de forma segura.	PR	L4
Responsable: Analista Técnico de base de datos, Programador de sistemas, Analista de seguridad informática			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgo – Aplicaciones
Fecha	01/06/2024		
Activos Involucrados: Sistema Administrativo / Financiero			
Riesgo – Amenaza: [E.20] Vulnerabilidades de los programas			
Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Herramientas de chequeo	Implementar un firewall y sistemas de detección de intrusiones para monitorear y bloquear intento de infiltración (DAM).	IM	L4

Cambios (Actualización y mantenimiento)	Aplicar las actualizaciones más recientes que solucionan la mayoría de las vulnerabilidades, además de los parches de seguridad para el cliente de correo.	CR	L2
Responsable: Analista Técnico de base de datos, Programador de sistemas, Analista de seguridad informática			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgo – Aplicaciones
Fecha	01/06/2024		
Activos Involucrados: Sistema Administrativo / Financiero			
Riesgo – Amenaza: [E.21] Errores de mantenimiento / actualizaciones			
Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Copias de Seguridad	Implementar un sistema de respaldo y recuperación para la restauración del sistema en caso de fallos durante el proceso de actualización y mantenimiento.	IM	L3
Cambios (Actualización y mantenimiento)	Realizar una revisión de las configuraciones del antes y después de cada actualización o mantenimiento.	PR	L2
	Implementar un procedimiento de rollback, en caso de querer deshacer los cambios de configuración incorrectas.	PR	L3
Operación / Producción	Controlar y verificar la integridad del código ejecutable que este enlazado a la base de datos.	IM	L3
Monitorización Continua	Realizar una revisión de las configuraciones del antes y después de cada actualización o mantenimiento.	PR	L3
Responsable: Analista Técnico de base de datos, Programador de sistemas, Analista de seguridad informática			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgo – Aplicaciones
Fecha	01/06/2024		
Activos Involucrados: Sistema Administrativo / Financiero			
Riesgo – Amenaza: [A.3] Manipulación de los registros de actividad [Log]			
Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Copia de seguridad	Realizar copias de seguridad de los logs de la base de datos mediante Oracle Recovery Manager (RMAN).	PR	L4
Aseguramiento de la integridad	Implementar el sistema de aseguramiento de integridad “Oracle Data Integrity” para garantizar la exactitud y fiabilidad de los logs.	IM	L4
Responsable: Analista Técnico de base de datos, Analista de seguridad informática			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgo – Aplicaciones
Fecha	01/06/2024		
Activos Involucrados: Sistema Administrativo / Financiero			
Riesgo – Amenaza: [A.5] Suplantación de identidad			
Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Identificación de usuarios	Implementar un sistema de autenticación adicional, como el envío de códigos a través de mensajes de texto o el uso de aplicaciones de autenticación para el ingreso al sistema administrativo (2FA).	PR – IM	L4
Protección de servicios y aplicaciones web	Implementar sistemas de monitoreo continuo para detectar cualquier intento de alteración de la información en tiempo real. Oracle Enterprise Manager (OEM).	CR	L4
Responsable: Analista Técnico de base de datos, Analista de seguridad informática			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgo – Aplicaciones
Fecha	01/06/2024		
Activos Involucrados: Sistema Administrativo / Financiero			
Riesgo – Amenaza: [A.6] Abuso de privilegios de acceso			
Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Identificación de usuarios	Implementar un sistema de autenticación adicional, como el envío de códigos a través de mensajes de texto o el uso de aplicaciones de autenticación para el ingreso al sistema administrativo (2FA).	PR – IM	L4
Protección de servicios y aplicaciones	Definir una ruta de confianza para la aplicación basada en la sesión iniciada, el objeto, los comandos y las consultas SQL.	PR	L3
Perfiles de seguridad	Aplicar la opción Oracle Label Security, para restringir el acceso de los usuarios a los datos en función de la clasificación de la organización.	PR	L4
Responsable: Analista Técnico de base de datos, Analista de seguridad informática			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgo – Aplicaciones
Fecha	01/06/2024		
Activos Involucrados: Sistema Administrativo / Financiero			
Riesgo – Amenaza: [A.8] Difusión de software dañino			
Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Aseguramiento de la disponibilidad	Implementar sistemas de respaldo y recuperación para asegurar la disponibilidad.	PR	L3
Protección de servicios y	Aplicar practicas seguras de codificación para evitar la inyección de códigos.	PR	L3
	Escanear archivos adjuntos y scripts antes de ser cargados en la base de datos.	PR	L3

aplicaciones web	Limitar los privilegios de carga de archivos a usuarios autorizados.	PR	L3
Responsable: Analista Técnico de base de datos, Analista de seguridad informática			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgo – Aplicaciones
Fecha	01/06/2024		
Activos Involucrados: Sistema Administrativo / Financiero			
Riesgo – Amenaza: [A.15] Alteración de la información - [A.18] Destrucción de la información - [A.19] Fugas de información			

Salvaguarda	Actividades propuestas:	TDP	Eficacia
Identificación de usuarios	Asignar permisos y accesos solo a aquellos usuarios que necesiten tener acceso al servicio del sistema web.	PR – IM	L3
	Implementar un sistema de autenticación adicional, como el envío de códigos a través de mensajes de texto o el uso de aplicaciones de autenticación para el ingreso al sistema administrativo (2FA).	IM	L4
Protección de la integridad	Implementar el sistema de aseguramiento de integridad “Oracle Data Integrity” para garantizar la exactitud y fiabilidad de la información almacenada.	PR	L4
	Implementar el sistema de Oracle Data Loss Prevention (DLP), para para prevenir la fuga de información confidencial y proteger los datos sensibles almacenados en la base de datos de Oracle.	PR	L4
Protección de la confidencialidad	Utilizar el sistema de datos trasparente (TPE) integrado con Oracle Database para el cifrado de datos sensibles de la base de datos.	PR – IM	L4

Aseguramiento de la disponibilidad	Implementar sistemas de monitoreo continuo para detectar cualquier intento de alteración de la información en tiempo real. Oracle Enterprise Manager (OEM).	CR	L4
Copias de Seguridad	Realizar copias de seguridad de los datos mediante Oracle Database Backup Cloud Service, para prevenir la alteración de datos en el sistema.	PR	L4
	Integrar el sistema de Oracle Recovery Manager (RMAN) para asegurar las copias de seguridad y restaurar de forma segura.	PR	L4
Responsable: Analista Técnico de base de datos, Analista de seguridad informática			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgo – Aplicaciones
Fecha	01/06/2024		
Activos Involucrados: SO Servidor de Producción, SO Servidor de Aplicaciones, SO Servidor NAS.			
Riesgo – Amenaza: [I.5.1] Averías de origen lógico			
Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Copias de Seguridad	Realizar respaldos diarios automáticos de los datos de configuración de los sistemas operativos.	PR	L3
	Utilizar sistema de almacenamiento con redundancia y tolerancia a fallos para evitar perdida de datos.	PR	L3
Aseguramiento de disponibilidad	Implementar monitoreo constante del sistema operativo de cada servidor para detectar posibles interrupciones.	PR	L3
	Diseñar un plan de contingencias para restablecer el servicio de manera rápida en caso de interrupciones.	CR	L4
Responsable: Analista de seguridad informática			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgo – Aplicaciones
Fecha	01/06/2024		

Activos Involucrados: SO Servidor de Producción, SO Servidor de Aplicaciones, SO Servidor NAS.

