UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE TELECOMUNICACIONES

INFORME FINAL DEL TRABAJO DE INTEGRACIÓN CURRICULAR, PROYECTO DE INVESTIGACIÓN

TEMA:

"PLAN DE SEGURIDAD PARA LA GESTIÓN DE RIESGOS UTILIZANDO METODOLOGÍA NIST SP 800-30 PARA EL DATA CENTER DE LA EMPRESA AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A."

Trabajo de titulación previo a la obtención del título de Ingeniero en Telecomunicaciones

Línea de investigación: Desarrollo, aplicación de software y cibersecurity (seguridad cibernética)

AUTOR:

Vinueza Bedoya Bryan Israel

DIRECTOR:

Ing. Cuzme Rodríguez Fabián Geovanny, MSc.

Ibarra, 2025

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

IDENTIFICACION DE LA OBRA

La Universidad Técnica del Norte dentro del proyecto Repositorio Digital Institucional, determinó la necesidad de disponer de textos completos en formato digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la Universidad.

Por medio del presente documento dejo sentada mi voluntad de participar en este proyecto, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	1003702832		
APELLIDOS Y NOMBRES:	VINUEZA BEDOYA BRYAN ISRAEL		
DIRECCIÓN:	IBARRA- FERNANDO DAQUILEMA Y 24 DE JULIO 5-54		
EMAIL:	bivinuezab@utn.edu.ec		
TELÉFONO FIJO:	062631660	**TELF. MÓVIL:**	0978619419

DATOS DE LA OBRA	
TÍTULO:	PLAN DE SEGURIDAD PARA LA GESTIÓN DE RIESGOS UTILIZANDO METODOLOGÍA NIST SP 800-30 PARA EL DATA CENTER DE LA EMPRESA AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A.
AUTOR (ES):	VINUEZA BEDOYA BRYAN ISRAEL
FECHA: DD/MM/AAAA	29/01/2025
SOLO PARA TRABAJOS DE GRADO DE INTEGRACIÓN CURRICULAR	
PROGRAMA:	■ **GRADO** □ **POSGRADO**
TITULO POR EL QUE OPTA:	INGENIERO EN TELECOMUNICACIONES
DIRECTOR:	ING. CUZME RODRÍGUEZ FABIÁN GEOVANNY. MSC
	ING. DOMÍNGUEZ LIMAICO HERNAN MAURICIO. MSC

AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, Vinueza Bedoya Bryan Israel, con cédula de identidad Nro. 1003702832, en calidad de autor (es) y titular (es) de los derechos patrimoniales de la obra o trabajo de integración curricular descrito anteriormente, hago entrega del ejemplar respectivo en formato digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y uso del archivo digital en la Biblioteca de la Universidad con fines académicos, para ampliar la disponibilidad del material y como apoyo a la educación, investigación y extensión; en concordancia con la Ley de Educación Superior Artículo 144.

Ibarra, a los 03 días del mes de febrero de 2025

EL AUTOR:

.....

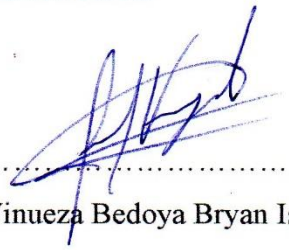
Vinueza Bedoya Bryan Israel

CONSTANCIAS

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 03 días del mes de febrero de 2025.

EL AUTOR:



.....

Vinueza Bedoya Bryan Israel

CERTIFICACIÓN DEL DIRECTOR DEL TRABAJO DE

INTEGRACIÓN CURRICULAR

Ibarra, 29 de enero de 2025

ING. CUZME RODRÍGUEZ FABIÁN GEOVANNY. MSC
DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

CERTIFICA:
Haber revisado el presente informe final del trabajo de Integración Curricular, el mismo que se ajusta a las normas vigentes de la Universidad Técnica del Norte; en consecuencia, autorizo su presentación para los fines legales pertinentes.

Ing. Cuzme Rodríguez Fabián Geovanny. Msc

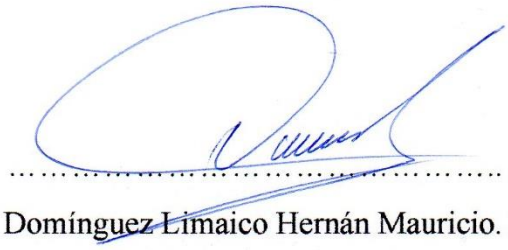
C.C.:1311527012

APROBACIÓN DEL COMITÉ CALIFICADOR

El Comité Calificador del trabajo de Integración Curricular **"Plan de seguridad para la gestión de riesgos utilizando Metodología NIST SP 800-30 para el Data Center de la empresa AirmaxTelecom Soluciones Tecnológicas S.A."** elaborado por **Vinueza Bedoya Bryan Israel**, previo a la obtención del título de **Ingeniero en Telecomunicaciones**, aprueba el presente informe de investigación en nombre de la **Universidad Técnica del Norte**.

Ing. Cuzme Rodríguez Fabián Geovanny. Msc

C.C.:1311527012



Ing. Domínguez Limaico Hernán Mauricio. Msc

C.C.:1002379301

DEDICATORIA

Este trabajo de titulación está dedicado a mi familia, por su apoyo incondicional, amor y comprensión a lo largo de todo este proceso. A mis padres, por ser mi mayor fuente de fortaleza, por enseñarme el valor del esfuerzo y por su constante aliento. A mi hermana, por su apoyo y por su motivación en cada paso de este camino.

A mis amigos de la universidad, quienes compartieron conmigo tanto los desafíos como los logros, y cuya amistad y compañía fueron esenciales para alcanzar este objetivo. A mis primos, por su apoyo y por estar presentes en los momentos más importantes, brindándome su ánimo y comprensión. Y a mis amigos fuera de la universidad, quienes, aunque no estuvieron directamente involucrados en mi recorrido académico, siempre estuvieron ahí para ofrecerme su apoyo, confianza y motivación.

A todos ellos y a todas aquellas personas que estuvieron presentes en cada etapa de este proceso, les dedico este logro, que no solo es mío, sino también el reflejo de su amor, su fe en mí y su constante apoyo.

AGRADECIMIENTO

Quiero expresar mi más sincero agradecimiento a mi padre Galo, por su apoyo incondicional, su sabiduría y por enseñarme el valor del trabajo arduo. A mi madre Janeth, por su amor, paciencia y por ser el pilar que siempre me ha impulsado a seguir adelante. A mi hermana Grace, por su constante apoyo y por ser una fuente de inspiración y fortaleza en cada paso de este proceso.

A mis amigos de la universidad, quienes fueron una parte fundamental de este camino. Gracias por compartir risas, desafíos y logros. Su compañía y apoyo me ayudaron a crecer profesional y emocionalmente, y sin ustedes, este recorrido no habría sido el mismo. También agradezco a mi grupo de amigos fuera de la universidad, quienes siempre estuvieron ahí para ofrecerme su apoyo y comprensión, contribuyendo a mi bienestar y motivación.

A AIRMAXTELECOM Soluciones Tecnológicas S.A., por brindarme la oportunidad de realizar esta investigación y por su colaboración en el desarrollo de este trabajo. Gracias por confiar en mi capacidad y por proporcionarme el entorno adecuado para llevar a cabo este proyecto.

Finalmente, a mi tutor, MSc. Fabián Cuzme, y a mi asesor, MSc. Mauricio Domínguez, les agradezco profundamente por su orientación, compromiso y apoyo constante. Su disposición para guiarme y su dedicación a mi crecimiento académico y personal han sido invaluables, y siempre atesoraré todo lo aprendido bajo su tutela.

RESUMEN

El presente trabajo tiene como propósito desarrollar un plan integral de seguridad orientado a la gestión de riesgos en el Data Center de AIRMAXTELECOM Soluciones Tecnológicas S.A., utilizando como base la metodología NIST SP 800-30. Este enfoque proporciona un marco sistemático y adaptable para identificar y mitigar amenazas potenciales, así como garantizar la protección de los activos críticos de la empresa, alineándose con las exigencias actuales en materia de seguridad de la información y continuidad operativa.

La metodología aplicada combina investigación descriptiva con un análisis técnico exhaustivo, respaldado por herramientas especializadas como Nessus y OpenVAS, que permitieron detectar vulnerabilidades específicas en la infraestructura tecnológica de la organización. Adicionalmente, se realizó una evaluación detallada de los riesgos asociados a los activos críticos, considerando tanto el impacto como la probabilidad de ocurrencia, lo que permitió construir una matriz de riesgos adaptada al contexto operativo de AIRMAXTELECOM. Los resultados obtenidos incluyen una clasificación minuciosa de amenazas y vulnerabilidades, así como la priorización de riesgos según su criticidad.

Estas conclusiones sirvieron de base para diseñar un plan de implementación que abarca medidas preventivas y correctivas, tales como la mejora de configuraciones de red, la implementación de sistemas de respaldo y la capacitación del personal técnico. Dicho plan busca fortalecer la resiliencia del Data Center frente a incidentes, garantizando la continuidad operativa de la empresa en un entorno tecnológico exigente. Este estudio destaca la relevancia de la gestión de riesgos y la utilidad del marco NIST SP 800-30 para proteger activos organizacionales frente a amenazas internas y externas.

ABSTRACT

The purpose of this work is to develop a comprehensive security plan oriented to risk management in the Data Center of AIRMAXTELECOM Soluciones Tecnológicas S.A., using the NIST SP 800-30 methodology as a basis. This approach provides a systematic and adaptable framework to identify and mitigate potential threats, as well as to guarantee the protection of the company's critical assets, aligned with the current requirements in terms of information security and operational continuity.

The applied methodology combines descriptive research with an exhaustive technical analysis, supported by specialized tools such as Nessus and OpenVAS, which allowed detecting specific vulnerabilities in the organization's technological infrastructure. Additionally, a detailed evaluation of the risks associated with critical assets was carried out, considering both the impact and the probability of occurrence, which allowed the construction of a risk matrix adapted to AIRMAXTELECOM's operational context. The results obtained include a detailed classification of threats and vulnerabilities, as well as the prioritization of risks according to their criticality.

These conclusions served as the basis for designing an implementation plan that includes preventive and corrective measures, such as improving network configurations, implementing backup systems and training technical personnel. This plan seeks to strengthen the resilience of the Data Center in the face of incidents, guaranteeing the company's operational continuity in a demanding technological environment. This study highlights the relevance of risk management and the usefulness of the NIST SP 800-30 framework to protect organizational assets against internal and external threat

Contenido

Índice de Figuras

Índice de Tablas

Capítulo 1

Antecedentes

En este capítulo, se tratará una concisa presentación del proyecto propuesto, explorando sus aspectos esenciales. Se abordarán temas como el contexto del proyecto, sus objetivos tanto generales como específicos, la justificación que respalda su implementación, así como el alcance previsto. Además, se proporcionará información adicional relevante para contextualizar de manera integral el proyecto, proporcionando una visión completa y detallada de los elementos clave que serán desarrollados en los siguientes apartados

1.1 Tema

Plan de Seguridad para la Gestión de Riesgos utilizando Metodología NIST SP 800-30 para el Data Center de la empresa AIRMAXTELECOM Soluciones Tecnológicas S.A.

1.2 Problema

La seguridad de la información es un aspecto crucial para garantizar la confiabilidad y protección de las infraestructuras y sistemas empresariales. Los centros de datos desempeñan un papel central al albergar información, aplicaciones y servicios esenciales para las operaciones diarias de las empresas. Por lo tanto, resulta imperativo que las organizaciones implementen medidas de seguridad adecuadas para resguardar estos centros.

La ausencia de una seguridad efectiva en los centros de datos conlleva el riesgo significativo de sufrir una violación de datos. Este escenario podría implicar la exposición o robo de información confidencial de la empresa, e incluso, de manera más grave, la información sensible de los clientes. Dada la creciente amenaza de ciberataques, las empresas se encuentran en

la búsqueda constante de estrategias que les permitan llevar a cabo análisis preventivos, de control y reducción de los riesgos asociados a la vulnerabilidad de la información. (Vmware, 2023)

AIRMAXTELECOM Soluciones Tecnológicas S.A. es una empresa dedicada a la prestación de servicios de telecomunicaciones, con su matriz principal ubicada en la ciudad de Ibarra. A lo largo del tiempo, la compañía ha experimentado un crecimiento significativo, incrementando su base de usuarios y estableciendo nuevos puntos de distribución en el norte del país. La organización cuenta con un Data Center que maneja información crucial para sus operaciones, sin embargo, carece de la aplicación de políticas y procedimientos, lo que expone la información y los activos a riesgos potenciales.

La falta de una planificación adecuada y la ausencia de protocolos claros pueden generar diversos problemas y vulnerabilidades de seguridad en el Data Center. Esto podría comprometer la integridad, confidencialidad y disponibilidad de los datos almacenados. Aunque actualmente el centro de datos no ha registrado ataques o penetraciones debido a un monitoreo constante por parte de la empresa, la situación destaca la necesidad de implementar medidas preventivas y correctivas.

El Data Center de la empresa enfrenta desafíos adicionales, ya que carece de un plan de riesgos y ha experimentado problemas de disponibilidad debido a interrupciones en el suministro de energía, afectando su operatividad. Sin medidas de seguridad adecuadas, el centro de datos se convierte en un blanco vulnerable para amenazas como ataques cibernéticos, intrusos físicos y desastres naturales. La ausencia de un plan de seguridad de riesgos obstaculiza una respuesta rápida y eficiente ante incidentes, lo que aumenta el tiempo de inactividad y tiene un impacto

negativo en la continuidad del negocio. Es imperativo implementar medidas proactivas para garantizar la seguridad y resiliencia del Data Center ante posibles amenazas.

1.3 Objetivos

1.3.1 Objetivo General

Desarrollar un plan de seguridad de riesgos para el Data Center de la empresa AIRMAXTELECOM Soluciones Tecnológicas S.A. utilizando la metodología NIST SP 800-30 que permita la protección contra amenazas y riesgos potenciales.

1.3.2 Objetivos Específicos

- Analizar el marco de la metodología NIST 800-30 y su aplicación en entornos tecnológicos sobre la gestión de riesgos y seguridad de la información.
- Valorar los riesgos de seguridad en el Data Center de la empresa AIRMAXTELECOM Soluciones Tecnológicas S.A. para determinar los activos críticos y evaluar el riesgo e impacto sobre estos.
- Elaborar un plan de seguridad para proteger los activos críticos del Centro de Datos y disminuir los riesgos a los que está expuesto.

1.4 Justificación

El MINTEL en el Plan Estratégico Institucional con el fin de lograr un Ecuador Digital Ciberseguro que proteja los servicios, las infraestructuras críticas y garantice el Estado de Derecho en el ciberespacio, ha establecido una estrategia basada en siete pilares fundamentales. Estos pilares son: 1) Gobernanza de ciberseguridad; 2) Sistemas de información y gestión de incidentes; 3) Protección de servicios e infraestructuras críticas digitales; 4) Soberanía y defensa; 5) Seguridad

pública y ciudadana; 6) Diplomacia en el ciberespacio y cooperación internacional; 7) Cultura y educación de ciberseguridad que está enmarcado en la Política de Ciberseguridad. El objetivo final es asegurar un entorno cibernético seguro para todos los ciudadanos lo que conlleva a brindar una infraestructura segura dentro de los sistemas que manejan información. (MINTEL, 2022)

La Ley Orgánica de Protección de Datos Personales indica la necesidad de proteger los derechos de privacidad de los individuos, cumplir con las obligaciones legales, prevenir incidentes de seguridad, generar confianza y mitigar los riesgos reputacionales asociados con la pérdida o el uso indebido de datos personales. Por esto las violaciones de seguridad de datos y los incidentes de pérdida de información pueden tener un impacto negativo significativo en la reputación de una organización. Al garantizar la seguridad de la información y proteger los datos personales de manera efectiva, se reducen los riesgos asociados con la pérdida de confianza y el daño a la reputación. (MINTEL, 2021)

En Plan de Creación de Oportunidades cuenta con un eje de seguridad integral en donde una de sus políticas es "Fortalecer al Estado para mantener la confidencialidad, integridad y disponibilidad frente a amenazas provenientes del ciberespacio y proteger su infraestructura crítica". Por este motivo es importante dentro de las organizaciones mantener un control de seguridad integral en los Centros de datos que proteja todos los ámbitos del triángulo CIA para la reducción de riegos frente a ataques cibernéticos. (Secretaría Nacional de Planificación, 2021)

1.5 Alcance

El objetivo principal de este proyecto es desarrollar un plan integral de seguridad de riesgos para el Data Center de AIRMAXTELECOM Soluciones Tecnológicas S.A., con el propósito de elevar el nivel de seguridad en sus instalaciones. Para lograr esto, se llevará a cabo un proceso de

investigación aplicada, centrado en contextualizar los parámetros de seguridad según la metodología NIST 800-30, abordando el análisis de riesgos y la seguridad de la información.

La metodología NIST 800-30, que utiliza categorías para clasificar la información según el nivel de riesgo y estándares para asegurar la información apropiada a su nivel, será la guía principal para este proyecto. Se realizará una revisión completa de fuentes bibliográficas que aborden casos similares en la seguridad de la información de centros de datos, así como herramientas pertinentes para llevar a cabo este tipo de análisis. El objetivo es implementar un plan de seguridad de riesgos que se adapte a las necesidades específicas del centro de datos.

En la fase inicial de la metodología NIST 800-30, se abordará la Caracterización del Sistema. Esto implica revisar el marco de la NIST SP 800-30, recopilar datos en la empresa y detectar los activos críticos del Data Center. Se utilizarán encuestas, cuestionarios y una inspección física para identificar de manera precisa estos activos críticos.