Riesgo – Amenaza: [E.8] Difusión de software dañino

Salvaguarda	Actividades propuestas:	TDP	Eficacia
Copias de Seguridad	Realizar respaldos diarios automáticos de los datos de configuración de los sistemas operativos.	PR	L3
	Verificar la integridad de las copias de seguridad, asegurando que los datos almacenados sean consistentes y no hayan sido alterados.	PR	L3
Perfiles de seguridad	Configurar perfiles de seguridad específicos, limitando privilegios y acceso.	PR	L3
Herramientas de chequeo	Contar con un sistema antivirus original y actualizado para detectar y prevenir la presencia de malware o código malicioso.	PR - IM	L4
	Implementar un firewall en el entorno del data center puede ayudar a filtrar el tráfico de red	PR – IM	L4

Responsable: Analista de seguridad informática

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgo – Aplicaciones
Fecha	01/06/2024		
Activos Involucrados: SO Servidor de Producción, SO Servidor de Aplicaciones, SO Servidor NAS.			
Riesgo – Amenaza: [E.20] Vulnerabilidades de los programas			
Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Herramientas de chequeo	Implementar un firewall y sistemas de detección de intrusiones para monitorear y bloquear intento de infiltración.	IM	L4
Cambios (Actualización y mantenimiento)	Aplicar las actualizaciones más recientes que solucionan la mayoría de las vulnerabilidades, además de los parches de seguridad de los sistemas operativos.	CR	L2
Responsable: Analista de seguridad informática			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgo – Aplicaciones
Fecha	01/06/2024		
Activos Involucrados: SO Servidor de Producción, SO Servidor de Aplicaciones, SO Servidor NAS.			
Riesgo – Amenaza: [E.21] Errores de mantenimiento / actualizaciones			
Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Copias de Seguridad	Implementar un sistema de respaldo y recuperación para la restauración del sistema en caso de fallos durante el proceso de actualización y mantenimiento.	IM	L3
	Realizar una revisión de las configuraciones del antes y después de cada actualización o mantenimiento.	PR	L2

Cambios (Actualización y mantenimiento)	Implementar un procedimiento de rollback, en caso de querer deshacer los cambios de configuración incorrectas.	IM	L4
Responsable: Analista de seguridad informática			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgo – Aplicaciones
Fecha	01/06/2024		
Activos Involucrados: SO Servidor de Producción, SO Servidor de Aplicaciones, SO Servidor NAS.			
Riesgo – Amenaza: [A.8] Difusión de software dañino			
Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Copias de Seguridad	Realizar respaldos de las versiones más estables del sistema operativo de los servidores.	PR	L3
Protección de las aplicaciones – Herramientas de chequeo	Contar con un sistema antivirus original y actualizado para detectar y prevenir la presencia de malware o código malicioso.	PR - IM	L4
	Aplicar actualizaciones y parches de seguridad de forma regular a los sistemas operativos.	CR	L3
	Implementar sistemas de detección de intrusiones para identificar actividades maliciosas en los sistemas operativos.	DC	L4
	Establecer restricciones de ejecución para scripts y programas en los servidores.	IM	L4

Aceptación y puesta en operación	Realizar pruebas de penetración para identificar y corregir posibles vulnerabilidades.	DC - CR	L3
Responsable: Analista de seguridad informática			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgo – Aplicaciones
Fecha	01/06/2024		
Activos Involucrados: Sistema Firewall (Cortafuegos)			
Riesgo – Amenaza: [I.5.1] Averías de origen lógico			
Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Copias de Seguridad	Realizar respaldos periódicos de las configuraciones del firewall.	PR	L4
Aseguramiento de disponibilidad	Diseñar un plan de contingencias para restablecer el servicio de manera rápida en caso de interrupciones.	CR	L4
Responsable: Analista de seguridad informática			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgo – Aplicaciones
Fecha	01/06/2024		
Activos Involucrados: Sistema Firewall (Cortafuegos)			
Riesgo – Amenaza: [E.8] Difusión de software dañino			
Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Perfiles de seguridad	Configurar políticas detalladas para permitir o denegar el tráfico en función de diversos criterios, como zonas, aplicaciones, direcciones IP, puertos, usuarios.	PR	L4

Protección de las aplicaciones	Implementar políticas de seguridad para que las aplicaciones no contengan programas que puedan perturbar el funcionamiento normal del sistema operativo o del firewall.	PR	L4
	Utilizar soluciones de filtrado de paquetes en el firewall para prevenir la difusión de software dañino.	IM	L3
Actualizaciones y Parches	Mantener actualizados los parches de seguridad y las actualizaciones del sistema operativo del firewall y de las aplicaciones.	CR	L3
Responsable: Analista de seguridad informática			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgo – Aplicaciones
Fecha	01/06/2024		
Activos Involucrados: Sistema Firewall (Cortafuegos)			
Riesgo – Amenaza: [E.21] Errores de mantenimiento / actualizaciones			
Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Copias de Seguridad	Implementar un sistema de respaldo y recuperación para la restauración del sistema en caso de fallos durante el proceso de actualización y mantenimiento.	IM	L4
Cambios (Actualización y mantenimiento)	Realizar una revisión de las configuraciones del antes y después de cada actualización o mantenimiento.	PR	L2
	Implementar un procedimiento de rollback, en caso de querer deshacer los cambios de configuración incorrectas.	IM	L4
Responsable: Analista de seguridad informática			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgo – Aplicaciones
Fecha	01/06/2024		
Activos Involucrados: Sistema Firewall (Cortafuegos)			
Riesgo – Amenaza: [E.24] Caída del sistema por agotamiento de recursos			

Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Aseguramiento de Disponibilidad	Configurar un cluster para el sistema de firewall. (Alta Disponibilidad "HA")	PR	L4
	Aplicar servicios de CND (Content Delivery Network) para reducir la carga en el servidor que aloja el firewall.	PR	L4
Gestión de Cambios	Implementar controles para evaluar y autorizar cambios antes de su implementación, así como establecer políticas y procedimientos claros para la gestión de cambios.	PR	L4
	Desarrollar un plan de cambios para revertir cambios en caso de problemas	CR	L4
Responsable: Analista de seguridad informática			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgo – Aplicaciones
Fecha	01/06/2024		
Activos Involucrados: Sistema Firewall (Cortafuegos)			
Riesgo – Amenaza: [A.8] Difusión de software dañino			

Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
	Implementar políticas de seguridad para que las aplicaciones no contengan programas que puedan	PR	L4

Protección de las aplicaciones	perturbar el funcionamiento normal del sistema operativo o del firewall.		
	Utilizar soluciones de filtrado de paquetes en el firewall para prevenir la difusión de software dañino.	IM	L4
	Mantener actualizados los parches de seguridad y las actualizaciones del sistema operativo del firewall y de las aplicaciones.	CR	L3
Responsable: Analista de seguridad informática			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgo – Aplicaciones
Fecha	01/06/2024		
Activos Involucrados: Servicio DNS			
Riesgo – Amenaza: [I.5.1] Averías de origen lógico			
Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Copias de Seguridad	Realizar respaldos periódicos de las configuraciones del servicio DNS.	PR	L2
Aseguramiento de disponibilidad	Implementar monitoreo constante del servicio DNS para detectar posibles interrupciones.	PR	L4
	Diseñar un plan de contingencias para restablecer el servicio de manera rápida en caso de interrupciones.	CR	L4
Responsable: Analista de seguridad informática			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgo – Aplicaciones
Fecha	01/06/2024		
Activos Involucrados: Servicio DNS			
Riesgo – Amenaza: [E.8] Difusión de software dañino			

Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Perfiles de seguridad	Configurar políticas detalladas para permitir o denegar el tráfico en función de diversos criterios, como zonas, aplicaciones, direcciones IP, puertos, usuarios.	PR	L4
Protección de las aplicaciones	Implementar políticas de seguridad para que las aplicaciones no contengan programas que puedan perturbar el funcionamiento normal del servicio DNS.	PR	L4
	Mantener actualizados los parches de seguridad y las actualizaciones del servicio DNS.	CR	L3
Responsable: Analista de seguridad informática			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgo – Aplicaciones
Fecha	01/06/2024		
Activos Involucrados: Servicio DNS			
Riesgo – Amenaza: [E.21] Errores de mantenimiento / actualizaciones			

Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Copias de Seguridad	Implementar un sistema de respaldo y recuperación para la restauración del sistema en caso de fallos durante el proceso de actualización y mantenimiento.	IM	L4

Cambios (Actualización y mantenimiento)	Realizar una revisión de las configuraciones del antes y después de cada actualización o mantenimiento.	PR	L3
	Implementar un procedimiento de rollback, en caso de querer deshacer los cambios de configuración incorrectas.	IM	L4
Responsable: Analista de seguridad informática			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgo – Aplicaciones
Fecha	01/06/2024		
Activos Involucrados: Servicio DNS			
Riesgo – Amenaza: [E.24] Caída del sistema por agotamiento de recursos			

Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Aseguramiento de Disponibilidad	Configurar un cluster para el sistema de DNS. (Alta Disponibilidad “HA”)	PR	L4
	Aplicar servicios de CND (Content Delivery Network) para reducir la carga en el servidor que aloja el DNS.	PR	L4
Gestión de Cambios	Implementar controles para evaluar y autorizar cambios antes de su implementación, así como establecer políticas y procedimientos claros para la gestión de cambios.	PR	L3
	Desarrollar un plan de cambios para revertir cambios en caso de problemas	CR	L4
Responsable: Analista de seguridad informática			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgo – Aplicaciones
Fecha	01/06/2024		
Activos Involucrados: Servicio DNS			
Riesgo – Amenaza: [A.8] Difusión de software dañino			

Salvaguarda	Actividades propuestas:	TDP	Eficacia
Protección de las aplicaciones	Implementar políticas de seguridad para que las aplicaciones no contengan programas que puedan perturbar el funcionamiento normal del DNS.	PR	L4
	Utilizar soluciones de filtrado de paquetes en el DNS para prevenir la difusión de software dañino.	IM	L4
	Mantener actualizados los parches de seguridad y las actualizaciones del DNS.	CR	L3
Responsable: Analista de seguridad informática			

Equipos [HW]

Realizado por:	Borbor Tumbaco Ariel	**Nombre del reporte:**	Plan De Tratamientos de riesgos – Equipos
Fecha	01/06/2024		
Activos Involucrados: Servidor de producción, Servidor de Aplicaciones, Servidor NAS – Switches – Routers			
Riesgo – Amenaza: [N.1] Fuego - [I.1] Fuego			

Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Aseguramiento de la disponibilidad	Almacenar los respaldos en ubicaciones seguras y fuera del sitio para minimizar el riesgo de pérdida de datos debido a eventos locales, como incendios o robos.	IM	L3
	Instalación de sistema contra incendios (alarmas).	PR	L3
	Establecer sistemas de recuperación rápida para equipos críticos.	IM	L4
Copias de seguridad	Realizar respaldos de los datos almacenados en servidores y hardware de comunicación en medios de almacenamientos externos o en la nube.	PR	L4
	Realizar copias de seguridad de los datos de configuración de los equipos informáticos.	PR	L4
Operación	Construcción de un piso y techo falso a partir de materiales incombustibles y resistentes al fuego.	PR	L4
	Realizar simulacros contra incendios de manera periódica.	IM	L3
	Capacitar al personal que interactúe directamente con el sitio sobre el uso correcto de los extintores.	IM	L3

	Mantener las conexiones eléctricas en perfecto estado para prevenir cortocircuitos.	PR	L4
Correcta instalación	Asegurar que los equipos informáticos y los racks estén debidamente conectados a un sistema de puesta a tierra.	PR	L4
Protección de cableado	Aplicar una protección adicional al cableado eléctrico y al cableado de red.	IM	L4
	Realizar inspecciones regulares del cableado para identificar desgaste o daños.	IM	L3
Responsable: Analista de seguridad informática, Coordinador/a del departamento de sistemas y recursos tecnológicos.			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del reporte:**	Plan De Tratamientos de riesgos – Equipos
Fecha	01/06/2024		
Activos Involucrados: Servidor de producción, Servidor de Aplicaciones, Servidor NAS – Switches – Routers			
Riesgo – Amenaza: [N.2] Daños por agua - [I.2] Daños por agua			
Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Aseguramiento de la disponibilidad	Realizar respaldos de los datos almacenados en servidores y hardware de comunicación en medios de almacenamientos externos o en la nube.	PR	L4
	Almacenar los respaldos en ubicaciones seguras y fuera del sitio para minimizar el riesgo de pérdida de datos debido a eventos locales, como incendios o robos.	IM	L3

	Colocar los equipos críticos y cables a una altura adecuada para evitar daños por agua.	PR	L4
	Establecer sistemas de recuperación rápida para equipos críticos.	IM	L4
Operación	Implementar techos y paredes impermeables para evitar daños por agua.	PR	L3
	Implementar un sistema de drenaje que sea adecuado en caso de inundaciones.	IM	L4
	Mantener los equipos que no se están utilizando apagados.	IM	L3
	Aplicar protección adicional a tomacorrientes e interruptores para mantener aislado para prevenir cortocircuitos.	PR	L3
Correcta instalación	Asegurar que los equipos informáticos y los racks estén debidamente conectados a un sistema de puesta a tierra.	PR	L4
Protección de cableado	Aplicar una protección adicional al cableado eléctrico y al cableado de red.	IM	L4
	Realizar inspecciones regulares del cableado para identificar desgaste o daños.	IM	L3
Responsable: Analista de seguridad informática, Coordinador/a del departamento de sistemas y recursos tecnológicos.			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del reporte:**	Plan De Tratamientos de riesgos – Equipos
Fecha	01/06/2024		