La siguiente fase se enfocará en la Identificación de amenazas y vulnerabilidades, donde se determinarán las posibles amenazas que podrían afectar los activos identificados y se analizarán las vulnerabilidades que podrían ser explotadas por esas amenazas. Posteriormente, en el proceso de Análisis de controles, se examinarán los controles de seguridad existentes y se verificarán los controles planificados por la empresa.

En la fase de Análisis de impacto, se llevará a cabo una evaluación completa del nivel de riesgo presente en el Data Center, identificando los posibles riesgos que podrían afectar la seguridad. Se desarrollarán y propondrán controles adecuados para contrarrestar y disminuir estos riesgos a niveles aceptables y manejables.

La fase de Determinación de probabilidades analizará las motivaciones que impulsan los ataques, la capacidad de las amenazas y la naturaleza de las vulnerabilidades para obtener una

comprensión clara de las probabilidades de que una amenaza se materialice. Posteriormente, se evaluará el riesgo real en el Data Center y se propondrán recomendaciones de control específicas para mitigar el riesgo identificado hasta un nivel manejable.

En la fase de Determinación del riesgo, se utilizará la información recopilada para clasificar el nivel de riesgo al que se enfrenta el Data Center, categorizándolo como bajo, medio o alto. Finalmente, se desarrollará un plan de seguridad que incluirá la recomendación de controles más adecuados para mitigar los riesgos y la documentación de los resultados, registrando todas las decisiones tomadas en relación con la seguridad del Centro de Datos.

Capítulo 2

Marco Teórico

En este capítulo, se realiza una recopilación de información reciente extraída de fuentes bibliográficas, abordando el tema de la seguridad de la información en los Data Centers. Se explora la relevancia de la vulnerabilidad de los datos, se analizan las herramientas diseñadas para detectar estas vulnerabilidades y se destaca la importancia de implementar un plan de seguridad efectivo en los centros de datos.

El capítulo inicia proporcionando una introducción a los conceptos fundamentales de los Data Centers, delineando sus funciones y su impacto crucial en el entorno empresarial. A continuación, se profundiza en la seguridad de la información, destacando sus aspectos más significativos. Posteriormente, se aborda el análisis y la gestión de los riesgos, junto con la explicación de la utilidad y relevancia de los planes de seguridad. Finalmente, se examina la metodología NIST SP 800-30, describiendo sus objetivos y los beneficios inherentes a su aplicación en la gestión de riesgos.

2.1 Data Centers

Un centro de datos es un lugar físico donde las empresas guardan todas sus aplicaciones y datos más importantes. Su diseño se basa en conectar diferentes recursos de computación y almacenamiento para facilitar la distribución de información y aplicaciones compartidas. En este diseño, se encuentran elementos esenciales como routers, switches, firewalls, dispositivos de almacenamiento, servidores y controladores de aplicaciones.

La importancia de un centro de datos radica en que asegura la disponibilidad y seguridad de los datos, mejorando el rendimiento de las aplicaciones y proporcionando una infraestructura

escalable para el crecimiento de las organizaciones. Además, se pone énfasis en la eficiencia energética y la refrigeración para mantener un funcionamiento sostenible y económico. También se aprovechan tecnologías avanzadas, como la virtualización y la nube, para optimizar el uso de recursos y simplificar la administración del centro de datos. (Cisco, 2023)

2.1.1 Componentes de un Data Center

En el núcleo de la operación efectiva de un centro de datos reside la construcción de una infraestructura robusta compuesta por componentes esenciales. Desde los recursos de cómputo que ejecutan aplicaciones vitales hasta la conectividad eficaz entre los dispositivos de red, cada elemento desempeña un papel crucial. La gestión de grandes volúmenes de datos, la organización estructurada en bastidores de servidor y la implementación de sistemas de refrigeración se entrelazan para garantizar el rendimiento óptimo y la continuidad operativa.

Los recursos de cómputo, como servidores y sistemas, juegan un rol central al ejecutar y gestionar aplicaciones y procesos esenciales, adaptándose a las demandas cambiantes de la carga de trabajo para mantener la eficacia operativa. La conectividad efectiva entre los elementos del centro de datos es esencial, con dispositivos de red, como switches y routers, siendo cruciales para establecer una red confiable y de alto rendimiento que facilite la comunicación fluida. La gestión eficiente de grandes volúmenes de datos se confía a servidores de almacenamiento, como sistemas NAS o SAN, asegurando accesibilidad y seguridad de la información. Los bastidores de servidor proporcionan una estructura organizada, optimizando el espacio y facilitando la gestión y mantenimiento de los equipos. Además, los sistemas de refrigeración son esenciales para mantener una temperatura óptima y prevenir el sobrecalentamiento, preservando así el rendimiento y la vida útil de los componentes.

La seguridad física se refuerza mediante sistemas contra incendios, como detectores de humo y extintores, para prevenir y mitigar posibles incendios y proteger los activos críticos. Un sistema de cableado estructurado organizado y eficiente es esencial para la conectividad interna, facilitando la expansión futura y reduciendo posibles fallas. Además, la implementación de un UPS garantiza la continuidad operativa al proporcionar energía de respaldo en casos de cortes eléctricos, protegiendo los datos y equipos de posibles pérdidas o daños. La combinación de estos componentes asegura la resiliencia y eficiencia del centro de datos. Los centros de datos enfrentan diversos riesgos y amenazas, desde situaciones de emergencia hasta amenazas operativas y cibernéticas. (Ramon Hurtado, 2023)

2.1.2 Riesgos y amenazas comunes en los Data Centers

En el informe del Uptime Institute, las principales causas de interrupciones en la operación de los centros de datos son los cortes de energía en las instalaciones, que representan el 33% de las interrupciones, seguidos por las fallas en la red, que constituyen el 30%, y los problemas de software o sistemas de TI, que representan el 28%. Estas interrupciones pueden tener consecuencias significativas para las empresas, dado que la mayor dependencia de los servicios digitales hace que los centros de datos sean fundamentales para la continuidad operativa y la eficiencia. (Lawrence Andy, 2018)

El conocimiento de los posibles riesgos y amenazas que podrían afectar el funcionamiento de los centros de datos es fundamental en su gestión. Varios aspectos se destacan como puntos críticos, donde la vulnerabilidad es más evidente. La interrupción del suministro de energía y la caída de la red se presentan como amenazas significativas, ya que podrían resultar en la pérdida temporal o permanente de acceso a los datos. Los fallos en el software o sistema de TI representan otra área de riesgo, ya que podrían desencadenar problemas operativos con consecuencias

potencialmente graves. Además, las filtraciones de ciberdelincuentes son una amenaza constante, resaltando la necesidad de medidas de seguridad avanzadas. La elección de proveedores de servicios de baja calidad también se identifica como un riesgo, ya que la dependencia de servicios poco confiables puede impactar negativamente en la continuidad operativa y la seguridad de la información. Abordar proactivamente estos riesgos se vuelve imperativo para garantizar la solidez y la seguridad de los centros de datos.

En la gestión de centros de datos, es crucial estar consciente de los riesgos potenciales y amenazas que podrían comprometer su funcionalidad. Diversas áreas se destacan como puntos críticos, donde la vulnerabilidad es más pronunciada. La interrupción de las fuentes de energía y la caída de la red se perfilan como amenazas significativas, ya que podrían resultar en la pérdida temporal o permanente de acceso a los datos. Los errores en el software o sistema de TI representan otra área de riesgo, ya que podrían desencadenar fallos operativos con consecuencias potencialmente graves. Además, las filtraciones de ciberdelincuentes son una amenaza constante, subrayando la necesidad de medidas de seguridad avanzadas. La elección de proveedores de servicios de baja calidad también se identifica como un riesgo, ya que la dependencia de servicios poco confiables puede impactar negativamente en la continuidad operativa y la seguridad de la información. Abordar estos riesgos de manera proactiva se convierte en un imperativo para garantizar la robustez y la seguridad de los centros de datos.(Benalcázar Gladys, 2019)

2.1.3 Importancia de los Data Centers para las empresas

Según Benalcázar Gladys (2019), los data centers desempeñan un rol importante en las empresas modernas, ya que son fundamentales para el almacenamiento seguro, procesamiento eficiente y acceso ágil a grandes cantidades de datos. Estas instalaciones tecnológicas posibilitan

a las organizaciones respaldar y mantener operaciones críticas y ofrecer servicios y aplicaciones sin interrupciones.

La agilidad en la adaptación a las dinámicas del mercado y las demandas de los clientes ha convertido en un aspecto crucial en el ámbito empresarial, y los centros de datos desempeñan un papel fundamental al proporcionar una infraestructura escalable y flexible. La capacidad de ajustar rápidamente los recursos según las necesidades cambiantes permite a las empresas mantenerse ágiles y competitivas en un entorno empresarial en constante evolución. Sin embargo, la agilidad no es el único pilar; la seguridad ocupa un lugar central en la gestión de centros de datos. Además de abordar amenazas físicas, como acceso no autorizado, los centros de datos implementan medidas avanzadas para contrarrestar las amenazas cibernéticas, protegiendo así la información sensible y manteniendo la integridad de los datos.

En su búsqueda de eficiencia, los centros de datos también buscan la optimización del consumo de recursos y la reducción del impacto ambiental. Esta doble estrategia no solo permite un uso más eficiente de los recursos, sino que también contribuye a la sostenibilidad ambiental, lo que se alinea con las crecientes preocupaciones en torno a la responsabilidad social corporativa. La combinación de escalabilidad, seguridad y sostenibilidad posiciona a los centros de datos como pilares fundamentales para el éxito empresarial en la era digital. (Benalcázar Gladys, 2019)

2.2 Seguridad de la Información

La seguridad de la información abarca la protección de datos en cualquier entorno, asegurando que no se divulguen, modifiquen o destruyan de manera no autorizada o intencionada. En la era tecnológica actual, la mera presencia de tecnología no es suficiente para garantizar la seguridad de la información; es imperativo contar con políticas de gestión sólidas que se implementen de manera eficaz. Para lograr el éxito en este ámbito, las organizaciones deben

dedicar recursos a soluciones técnicas y establecer incentivos que fomenten el comportamiento responsable de sus empleados. (Li & Hoffman, 2023)

2.2.1 Principios de la Seguridad y Conceptos Clave

La seguridad de la información constituye un conjunto integral de medidas y acciones estratégicas diseñadas para salvaguardar la confidencialidad, integridad y disponibilidad de los datos. En este contexto, se busca prevenir accesos no autorizados, manipulaciones indebidas y asegurar que la información esté accesible cuando sea necesario. Esta disciplina no solo aborda aspectos tecnológicos, sino que también implica la implementación de políticas, procesos y concienciación entre los usuarios. (Regina Baena et al., 2019)

La protección de la información es fundamental en cualquier entorno digital, abarcando diversos aspectos clave para garantizar la seguridad de los datos. La confidencialidad se encarga de restringir el acceso a la información solo a personas autorizadas, evitando divulgaciones no deseadas. Por su parte, la integridad asegura la precisión y completitud de los datos, previniendo modificaciones no autorizadas. Asimismo, la disponibilidad garantiza que la información esté accesible para los usuarios autorizados cuando sea necesario. La autenticación, a su vez, es un proceso esencial para verificar la identidad de los usuarios o sistemas, fortaleciendo las capas de seguridad. Finalmente, la autorización establece los permisos necesarios para acceder a información o recursos específicos, asegurando un control riguroso sobre el acceso a los datos.

La seguridad de la información en el entorno digital es crucial para proteger la confidencialidad, integridad y disponibilidad de los datos. Esta protección abarca aspectos como la prevención de riesgos de contenido y de contacto en el entorno digital, la gestión del riesgo de seguridad digital, la implementación efectiva de medidas de ciberseguridad y el uso efectivo de las capacidades de ciberdefensa. La seguridad digital o ciberseguridad se refiere a la protección

de datos, redes y dispositivos contra el acceso no autorizado, siendo fundamental para prevenir el acceso no intencionado o no autorizado a la información. En este sentido, la seguridad de la información en la era digital se ha convertido en un aspecto de vital importancia, especialmente con el crecimiento de los ataques a la privacidad de particulares y de las empresas. (Regina Baena et al., 2019)

2.2.2 Importancia de La Seguridad de la Información en los Data Centers

Los Data Centers, como nodos neurálgicos de información empresarial, desempeñan un papel crucial al almacenar, procesar y transmitir vastas cantidades de datos críticos. Su papel es aún más vital en la era digital, donde la rapidez y la eficiencia en la gestión de la información son imperativas para el éxito organizacional.

En este contexto, la seguridad de la información en los Data Centers se establece como un pilar esencial. Más allá de simplemente salvaguardar la integridad y confidencialidad de los datos, la seguridad en estos centros se convierte en la primera línea de defensa contra amenazas cibernéticas en constante evolución. Asimismo, garantiza la disponibilidad ininterrumpida de servicios y recursos, mitigando riesgos financieros asociados con interrupciones costosas. La implementación de medidas de seguridad robustas no solo protege los intereses comerciales y la reputación de la empresa, sino que también contribuye a cumplir con las regulaciones cada vez más estrictas en torno a la privacidad de los datos y la ciberseguridad.(Ruben et al., 2017)

2.3 Análisis y Gestión de Riesgos

Según Regina Baena et al. (2019) el análisis y la gestión de riesgos juegan un papel esencial en diversos sectores, abarcando desde el ámbito empresarial hasta la seguridad y más. Este proceso engloba la identificación, evaluación y aplicación de medidas destinadas a mitigar o administrar los riesgos que podrían afectar los objetivos de una organización o proyecto.

En una primera etapa, se realiza un análisis exhaustivo para reconocer y comprender los diversos riesgos, abarcando aspectos financieros, operativos, de seguridad, legales, entre otros. Una vez identificados, se procede a evaluar tanto la probabilidad de ocurrencia como el impacto potencial. En la fase subsiguiente, la gestión de riesgos implica la formulación de estrategias para abordar estos riesgos. Esto puede implicar evitarlos, mitigarlos, compartirlos a través de seguros, o asumirlos con pleno conocimiento de las posibles consecuencias.

En el contexto empresarial, la gestión de riesgos desempeña un papel fundamental para resguardar las inversiones y garantizar la continuidad de las operaciones comerciales. En el ámbito de la seguridad, este proceso implica la evaluación minuciosa de amenazas y vulnerabilidades, con el objetivo de implementar medidas de protección adecuadas y efectivas. (Regina Baena et al., 2019)

2.3.1 Análisis y Procesos Generales para la Resolución de Riesgos

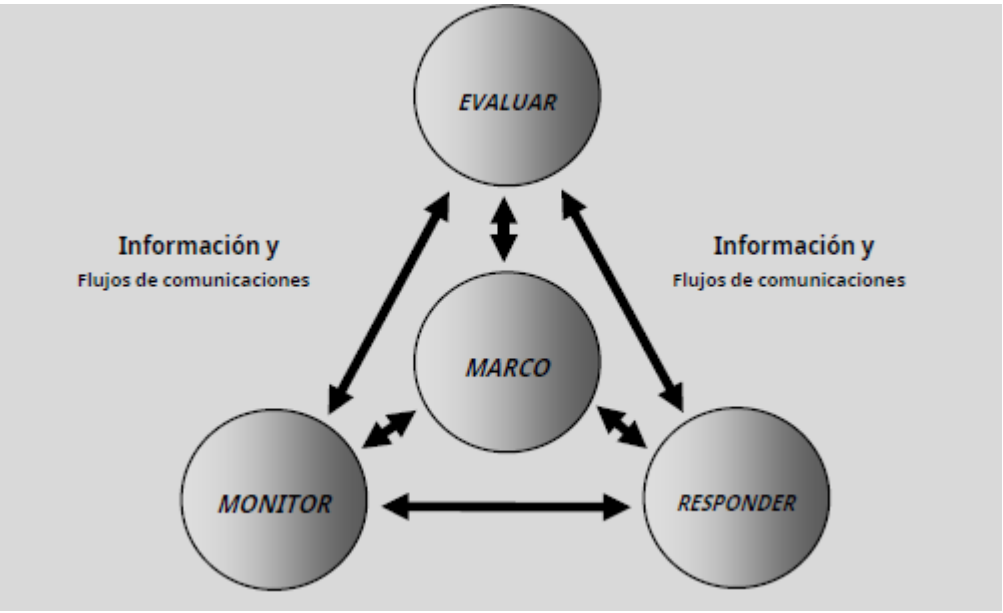
Supriyadi & Hardani (2018) señalan que abordar y mitigar posibles amenazas a través de la resolución de riesgos implica llevar a cabo análisis detallados y procesos fundamentales. Inicialmente, se realiza una evaluación completa para identificar y comprender los riesgos potenciales que podrían impactar los objetivos de una organización o proyecto, abarcando áreas como los riesgos financieros, operativos, de seguridad y legales.