Activos Involucrados: Servidor de producción, Servidor de Aplicaciones, Servidor NAS – Switches – Routers

Riesgo – Amenaza: [I.6] Corte de suministro eléctrico

Salvaguarda	Actividades propuestas:	TDP	Eficacia
Aseguramiento de la disponibilidad	Implementar procedimientos de respaldo de los servicios, configuraciones de equipos y activos críticos.	PR	L4
	Establecer procedimientos de apagado seguro y arranque escalonado para los equipos tras un corte de energía.	IM	L3
Correcta Instalación	Configurar adecuadamente los equipos para minimizar el consumo de energía y maximizar la eficiencia energética.	IM	L3
	Distribuir la carga eléctrica de manera equilibrada entre los diferentes circuitos para evitar sobrecargas.	PR	L3
Suministro Eléctrico	Implementar sistemas de alimentación ininterrumpida (UPS) para respaldo de energía.	IM	L3
	Asegurarse de que los UPS estén dimensionados correctamente para soportar todos los equipos críticos durante el tiempo necesario.	PR	L3
	Sustituir baterías de UPS y realizar pruebas de carga en generadores para asegurar su operatividad.	CR	L3

Responsable: Analista de seguridad informática, Coordinador/a del departamento de sistemas y recursos tecnológicos

Realizado por:	Borbor Tumbaco Ariel	**Nombre del reporte:**	Plan De Tratamientos de riesgos – Equipos
Fecha	01/06/2024		

Activos Involucrados: Servidor de producción, Servidor de Aplicaciones, Servidor NAS – Switches – Routers

Riesgo – Amenaza: [I.7] Condiciones inadecuadas de temperatura

Salvaguarda	Actividades propuestas:	TDP	Eficacia
Climatización	Implementar un sistema de ventilación y aire acondicionado para garantizar un control de temperatura adecuado y continuo solamente para el Data Center.	IM	L3
	Realizar mantenimiento regular de los sistemas de climatización, enfriamiento, y ventilación para un rendimiento óptimo.	IM	L3
Correcta Instalación	Configurar y mantener una temperatura adecuada del equipo de climatización entre unos 18 – 27 C° (64 – 80 F°).	PR	L3
	Asegurarse de que los sistemas de climatización estén dimensionados correctamente para manejar la carga térmica de los equipos.	PR	L3
	Ubicar los equipos de alta densidad térmica en áreas donde la climatización es más eficiente.	IM	L2
Control del flujo de aire	Instalar paneles de obturación entre los racks para mejorar el flujo de aire y prevenir la recirculación del aire caliente.	PR	L3

Responsable: Analista de seguridad informática, Coordinador/a del departamento de sistemas y recursos tecnológicos

Realizado por:	Borbor Tumbaco Ariel	**Nombre del reporte:**	Plan De Tratamientos de riesgos – Equipos
Fecha	01/06/2024		

Activos Involucrados: Servidor de producción, Servidor de Aplicaciones, Servidor NAS – Switches – Routers

Riesgo – Amenaza: [E.23] Errores de mantenimiento / actualización

Salvaguarda	Actividades propuestas:	TDP	Eficacia
Aseguramiento de la disponibilidad	Implementar un sistema de alta disponibilidad y redundancia para mantener la operación en casos de errores de mantenimiento o actualizaciones.	PR	L4
	Elegir el nivel RAID que mejor se ajuste a las necesidades de disponibilidad y rendimiento de los servidores. RAID 1, RAID 5, RAID 6 y RAID 10 son comunes para alta disponibilidad.	PR	L4
	Configurar el RAID en un controlador dedicado o en un arreglo de almacenamiento externo para optimizar el rendimiento y la fiabilidad.	PR	L4
	Optimizar el sistema operativo y las aplicaciones para trabajar eficientemente con el RAID configurado.	IM	L3
Operación	Establecer una gestión de incidencias para la respuesta a incidentes durante o después del mantenimiento o actualizaciones.	CR	L4
Cambios (Actualizaciones y mantenimiento)	Realizar una revisión de las configuraciones del antes y después de cada actualización o mantenimiento.	PR	L3
	Implementar un procedimiento de rollback, en caso de querer deshacer los cambios de configuración incorrectas.	PR	L4

Responsable: Analista de seguridad informática.

Realizado por:	Borbor Tumbaco Ariel	**Nombre del reporte:**	Plan De Tratamientos de riesgos – Equipos
Fecha	01/06/2024		

Activos Involucrados: Servidor de producción, Servidor de Aplicaciones, Servidor NAS – Switches – Routers

Riesgo – Amenaza: [E.24] Caída del sistema por agotamiento de recursos

Salvaguarda	Actividades propuestas:	TDP	Eficacia
Aseguramiento de Disponibilidad	Optimizar las configuraciones de los equipos para asegurar un uso eficiente de los recursos y prevenir agotamientos innecesarios.	PR	L3
	Establecer un sistema de monitoreo constante de los recursos del sistema, como uso de CPU, memoria y almacenamiento. Implementar herramientas automatizadas que generen alertas cuando se detecten umbrales críticos.	PR	L3
	Optimizar las configuraciones del sistema operativo y las aplicaciones para utilizar los recursos de manera eficiente.	PR	L3
	Implementar balanceadores de carga para distribuir el tráfico y las solicitudes entre múltiples servidores, evitando la sobrecarga de un solo sistema.	IM	L4
Gestión de Cambios	Diseñar un plan de cambios que cumpla con las condiciones en caso de que el recurso sufra una caída por agotamiento.	CR	L4

Responsable: Analista de seguridad informática

Realizado por:	Borbor Tumbaco Ariel	**Nombre del reporte:**	Plan De Tratamientos de riesgos – Equipos
Fecha	01/06/2024		

Activos Involucrados: Servidor de producción, Servidor de Aplicaciones, Servidor NAS – Switches – Routers

Riesgo – Amenaza: [A.4] Manipulación de los ficheros de configuración

Salvaguarda	Actividades propuestas:	TDP	Eficacia
Identificación y autenticación	Implementar autenticación multifactor (MFA) para todos los usuarios que necesiten acceso a los ficheros de configuración.	PR	L3
	Configurar permisos específicos para cada usuario o grupo de usuarios, limitando el acceso a los ficheros de configuración solo a aquellos que lo necesiten.	PR	L3
	Implementar políticas de contraseñas seguras, incluyendo requisitos de longitud, complejidad y caducidad.	PR	L3
Control de acceso lógico	Utilizar certificados digitales o claves SSH para la autenticación de usuarios remotos en los equipos.	PR	L3
	Aplicar el principio de mínimos privilegios, asegurando que los usuarios solo tengan los permisos necesarios para realizar sus tareas específicas.	IM	L3
Protección de la integridad	Asignar roles y responsabilidades claras para la creación, revisión y aprobación de cambios en los ficheros de configuración.	IM	L2
Protección de la confidencialidad	Implementar el cifrado de los ficheros de configuración tanto en reposo como en tránsito.	PR	L3

Responsable: Analista de seguridad informática

Realizado por:	Borbor Tumbaco Ariel	**Nombre del reporte:**	Plan De Tratamientos de riesgos – Equipos
Fecha	01/06/2024		

Activos Involucrados: Servidor de producción, Servidor de Aplicaciones, Servidor NAS – Switches – Routers

Riesgo – Amenaza: [A.24] Denegación de servicios

Salvaguarda	Actividades propuestas:	TDP	Eficacia
Aseguramiento de disponibilidad	Asegurar que la infraestructura de red y servidores pueda escalar para manejar incrementos repentinos en el tráfico.	IM	L3
	Optimizar la configuración del sistema operativo y aplicaciones para utilizar los recursos de manera eficiente y reducir la carga en los servidores.	IM	L3
	Implementar caching de contenido para reducir la carga en los servidores principales.	IM	L3
Herramientas de chequeo	Implementar sistemas de protección Anti-DDoS en la nube, como Cloudflare, Akamai Kona Site Defender, AWS Shield o Azure DDoS Protection, para desviar y mitigar el tráfico malicioso antes de que alcance los servidores de la organización.	PR	L3
	Desplegar dispositivos de mitigación de DDoS, como los ofrecidos por Arbor Networks, Radware DefensePro o Fortinet FortiDDoS, para filtrar el tráfico malicioso en el perímetro de la red.	PR	L3
Operación	Configurar la red para minimizar la superficie de ataque, utilizando técnicas como la segmentación de red y el uso de VLANs.	PR	L3

Herramienta de monitorización de tráfico	Implementar firewalls de aplicaciones web (WAF) y sistemas de detección y prevención de intrusiones (IDS/IPS) para filtrar el tráfico malicioso.	PR	L4
Responsable: Analista de seguridad informática			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del reporte:**	Plan De Tratamientos de riesgos – Equipos
Fecha	01/06/2024		
Activos Involucrados: Servidor de producción, Servidor de Aplicaciones, Servidor NAS – Switches – Routers			
Riesgo – Amenaza: [A.7] Uso no previsto - [A.11] Acceso no autorizado - [A.23] Manipulación de hardware - [A.25] Robo de equipos -			

Salvaguarda	Actividades propuestas:	TDP	Eficacia
Identificación de usuarios	Implementar un sistema de credenciales con códigos QR para el acceso al cuarto de servidores.	PR	L4
Biometría	Implementar un sistema biométrico para el acceso al cuarto de servidores solo personal autorizado.	PR	L4
Protección de las instalaciones	Implementar un sistema de vigilancia en video en las áreas de acceso físico del data center.	PR	L4
	Aplicar políticas de identificación para los usuarios que visitan el data center y no son parte del	PR	L3
	Evitar el acceso de persona no autorizado al cuarto de servidore.	IM	L3
	Establecer políticas de uso y manejo de dispositivos móviles dentro del cuarto de servidores.	PR	L3
Responsable: Analista de seguridad informática, Coordinador/a del departamento de sistemas y recursos tecnológicos.			

Comunicaciones [COM]

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgo
Fecha	01/06/2024		
Activos Involucrados: Internet, Red Local, Red inalámbrica, Telefonía IP			
Riesgo – Amenaza: [I.8] Fallo de servicios de comunicaciones			

Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Aseguramiento de disponibilidad	Implementar enlaces redundantes con diferentes proveedores de servicios de Internet (ISP) para garantizar la conectividad continua en caso de fallo de un enlace.	PR	L4
	Configuración de balanceo de carga para distribuir el tráfico y minimizar el impacto de fallos.	IM	L4
	Establecimiento de procedimientos de recuperación ante fallos para restablecer la conectividad.	CR	L4
	Implementar sistemas de monitoreo de red en tiempo real para detectar y alertar sobre cualquier interrupción o degradación del servicio de comunicaciones.	DC	L4
Operación	Implementación de sistemas de respaldo garantizando la continuidad del servicio de internet restableciendo la conectividad de manera rápida y eficiente.	PR	L4
	Implementar redundancia en la infraestructura de comunicaciones.	PR	L4
	Diseñar la red local (LAN) y la red inalámbrica con topologías redundantes, utilizando switches y routers con capacidades de failover.	PR	L3
Responsable: Analista de seguridad informática			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del Reporte:**	Plan De Tratamiento de Riesgo
Fecha	01/06/2024		
Activos Involucrados: Internet, Red Local, Red inalámbrica, Telefonía IP			
Riesgo – Amenaza: [E.2] Errores del administrador del sistema			

Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Control de acceso lógico	Implementar un sistema IAM para gestionar y controlar de manera centralizada las identidades y los accesos a los recursos de red	PR	L4
Perfiles de seguridad	Asegurar que cada usuario tenga un único identificador y que los permisos se asignen basados en el principio de menor privilegio	PR	L3
Aseguramiento de disponibilidad	Implementar políticas y procedimientos de cambios controlados para evitar errores de configuración.	PR	L4
	Mantener documentación actualizada de la configuración y procedimientos operativos.	IM	L4
	Implementación de redundancia de enlaces de Internet para garantizar la disponibilidad	PR	L4
	Configurar sistemas para registrar todas las actividades de acceso y cambios realizados por administradores en la red y servicios de comunicación	IM	L3
Protección de la integridad de los datos intercambiados	Aplicar métodos de cifrado para la proteger la integridad de los datos durante la transmisión.	PR	L4
	Mantener Backups regulares de los datos para garantizar la disponibilidad de versiones integras.	IM	L4
Responsable: Analista de seguridad informática			

Realizado por:	Borbor Tumbaco	**Nombre del Reporte:**	Plan De Tratamiento de Riesgo
Fecha	01/06/2024		
Activos Involucrados: Internet, Red Local, Red inalámbrica, Telefonía IP			
Riesgo – Amenaza: [E.4] Errores de configuración			
Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Aseguramiento de disponibilidad	Establecer procesos de verificación de cambios antes de implementarlos para prevenir errores.	DC	L4
	Mantener documentación actualizada de la configuración y procedimientos operativos.	DC	L4
Protección de la integridad	Mantener backups regulares de los datos de configuración de los equipos de comunicación.	IM	L4
Responsable: Analista de seguridad informática			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del reporte:**	Plan De Tratamientos de riesgos
Fecha	01/06/2024		
Activos Involucrados: Internet, Red Local, Red inalámbrica, Telefonía IP			
Riesgo – Amenaza: [E.9] Errores de [Re] - encaminamiento			
Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Protección de la integridad de los datos intercambiados	Implementar filtros de seguridad en los dispositivos de red para prevenir rutas no autorizadas.	PR	L4
	Implementar protocolos de enrutamiento seguros como Secure BGP (Border Gateway Protocol) o RPKI (Resource Public Key Infrastructure) para verificar la autenticidad de los anuncios de rutas y prevenir el enrutamiento malicioso o erróneo	PR	L3