Después de identificar estos riesgos, se procede a evaluar su probabilidad de ocurrencia y el impacto que podrían tener en caso de concretarse. Esta evaluación permite priorizar los riesgos, concentrándose en aquellos con mayores posibilidades de ocurrir y con un impacto significativo. Posteriormente, se desarrollan estrategias de gestión de riesgos, que pueden comprender la implementación de medidas preventivas, la transferencia de riesgos mediante seguros, o la preparación para enfrentar las consecuencias. La Figura 1 muestra el proceso de evaluación de

riesgos dentro del marco de la gestión de riesgos, proporcionando una representación gráfica de la identificación, evaluación y priorización de riesgos, así como la implementación de estrategias de gestión.(Supriyadi & Hardani, 2018)

Figura 1

Evaluación de riesgos dentro del proceso de gestión de riesgos



Nota. En la figura se puede observar el proceso de evaluación de riesgos dentro del proceso de gestión de riesgos. Tomado de la NIST SP 800-30 (Blank & Gallagher, 2012)

2.3.2 Metodologías para el Análisis y Gestión de Riesgos

Existen diversas metodologías para llevar a cabo el análisis y gestión de riesgos, cada una con enfoques y técnicas particulares. Estas metodologías son herramientas estructuradas que ayudan a las organizaciones a identificar, evaluar y gestionar eficazmente los riesgos(Ramírez Castro & Ortiz Bayona, 2011). La Tabla 1 presenta un resumen de algunas de las metodologías

destacadas para la gestión de riesgos, destacando sus características distintivas y áreas de aplicación específicas. Esta referencia proporciona a las organizaciones una guía valiosa al seleccionar la metodología más apropiada según las necesidades y contexto operativo. (Torres, 2015)

Tabla 1

Metodologías para la Gestión de Riesgos

Características	**OCTAVE**	**MAGERIT**	**OSTMMv3**	**NIST 800-30**	**ISO 27005**
Enfoque principal	Riesgos organizativos	Gestión de riesgos de TI	Pruebas de seguridad de código abierto	Gestión de riesgos de seguridad de TI	Gestión de riesgos de seguridad de la información
Ámbito de aplicación	Organizaciones en general	Gobierno y sectores públicos	Enfoque más amplio, pero centrado en seguridad de TI	Gobierno y sectores públicos	Todas las organizaciones y sectores
Proceso de evaluación de riesgos	Iterativo y centrado en la organización	Basado en modelos de amenazas y	Amplio espectro de	Ciclo de vida de gestión de riesgos	Identificación, evaluación,

		vulnerabilidades	pruebas de seguridad		tratamiento y revisión
Enfoque de tratamiento de riesgos	Gestión y mitigación de riesgos	Implementación de salvaguardas	Enfoque en identificación y abordaje de problemas de seguridad	Implementación de controles de seguridad	Selección y aplicación de controles
Orientación temporal	Enfoque a largo plazo	Enfoque a medio y largo plazo	Orientado a proyectos específicos	Ciclo de vida de gestión de riesgos	Orientado a proyectos y operaciones
Uso de estándares	Basado en principios y buenas prácticas	Se apoya en estándares ISO	Enfoque más específico sin depender de estándares específicos	Basado en estándares de seguridad y gestión de riesgos	Se basa en estándares de gestión de riesgos y seguridad de la información

Nota. En la tabla se puede observar las metodologías más comunes para realizar un análisis de riegos. Tomado de la Conferencia Internacional de Tecnología e Información (Supriyadi & Hardani, 2018)

Estas metodologías proporcionan marcos de trabajo que permiten a las organizaciones adaptarse a sus necesidades específicas. La elección de una metodología dependerá de factores como la naturaleza de los riesgos, los recursos disponibles y los objetivos organizacionales.

2.3.3 Herramientas para el Análisis y Gestión de Riesgos

El análisis y la gestión de riesgos se ven favorecidos por una variedad de herramientas que facilitan la identificación, evaluación y control de posibles amenazas. Estas herramientas no solo agilizan el proceso, sino que también permiten una mayor precisión en la evaluación de riesgos al emplear algoritmos y modelos avanzados. Además de las herramientas de software libre mencionadas, algunas soluciones comerciales también ofrecen funcionalidades más avanzadas y personalizadas para abordar riesgos específicos.(Louis, 2018)

Es fundamental resaltar que la elección de herramientas debe alinearse con la naturaleza y complejidad de los riesgos a los que se enfrenta una organización. Algunas herramientas se especializan en riesgos cibernéticos, mientras que otras pueden ser más efectivas en la gestión de riesgos operativos o financieros. La combinación de metodologías sólidas y herramientas especializadas contribuye a un enfoque integral en la gestión de riesgos, fortaleciendo así la capacidad de una organización para anticipar y mitigar posibles amenazas en su entorno operativo. (Louis, 2018) La Tabla 2 detalla estas herramientas, resaltando sus características clave, capacidades específicas y áreas de aplicación recomendadas. Al proporcionar información detallada sobre las opciones disponibles, la tabla sirve como una valiosa guía para las organizaciones que buscan adoptar herramientas eficientes para la gestión de riesgos, permitiendo una toma de decisiones informada y personalizada según sus necesidades particulares.

Tabla 2

Herramientas Para la Gestión de Riesgos

Característica	**Pilar**	**OpenVAS**	**Snort**	**OpenSCAP**	**OSSIM**	**Nessus**
Tipo de Herramienta	Gestión de Riesgos	Escáner de Vulnerabilidades	Detección de Intrusiones	Evaluación de Configuraciones	Gestión de la Seguridad	Escáner de Vulnerabilidades
Código Abierto	Sí	Sí	Sí	Sí	Sí	No
Protocolos Soportados	No especificado	TCP, UDP, ICMP, SNMP	TCP, UDP, ICMP	No especificado	TCP, UDP, ICMP, SNMP	TCP, UDP, ICMP, SNMP
Detección de Intrusiones	No	No	Sí	No	Sí	No
Escaneo de Vulnerabilidades	No	Sí	No	Sí	Sí	Sí
Automatización de Procesos	No	Sí	No	Sí	Sí	Sí

Informes Detallados	Sí	Sí	Sí	Sí	Sí	Sí
Integración con Otros Sistemas	No	Sí	Sí	Sí	Sí	Sí
Comunidad y Soporte	No especificado	Activa	Activa	Activa	Activa	Activa

Nota. En la tabla se puede observar las herramientas más comunes para realizar un análisis de riegos. Tomado del documento Targeted Attack Detection by Means of Free and Open Source Solutions(Louis, 2018)

2.4 Plan de Seguridad

Un plan de seguridad representa un documento estratégico que delinea las medidas y procedimientos diseñados para resguardar activos, personas o información frente a posibles amenazas y riesgos. Estos planes desempeñan un papel crucial en una variedad de contextos, desde entornos empresariales hasta instalaciones físicas, sistemas informáticos e incluso eventos.(Figueroa et al., 2017)

La elaboración de un plan integral de seguridad implica una serie de componentes fundamentales que van más allá de simplemente identificar riesgos y amenazas. Comienza con la identificación completa de posibles riesgos, desde situaciones de emergencia hasta amenazas operativas y cibernéticas. Este análisis sienta las bases para establecer objetivos de seguridad claros y definidos, que van desde la protección de vidas hasta la preservación de la integridad física y la seguridad de la información.

Además, el plan aborda la implementación de medidas preventivas y correctivas, detallando acciones y procedimientos específicos para prevenir o mitigar los riesgos identificados. Desde sistemas físicos, como alarmas y control de acceso, hasta políticas y capacitación del personal, se busca crear un entorno seguro y resiliente. Se establecen roles y responsabilidades de manera clara, asignando funciones específicas durante situaciones de emergencia para garantizar una respuesta efectiva.

La comunicación de crisis también ocupa un lugar central, delineando cómo se compartirá la información en situaciones de emergencia tanto internamente como con partes externas, con el objetivo de lograr una respuesta rápida y coordinada. Finalmente, el plan incluye un proceso de evaluación y actualización regular para garantizar su eficacia continua, adaptándose a cambios en el entorno operativo y en los riesgos identificados.(Figueroa et al., 2017)

2.4.1 Políticas de Seguridad

Tanto en el sector público como en el privado, las organizaciones adoptan políticas de seguridad con el fin de proteger su información. Este enfoque fortalece las conductas deseadas en materia de seguridad de la información y refuerza las restricciones contra comportamientos no deseados. Estas políticas, que suelen basarse en estándares reconocidos y buenas prácticas, establecen un marco normativo que abarca desde la clasificación de la información hasta las medidas de mitigación de riesgos.

La implementación de políticas de seguridad no solo se trata de imponer restricciones, sino también de crear una cultura organizacional que valore y priorice la seguridad. La ausencia de una política clara implica que las prácticas de seguridad carecen de límites definidos en cuanto a sus objetivos y responsabilidades, lo que podría conducir a una postura reactiva en lugar de proactiva frente a las amenazas cibernéticas y los riesgos de seguridad de la información.(Ruben et al., 2017)

2.5 Metodología NIST SP 800-30

La metodología NIST SP 800-30, desarrollada por el Instituto Nacional de Estándares y Tecnología (NIST) de Estados Unidos, es una guía para la gestión de riesgos de la información. Esta metodología se utiliza para identificar, evaluar y gestionar los riesgos relacionados con la seguridad de la información en organizaciones.(Blank & Gallagher, 2012)

2.5.1 Descripción y fases del NIST SP 800-30

La NIST SP 800-30 emerge como una guía fundamental para la ejecución precisa de cada fase en el proceso de evaluación de riesgos, delineando de manera efectiva cómo estas evaluaciones se integran armoniosamente en el tejido organizativo. Ofrece una dirección esencial para la identificación completa de los diversos factores de riesgo, proponiendo un enfoque de monitoreo continuo. Este enfoque capacita a las organizaciones para analizar de manera sistemática los niveles de riesgo a los que están expuestas, facultándolas para emprender acciones decisivas en la lucha contra dichos riesgos.(Blank & Gallagher, 2012)

La Tabla 3, que resume las Fases de la Metodología NIST SP 800-30, proporciona una visión detallada de cada etapa del proceso, desde la preparación hasta la monitorización continua, brindando así una referencia práctica y estructurada para la implementación exitosa de esta metodología. La integración de estas fases no solo fortalece la capacidad de la organización para identificar y gestionar riesgos, sino que también establece una base sólida para la mejora continua en la gestión de la seguridad de la información.

Tabla 3

Fases de la Metodología NIST SP 800-30

Fase	Descripción
1.-Preparación	Identificación de los objetivos y contexto organizativo para la evaluación de riesgos. Establecimiento del alcance y criterios.
2.-Realización de la evaluación	Identificación de las fuentes de amenaza.
2.1.-Identificar fuentes y eventos de amenazas	Reconocimiento y documentación de eventos potenciales que podrían afectar negativamente los objetivos organizativos.
2.2.-Identificar vulnerabilidades y condiciones predisponentes	Identificar las vulnerabilidades y las condiciones predisponentes que afectan la probabilidad de que los eventos de amenaza de interés resulten en impactos adversos.
2.3.-Determinar la probabilidad de ocurrencia	Determinar la probabilidad de que los eventos de amenazas de interés resulten en impactos adversos.
2.4.-Determinar la magnitud del impacto	Determinar los impactos adversos de los eventos de amenazas de interés
2.5.-Determinar el riesgo	Determinar el riesgo para la organización de los eventos de amenaza de interés
3.-Comunicar los resultados	Garantizar que los responsables de la toma de

	decisiones en toda la organización tengan la información adecuada relacionada con el riesgo.
4.-Mantener la evaluación	Ejecución de los controles seleccionados y seguimiento de su eficacia en la reducción del riesgo.

Nota. En la tabla se puede observar las fases para realizar la evaluación de riesgos de la metodología NIST SP 800-30. Tomado de la NIST (Blank & Gallagher, 2012)

2.5.2 Beneficios NIST SP 800-30 en la Gestión de Riesgos

La metodología NIST se destaca por su enfoque en la gestión de riesgos durante el desarrollo de proyectos de tecnologías de la información. Se centra en el triángulo CIA (Confidencialidad, Integridad y Disponibilidad) para realizar un análisis exhaustivo y estimar la probabilidad de que las amenazas se materialicen, así como su impacto en los elementos clave de la infraestructura tecnológica. (Supriyadi & Hardani, 2018)

La metodología proporciona un marco reconocido internacionalmente para la gestión de riesgos de la información, lo que facilita la adopción coherente de prácticas efectivas en diversas organizaciones, promoviendo la cohesión en los enfoques de seguridad. Además, la metodología se distingue por su enfoque sistemático y estructurado en la identificación, evaluación y gestión de riesgos, ofreciendo un marco sólido para la toma de decisiones informadas. La priorización efectiva de riesgos es otro punto fuerte, combinando la probabilidad e impacto para que las organizaciones se centren en abordar los riesgos más críticos y significativos, mejorando así la eficiencia de los recursos. Al mismo tiempo, la metodología facilita la toma de decisiones

informada mediante una evaluación detallada de costos y beneficios asociados con las contramedidas propuestas, promoviendo así decisiones fundamentadas en la gestión de riesgos.

La adaptabilidad es una característica esencial que permite a las organizaciones revisar continuamente sus análisis de riesgos para reflejar cambios en el entorno operativo o amenazas emergentes, garantizando la relevancia continua del enfoque de gestión de riesgos. La documentación rigurosa respaldada por esta metodología, crucial para auditorías internas y externas, proporciona un registro completo y accesible. Por último, la metodología fomenta la mejora continua, instando a las organizaciones a revisar periódicamente sus enfoques de gestión de riesgos, asegurando así una postura de seguridad siempre actualizada ante la evolución constante de amenazas y tecnologías.

2.5.3 Aplicaciones del NIST SP 800-30 en la Gestión de Riesgos

La implementación del NIST SP 800-30 en la gestión de riesgos engloba una variedad de aplicaciones cruciales y de gran alcance. Este marco proporciona una metodología sólida y bien estructurada, simplificando los procesos de identificación, evaluación y gestión de riesgos en diversos contextos organizativos. Además, es esencial destacar que este marco no solo se limita a ofrecer una guía efectiva para abordar riesgos en la seguridad de la información, sino que también se adapta de manera versátil a las necesidades específicas de distintos sectores y entornos operativos.(Noheli & Jiménez, 2021)

En entornos empresariales, este marco proporciona una metodología robusta y estructurada para gestionar riesgos relacionados con la seguridad de la información y la continuidad del negocio. Asimismo, en el sector gubernamental, agencias gubernamentales utilizan el NIST SP 800-30 para garantizar la seguridad y protección de la información sensible y crítica, estableciendo un sólido marco para la gestión de riesgos.

En otros sectores específicos, como la industria de la tecnología de la información, organizaciones financieras y el sector de la salud, este marco se revela relevante y aplicable. En la industria de la tecnología de la información, aborda de manera efectiva riesgos cibernéticos y de datos, mientras que, en organizaciones financieras, se utiliza para gestionar riesgos asociados con transacciones electrónicas, privacidad financiera y seguridad de la información. En el sector de la salud, el NIST SP 800-30 es implementado para abordar riesgos relacionados con la confidencialidad y seguridad de la información de pacientes, ofreciendo directrices específicas para salvaguardar la integridad de la información crítica en el ámbito de la atención médica.

2.6 Normativa legal

La normativa legal en torno a la gestión de riesgos juega un papel crucial en la salvaguarda de activos y la protección de información sensible. La legislación nacional establece directrices específicas para la identificación, evaluación y gestión de riesgos en diversas áreas, desde la seguridad informática hasta la protección de infraestructuras críticas. Este marco legal busca no solo fortalecer la resiliencia frente a amenazas potenciales, como desastres naturales o ciberataques, sino también promover una cultura organizacional enfocada en la prevención y respuesta ante posibles contingencias.

2.6.1 Constitución de República

Dentro del marco normativo de la Constitución de la República del Ecuador de 2008, el Artículo 66 destaca como un pilar fundamental al reconocer el derecho a la intimidad. Este reconocimiento establece una base crucial para abordar aspectos relacionados con la protección de datos personales y la imperiosa necesidad de prevenir riesgos asociados a la violación de la privacidad.

En este contexto, la protección de la intimidad se convierte en un componente esencial para garantizar la dignidad y el respeto a la vida privada de los ciudadanos. La relevancia de este derecho adquiere mayor importancia en la era digital, donde la recopilación, procesamiento y almacenamiento de datos personales se ha vuelto omnipresente. Por ende, surge la necesidad imperativa de llevar a cabo un análisis de riesgos exhaustivo para evaluar posibles amenazas a la privacidad y establecer medidas adecuadas de seguridad de la información.(Asamblea Nacional, 2011)

2.6.2 Código Orgánico Integral Penal (COIP)

El Código Orgánico Integral Penal (COIP) de Ecuador no aborda explícitamente el análisis de riesgos y la seguridad de la información. A pesar de esto, el COIP contempla la penalización de los delitos informáticos, los cuales involucran el uso de tecnología para atentar contra la confidencialidad y disponibilidad de datos personales. Estos actos, perpetrados a través de Internet, abarcan actividades como fraude, robo, falsificaciones, suplantación de identidad, espionaje y clonación de tarjetas de crédito.

En el ámbito público ecuatoriano, cumplir con las leyes y regulaciones establecidas por los organismos de control se presenta como un desafío. El acuerdo ministerial 166 EGSI establece que las entidades del sector público deben llevar a cabo evaluaciones de riesgos y desarrollar e implementar planes de manejo de riesgos en sus instituciones.(COIP, 2021)

2.6.3 Ley Orgánica de Protección de Datos Personales

Dentro del marco legal de la Ley Orgánica de Protección de Datos Personales (LOPD) de Ecuador, se establecen principios fundamentales para la protección de información personal e infiere en la necesidad de medidas adecuadas para garantizar la seguridad de los datos. La LOPD establece principios de licitud y transparencia en el tratamiento de datos, requiere el

consentimiento del titular y exige medidas de seguridad. Esto implica la importancia de realizar un análisis de riesgos para identificar amenazas potenciales a la privacidad y la seguridad de la información, asegurando el cumplimiento de la ley y protegiendo los derechos de los titulares de datos.(Asamblea Nacional, 2021)

2.6.4 Ley de Comercio Electrónico

En el marco de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos de Ecuador, se erige un sólido fundamento para fomentar la confianza en el entorno digital. Esta normativa sienta las bases esenciales para la protección en transacciones electrónicas y la validación de firmas electrónicas, reconociendo la relevancia de los proveedores de servicios de certificación. Asimismo, establece requisitos rigurosos para asegurar la integridad de sus infraestructuras y una gestión segura de claves criptográficas. Aunque la ley no se enfoca exclusivamente en la salvaguarda de datos personales, introduce principios fundamentales que deben considerarse en el manejo seguro de información personal, especialmente en el contexto dinámico del comercio electrónico. (Congreso Nacional, 2018)

Capítulo 3

Metodología

En este capítulo, se explora la aplicación de la metodología NIST SP 800-30 para la evaluación de riesgos en el data center de AirmaxTelecom Soluciones Tecnológicas S.A. El objetivo es fortalecer la gestión de la seguridad de la información mediante un proceso estructurado y detallado que guíe la identificación, análisis y mitigación de riesgos. La metodología NIST SP 800-30 proporciona un marco robusto para garantizar que las operaciones del data center sean seguras y resilientes frente a amenazas potenciales, cumpliendo con las regulaciones de seguridad y las expectativas de los clientes en un entorno tecnológico en constante evolución. A lo largo de este capítulo, se detallan los pasos específicos seguidos para preparar, ejecutar y concluir una evaluación de riesgos completa, adaptando las directrices del NIST a las particularidades del Data Center en AirmaxTelecom.

3.1 Metodología de Investigación

Esta sección es fundamental para definir la estrategia apropiada, donde se eligen los métodos para abordar el problema de investigación a través de la recopilación de datos empleando diversas técnicas. Estas técnicas facilitan la obtención de conclusiones basadas en los datos recolectados durante la investigación.

En la evaluación de amenazas y vulnerabilidades en la seguridad de la información del data center de AirmaxTelecom Soluciones Tecnológicas S.A., se realiza un análisis de la infraestructura tecnológica. Para este estudio, se emplean dos tipos de investigación:

- Investigación Descriptiva: Se adopta la investigación descriptiva para examinar las características técnicas, los procedimientos operativos y las configuraciones de

seguridad del Data Center de AirmaxTelecom Soluciones Tecnológicas S.A. El propósito es identificar y evaluar los riesgos asociados con la seguridad de la información en los procesos operativos del centro.

- Investigación Mixta: Se emplea un enfoque de investigación mixta para verificar las políticas de seguridad vigentes en el data center de AirmaxTelecom Soluciones Tecnológicas S.A. y en su departamento de Tecnología. Se realiza una encuesta estructurada al personal encargado y se condujeron entrevistas para recoger información detallada sobre las prácticas actuales de seguridad.

3.1.1 Técnicas de Recolección de Información

Para la recolección de datos en este estudio, se implementan diversas técnicas que permitieron adquirir información relevante sobre la gestión de riesgos y la seguridad de la información en el data center de AirmaxTelecom Soluciones Tecnológicas S.A.:

- Revisión de Documentación: Se solicita y revisa documentación clave para comprender los procesos internos que inciden en la seguridad del data center. Los documentos examinados incluyeron el inventario de activos tecnológicos, los manuales de políticas y procedimientos de seguridad, y las regulaciones internas relacionadas con la gestión tecnológica y la seguridad de la información.
- Entrevistas: Se lleva a cabo una serie de entrevistas con el encargado del data center de AirmaxTelecom Soluciones Tecnológicas S.A. Estas entrevistas se centran en obtener un entendimiento de los procedimientos de seguridad operativa y de la infraestructura tecnológica actual. A través de estas conversaciones, se exploran las políticas y prácticas de seguridad implementadas, los desafíos enfrentados en la gestión diaria de la seguridad,

y las percepciones sobre las áreas de mejora en la protección de la información y los recursos tecnológicos.

- Encuesta: Se realiza una encuesta detallada al encargado del data center de AirmaxTelecom Soluciones Tecnológicas S.A. para abordar múltiples fases de la gestión de riesgos, incluyendo la preparación, identificación de amenazas, análisis de probabilidad, evaluación del impacto, y estrategias de mitigación. Las preguntas del Anexo A cubren desde el propósito y función del data center hasta la efectividad de las medidas de seguridad implementadas, permitiendo una recopilación de datos integral para desarrollar un plan de seguridad robusto y fundamentado.
- Evaluación de Vulnerabilidad: Para la evaluación de vulnerabilidad, se ejecutan pruebas técnicas mediante el uso de las herramientas Nessus y OpenVAS. Estas herramientas permitieron detectar y evaluar posibles debilidades de seguridad en la infraestructura de la red de telecomunicaciones que podrían ser explotadas. Este enfoque ayudó a identificar riesgos específicos y formular estrategias de mitigación efectivas, alineadas con la metodología NIST SP 800-30.

3.2 Preparación para la Evaluación de Riesgos

La preparación para la evaluación de riesgos es un paso crucial para asegurar que el proceso sea exhaustivo y bien estructurado. En esta sección, se definen el alcance y los objetivos de la evaluación, se identifican los recursos y las partes interesadas, y se establecen los criterios para la evaluación de riesgos. Basado en la encuesta realizada al encargado del data center, se lleva a cabo este proceso, lo que permite mostrar la situación actual del data center. Este enfoque sistemático garantiza que todos los aspectos críticos del data center sean considerados y que las medidas de mitigación se enfoquen en los riesgos más significativos.

3.2.1 Definición del Alcance, Objetivos y Funciones del Data Center para la Evaluación de Riesgos

La evaluación de riesgos para el Data Center de AirmaxTelecom Soluciones Tecnológicas S.A. comienza con la definición del alcance y los objetivos de la evaluación. El alcance incluye todos los componentes críticos de la infraestructura de TI, tales como servidores, redes, aplicaciones y datos sensibles. Esta definición es esencial para garantizar que todas las áreas relevantes sean evaluadas y que las medidas de mitigación se enfoquen adecuadamente en los riesgos más significativos.

El propósito principal y la función del Data Center de AirmaxTelecom es concentrar el ancho de banda de los proveedores y establecer sesiones BGP para el anuncio de los recursos IP públicos al mundo. Además, en el Data Center se alojan servidores caché y CDNs, lo que mejora significativamente el rendimiento de la provisión del servicio de Internet. Estas funciones hacen del Data Center una pieza fundamental en la infraestructura tecnológica de la empresa.

Además de las funciones mencionadas, el Data Center de AirmaxTelecom proporciona diversos servicios esenciales que destacan su importancia para la empresa. Entre estos servicios se incluye la virtualización y almacenamiento para sistemas informáticos de la institución, lo cual proporciona un entorno flexible y escalable para las operaciones diarias. También se cuenta con equipos para brindar servicios de VPN, asegurando conexiones seguras y privadas para usuarios remotos y oficinas descentralizadas.

El Data Center también ofrece servicios de hosting y dominio, alojando sitios web y gestionando nombres de dominio para clientes, lo que garantiza una presencia en línea estable y segura. Además, cuenta con servidores AAA (Authentication, Authorization, and Accounting),

que gestionan servicios de autenticación, autorización y contabilidad para abonados del servicio de Internet, asegurando un acceso seguro y controlado a los recursos de la red.

Otra característica importante del Data Center es la implementación de areneros para la identificación de vulnerabilidades, conocidos como honeynets. Estos honeynets permiten la detección y el análisis de vulnerabilidades y amenazas en un entorno controlado, mejorando así la seguridad proactiva del Data Center.

La evaluación de riesgos se enfoca en varios aspectos críticos de la infraestructura del Data Center, incluyendo la infraestructura física, la seguridad lógica, los sistemas eléctricos, la climatización, la gestión de datos y la recuperación ante desastres. Los objetivos principales de esta evaluación son identificar las amenazas y vulnerabilidades específicas del Data Center, evaluar la probabilidad y el impacto de estas amenazas, y desarrollar estrategias efectivas para mitigar los riesgos. Este enfoque integral asegura que todas las áreas críticas sean consideradas y que los esfuerzos de mitigación se dirijan de manera eficiente hacia los riesgos más significativos.

3.2.2 Identificación de los Activos, Partes Interesadas y Establecimiento de la Topología Física y Lógica

En esta fase, se identifican los activos y las partes interesadas que participarían en la evaluación de riesgos. Los datos obtenidos de la encuesta realizada al encargado del data center se utilizan para identificar estos activos y partes interesadas, asegurando una visión precisa y actualizada de la situación del data center. Esta identificación se documenta en las Tablas 4 y 5, así como en la Figura 1.

La Tabla 4 enumera los componentes del data center, tales como enrutadores de borde, conmutadores de agregación, servidores, sistemas de almacenamiento y sistemas de energía. Estos

activos son vitales para la operación diaria y la seguridad del data center y han sido obtenidos de las entrevistas y encuesta realizada al encargado

Tabla 4

Activos Data Center ArimaxTelecom

Activos	**Descripción**
Enrutadores de Borde	Mikrotik serie CCR, dispositivos que gestionan el tráfico de red en el borde del Data Center, conectando el Data Center con proveedores de Internet externos.
Conmutadores de Agregación	Dispositivos que consolidan múltiples conexiones de red y gestionan el tráfico interno, distribuyendo datos entre servidores y almacenamiento.
Sistemas de Almacenamiento (SAN/NAS)	Dispositivos que almacenan grandes volúmenes de datos, asegurando su disponibilidad y redundancia en caso de fallos.
Sistemas de Alimentación Ininterrumpida (UPS)	Modelos como APC Symmetra PX y Eaton 93PM, que proporcionan energía temporal durante cortes eléctricos para garantizar la continuidad operativa.
Generadores de Respaldo	Motores de marcas como Caterpillar y Cummins, que proporcionan energía durante cortes eléctricos prolongados, asegurando la operación continua del Data Center.
Sistemas de Distribución de Energía (PDU)	Modelos de APC y Raritan, que distribuyen energía de manera eficiente a los equipos críticos del Data Center.

Sistemas de Protección contra Sobretensiones	Dispositivos que protegen los equipos contra picos de voltaje, reduciendo el riesgo de fallos eléctricos.
Sistemas de Climatización y HVAC	CRAC (Computer Room Air Conditioner) que aseguran el control de la temperatura y humedad, evitando el sobrecalentamiento de los equipos críticos.
Sistemas de Monitorización y Gestión	Software y hardware utilizados para supervisar el rendimiento, estado y seguridad del Data Center, alertando de fallos y permitiendo una gestión proactiva.
Firewalls	Dispositivos que protegen la red del Data Center frente a amenazas externas, garantizando que solo el tráfico autorizado pase a través de la red.
Switches de Acceso	Dispositivos que conectan servidores individuales y estaciones de trabajo al núcleo de la red, permitiendo la segmentación y control del tráfico interno.
Sistemas de Respaldo y Recuperación	Sistemas que aseguran la restauración de datos críticos en caso de pérdida o corrupción, facilitando la continuidad operativa ante incidentes.
Sistemas de Seguridad Física	Sistemas que incluyen control de acceso, cámaras de vigilancia, y detección de intrusos, protegiendo las instalaciones físicas del Data Center contra accesos no autorizados.
Software de Gestión de Infraestructura (DCIM)	Herramientas que optimizan la gestión de recursos del Data Center, permitiendo un uso eficiente de energía, espacio y recursos de TI.

Documentación Técnica	Manuales, políticas, procedimientos y configuraciones actuales del Data Center, que son esenciales para la gestión y mantenimiento de los equipos y operaciones.
Sistemas de Cableado Estructurado	Infraestructura que conecta los diferentes dispositivos dentro del Data Center, asegurando un flujo de datos eficiente entre equipos y redes.

.

Por otra parte, la Tabla 5 lista a las partes interesadas clave, que incluyen al Personal de Planta Interna, la Jefatura de Networking y la Jefatura de Planta Externa. Estas partes interesadas desempeñan un papel fundamental en la operación y seguridad del data center, y su participación es esencial para una evaluación de riesgos efectiva.

Tabla 5

Partes Interesadas en la Gestión del Data Center

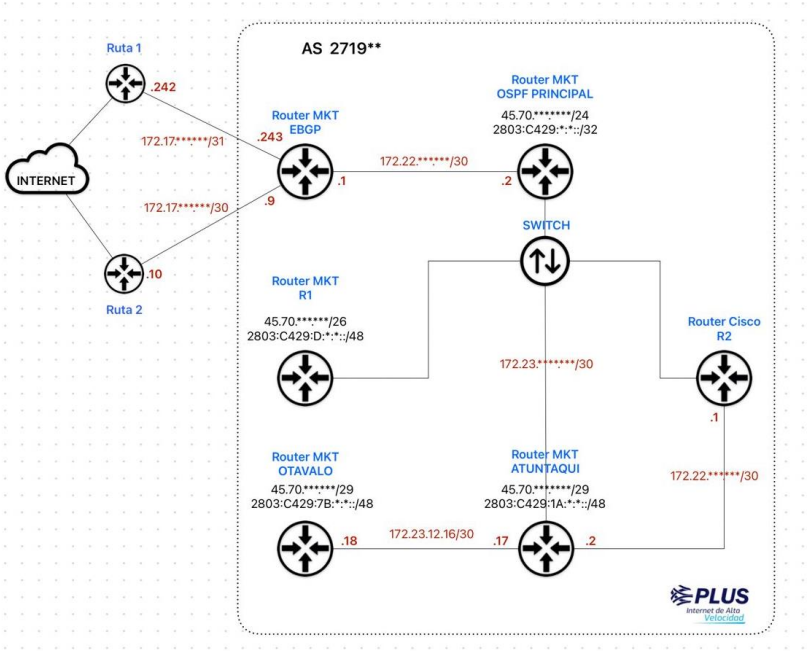
Parte Interesada	Descripción
Personal de Planta Interna	Encargado de la gestión y mantenimiento de la infraestructura física del data center.
Jefatura de Networking	Responsable de la configuración, supervisión y optimización de las redes del data center.
Jefatura de Planta Externa	Supervisa y coordina las conexiones externas y la integración con proveedores y clientes.

Por otra parte, la red de la empresa AirmaxTelecom se muestra en la Figura 2, donde se puede observar la topología física y lógica del Data Center que cuenta con una topología de red mixta, diseñada para proporcionar flexibilidad, escalabilidad y eficiencia.

En cuanto a la topología lógica de la red, se ha decidido ocultar la dirección IP interna utilizada en toda la infraestructura de telecomunicaciones de la empresa. Esta red opera con un rango de direcciones de clase B, específicamente 172.17.x.x/31, lo que proporciona un amplio espacio de direcciones IP para la red principal interna en Ibarra. Para las conexiones con los routers ubicados fuera de la red principal, que suministran el servicio de internet hacia Otavalo y Atuntaqui, se emplea la red 172.23.x.x/30.

Figura 2

Topología de Red AirmaxTelecom



3.2.3Establecimiento de los activos críticos y criterios de evaluación de riesgos.

En base a la información obtenida a través de la encuesta realizada que se muestra en el Anexo A y la tabla 4, se identifican los activos críticos esenciales para el funcionamiento del Data Center de AirmaxTelecom Soluciones Tecnológicas S.A. Los equipos principales que soportan la infraestructura de la red son los enrutadores de borde y los conmutadores de agregación. Estos dispositivos son vitales para la operación continua y eficiente del Data Center, ya que facilitan la comunicación y el manejo del tráfico de datos dentro y fuera de la red.

Para determinar los activos críticos en el Data Center de AirmaxTelecom, se ha desarrollado una matriz que evalúa la relevancia de cada activo en función de los departamentos más importantes de la empresa. Esta matriz muestra qué activos son fundamentales para áreas como Red, Operaciones, Seguridad, Atención al Cliente, Desarrollo de Infraestructura, y TI. A través de la tabla 6, se ha asignado un valor de 1 a aquellos activos que son esenciales para el funcionamiento de cada departamento, y 0 a aquellos que no son determinantes.

La tabla 6 ofrece una representación clara de la importancia de cada activo para las operaciones de la empresa, donde la suma final de los valores permite identificar cuáles son los activos más críticos dando una prioridad alta, media y baja. Aquellos con mayor puntaje y de prioridad alta son los más relevantes para el soporte de múltiples funciones dentro de la infraestructura del Data Center. Así, se garantiza que los activos más críticos reciben la atención prioritaria en términos de seguridad, mantenimiento y contingencia, minimizando el riesgo de interrupciones operativas y asegurando la continuidad del negocio.

Tabla 6

Identificación Activos Críticos Data Center AirmaxTelecom

Activo Crítico	Red	Operaciones	Seguridad	Atención al Cliente	Infraestructura	TI	Suma	Prioridad
Enrutadores de Borde	1	1	1	1	1	1	**6**	**Alta**
Conmutadores de Agregación	1	1	1	1	1	0	**5**	**Alta**
Servidores	1	1	1	0	1	1	**5**	**Alta**
Sistemas de Almacenamiento	1	1	1	0	1	1	**5**	**Alta**
Sistemas de Alimentación (UPS)	1	1	1	0	1	0	**4**	**Media**
Generadores de Respaldo	1	1	1	0	1	0	**4**	**Media**
Sistemas de Climatización (HVAC)	1	1	0	0	1	0	**3**	**Media**
Sistemas de Monitorización	1	1	1	0	1	1	**5**	**Alta**
Conexiones de Red Externas	1	1	1	1	1	0	**5**	**Alta**

Sistemas de Respaldo y Recuperación	1	1	1	0	1	1	**5**	**Alta**
Sistemas de Seguridad Física	1	1	1	0	1	0	**4**	**Media**
Switches de Acceso	1	1	0	1	1	0	**4**	**Media**
Firewalls	1	1	1	0	0	1	**4**	**Media**
Sistemas de Distribución Eléctrica	1	1	0	0	1	0	**3**	**Baja**
Sistemas de Control de Humedad	0	1	0	0	1	0	**2**	**Baja**
Sistemas de Cableado Estructurado	1	1	0	0	1	0	**3**	**Baja**
Bastidores y Racks de Servidores	0	1	0	0	1	0	**2**	**Baja**
Sistemas de Detección de Incendios	1	1	1	0	1	0	**4**	**Media**

Después de realizar los cálculos y evaluar las áreas clave involucradas en el funcionamiento del Data Center, se determinó que los siguientes activos son considerados críticos. Estos activos obtuvieron una puntuación igual o superior a 5, lo que refleja su alta relevancia en la continuidad operativa y la disponibilidad de los servicios. La tabla 7 presenta los activos críticos junto con su respectiva descripción funcional.