	Aplicar mecanismos de cifrado para proteger la integridad de los datos que se transmiten,	PR	L4
Operación	Configurar rutas de enrutamiento redundantes para proporcionar caminos alternativos en caso de fallo o error de encaminamiento	PR	L3
	Mantener todos los dispositivos de red, incluidos enrutadores y switches, actualizados con los últimos parches y actualizaciones de firmware.	CR	L3
	Realizar revisiones regulares de las configuraciones de enrutamiento.	DC	L3
	Implementar segmentación de redes mediante VLANs para aislar diferentes tipos de tráfico y minimizar el impacto de errores de enrutamiento en segmentos específicos de la red	PR	L3
Responsable: Analista de seguridad informática			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del reporte:**	Plan De Tratamientos de riesgos
Fecha	01/06/2024		
Activos Involucrados: Internet, Red Local, Red inalámbrica, Telefonía IP			
Riesgo – Amenaza: [E.10] Errores de Secuencia			
Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Protección de la integridad de los datos intercambiados	Utilizar protocolos de comunicación confiables como TCP (Transmission Control Protocol), que incluyen mecanismos de control de secuencia para asegurar que los paquetes de datos se entreguen en el orden correcto.	PR	L4

	Configurar firewall y sistemas de detección de intrusos (IDS) para bloquear tráfico sospechoso.	PR	L4
	Implementar protocolos de enrutamiento seguro y autenticados.	PR	L3
	Aplicar mecanismos de cifrado para proteger la integridad de los datos que se transmiten,	PR	L4
Operación	Mantener todos los dispositivos de red, incluidos enrutadores y switches, actualizados con los últimos parches y actualizaciones de firmware.	PR	L3
	Realizar revisiones regulares de las configuraciones de enrutamiento.	DC	L3
	Configurar sistemas de monitoreo de red para identificar anomalías en la secuencia de datos.	DC	L4
	Implementar segmentación de redes mediante VLANs para aislar diferentes tipos de tráfico y minimizar el impacto de errores de enrutamiento en segmentos específicos de la red	PR	L3
	Mantener una configuración adecuada y actualizada de todos los dispositivos de red para asegurar que los datos se enruten correctamente y se entreguen en el orden correcto	CR	L3
Responsable: Analista de seguridad informática			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del reporte:**	Plan De Tratamientos de riesgos
Fecha	01/06/2024		

Activos Involucrados: Internet, Red Local, Red inalámbrica, Telefonía IP

Riesgo – Amenaza: [E.15] Alteración de la información - [E.19] Fugas de información - [A.11] Acceso no autorizado

Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Identificación de los usuarios	Establecer un sistema de control de acceso basado en roles para limitar el acceso a la información mediante estos activos.	PR	L4
Cifrado de información	Implementar cifrado de extremo a extremo para la protección de la información durante la transmisión.	PR	L4
	Configurar firewalls y sistemas de detección de intrusiones para filtrar y bloquear intentos de alteración de la información	PR	L4
Copias de seguridad	Realizar copias de seguridad periódicas de los datos para poder recuperar la información original en caso de alteraciones.	CR	L4
Seguridad Wireless (WiFi)	Aplicar el protocolo robusto WPA2 (Wi-Fi Protected Access 3), para la protección de la autenticidad y confidencialidad de la conexión.	PR	L3
	Utilizar claves (contraseñas) de seguridad fuertes y complejas en las diferentes redes inalámbricas.	PR	L3

Responsable: Analista de seguridad informática

Realizado por:	Borbor Tumbaco Ariel	**Nombre del reporte:**	Plan De Tratamientos de riesgos
Fecha	01/06/2024		
Activos Involucrados: Internet, Red Local, Red inalámbrica, Telefonía IP			
Riesgo – Amenaza: [E.24] Caída del sistema por agotamiento de recursos			

Salvaguarda	Actividades propuestas:	TDP	Eficacia
Aseguramiento de disponibilidad	Establecer límites de recursos para usuarios y servicios evitando el uso excesivo.	PR	L4
	Establecer procedimientos de escalado automático de recursos para manejar picos inesperados de demanda.	IM	L4
Operación	Configurar sistemas de monitoreo de salud del hardware asociado a los activos de comunicación.	DC	L4
	Implementar sistemas de alerta temprana para identificar signos de agotamiento de recursos.	DC	L3
Responsable: Analista de seguridad informática			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del reporte:**	Plan De Tratamientos de riesgos
Fecha	01/06/2024		
Activos Involucrados: Internet, Red Local, Red inalámbrica, Telefonía IP			
Riesgo – Amenaza: [A.24] Denegación de servicios			

Salvaguarda	Actividades propuestas:	TDP	Eficacia
Protección de las comunicaciones	Implementar sistema de firewall y filtros de seguridad para bloquear tráfico malicioso.	PR	L4
	Configurar sistema de detección de intrusos (IDS) para identificar patrones de ataque y comportamiento sospechoso.	DC	L4

	Configurar sistema de prevención de intrusos (IPS).	PR	L4
Responsable: Analista de seguridad informática			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del reporte:**	Plan De Tratamientos de riesgos
Fecha	01/06/2024		
Activos Involucrados: Internet, Red Local, Red inalámbrica, Telefonía IP			
Riesgo – Amenaza: [A.24.1] Saturación de los canales de información			
Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Aseguramiento de la disponibilidad	Implementar sistemas de control de ancho de banda para evitar la saturación de los canales de información.	PR	L4
	Establecer límites de transferencia de datos para usuarios y servicios.	PR	L4
	Implementar sistemas de balanceo de carga para distribuir equitativamente la carga entre los canales.	IM	L4
	Priorizar el tráfico crítico y esencial en situaciones de saturación.	IM	L4
	Realizar análisis periódicos de la capacidad de los canales y enlaces de red.	IM	L3
Responsable: Analista de seguridad informática			

Elementos auxiliares [AUX]

Realizado por:	Borbor Tumbaco Ariel	**Nombre del reporte:**	Plan De Tratamientos de riesgos
Fecha	01/06/2024		
Activos Involucrados: Fuente de Alimentación, Sistema de alimentación Ininterrumpida, Cableado Estructurado, Equipos de climatización, Cámaras de seguridad			
Riesgo – Amenaza: [N.1] Fuego - [I.1] Fuego			

Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Aseguramiento de la disponibilidad	Instalación de sistema contra incendios (alarmas).	PR	L4
	Implementación de señales de Prohibido Fumar, Prohibido comer, en el interior de centro de cómputo como sus alrededores.	PR	L3
	Instalación de suficientes extintores contra incendios en puntos estratégicos del Data Center.	PR	L3
	Mantener las conexiones eléctricas en perfecto estado para prevenir cortocircuitos.	PR	L4
Operación	Construcción de un piso y techo falso a partir de materiales incombustibles y resistentes al fuego.	PR	L4
	Realizar simulacros contra incendios de manera periódica.	IM	L3
	Capacitar al personal que interactúe directamente con el sitio sobre el uso correcto de los extintores.	IM	L3
	Dar mantenimiento y revisión periódica a los sistemas contra incendios.	IM	L3