Tabla 7
Activos Críticos del Data Center

Activo Crítico	Puntuación	Descripción
Enrutadores de Borde	6	Dispositivos que gestionan el tráfico de datos de entrada y salida del Data Center, asegurando conectividad externa e interna.
Conmutadores de Agregación	5	Dispositivos que consolidan y distribuyen el tráfico de datos dentro del Data Center, conectando los diferentes segmentos de red.
Servidores	5	Equipos que alojan aplicaciones y datos críticos para las operaciones del negocio.
Sistemas de Almacenamiento	5	Dispositivos y sistemas que almacenan grandes cantidades de datos, esenciales para el acceso y gestión de la información empresarial.
Sistemas de Monitorización	5	Software y hardware utilizados para supervisar el rendimiento, la seguridad y el estado de los equipos y redes del Data Center.

Conexiones de Red Externas	5	Enlaces de comunicación con proveedores de servicios de Internet y otras redes, garantizando la conectividad externa del Data Center.
Sistemas de Respaldo y Recuperación	5	Soluciones diseñadas para garantizar que los datos puedan ser restaurados en caso de pérdida, corrupción o desastres, asegurando continuidad.

Por otra parte, los criterios para la evaluación de riesgos se establecen en la Tabla 8 proporcionando un marco estructurado para evaluar tanto la probabilidad como el impacto de las amenazas. Esta tabla incluye criterios como la frecuencia de incidentes, impacto operativo, financiero, reputacional, y la capacidad de recuperación del data center. Estos criterios son esenciales para una evaluación comparativa y coherente de los riesgos identificados.

Tabla 8

Criterios de Evaluación de Riesgos

Criterio	Descripción
Frecuencia de Incidentes	Evaluación basada en la frecuencia histórica de amenazas similares.
Impacto Operativo	Evaluación del impacto en las operaciones diarias del data center.
Impacto Financiero	Evaluación del impacto financiero, incluyendo costos de recuperación y pérdida de ingresos.
Impacto Reputacional	Evaluación del impacto en la reputación de la empresa y la confianza de los clientes.
Capacidad de Recuperación	Evaluación de la capacidad del data center para recuperarse de incidentes y restaurar operaciones normales.

3.3 Identificación de Amenazas y Vulnerabilidades

La identificación efectiva de amenazas y vulnerabilidades es fundamental para la gestión de riesgos. En este apartado, se explica cómo se lleva a cabo este proceso en el data center, incluyendo la utilización de herramientas específicas para identificar vulnerabilidades en la infraestructura de TI y la catalogación de las amenazas y vulnerabilidades detectadas a partir de una mesa de trabajo realizada con el encargado del Data Center.

3.3.1 Identificación de amenazas específicas al Data Center.

Para identificar las amenazas específicas que enfrenta el data center de AirmaxTelecom Soluciones Tecnológicas S.A., se utiliza una encuesta dirigida al personal encargado del centro de datos. Los resultados de la encuesta proporcionan información detallada sobre las amenazas percibidas, que fueron documentadas en la Tabla 9. Esta tabla clasifica las amenazas según su origen y los activos del data center potencialmente afectados. La organización de esta información en la tabla es crucial para facilitar un análisis posterior sobre cómo cada amenaza puede impactar en la operatividad del data center y permite una evaluación sistemática de los riesgos asociados.

Tabla 9

Registro de Amenazas Identificadas

ID de Amenaza	Descripción de la Amenaza	Origen de la Amenaza	Activos Afectados
A001	Terremotos	Externo	Infraestructura física
A002	Inundaciones	Externo	Infraestructura física y TI

A003	Incendios	Externo/Interno	Infraestructura física y equipos
A004	Fallos de hardware debido a clasificación Tier 1	Interno	Infraestructura de TI
A005	Evolución de técnicas de cibercriminales	Externo	Servidores e infraestructura
A006	Redundancia insuficiente en equipos activos	Interno	Infraestructura de red
A007	Ausencia de un Data Center espejo	Interno	Infraestructura de TI

Nota. En la tabla se puede observar el registro de amenazas percibidas por la empresa hacia el Data Center.

3.3.2 Identificación de vulnerabilidades en la infraestructura del Data Center

Para el análisis de vulnerabilidades en la infraestructura de TI del Data Center de AirmaxTelecom, se implementan, junto con el jefe de networking de la empresa, Nessus y OpenVAS, dos herramientas destacadas por su robustez y amplia adopción en la industria de la seguridad informática. Estas herramientas son ampliamente reconocidas por su capacidad para detectar una extensa gama de vulnerabilidades de seguridad, desde configuraciones inseguras hasta software desactualizado. Adicionalmente se utiliza una honeynet que está implementada en la empresa como parte de las estrategias de detección y análisis de amenazas en la red.

Utilizando Nessus, OpenVAS y el honeynet, se realiza un escaneo detallado de la red y los sistemas del data center, lo que permite identificar vulnerabilidades que podrían ser explotadas por

agentes maliciosos. De este análisis, se detecta un riesgo bajo relacionado con ICMP en los routers Mikrotik. Los resultados de estos análisis se registran meticulosamente en la Tabla 10 donde cada vulnerabilidad se clasifica por su severidad y los sistemas específicos afectados. Esta clasificación es crucial para priorizar las correcciones y fortalecer la seguridad del data center.

Tabla 10

Registro de Vulnerabilidades Detectadas

ID de Vulnerabilidad	Descripción de la Vulnerabilidad	Severidad	Sistemas Afectados
V001	ICMP Timestamp expuesto, podría usarse para sincronización en ataques	Baja	Servidores de aplicación

Nota. En la tabla se puede observar el registro de vulnerabilidades detectadas en los equipos del Data Center.

3.3.3 Categorización de las amenazas y vulnerabilidades identificadas.

Para valorar adecuadamente los riesgos asociados a un activo crítico del Data Center de AIRMAXTELECOM Soluciones Tecnológicas S.A., es esencial determinar su valor tanto cualitativo como cuantitativo. No obstante, debido a la sensibilidad y privacidad de los datos relativos al valor monetario tangible de estos activos, se presenta exclusivamente una matriz que refleja la importancia de la confidencialidad, integridad y disponibilidad para la organización. Esta matriz se basa en el apéndice F de la metodología NIST SP 800-30.

En la Tabla 11, se presenta una escala cualitativa y cuantitativa que determina el nivel de riesgo de las vulnerabilidades y activos dentro de la empresa basándose en la metodología NIST 800-30 en la cual se obtiene estos rangos de valores cuantitativos a partir de la multiplicación de la probabilidad y el impacto para determinar el nivel de riesgo. Este enfoque ha sido adaptado al

proceso realizado en la mesa de trabajo y desarrollado en colaboración con el encargado del Data Center.

Tabla 11

Escala de medición del nivel de riesgo de los activos y vulnerabilidades de AirmaxTelecom

Escala Medición Nivel de Riesgo		
Cualitativo	**Cuantitativo**	**Descripción**
Muy alto	96-100	La vulnerabilidad está expuesta y es explotable, y su explotación podría resultar en impactos severos. No se implementa ni planifica el control de seguridad pertinente u otra remediación; o no se puede identificar ninguna medida de seguridad para remediar la vulnerabilidad.
Alto	80-95	La vulnerabilidad es de alta preocupación, con base en la exposición de la vulnerabilidad y facilidad de explotación y/o en la severidad de los impactos que podrían resultar de su explotación. El control de seguridad relevante u otra remediación está planificada pero no implementada; los controles de compensación están en su lugar y son al menos mínimamente efectivos.
Moderado	21-79	La vulnerabilidad es de preocupación moderada, con base en la exposición de la vulnerabilidad y facilidad de explotación y/o en la severidad de los impactos que podrían resultar de su

		explotación. El control de seguridad relevante u otra remediación se implementa parcialmente y es algo efectivo.
Bajo	5-20	La vulnerabilidad es una preocupación menor, pero se podría mejorar la efectividad de la remediación. El control de seguridad relevante u otra remediación está completamente implementado y es algo efectivo.
Muy bajo	0-4	La vulnerabilidad no es motivo de preocupación. El control de seguridad relevante u otra remediación se implementa, evalúa y es efectivo en su totalidad.

Nota. En la tabla se puede observar la escala de criticidad de los activos y vulnerabilidades para el Data Center de AirmaxTelecom. Tomado del apéndice F de la NIST SP 800-30.

La información recopilada en las fases anteriores se consolidó utilizando la Tabla 12, la cual integra y categoriza todas las amenazas y vulnerabilidades identificadas a partir de la NIST 800-30, evaluando cada una en términos de probabilidad e impacto y priorizando su mitigación. En la tabla 9, las vulnerabilidades como la Redundancia insuficiente o la Ausencia de un Data Center espejo se trataban como amenazas con los identificadores A006 y A007. Sin embargo, en esta tabla actualizada, dichas vulnerabilidades han sido recategorizadas adecuadamente bajo los identificadores V001 y V002, respectivamente. Esto permite una distinción clara entre amenazas, que son eventos externos o internos como los terremotos o los fallos de hardware, y vulnerabilidades, que son debilidades inherentes en el sistema, como la falta de redundancia o la vulnerabilidad al protocolo ICMP.

Tabla 12

Amenazas y Vulnerabilidades en términos de probabilidad e impacto inicial

ID	Tipo	Descripción	Probabilidad	Impacto	Nivel de Riesgo Cuantitativo (P x I)	Nivel de Riesgo Cualitativo
A001	Amenaza	Terremotos	7	9	63	Moderado
A002	Amenaza	Inundaciones	6	8	48	Moderado
A003	Amenaza	Incendios	5	9	45	Moderado
A004	Amenaza	Fallos de hardware (Tier 1)	5	9	45	Moderado
A005	Amenaza	Evolución de técnicas de cibercriminales	8	9	72	Alto
V001	Vulnerabilidad	Redundancia insuficiente en	4	6	24	Bajo

		equipos activos				
V002	Vulnerabilidad	Ausencia de un Data Center espejo	9	9	81	Alto
V003	Vulnerabilidad	ICMP	3	5	15	Bajo

Nota. En la tabla se puede observar los valores de la probabilidad e impacto para cada amenaza y vulnerabilidad.

3.3.4 Asociación de Activos Críticos con las Amenazas y Vulnerabilidades del Data Center

La asociación de activos críticos con amenazas y vulnerabilidades en el Data Center de AirmaxTelecom Soluciones Tecnológicas S.A. permite una evaluación integral del riesgo. Los activos como enrutadores de borde, conmutadores de agregación, servidores y sistemas de almacenamiento están expuestos a amenazas como desastres naturales, fallos de hardware y ciberataques. La Tabla 13 asocia los activos críticos con amenazas y vulnerabilidades para así facilitar la implementación de medidas de mitigación efectivas. Este enfoque mejora la resiliencia del Data Center, optimiza la asignación de recursos de seguridad y asegura la continuidad operativa, protegiendo así los servicios esenciales de la organización ante posibles eventos adversos.

Tabla 13

Asociación de Activos críticos con amenazas y vulnerabilidades

Activo Crítico	Descripción	Amenazas	Vulnerabilidades	Impacto Potencial
Enrutadores de Borde	Dispositivos que gestionan el tráfico de datos de entrada y salida del Data Center.	Terremotos (A001), Inundaciones (A002), Incendios (A003), Fallos de hardware (A004), Evolución de ciberataques (A005)	Redundancia insuficiente (V001), ICMP (V003), Ausencia de Data Center Espejo (V002)	Daño físico, interrupción del servicio, compromiso de la seguridad.
Conmutadores de Agregación	Dispositivos que consolidan y distribuyen el tráfico de datos dentro del Data Center.	Terremotos (A001), Inundaciones (A002), Incendios (A003), Fallos de hardware (A004),	Redundancia insuficiente (V001), ICMP (V003), Ausencia de Data Center Espejo (V002)	Daño físico, interrupción del servicio, compromiso de la seguridad.

		Evolución de ciberataques (A005)		
Servidores	Equipos que alojan aplicaciones y datos críticos para las operaciones del negocio.	Terremotos (A001), Inundaciones (A002), Incendios (A003), Fallos de hardware (A004), Evolución de ciberataques (A005)	Redundancia insuficiente (V001), Ausencia de Data Center Espejo (V002)	Interrupción del servicio, pérdida de datos, exposición de información.
Sistemas de Almacenamiento (SAN/NAS)	Dispositivos y sistemas que almacenan grandes cantidades de datos.	Terremotos (A001), Inundaciones (A002), Incendios (A003), Fallos de hardware (A004), Evolución de	Redundancia insuficiente (V001), Ausencia de Data Center Espejo (V002)	Pérdida de datos, interrupción del servicio.

		ciberataques (A005)		
Sistemas de Monitorización	Software y hardware utilizados para supervisar el rendimiento y el estado del Data Center.	Terremotos (A001), Inundaciones (A002), Incendios (A003), Evolución de ciberataques (A005)	Redundancia insuficiente (V001), ICMP (V003)	Compromiso de la seguridad, pérdida de visibilidad operativa.
Sistemas de Respaldo y Recuperación	Aseguran que los datos puedan ser restaurados en caso de pérdida o corrupción.	Terremotos (A001), Inundaciones (A002), Incendios (A003), Fallos de hardware (A004), Evolución de ciberataques (A005)	Redundancia insuficiente (V001), Ausencia de Data Center Espejo (V002)	Pérdida de datos, interrupción del servicio.

Conexiones de Red Externas	Enlaces de comunicación con proveedores de servicios de Internet y otras redes.	Terremotos (A001), Inundaciones (A002), Incendios (A003), Fallos de hardware (A004), Evolución de ciberataques (A005)	Redundancia insuficiente (V001), ICMP (V003)	Interrupción del servicio, compromiso de la seguridad.

Nota. En la tabla se puede observar las amenazas y vulnerabilidades para cada activo crítico del Data Center de AirmaxTelecom.

3.4 Análisis de Probabilidad

El análisis de probabilidad busca determinar la frecuencia esperada de cada amenaza identificada y evaluar la exposición del Data Center a estas amenazas. Este análisis se fundamenta en las directrices del Anexo G de la NIST SP 800-30, el cual proporciona un ejemplo para estimar la probabilidad teniendo en cuenta el contexto operativo del Data Center y las experiencias anteriores con amenazas similares.

3.4.1 Determinación de la frecuencia esperada de amenazas identificadas.

Para determinar la frecuencia esperada de amenazas, se evalúa la probabilidad de ocurrencia de cada amenaza identificada. Esta evaluación se realiza tomando en cuenta la mesa de trabajo con el Jefe de Networking de la empresa. La tabla 14 presenta la frecuencia esperada de todas las amenazas identificadas para los activos críticos del Data Center de AirmaxTelecom Soluciones Tecnológicas S.A.

Tabla 14

Frecuencia esperada de Amenazas y Vulnerabilidades identificadas

ID	Amenaza / Vulnerabilidad	Probabilidad	Frecuencia Esperada
A001	Terremotos	5	Moderada (Anual)
A002	Inundaciones	5	Moderada (Anual)
A003	Incendios	5	Moderada (Anual)
A004	Fallos de hardware (Tier 1)	7	Alta (Semestral)
A005	Evolución de técnicas de cibercriminales	7	Alta (Semestral)
V001	Redundancia insuficiente en equipos	4	Moderada (Anual)
V002	Ausencia de un Data Center espejo	8	Alta (Semestral)
V003	ICMP	3	Baja (Anual)

Nota. En la tabla se puede observar la frecuencia esperada de las amenazas detectadas para el Data Center de AirmaxTelecom.

3.4.2 Evaluación de la exposición del Data Center a las amenazas

La evaluación de la exposición del Data Center a las amenazas se realiza analizando cómo cada amenaza podría afectar los diferentes activos críticos del Data Center. La exposición se evalúa en función de la vulnerabilidad y la criticidad de cada activo a partir de la entrevista realizada al encargado del Data Center, así como la frecuencia esperada de la amenaza. La tabla 15 muestra la exposición del Data Center a las amenazas identificadas, asociadas a cada activo crítico.

Tabla 15

Exposición de los Activos Críticos del Data Center ante las amenazas y vulnerabilidades

Activo Crítico	Amenazas y Vulnerabilidades	Exposición	Justificación
Enrutadores de Borde	Terremotos (A001)	Moderada	Alta criticidad y exposición geográfica a sismos que pueden dañar la infraestructura física.
	Inundaciones (A002)	Moderada	Alta criticidad con moderada vulnerabilidad a inundaciones que pueden dañar los equipos.
	Incendios (A003)	Alta	Alta probabilidad de daños físicos significativos en caso de incendio en el Data Center.
	Fallos de hardware (A004)	Alta	Alta criticidad y frecuencia semestral de fallos, afectando

			la conectividad y disponibilidad.
	Evolución de técnicas de cibercriminales (A005)	Alta	Alta probabilidad de ataques sofisticados dirigidos a comprometer la seguridad de la red.
	Redundancia insuficiente en equipos (V001)	Moderada	Alta criticidad con moderada probabilidad de fallos por falta de redundancia en los sistemas.
	Ausencia de un Data Center espejo (V002)	Alta	Alta criticidad debido a la falta de continuidad operativa y respaldo de datos.
	ICMP (V003)	Moderada	Moderada probabilidad de explotación del protocolo ICMP, con potencial impacto en la seguridad.
Conmutadores de Agregación	Terremotos (A001)	Moderada	Alta criticidad y riesgo geográfico de sismos que afectan la infraestructura interna.

	Inundaciones (A002)	Moderada	Alta criticidad ante posibles daños por inundaciones que impacten la operación interna.
	Incendios (A003)	Alta	Alta probabilidad de daños físicos significativos por incendios en las instalaciones.
	Fallos de hardware (A004)	Alta	Alta criticidad y frecuencia semestral de fallos, afectando la conectividad de múltiples sistemas.
	Evolución de técnicas de cibercriminales (A005)	Alta	Alta probabilidad de ataques cibernéticos que comprometan la integridad de la red.
	Redundancia insuficiente en equipos (V001)	Moderada	Moderada probabilidad de fallos por la falta de sistemas redundantes en los conmutadores.
	Ausencia de un Data Center espejo (V002)	Alta	Alta criticidad ante la pérdida de datos y continuidad operativa sin un sistema espejo.
	ICMP (V003)	Moderada	Moderada probabilidad de explotación del protocolo

			ICMP, con alto impacto potencial.
Servidores	Terremotos (A001)	Moderada	Alta criticidad ante la exposición a sismos que afecten la infraestructura física.
	Inundaciones (A002)	Moderada	Moderada vulnerabilidad a inundaciones que pueden dañar los equipos físicos.
	Incendios (A003)	Alta	Alta probabilidad de daños físicos por incendios en el Data Center.
	Fallos de hardware (A004)	Alta	Alta frecuencia de fallos en hardware crítico que sostiene aplicaciones esenciales.
	Evolución de técnicas de cibercriminales (A005)	Alta	Alta probabilidad de ataques sofisticados dirigidos a los servidores críticos.
	Redundancia insuficiente en equipos (V001)	Moderada	Moderada probabilidad de interrupciones por falta de sistemas redundantes.

	Ausencia de un Data Center espejo (V002)	Alta	Alta criticidad ante la falta de un sistema espejo que afecte la continuidad operativa.
Sistemas de Almacenamiento (SAN/NAS)	Terremotos (A001)	Moderada	Alta criticidad con moderada exposición a daños físicos por sismos.
	Inundaciones (A002)	Moderada	Moderada vulnerabilidad a inundaciones que pueden afectar los sistemas de almacenamiento.
	Incendios (A003)	Alta	Alta probabilidad de daños físicos significativos por incendios en el Data Center.
	Fallos de hardware (A004)	Alta	Alta frecuencia de fallos que afectan la disponibilidad y almacenamiento de datos críticos.
	Evolución de técnicas de cibercriminales (A005)	Alta	Alta probabilidad de ataques dirigidos a comprometer la integridad de los datos almacenados.

	Redundancia insuficiente en equipos (V001)	Moderada	Moderada probabilidad de interrupciones por falta de redundancia en los sistemas de almacenamiento.
	Ausencia de un Data Center espejo (V002)	Alta	Alta probabilidad de pérdida de datos críticos por la falta de respaldo.
Sistemas de Monitorización	Evolución de técnicas de cibercriminales (A005)	Alta	Alta probabilidad de ataques cibernéticos que comprometan la monitorización de la infraestructura.
	ICMP (V003)	Moderada	Moderada probabilidad de explotación del protocolo ICMP, con impacto en la seguridad.
Sistemas de Respaldo y Recuperación	Terremotos (A001)	Moderada	Moderada probabilidad de daños físicos por sismos que afecten los sistemas de respaldo.
	Inundaciones (A002)	Moderada	Moderada vulnerabilidad a inundaciones que comprometan los sistemas de recuperación.

	Incendios (A003)	Alta	Alta probabilidad de daños físicos significativos por incendios en las instalaciones.
	Fallos de hardware (A004)	Alta	Alta criticidad y frecuencia semestral de fallos que afectan la recuperación de datos.
	Evolución de técnicas de cibercriminales (A005)	Alta	Alta probabilidad de ataques que comprometan la integridad de los datos respaldados.
	Redundancia insuficiente en equipos (V001)	Moderada	Moderada probabilidad de interrupciones por falta de sistemas redundantes en los respaldos.
	Ausencia de un Data Center espejo (V002)	Alta	Alta probabilidad de pérdida de datos críticos sin la capacidad de recuperación inmediata.
Conexiones de Red Externas	Fallos de hardware (A004)	Alta	Alta frecuencia de fallos en las conexiones con proveedores de servicios externos.

	Evolución de técnicas de cibercriminales (A005)	Alta	Alta criticidad ante ataques sofisticados dirigidos a las conexiones externas.

Nota. En la tabla se puede observar la exposición de los activos críticos del Data Center ante las amenazas detectadas.

3.4.3 Probabilidad de ocurrencia

La probabilidad de ocurrencia de las amenazas se determina en función de la frecuencia esperada y la exposición del Data Center a estas amenazas. Esta evaluación permite priorizar las amenazas que requieren atención inmediata. La tabla 16 resume la probabilidad de ocurrencia para cada amenaza realizada en la mesa de trabajo con el jefe de networking.

Tabla 16

Probabilidad de ocurrencia para cada amenaza y vulnerabilidad

Amenaza	**Frecuencia Esperada**	**Exposición**	**Probabilidad de Ocurrencia**
Terremotos	Moderada (Anual)	Alta	Baja
Inundaciones	Moderada (Anual)	Alta	Baja
Incendios	Moderada (Anual)	Alta	Baja
Fallos de hardware	Alta (Semestral)	Alta	Alta
Evolución de técnicas de cibercriminales	Alta (Semestral)	Alta	Alta

Redundancia insuficiente en equipos	Moderada (Anual)	Moderada	Moderada
Ausencia de un Data Center espejo	Alta (Semestral)	Alta	Alta
ICMP	Baja (Anual)	Baja	Baja

Nota. En la tabla se puede observar la frecuencia esperada para cada amenaza y la probabilidad de ocurrencia.

3.5 Evaluación del Impacto

La evaluación del impacto implica analizar las consecuencias de que las amenazas identificadas se materialicen. Se considerarán tanto el impacto inmediato como a largo plazo en el Data Center, abarcando aspectos financieros, operativos y reputacionales. Para realizar esta evaluación, se utilizó el Apéndice H de la NIST SP 800-30, que proporciona guías y modelos para la estimación de impactos y riesgos, asegurando una calificación y cuantificación detallada de cómo los riesgos pueden afectar los activos y operaciones críticas.

3.5.1 Impacto potencial de las amenazas y vulnerabilidades en las operaciones del data center.

El impacto potencial de las amenazas en las operaciones del Data Center se evalúa en términos de la gravedad de las consecuencias. Esta evaluación permite identificar las amenazas que podrían tener los efectos más perjudiciales en las operaciones diarias. La tabla 17 presenta el impacto potencial de cada amenaza identificada.

Tabla 17

Impacto potencial de las amenazas y vulnerabilidades

Amenaza	**Impacto Potencial**	**Justificación**
Incendios	Daño físico a la infraestructura	Los incendios pueden destruir o dañar físicamente el Data Center, afectando la infraestructura crítica y la continuidad operativa de los servicios.
Terremotos	Daño físico a la infraestructura	Los terremotos pueden generar daños estructurales severos que comprometen la operatividad de los equipos y sistemas clave del Data Center.
Inundaciones	Daño físico a la infraestructura	Las inundaciones pueden provocar daños significativos en los sistemas eléctricos y de TI, afectando seriamente la operatividad del Data Center.
Fallos de hardware (Tier 1)	Interrupción del servicio	Un fallo en equipos críticos como servidores y enrutadores podría detener operaciones esenciales hasta su reemplazo o reparación.
Evolución de técnicas de cibercriminales	Compromiso de la seguridad	Las técnicas avanzadas de cibercrimen pueden vulnerar las defensas actuales, comprometiendo la confidencialidad, integridad y disponibilidad de datos.

Redundancia insuficiente en equipos	Fallos en la red	La falta de redundancia en los equipos puede provocar fallos de conectividad, afectando la disponibilidad de servicios clave.
Ausencia de un data center espejo	Pérdida de datos y servicio	Sin un centro de datos de respaldo, una pérdida o fallo mayor podría ser irreparable, afectando la continuidad operativa.
ICMP	Fallos en la red e intrusiones	El mal uso del protocolo ICMP puede permitir ataques de denegación de servicio (DoS) o accesos no autorizados a la red, comprometiendo su seguridad.

3.5.2 Evaluación del impacto sobre la continuidad del negocio.

La continuidad del negocio depende de la capacidad del Data Center para recuperarse de las amenazas. La evaluación del impacto sobre la continuidad del negocio permite identificar las amenazas que podrían interrumpir las operaciones críticas y afectar la viabilidad de la empresa.

En el contexto de la planificación de la continuidad operativa y la recuperación ante desastres, es esencial definir dos parámetros clave: el Recovery Time Objective (RTO) y el Recovery Point Objective (RPO). Estas métricas permiten cuantificar el impacto temporal y de datos ante una interrupción de los servicios críticos.

Para definir los Tiempos Objetivo de Recuperación (RTO) y los Puntos Objetivo de Recuperación (RPO) en el plan de recuperación ante desastres, se utilizan las siguientes fórmulas:

1. **Cálculo del RTO:**

$$RTO=Tdetect+Tresponse+Trecover$$

Donde:

- Tdetect: Tiempo necesario para detectar el fallo.
- Tresponse: Tiempo necesario para responder al incidente.
- Trecover : Tiempo necesario para recuperar los sistemas afectados.

Ejemplo de RTO:

Para un servidor crítico que aloja servicios empresariales esenciales:

- Tdetect=10 minutos = 10 (detección automática del fallo).
- Tresponse=20 minutos (inicio de la respuesta técnica).
- Trecover=30 minutos (restauración del sistema).

$$RTO=10+20+30=60minutos(1hora)$$

2. **Cálculo del RPO:**

$$RPO=Tbackup$$

Donde:

- Tbackup: Intervalo entre las copias de seguridad o sincronizaciones de datos.

Ejemplo de RPO:

Si las copias de seguridad se realizan cada 4 horas, el RPO sería:

$$RPO=4horas$$

El RTO representa el tiempo máximo permitido que un sistema puede estar inactivo antes de afectar significativamente las operaciones del Data Center. En otras palabras, define el período de tiempo en el cual se debe restablecer un sistema, aplicación o función después de una interrupción para evitar consecuencias críticas.

En la Tabla 18, se presentan los activos críticos del Data Center, junto con sus valores de RTO asignados. Estos valores reflejan la prioridad que cada activo tiene en la recuperación, considerando su impacto en las operaciones del negocio.

Tabla 18

Valores RTO para activos críticos

Activo Crítico	RTO (Tiempo Máximo de Inactividad)	Impacto Operativo
Enrutadores de Borde	15 minutos	Pérdida de conectividad externa
Conmutadores de Agregación	30 minutos	Interrupción de la red interna
Servidores	1 hora	Caída de servicios empresariales clave

Sistemas de Almacenamiento (SAN/NAS)	1 hora	Pérdida de acceso a datos críticos
Sistemas de Respaldo y Recuperación	2 horas	Retraso en la recuperación de datos

Por otra parte, el RPO establece el punto en el tiempo al que se debe restaurar los datos tras un incidente, es decir, la cantidad máxima de datos que la empresa puede permitirse perder. Este parámetro determina la frecuencia con la que se deben realizar las copias de seguridad de los sistemas y datos críticos del Data Center.

En la Tabla 19, se muestra un ejemplo de valores RPO para activos clave. Estos valores están directamente relacionados con la criticidad de los datos que manejan y la tolerancia de la empresa a la pérdida de información.

Tabla 19

Valores RPO para activos críticos

Activo Crítico	RPO (Máxima Pérdida de Datos Permitida)	Frecuencia de Copias de Seguridad
Servidores	5 minutos	Copias incrementales cada 5 minutos
Sistemas de Almacenamiento (SAN/NAS)	10 minutos	Copias completas cada 10 minutos
Sistemas de Respaldo y Recuperación	30 minutos	Copias diarias

Enrutadores de Borde	1 día	Configuraciones respaldadas diariamente

Ambos objetivos, RTO y RPO, son fundamentales para determinar las prioridades de recuperación y la secuencia en la que se deben restaurar los servicios. Como se observa en las Tablas 17 y 18, los activos críticos con tiempos de RTO y RPO más cortos requieren una atención prioritaria durante la fase de recuperación. Los enrutadores de borde tienen un RTO de 15 minutos, lo que significa que deben restaurarse rápidamente para evitar interrupciones en la conectividad externa. De manera similar, los servidores de bases de datos tienen un RPO de 5 minutos, lo que implica que las copias de seguridad deben realizarse con alta frecuencia para minimizar la pérdida de información crítica.

En función de estas métricas, el plan de seguridad debe definir estrategias específicas que aseguren una recuperación rápida de los activos prioritarios y minimicen la pérdida de datos, garantizando así la continuidad de las operaciones. Al integrar estas métricas en la evaluación del impacto, se logra un enfoque más estructurado para priorizar la recuperación de los activos más importantes en situaciones de emergencia. Esto también proporciona una base para evaluar qué tan preparado está el Data Center para manejar posibles incidentes y mantener un alto nivel de disponibilidad y confiabilidad operativa. La tabla 20 presenta la evaluación del impacto de las amenazas sobre la continuidad del negocio.

Tabla 20

Impacto sobre la continuidad del negocio

Amenaza	Impacto Potencial	Justificación
Terremotos	Daño físico a la infraestructura	Los terremotos pueden causar daños severos a la infraestructura física del Data Center, comprometiendo su operatividad.
Inundaciones	Daño físico a la infraestructura	Las inundaciones pueden afectar los equipos eléctricos y críticos del Data Center, interrumpiendo su funcionamiento.
Incendios	Daño físico a la infraestructura	Los incendios pueden destruir o dañar físicamente los equipos y la infraestructura, paralizando las operaciones del Data Center.
Fallos de hardware	Interrupción significativa del servicio	Un fallo en servidores, enrutadores o dispositivos críticos puede detener las operaciones hasta su reparación o reemplazo.
Evolución de técnicas de cibercriminales	Compromiso de la seguridad	Las técnicas avanzadas de cibercrimen pueden superar las defensas de seguridad actuales, exponiendo datos sensibles y la integridad de los sistemas.
Redundancia insuficiente en equipos	Fallos en la red	La falta de redundancia en equipos críticos puede causar fallos en la conectividad y reducir la disponibilidad de los servicios.

Ausencia de un Data Center espejo	Pérdida de datos y servicios	La falta de un centro de respaldo puede hacer que una pérdida de datos o una interrupción mayor sea difícil de recuperar, afectando gravemente las operaciones.
ICMP	Fallos en la red y posibles intrusiones	El uso indebido del protocolo ICMP puede facilitar ataques de denegación de servicio (DoS) y acceso no autorizado a la red.

Nota. En la tabla se puede observar el impacto de las amenazas sobre la continuidad del negocio.

3.6 Determinación del Riesgo

Esta sección se centra en la determinación del nivel de riesgo asociado a cada amenaza y vulnerabilidad identificada en el Data Center de AirmaxTelecom Soluciones Tecnológicas S.A. a partir del análisis inicial, se combinan las evaluaciones de probabilidad e impacto para calcular el nivel de riesgo y se utiliza una matriz de riesgo para su visualización y priorización. Según las guías y métodos descritos en el Apéndice I de la NIST SP 800-30, estos cálculos aseguran una evaluación coherente y repetible de los riesgos, facilitando la toma de decisiones informadas sobre las medidas de mitigación necesarias.

3.6.1 Integración de las evaluaciones de probabilidad e impacto para calcular el nivel de riesgo.

Para cada amenaza y vulnerabilidad identificada, se calcula el nivel de riesgo combinando las evaluaciones de probabilidad e impacto. La fórmula utilizada, descrita en el Apéndice I de la NIST SP 800-30 es:

Nivel de Riesgo = Probabilidad × Impacto

Esta metodología permite una cuantificación precisa del riesgo al asignar valores específicos a la probabilidad de ocurrencia de una amenaza y vulnerabilidad al impacto que tendría en los activos y operaciones del Data Center. En la tabla 21 Al utilizar esta fórmula, se obtiene un valor numérico que facilita la comparación y priorización de los riesgos, permitiendo focalizar los recursos y esfuerzos en mitigar aquellos riesgos que representan mayores amenazas para la seguridad y operatividad de la organización.

Se asignan puntuaciones de 0 a 10 para la probabilidad y el impacto de cada evento y se utilizan los valores obtenidos en la tabla 12 en donde realizó la categorización de las amenazas y vulnerabilidades a partir del nivel de riesgo inicial.

Tabla 21

Cálculo del Nivel de Riesgo para Amenazas y Vulnerabilidades final

Amenaza	Descripción	Probabilidad (P)	Impacto (I)	Nivel de Riesgo (P x I)	Categoría de Riesgo
A001 - Terremotos	Daños físicos por sismos	6	9	54	Moderado
A002 - Inundaciones	Daños físicos por exposición a inundaciones	6	8	48	Moderado
A003 - Incendios	Daños físicos significativos por fuego	5	8	40	Moderado

A004 - Fallos de hardware (Tier 1)	Fallos en equipos críticos del nivel 1	5	9	45	Moderado
A005 - Evolución de técnicas de cibercriminales	Incremento en sofisticación de ataques cibernéticos	8	9	72	Alto
V001 - Redundancia insuficiente en equipos activos	Insuficiencia de equipos de respaldo	4	6	24	Bajo
V002 - Ausencia de un Data Center espejo	Falta de respaldo operativo y de datos	9	10	90	Alto
V003 - Vulnerabilidad ICMP	Riesgo de explotación del protocolo ICMP	3	5	15	Bajo

Nota. En la tabla se puede observar el cálculo realizado para obtener el nivel de riesgo.

3.6.2 Matriz de Riesgo para los Activos Críticos del Data Center

La matriz de riesgo es una herramienta esencial en la gestión de riesgos, permitiendo visualizar y priorizar los riesgos basados en su probabilidad de ocurrencia y su impacto potencial. Esta matriz es particularmente útil para tomar decisiones estratégicas, determinando qué riesgos

requieren atención inmediata y cuáles pueden ser monitoreados regularmente. En la tabla 22 se presenta la matriz de riesgo utilizada en el análisis, basada en las guías y métodos descritos en el Apéndice I de la NIST SP 800-30.