	Implementar y configurar sistema de detección de humo y fuego para una alerta temprana en caso de incendio.	DC	L4
Correcta Instalación	Asegurar que los equipos de elementos auxiliares estén debidamente conectados a un sistema de puesta a tierra.	PR	L4
Protección de cableado	Aplicar una protección adicional al cableado eléctrico y al cableado de red.	IM	L4
	Realizar inspecciones regulares del cableado para identificar desgaste o daños.	IM	L3
Responsable: Analista de seguridad informática, Coordinador/a del departamento de Tics, Técnicos y personal de mantenimiento.			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del reporte:**	Plan De Tratamientos de riesgos
Fecha	01/06/2024		
Activos Involucrados: Fuente de Alimentación, Sistema de alimentación Ininterrumpida, Cableado Estructurado, Equipos de climatización, Cámaras de seguridad			
Riesgo – Amenaza: [N.2] Daños por agua - [I.2] Daños por agua			
Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Aseguramiento de la disponibilidad	Realizar respaldos de los datos almacenados en servidores y hardware de comunicación en medios de almacenamientos externos o en la nube.	PR	L4
	Almacenar los respaldos en ubicaciones seguras y fuera del sitio para minimizar el riesgo de pérdida de datos debido a eventos locales, como incendios o robos.	IM	L3

	Colocar los equipos críticos y cables a una altura adecuada para evitar daños por agua.	PR	L4
	Establecer sistemas de recuperación rápida para equipos críticos.	IM	L4
Operación	Implementar techos y paredes impermeables para evitar daños por agua.	PR	L3
	Implementar un sistema de drenaje que sea adecuado en caso de inundaciones.	IM	L4
	Mantener los equipos que no se están utilizando apagados.	IM	L3
	Aplicar protección adicional a tomacorrientes e interruptores para mantener aislado para prevenir cortocircuitos.	PR	L3
Correcta instalación	Asegurar que los equipos informáticos y los racks estén debidamente conectados a un sistema de puesta a tierra.	PR	L4
	Asegurar que las cámaras de seguridad estén a una altura adecuada en caso de inundaciones.	PR	L3
Protección de cableado	Aplicar una protección adicional al cableado eléctrico y al cableado de red.	IM	L4
	Realizar inspecciones regulares del cableado para identificar desgaste o daños.	IM	L3
Responsable: Analista de seguridad informática, Coordinador/a del departamento de sistemas y recursos tecnológicos.			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del reporte:**	Plan De Tratamientos de riesgos
Fecha	01/06/2024		

Activos Involucrados: Fuente de Alimentación, Sistema de alimentación Ininterrumpida, Cableado Estructurado, Equipos de climatización, Cámaras de seguridad

Riesgo – Amenaza: [I.6] Corte de suministro eléctrico

Salvaguarda	Actividades propuestas:	TDP	Eficacia
Aseguramiento de la disponibilidad	Implementar procedimientos de respaldo de los servicios, configuraciones de equipos y activos críticos.	PR	L4
	Establecer procedimientos de apagado seguro y arranque escalonado para los equipos tras un corte de energía.	IM	L3
Suministro Eléctrico	Implementar sistemas de alimentación ininterrumpida (UPS) para respaldo de energía.	IM	L4

Responsable: Analista de seguridad informática, Coordinador/a del departamento de sistemas y recursos tecnológicos.

Realizado por:	Borbor Tumbaco Ariel	**Nombre del reporte:**	Plan De Tratamientos de riesgos
Fecha	01/06/2024		

Activos Involucrados: Fuente de Alimentación, Sistema de alimentación Ininterrumpida, Cableado Estructurado, Equipos de climatización, Cámaras de seguridad

Riesgo – Amenaza: [E.23] Errores de mantenimiento / actualización

Salvaguarda	Actividades propuestas:	TDP	Eficacia

Aseguramiento de la disponibilidad	Realizar las respectivas revisiones y mantenimiento periódicos de los elementos auxiliares.	PR	L4
Gestión Cambios	Diseñar una gestión de cambios en caso de que el equipo auxiliar no pueda seguir en funcionamiento o se necesite un cambio de alguna pieza.	CR	L4
Responsable: Analista de seguridad informática, Coordinador/a del departamento de sistemas y recursos tecnológicos.			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del reporte:**	Plan De Tratamientos de riesgos
Fecha	01/06/2024		
Activos Involucrados: Fuente de Alimentación, Sistema de alimentación Ininterrumpida, Cableado Estructurado, Equipos de climatización, Cámaras de seguridad			
Riesgo – Amenaza: [A.7] Uso no previsto - [A.11] Acceso no autorizado – [A.23] Manipulación del Hardware - [A.25] Robo de equipos			
Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Identificación de usuarios	Implementar un sistema de credenciales con códigos QR para el acceso al cuarto de servidores.	PR	L3
Biometría	Implementar un sistema biométrico para el acceso al cuarto de servidores solo personal autorizado.	PR	L3
Protección de las instalaciones	Implementar un sistema de vigilancia en video en las áreas de acceso físico del data center.	PR	L3
	Aplicar políticas de identificación para los usuarios que visitan el data center y no son parte del departamento encargado.	PR	L4

	Evitar el acceso de personal no autorizado al cuarto de servidores.	IM	L3
	Establecer políticas de uso y manejo de dispositivos móviles dentro del cuarto de servidores.	PR	L4
Responsable: Analista de seguridad informática, Coordinador/a del departamento de sistemas y recursos tecnológicos.			

Instalaciones [L]

Realizado por:	Borbor Tumbaco Ariel	**Nombre del reporte:**	Plan De Tratamientos de riesgos
Fecha	01/06/2024		
Activos Involucrados: Cuarto de Servidores			
Riesgo – Amenaza: [N.1] Fuego - [I.1] Fuego			
Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Protección frente a desastres	Instalación de sistema contra incendios (alarmas).	PR	L4
	Implementación de señales de Prohibido Fumar, Prohibido comer, en el interior de centro de cómputo como sus alrededores.	PR	L3
	Instalación de suficientes extintores contra incendios en puntos estratégicos del Data Center.	PR	L3
	Implementación de sistemas de detección y extinción de incendios.	PR	L4
Operación	Construcción de un piso y techo falso a partir de materiales incombustibles y resistentes al fuego.	PR	L4

	Realizar simulacros contra incendios de manera periódica.	IM	L3
	Capacitar al personal que interactúe directamente con el sitio sobre el uso correcto de los extintores.	IM	L3
	Mantener las conexiones eléctricas en perfecto estado para prevenir cortocircuitos.	PR	L4
Correcta Instalación	Asegurar que los equipos informáticos y los racks estén debidamente conectados a un sistema de puesta a tierra.	PR	L4
Protección del Cableado	Separar el cableado de energía del cableado de datos para reducir el riesgo de incendios por sobrecalentamiento.	PR	L3
Responsable: Analista de seguridad informática, Coordinador/a del Área de sistemas y recursos tecnológicos.			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del reporte:**	Plan De Tratamientos de riesgos
Fecha	01/06/2024		
Activos Involucrados: Cuarto de Servidores			
Riesgo – Amenaza: [N.2] Daños por agua - [I.2] Daños por agua			
Salvaguarda	**Actividades propuestas:**	**TDP**	**Eficacia**
Aseguramiento de la disponibilidad	Realizar respaldos de los datos almacenados en servidores y hardware de comunicación en medios de almacenamientos externos o en la nube.	PR	L4
	Almacenar los respaldos en ubicaciones seguras y fuera del sitio para minimizar el riesgo de pérdida de	IM	L3