La utilización de una matriz de riesgo facilita la comunicación y comprensión de los riesgos entre los diferentes niveles de la organización. Al proporcionar una representación visual clara, todos los interesados pueden identificar rápidamente los riesgos críticos y colaborar en la implementación de medidas de mitigación. Además, esta herramienta permite una evaluación continua, adaptándose a los cambios en el entorno y asegurando que la gestión de riesgos sea un proceso dinámico y efectivo.

Tabla 22

Matriz de Riesgo para AirmaxTelecom

Probabilidad	**Impacto**				
	Muy bajo	**Bajo**	**Moderado**	**Alto**	**Muy Alto**
Muy Alta	Alto	Alto	Muy Alto	Muy Alto	Muy Alto
Alta	Moderado	Alto	Alto	Muy Alto	Muy Alto
Moderado	Bajo	Moderado	Alto	Muy Alto	Muy Alto
Baja	Bajo	Bajo	Moderado	Alto	Muy Alto
Muy Baja	Bajo	Bajo	Moderado	Alto	Alto

Zona de riesgo “Baja”: Aceptar el riesgo

Zona de riesgo “Moderada”: Evaluar la posibilidad de asumir riesgo

Zona de riesgo “Alta”: Implementar estrategias de mitigación para reducir el riesgo

Zona de riesgo “Crítica”: Imprescindible reducir el riesgo a través de medidas robustas de mitigación.

Nota: Matriz de Riesgo Adaptado de (Cauja Altamirano, 2024)

Por otra parte, la tabla 23 presenta un análisis detallado de los activos críticos, las amenazas a las que están expuestos, y la evaluación de riesgo final asociada a cada uno. Cada fila de la tabla identifica un activo crítico específico y la amenaza correspondiente. La probabilidad de ocurrencia de cada amenaza se expresa en la columna "Probabilidad (P)", mientras que la columna "Impacto (I)" detalla la gravedad de las consecuencias en caso de que la amenaza se materialice.

El "Nivel de Riesgo" se calcula combinando la probabilidad y el impacto, proporcionando una medida cuantitativa del riesgo total. Finalmente, la columna "Nivel de Riesgo (Categoría)" clasifica el nivel de riesgo en una categoría cualitativa, facilitando la priorización de los riesgos y la toma de decisiones estratégicas. Esta estructura final la cual parte de todo el análisis previo permite a la organización enfocarse en los riesgos más críticos y gestionar eficientemente los recursos para su mitigación.

Tabla 23

Activos críticos con su nivel de riesgo para cada amenaza final

Activo Crítico	Amenaza/ Vulnerabilidad	Probabilidad (P)	Impacto (I)	Nivel de Riesgo (P x I)	Nivel de Riesgo (Categoría)
Enrutadores de Borde	Terremotos (A001)	6	9	54	Moderado
	Inundaciones (A002)	6	8	48	Moderado

	Incendios (A003)	5	8	40	Moderado
	Fallos de hardware (A004)	5	9	45	Moderado
	Evolución de técnicas de cibercriminales (A005)	8	9	72	Alto
	Ausencia de un Data Center espejo (V002)	9	10	90	Alto
	Redundancia insuficiente (V001)	7	9	63	Alto
	ICMP (V003)	7	8	56	Moderado
Conmutadores de Agregación	Terremotos (A001)	6	9	54	Moderado
	Inundaciones (A002)	6	8	48	Moderado
	Incendios (A003)	5	8	40	Moderado
	Fallos de hardware (A004)	5	9	45	Moderado
	Evolución de técnicas de cibercriminales (A005)	8	9	72	Alto
	Ausencia de un Data Center espejo (V002)	9	10	90	Alto
	Redundancia insuficiente (V001)	7	9	63	Alto

	ICMP (V003)	7	8	56	Moderado
Servidores	Terremotos (A001)	6	9	54	Moderado
	Inundaciones (A002)	6	8	48	Moderado
	Incendios (A003)	5	8	40	Moderado
	Fallos de hardware (A004)	5	9	45	Moderado
	Evolución de técnicas de cibercriminales (A005)	8	9	72	Alto
	Ausencia de un Data Center espejo (V002)	9	10	90	Alto
	Redundancia insuficiente (V001)	7	9	63	Alto
Sistemas de Almacenamiento (SAN/NAS)	Terremotos (A001)	6	9	54	Moderado
	Inundaciones (A002)	6	8	48	Moderado
	Incendios (A003)	5	8	40	Moderado
	Fallos de hardware (A004)	5	9	45	Moderado
	Evolución de técnicas de cibercriminales (A005)	8	9	72	Alto
	Ausencia de un Data Center espejo (V002)	9	10	90	Alto

	Redundancia insuficiente (V001)	7	9	63	Alto
Sistemas de Monitorización	Terremotos (A001)	6	9	54	Moderado
	Inundaciones (A002)	6	8	48	Moderado
	Incendios (A003)	5	8	40	Moderado
	Evolución de técnicas de cibercriminales (A005)	8	9	72	Alto
	Redundancia insuficiente (V001)	7	9	63	Alto
	ICMP (V003)	7	8	56	Moderado
Sistemas de Respaldo y Recuperación	Terremotos (A001)	6	9	54	Moderado
	Inundaciones (A002)	6	8	48	Moderado
	Incendios (A003)	5	8	40	Moderado
	Fallos de hardware (A004)	5	9	45	Moderado
	Evolución de técnicas de cibercriminales (A005)	8	9	72	Alto
	Ausencia de un Data Center espejo (V002)	9	10	90	Alto
	Redundancia insuficiente (V001)	7	9	63	Alto

Conexiones de Red Externas	Terremotos (A001)	6	9	54	Moderado
	Inundaciones (A002)	6	8	48	Moderado
	Incendios (A003)	5	8	40	Moderado
	Fallos de hardware (A004)	5	9	45	Moderado
	Evolución de técnicas de cibercriminales (A005)	8	9	72	Alto
	Redundancia insuficiente (V001)	7	9	63	Alto
	ICMP (V003)	7	8	56	Moderado

Nota: En la tabla se puede observar el nivel de riesgo para cada activo críticos junto con cada una de las amenazas dentro del Data Center.

Capítulo 4

Desarrollo del Plan de Seguridad

En el presente capítulo se exponen de manera detallada los resultados obtenidos de la evaluación de riesgos realizada en el Capítulo 3. Este análisis se centró en la aplicación de la metodología NIST SP 800-30 para identificar, evaluar y gestionar los riesgos asociados con la seguridad del Data Center de AirmaxTelecom Soluciones Tecnológicas S.A. La implementación de esta metodología no solo garantiza una evaluación integral y sistemática, sino que también facilita la elaboración de estrategias de mitigación efectivas y adaptadas a las necesidades específicas del Data Center. El objetivo de este capítulo es proporcionar un contexto completo y comprensible sobre los resultados de la evaluación, destacando los activos críticos, las amenazas y vulnerabilidades identificadas, así como las estrategias y planes de mitigación desarrollados para asegurar la protección y resiliencia del Data Center.

4.1 Resumen de la Metodología Aplicada

La metodología NIST SP 800-30 ofrece un marco estructurado y bien definido para la gestión de riesgos de la información, abarcando todas las fases necesarias para una evaluación completa. Esta metodología se divide en varias etapas clave, que incluyen la preparación para la evaluación, la identificación de activos críticos, amenazas y vulnerabilidades, el análisis de probabilidad y la evaluación del impacto, y finalmente, la determinación del nivel de riesgo y la comunicación de los resultados. Cada una de estas fases es crucial para asegurar una comprensión completa y detallada de los riesgos a los que está expuesto el Data Center, y para desarrollar estrategias de mitigación efectivas y adecuadas.

La fase de preparación implica la definición clara del alcance y los objetivos de la evaluación, así como la identificación de los recursos y las partes interesadas involucradas. Esta etapa es fundamental para asegurar que todas las áreas relevantes sean consideradas y que la evaluación se realice de manera sistemática y organizada. La fase de identificación de activos críticos, amenazas y vulnerabilidades permite una comprensión detallada de los elementos esenciales que necesitan protección y de las posibles fuentes de riesgo. El análisis de probabilidad y la evaluación del impacto son pasos críticos para determinar la severidad de las amenazas identificadas, considerando tanto su frecuencia esperada como sus posibles consecuencias. Finalmente, la determinación del nivel de riesgo integra las evaluaciones de probabilidad e impacto para proporcionar una visión clara de los riesgos más críticos, facilitando la priorización de las amenazas y el desarrollo de estrategias de mitigación adecuadas.

4.2 Resultados de la Evaluación de Riesgos

4.2.1 Identificación de Activos Críticos

La identificación de activos críticos es una etapa esencial en la evaluación de riesgos, ya que estos activos representan los elementos fundamentales que necesitan protección para asegurar la operatividad y seguridad del Data Center. En el caso del Data Center de AirmaxTelecom Soluciones Tecnológicas S.A., los activos críticos identificados incluyen una variedad de componentes esenciales que desempeñan roles clave en la infraestructura tecnológica de la empresa.

- **Enrutadores de Borde**: Los enrutadores de borde son dispositivos fundamentales que gestionan todo el tráfico de datos de entrada y salida del Data Center. Estos equipos son responsables de mantener la conectividad continua y estable con los proveedores de

servicios de Internet, asegurando que los datos puedan fluir sin interrupciones hacia y desde el Data Center. Además, implementan políticas de seguridad y filtrado de paquetes para proteger la red contra amenazas externas y optimizar el enrutamiento del tráfico de datos, lo que es crucial para mantener la seguridad y eficiencia operativa.

- **Conmutadores de Agregación**: Los conmutadores de agregación consolidan y distribuyen el tráfico de datos dentro del Data Center. Estos dispositivos conectan múltiples servidores y sistemas de almacenamiento, proporcionando redundancia y aumentando la fiabilidad de la red. Su capacidad para manejar grandes volúmenes de tráfico y permitir la escalabilidad es esencial para el crecimiento y la adaptación de la red a las demandas cambiantes de los servicios.
- **Servidores**: Los servidores alojan aplicaciones y datos críticos para las operaciones del negocio. Estos equipos aseguran la disponibilidad y redundancia de la información, lo que es vital para la ejecución de aplicaciones esenciales y la recuperación rápida de datos en caso de fallos. Los servidores son responsables de procesar y almacenar datos, y son esenciales para la continuidad de las operaciones del Data Center.
- **Sistemas de Almacenamiento**: Los sistemas de almacenamiento proporcionan la capacidad necesaria para gestionar grandes volúmenes de información de manera segura y eficiente. Estos dispositivos son cruciales para asegurar que los datos críticos estén disponibles y respaldados, permitiendo la recuperación de datos en caso de desastre.
- **Sistemas de Monitorización**: El software y hardware utilizados para supervisar y gestionar el rendimiento y el estado del Data Center son cruciales para la detección temprana de problemas y la gestión eficiente de los recursos. Estos sistemas permiten una

gestión proactiva de la infraestructura, facilitando la identificación y resolución rápida de incidencias antes de que puedan afectar las operaciones del Data Center.

- **Conexiones de Red Externas**: Son enlaces de comunicación con proveedores de servicios de Internet y otras redes externas. La conectividad continua y eficiente es esencial para mantener las operaciones del Data Center funcionando correctamente, especialmente en situaciones de alta demanda o de fallo de otros enlaces internos.
- **Sistemas de Respaldo y Recuperación**: Soluciones diseñadas para garantizar que los datos puedan ser restaurados en caso de pérdida, corrupción o desastres, asegurando la continuidad operativa. Estos sistemas proporcionan la capacidad de recuperación ante desastres, lo cual es crítico para la protección de los datos de la empresa.

4.2.2 Amenazas y Vulnerabilidades Identificadas

La identificación de amenazas y vulnerabilidades es un componente crucial del proceso de evaluación de riesgos. Las amenazas y vulnerabilidades clave identificadas para el Data Center de AirmaxTelecom Soluciones Tecnológicas S.A. se pueden clasificar en tres categorías principales: amenazas externas, amenazas internas y vulnerabilidades.

- Amenazas Externas: Las amenazas externas incluyen ciberataques, desastres naturales y las intrusiones físicas. Los ciberataques, como el malware, phishing, y los ataques de denegación de servicio (DoS), representan un riesgo significativo para la confidencialidad, integridad y disponibilidad de la información crítica almacenada en el Data Center. Los desastres naturales, como terremotos, inundaciones e incendios, pueden causar daños físicos graves a la infraestructura del Data Center, afectando su operatividad. Las intrusiones físicas, por otro lado, pueden comprometer la seguridad de los activos críticos si no se implementan medidas de seguridad adecuadas.

- Amenazas Internas: Las amenazas internas incluyen errores humanos, fallos de equipo y problemas de mantenimiento. Los errores humanos, como configuraciones incorrectas, negligencia o falta de capacitación, pueden introducir vulnerabilidades en el sistema que pueden ser explotadas por atacantes externos o causar interrupciones operativas. Los fallos de equipo, como el mal funcionamiento de hardware o software, pueden interrumpir las operaciones del Data Center y poner en riesgo la disponibilidad de los datos. Los problemas de mantenimiento, como el retraso en la actualización de sistemas o la falta de pruebas regulares de los equipos de respaldo, pueden aumentar la vulnerabilidad del Data Center a las amenazas.
- Vulnerabilidades: Las vulnerabilidades identificadas incluyen la falta de políticas de seguridad robustas, sistemas de energía no redundantes e insuficiente capacitación del personal. La ausencia de políticas de seguridad claras y bien definidas puede llevar a una implementación inconsistente de medidas de seguridad, aumentando el riesgo de incidentes de seguridad. Los sistemas de energía no redundantes pueden fallar en proporcionar el soporte necesario durante cortes de energía, lo que puede resultar en interrupciones operativas y pérdida de datos. La insuficiente capacitación del personal en prácticas de seguridad puede aumentar la probabilidad de errores humanos y la vulnerabilidad del Data Center a las amenazas internas y externas.

4.2.3 Análisis de Probabilidad y Evaluación del Impacto

El análisis de probabilidad y la evaluación del impacto son pasos esenciales para determinar la severidad de las amenazas identificadas. Estos pasos permiten entender mejor las posibles consecuencias de las amenazas y desarrollar estrategias de mitigación efectivas.

- Probabilidad de Ocurrencia: La probabilidad de ocurrencia de las amenazas se evalúa en función de su frecuencia esperada. Las amenazas con mayor probabilidad incluyen ciberataques y fallos de energía. Los ciberataques son cada vez más frecuentes y sofisticados, representando una amenaza constante para la seguridad del Data Center. Los fallos de energía también son comunes, especialmente en regiones propensas a interrupciones eléctricas, y pueden afectar gravemente la operatividad del Data Center si no se cuenta con sistemas de respaldo adecuados.
- Evaluación del Impacto: La evaluación del impacto estima las consecuencias potenciales de las amenazas para las operaciones del Data Center. El impacto potencial de los ciberataques incluye la interrupción de las operaciones, pérdida de datos, daños a la reputación y costos financieros significativos. Los fallos de energía pueden resultar en la pérdida de datos, daños a los equipos y la interrupción de los servicios críticos. La evaluación del impacto ayuda a priorizar las amenazas y a desarrollar estrategias de mitigación que se centren en las amenazas más severas y con mayor probabilidad de ocurrencia.

4.2.4 Determinación del Riesgo

La determinación del riesgo implica la integración de las evaluaciones de probabilidad e impacto para calcular el nivel de riesgo asociado con cada amenaza identificada. Esta integración se realiza a través del desarrollo de una matriz de riesgo, que clasifica las amenazas en niveles de riesgo bajo, medio y alto.

La matriz de riesgo proporciona una visión clara de los niveles de riesgo asociados con cada amenaza, facilitando la toma de decisiones informadas para la gestión de riesgos. Las amenazas con alto nivel de riesgo requieren una atención prioritaria y la implementación de

medidas de mitigación efectivas. La matriz de riesgo se basa en una combinación de la probabilidad de ocurrencia y el impacto potencial de las amenazas, permitiendo una evaluación completa y precisa de los riesgos.

4.3 Desarrollo de Estrategias de Mitigación

Las estrategias de mitigación se desarrollan para reducir los riesgos identificados a niveles aceptables y manejables. Estas estrategias se enfocan en las amenazas y vulnerabilidades más críticas y se priorizan en función de su eficacia y costo.

- Ciberseguridad: Se proponen medidas como la implementación de firewalls avanzados, sistemas de detección de intrusos (IDS) y capacitación en ciberseguridad para el personal. La implementación de firewalls avanzados ayuda a proteger la red contra accesos no autorizados y ataques cibernéticos, mientras que los sistemas de detección de intrusos permiten identificar y responder rápidamente a actividades sospechosas. La capacitación en ciberseguridad para el personal es esencial para asegurar que todos los empleados estén al tanto de las mejores prácticas y procedimientos de seguridad, reduciendo el riesgo de errores humanos y aumentando la resiliencia del Data Center frente a ciberataques.

Dentro del ámbito de ciberseguridad, una de las estrategias de mitigación más importantes ha sido la implementación de herramientas de escaneo de vulnerabilidades. Estas herramientas juegan un papel crucial en la identificación y gestión de amenazas potenciales en la red y los sistemas del Data Center. A continuación, se describen las herramientas específicas implementadas:

- Nessus: La implementación de Nessus ha permitido a la empresa identificar vulnerabilidades críticas en su infraestructura de TI de manera eficiente. Nessus realiza escaneos exhaustivos y proporciona informes detallados sobre las vulnerabilidades

encontradas. Esto permite a los administradores de sistemas priorizar y abordar los riesgos de seguridad de forma proactiva, asegurando así la integridad y seguridad de los datos y sistemas.