	datos debido a eventos locales, como incendios o robos.		
	Colocar los equipos críticos y cables a una altura adecuada para evitar daños por agua.	PR	L4
	Establecer sistemas de recuperación rápida para equipos críticos.	IM	L4
Operación	Implementar techos y paredes impermeables para evitar daños por agua.	PR	L3
	Implementar un sistema de drenaje que sea adecuado en caso de inundaciones.	IM	L4
	Mantener los equipos que no se están utilizando apagados.	IM	L3
	Aplicar protección adicional a tomacorrientes e interruptores para mantener aislado para prevenir cortocircuitos.	PR	L3
Correcta instalación	Asegurar que los equipos informáticos y los racks estén debidamente conectados a un sistema de puesta a tierra.	PR	L4
Protección de cableado	Aplicar una protección adicional al cableado eléctrico y al cableado de red.	IM	L4
	Realizar inspecciones regulares del cableado para identificar desgaste o daños.	IM	L3
Responsable: Analista de seguridad informática, Coordinador/a del Área de sistemas y recursos tecnológicos			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del reporte:**	Plan De Tratamientos de riesgos
Fecha	01/06/2024		

Activos Involucrados: Cuarto de Servidores

Riesgo – Amenaza: [I.6] Corte de suministro eléctrico

Salvaguarda	Actividades propuestas:	TDP	Eficacia
Aseguramiento de la disponibilidad	Implementar sistemas de alimentación ininterrumpida (UPS) para respaldo de energía.	IM	L4
	Implementar procedimientos de respaldo de los servicios, configuraciones de equipos y activos críticos.	PR	L4
	Establecer procedimientos de apagado seguro y arranque escalonado para los equipos tras un corte de energía.	IM	L3

Responsable: Analista de seguridad informática, Coordinador/a del Área de sistemas y recursos tecnológicos.

Realizado por:	Borbor Tumbaco Ariel	**Nombre del reporte:**	Plan De Tratamientos de riesgos
Fecha	01/06/2024		

Activos Involucrados: Cuarto de Servidores

Riesgo – Amenaza: [I.7] Condiciones inadecuadas de temperatura

Salvaguarda	Actividades propuestas:	TDP	Eficacia
Climatización	Implementar sistema de climatización para garantizar un control de temperatura adecuado y continuo.	IM	L3
	Realizar mantenimiento regular de los sistemas de climatización para un rendimiento optimo.	IM	L3

Responsable: Administrador del sistema, Técnicos y personal de mantenimiento.

Realizado por:	Borbor Tumbaco Ariel	**Nombre del reporte:**	Plan De Tratamientos de riesgos
Fecha	01/06/2024		
Activos Involucrados: Cuarto de Servidores			
Riesgo – Amenaza: [A.7] Uso no previsto - [A.11] Acceso no autorizado - [A.25] Robo de equipos			

Salvaguarda	Actividades propuestas:	TDP	Eficacia
Identificación de usuarios	Implementar un sistema de credenciales con códigos QR para el acceso al cuarto de servidores.	PR	L3
Biometría	Implementar un sistema biométrico para el acceso al cuarto de servidores solo personal autorizado.	PR	L3
Protección de las instalaciones	Implementar un sistema de vigilancia en video en las áreas de acceso físico del data center.	PR	L3
	Aplicar políticas de identificación para los usuarios que visitan el data center y no son parte del departamento encargado.	PR	L4
	Evitar el acceso de personal no autorizado al cuarto de servidores.	IM	L3
	Establecer políticas de uso y manejo de dispositivos móviles dentro del cuarto de servidores.	PR	L4
Responsable: Analista de seguridad informática, Coordinador/a del departamento de Tics			

Personal [L]

Realizado por:	Borbor Tumbaco Ariel	**Nombre del reporte:**	Plan De Tratamientos de riesgos
Fecha	01/06/2024		
Activos Involucrados: Coordinador/a, Administrador del Sistema, Administrador de base de datos, Desarrolladores/Programadores			
Riesgo – Amenaza: [E.18] Destrucción de Información – [E.19] Fugas de información – [A.18] Destrucción de Información - [A.19] Revelación de Información			

Salvaguarda	Actividades propuestas:	TDP	Eficacia
Formación y concienciación	Implementar políticas sobre la protección y confidencialidad de la información relevante y sensible del Data Center.	PR - AW	L3
	Impartir sesiones de formación sobre políticas de seguridad de la información y procedimientos para el manejo adecuado de datos sensibles.	PR - AW	L3
	Proporcionar formación continua sobre nuevas amenazas y técnicas de ataque para mantener actualizado al personal.	PR - AW	L3
Responsable: Coordinador/a del Área de sistemas y recursos tecnológicos			

Realizado por:	Borbor Tumbaco Ariel	**Nombre del reporte:**	Plan De Tratamientos de riesgos
Fecha	01/06/2024		

Activos Involucrados: Coordinador/a, Administrador del Sistema, Administrador de base de datos, Desarrolladores/Programadores

Riesgo – Amenaza: [A.28] Indisponibilidad del Personal

Salvaguarda	Actividades propuestas:	TDP	Eficacia
Gestión del Personal	Definir y documentar claramente los roles y responsabilidades de cada empleado en las funciones críticas asociadas al Centro de Datos.	PR	L4
	Evaluar y ajustar periódicamente las políticas y procedimientos de segregación de tareas en función de cambios en la estructura organizativa del Departamento de TIC's.	PR	L4
Aseguramiento de la disponibilidad	Ofrecer programas de capacitación y desarrollo profesional para el personal en roles críticos, asegurando que estén actualizados con las últimas tecnologías y prácticas de la industria.	PR	L3
	Identificar y capacitar a miembros del equipo secundarios como respaldo para roles críticos.	CR	L3

Responsable: Coordinador/a del Área de sistemas y recursos tecnológicos

Realizado por:	Borbor Tumbaco Ariel	**Nombre del reporte:**	Plan De Tratamientos de riesgos
Fecha	01/06/2024		
Activos Involucrados: Coordinador/a, Administrador del Sistema, Administrador de base de datos, Desarrolladores/Programadores			
Riesgo – Amenaza: [A.29] Extorsión - [A.30] Ingeniería social			

Salvaguarda	Actividades propuestas:	TDP	Eficacia
Formación y concienciación	Implementar políticas sobre la protección y confidencialidad de la información relevante y sensible del Data Center.	PR	L3
	Impartir formación regular sobre tácticas de ingeniería social y métodos utilizados en ataques de extorsión.	PR	L3
Identificación de usuarios	Implementar medidas de control de acceso y autenticación robustas para reducir el riesgo de manipulación de credenciales.	IM	L4
	Establecer políticas de autenticación sólidas que requieran contraseñas complejas, autenticación multifactor (MFA) y/o biometría para acceder a sistemas y datos críticos.	PR	L4

Responsable: Coordinador/a del Área de sistemas y recursos tecnológicos