- OpenVAS: OpenVAS ha sido implementado como una herramienta complementaria a Nessus, proporcionando capacidades avanzadas de escaneo de vulnerabilidades. Como una solución de código abierto, OpenVAS ofrece flexibilidad y personalización en los análisis de seguridad. Su integración en la política de seguridad del Data Center garantiza un monitoreo continuo y la capacidad de respuesta rápida ante cualquier amenaza identificada.
- Resiliencia de Energía: La instalación de sistemas de UPS y generadores de respaldo redundantes asegura la continuidad operativa durante cortes eléctricos, protegiendo los equipos y datos críticos. Los sistemas de UPS proporcionan energía temporal durante interrupciones breves, mientras que los generadores de respaldo pueden mantener el funcionamiento del Data Center durante cortes prolongados. Estas medidas son esenciales para garantizar que el Data Center pueda seguir operando sin interrupciones, minimizando el impacto de los fallos de energía en las operaciones.
- Seguridad Física: La mejora de los controles de acceso y sistemas de vigilancia protege el Data Center contra intrusiones físicas y garantiza la integridad de los activos. Los controles de acceso aseguran que solo el personal autorizado pueda acceder a áreas sensibles del Data Center, mientras que los sistemas de vigilancia permiten monitorear continuamente el entorno y detectar cualquier actividad sospechosa. Estas medidas son cruciales para proteger los activos físicos y asegurar un entorno seguro para las operaciones del Data Center.

4.4 Plan de Implementación de Medidas de Seguridad

El plan de implementación de medidas de seguridad detalla el cronograma, la asignación de recursos y las responsabilidades para la implementación de las estrategias de mitigación desarrolladas. Este plan es esencial para asegurar que las medidas de seguridad se implementen de manera efectiva y oportuna, minimizando el riesgo de incidentes de seguridad y asegurando la continuidad operativa del Data Center.

- Cronograma: Se establece un cronograma detallado para la implementación de las medidas de seguridad, con fases claramente definidas y plazos específicos. Este cronograma asegura que todas las actividades de implementación se realicen de manera organizada y dentro de los plazos establecidos, minimizando las interrupciones operativas y asegurando una transición suave hacia un entorno más seguro.
- Asignación de Recursos: Se identifican los recursos necesarios para la implementación de las medidas de seguridad, incluyendo personal, equipos y presupuesto. La asignación adecuada de recursos es crucial para asegurar que todas las medidas de seguridad se implementen de manera efectiva y que los objetivos de seguridad se alcancen dentro del plazo y el presupuesto establecidos.
- Planes de Monitoreo y Revisión Periódica: Se desarrollan planes para el monitoreo continuo y la revisión periódica de las medidas de seguridad implementadas, asegurando su eficacia continua y la adaptación a nuevas amenazas. Estos planes incluyen la realización de auditorías de seguridad regulares, pruebas de penetración y la actualización continua de las políticas y procedimientos de seguridad para asegurar que el Data Center se mantenga protegido contra las amenazas emergentes.

4.5 Plan de Seguridad para la Gestión de Riesgos

En este plan se define la estructura y los procedimientos necesarios para la gestión integral de riesgos en el Data Center de AIRMAXTELECOM Soluciones Tecnológicas S.A. Este plan incluye la identificación de activos críticos, la evaluación de amenazas y vulnerabilidades, y la implementación de controles específicos para mitigar los riesgos detectados, en conformidad con la metodología NIST SP 800-30. Las acciones descritas en este documento están diseñadas para garantizar la continuidad operativa, la protección de los datos críticos y el cumplimiento de los objetivos de seguridad establecidos por la empresa. Además, se prioriza la recuperación rápida de los sistemas afectados y la minimización de la pérdida de datos, alineándose con las mejores prácticas de la industria en gestión de riesgos.

4.6 Manual de Políticas de Seguridad

Este manual establece las políticas y directrices necesarias para garantizar la protección de los activos de información en AIRMAXTELECOM Soluciones Tecnológicas S.A., con un enfoque específico en la seguridad del Data Center. En él se detallan los procesos y procedimientos relacionados con el control de acceso, la protección de datos sensibles y la gestión de incidentes de seguridad, siguiendo los lineamientos de la metodología NIST SP 800-30. Además, se emplean templates de la organización SANS para estructurar y documentar las políticas, asegurando que estas sean prácticas, claras y fáciles de implementar. Este manual también incluye políticas orientadas a la prevención de fugas de información y a la gestión de la continuidad operativa, garantizando que las medidas adoptadas sean consistentes con los objetivos estratégicos de la empresa. La estructura del documento busca minimizar los riesgos asociados a amenazas internas y externas, proporcionando un marco sólido para la seguridad integral del Data Center.

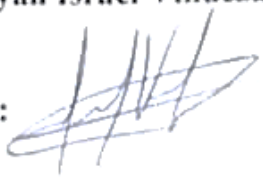
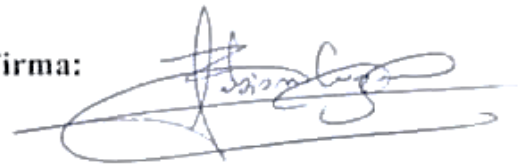
AIRMAXTELECOM

SOLUCIONES TECNOLÓGICAS S.A.

PLAN DE SEGURIDAD PARA LA GESTIÓN DE RIESGOS DEL DATA CENTER

Versión 1.0

Plan de Seguridad para la Gestión de Riesgos para el Data Center de AIRMAXTELECOM

Versión	1.0
Elaborado por:	Sr. Bryan Israel Vinueza Bedoya Firma:  MSc. Fabián Cuzme Rodríguez Firma: 
Fecha de elaboración:	05/11/2024
Revisado por:	Ing. Andrés Benavides Firma: 
Fecha de revisión:	14/01/2025
Aprobado por:	
Fecha de aprobación:	

Contenido

I. Introducción

El Plan de Seguridad para la Gestión de Riesgos del Data Center de AIRMAXTELECOM tiene como propósito principal garantizar la continuidad operativa y la protección integral de los activos críticos de la organización frente a un entorno de amenazas crecientes y complejas. Este documento es un marco estratégico que, basado en la metodología NIST SP 800-30, identifica, evalúa y mitiga riesgos potenciales tanto en el ámbito físico como lógico. La seguridad de la información, el cumplimiento normativo, y la resiliencia ante incidentes son elementos clave que sustentan este plan, el cual busca no solo proteger la infraestructura tecnológica, sino también asegurar la integridad, confidencialidad y disponibilidad de los datos sensibles. El plan incluye políticas y procedimientos diseñados para anticipar, prevenir y responder ante incidentes de seguridad, alineándose con los estándares internacionales y promoviendo una cultura de seguridad en toda la organización.

Objetivo del Plan: El objetivo de este Plan de Gestión de Riesgos es establecer medidas efectivas para gestionar y mitigar los riesgos de seguridad de la información en el Data Center de AIRMAXTELECOM, siguiendo la metodología NIST SP 800-30. Este plan está diseñado para identificar y evaluar riesgos potenciales, implementar controles y procedimientos adecuados, y asegurar la continuidad de las operaciones críticas del data center.

Además, este plan no solo se enfoca en la protección de los activos críticos del Data Center de AIRMAXTELECOM, sino que también está alineado con la estrategia general de la empresa, garantizando la resiliencia operativa, mitigando los riesgos reputacionales y manteniendo la confianza de clientes y socios. La adecuada gestión de los riesgos de seguridad de la información

es esencial para el crecimiento sostenible de AIRMAXTELECOM en un entorno digital cada vez más complejo.

Alcance del Plan: Este plan abarca la identificación de activos críticos, evaluación de riesgos, estrategias de mitigación, plan de implementación, respuesta a incidentes, programa de formación y concientización, monitoreo y revisión, y mejora continua. Se enfocará en todos los componentes del data center, incluyendo hardware, software, datos e infraestructura física, con una visión integral que considera tanto las amenazas internas como externas.

Importancia del Plan: Garantizar la disponibilidad, integridad y confidencialidad de los datos críticos de la empresa es fundamental para el éxito continuo de AIRMAXTELECOM. Un plan de seguridad bien estructurado no solo protege contra posibles incidentes de seguridad, sino que también minimiza el impacto financiero y reputacional en caso de una brecha. La implementación de este plan fortalece la confianza de los clientes y socios, demostrando el compromiso de la empresa con la seguridad de la información.

Metodología Utilizada (NIST SP 800-30): Se utiliza la metodología NIST SP 800-30 para realizar un análisis exhaustivo de riesgos y establecer controles adecuados. Esta metodología proporciona un marco estructurado para la identificación, evaluación y gestión de riesgos, alineándose con las mejores prácticas internacionales y asegurando un enfoque sistemático y documentado.

La efectividad de las medidas implementadas bajo la metodología NIST SP 800-30 será monitoreada a través de Indicadores de Rendimiento Clave (KPIs), tales como el Tiempo Medio para Detectar Incidentes (MTTD) y el Tiempo Medio para Responder a Incidentes (MTTR). Esto

permitirá a la empresa ajustar las estrategias de mitigación según sea necesario para garantizar un enfoque proactivo y adaptable.

II. Glosario

Definiciones Clave:

- **Activo:** Recursos, sistemas, y componentes vitales para la operación del Data Center, incluyendo hardware, software, datos y la infraestructura física.
- **Amenaza:** Cualquier circunstancia o evento que puede causar daño a los activos del data center, desde ataques cibernéticos hasta desastres naturales.
- **Vulnerabilidad:** Debilidad que puede ser explotada por una amenaza para causar daño o pérdida.
- **Control:** Medidas implementadas para gestionar riesgos, incluyendo controles preventivos, detectivos y correctivos.
- **Amenaza Interna:** Individuo o grupo dentro de la organización que, de manera intencional o accidental, pone en peligro los activos de la empresa. Las amenazas internas pueden incluir errores humanos, negligencia o actos maliciosos de empleados.
- **Incidente de Seguridad:** Evento o conjunto de eventos que comprometen la integridad, confidencialidad o disponibilidad de la información o los sistemas. Puede incluir violaciones de seguridad, fallos en el acceso, malware o ciberataques.
- **Plan de Recuperación ante Desastres (DRP):** Estrategia y conjunto de procedimientos que aseguran la recuperación de los sistemas críticos tras un evento catastrófico, como un desastre natural o un ataque cibernético.

- **Plan de Continuidad del Negocio (BCP):** Conjunto de estrategias y procedimientos que permiten a una organización continuar operando durante y después de una interrupción significativa, garantizando la mínima pérdida de operaciones.
- **Indicadores de Rendimiento Clave (KPIs):** Métricas utilizadas para medir la efectividad de los controles de seguridad implementados. Algunos ejemplos incluyen el Tiempo Medio para Detectar Incidentes (MTTD) y el Tiempo Medio para Responder a Incidentes (MTTR).
- **Riesgo Residual:** El nivel de riesgo que permanece después de que se hayan implementado las medidas de mitigación. Es importante monitorearlo y gestionarlo de manera continua.
- **Riesgo:** Es la posibilidad de que una amenaza aproveche una vulnerabilidad para causar un impacto negativo sobre los activos del Data Center. El riesgo es el producto de la probabilidad de que ocurra un evento y el impacto que tendría en la organización.
- **Probabilidad:** La estimación de la posibilidad de que ocurra un evento o amenaza que pueda afectar los activos del Data Center. La probabilidad es uno de los factores clave que se consideran en la evaluación de riesgos.
- **Impacto:** La consecuencia o daño potencial que un evento puede causar a los activos críticos del Data Center, afectando su confidencialidad, integridad o disponibilidad. Se utiliza junto con la probabilidad para evaluar el nivel de riesgo.
- **Evaluación de Riesgos:** El proceso de identificar, analizar y evaluar amenazas y vulnerabilidades que pueden afectar los activos de la organización, determinando la probabilidad y el impacto de su ocurrencia para priorizar los riesgos.

- **Mitigación de Riesgos:** Acciones o controles implementados para reducir la probabilidad de ocurrencia o el impacto de un riesgo sobre los activos de la organización. Estas acciones pueden ser preventivas, detectivas o correctivas.
- **Control de Acceso:** Proceso mediante el cual se regulan los permisos y la autenticación de usuarios que acceden a los sistemas, redes y datos del Data Center. Puede incluir mecanismos como la autenticación multifactor, la asignación de roles y la gestión de privilegios.
- **Ciberseguridad:** Conjunto de prácticas, controles y tecnologías implementadas para proteger los sistemas de información y redes de ataques cibernéticos, acceso no autorizado, corrupción de datos o interrupciones en la continuidad operativa.
- **Resiliencia Operativa:** La capacidad del Data Center para continuar operando bajo condiciones adversas o tras un evento disruptivo, minimizando la pérdida de datos o servicios críticos.
- **Plan de Respuesta a Incidentes (IRP):** Conjunto de procedimientos diseñados para identificar, contener, erradicar y recuperar los sistemas tras un incidente de seguridad, minimizando el impacto en la operación.
- **Auditoría de Seguridad:** Proceso de revisión y evaluación de los controles de seguridad implementados en el Data Center para garantizar su efectividad y el cumplimiento de las políticas de seguridad establecidas.
- **RTO (Recovery Time Objective):** Tiempo máximo aceptable para restaurar un sistema, aplicación o proceso después de una interrupción, minimizando el impacto en las operaciones.

- **RPO (Recovery Point Objective):** Punto máximo en el tiempo hasta el que los datos pueden ser recuperados tras un incidente, indicando la cantidad de datos que se pueden perder sin afectar significativamente al negocio.
- **Monitoreo Continuo:** Estrategia de vigilancia constante de los sistemas y redes para detectar anomalías, fallos o amenazas en tiempo real, permitiendo una respuesta rápida ante posibles incidentes de seguridad.

Principios de Seguridad de la Información:

- **Confidencialidad:** Garantizar que la información sea accesible solo para aquellos autorizados, protegiéndola contra accesos no autorizados y divulgación indebida.
- **Integridad:** Asegurar que la información sea precisa, completa y no haya sido alterada de manera indebida, protegiendo la exactitud y consistencia de los datos.
- **Disponibilidad:** Asegurar que la información y los recursos estén disponibles para los usuarios autorizados cuando los necesiten, garantizando un acceso confiable y oportuno.

Descripción de la Metodología NIST SP 800-30: La metodología NIST SP 800-30 incluye fases de preparación, análisis de riesgos, y gestión de riesgos conforme a estándares internacionales. Esta metodología proporciona un marco para la evaluación sistemática de riesgos, desde la identificación de activos y amenazas hasta la implementación de controles y el monitoreo continuo de la efectividad de las medidas de seguridad.

III. Levantamiento de Políticas de Seguridad

Proceso para el Levantamiento de Políticas de Seguridad:

1. **Formación del Equipo de Trabajo:** Establecer un equipo multidisciplinario que será responsable de definir y revisar las políticas de seguridad. Este equipo debe incluir personal de TI, seguridad, operaciones y representantes de la alta dirección.
2. **Identificación de Requisitos:** Identificar los requisitos legales, normativos y corporativos que deben cumplirse. Esto incluye la revisión de normativas nacionales e internacionales, así como las políticas internas de la empresa.
3. **Análisis de Riesgos:** Realizar un análisis de riesgos exhaustivo para identificar las amenazas y vulnerabilidades que deben abordarse en las políticas de seguridad.
4. **Desarrollo de Políticas:** Redactar las políticas de seguridad basadas en los requisitos identificados y los resultados del análisis de riesgos. Las políticas deben cubrir aspectos como la gestión de accesos, protección de datos, gestión de incidentes y continuidad del negocio.
5. **Revisión y Aprobación:** Someter las políticas a una revisión detallada por parte del equipo de trabajo y obtener la aprobación de la alta dirección.
6. **Implementación y Difusión:** Implementar las políticas de seguridad y asegurar su difusión a todo el personal relevante. Esto incluye la capacitación y concienciación de los empleados sobre las nuevas políticas.
7. **Monitoreo y Actualización:** Establecer un proceso de monitoreo continuo y revisión periódica para asegurar que las políticas de seguridad se mantengan actualizadas y efectivas.

IV. Políticas de Seguridad Específicas

1. **Política de Gestión de Accesos**

- Definir los niveles de acceso y permisos para el personal basado en sus roles y responsabilidades.
- Implementar mecanismos de autenticación robustos, como autenticación multifactor.
- Realizar revisiones periódicas de los accesos para asegurar que sean apropiados y necesarios.

2. **Política de Protección de Datos**
    - Establecer directrices para la clasificación y protección de datos sensibles.
    - Implementar medidas de encriptación para proteger los datos en tránsito y en reposo.
    - Asegurar que los datos se almacenen y manejen de acuerdo con las normativas de protección de datos aplicables.
3. **Política de Gestión de Incidentes**
    - Definir un proceso claro para la identificación, reporte y respuesta a incidentes de seguridad.
    - Establecer un equipo de respuesta a incidentes con roles y responsabilidades definidos.
    - Implementar un sistema de registro y análisis de incidentes para mejorar la respuesta y prevención futura.
4. **Política de Continuidad del Negocio**
    - Desarrollar planes de continuidad del negocio que aseguren la operatividad del Data Center en caso de desastres.

- Implementar pruebas periódicas de los planes de continuidad para asegurar su efectividad.
- Establecer procedimientos de recuperación ante desastres y asegurar la disponibilidad de los recursos necesarios.

V. Identificación de Activos Críticos del Data Center

La identificación de los activos críticos es esencial para garantizar la seguridad y operatividad del Data Center. Los activos críticos representan los elementos fundamentales para el funcionamiento del Data Center y deben ser protegidos de manera efectiva frente a amenazas y riesgos. La tabla 1 describe los activos críticos de AirmaxTelecom Soluciones Tecnológicas S.A., según su rol y relevancia dentro de la infraestructura tecnológica del Data Center.

Tabla 1
Activos Críticos Data Center AirmaxTelecom

Activo Crítico	Descripción
Enrutadores de Borde	Dispositivos fundamentales que gestionan el tráfico de datos de entrada y salida del Data Center, asegurando conectividad externa e interna. Implementan políticas de seguridad y optimizan el enrutamiento del tráfico de datos.
Conmutadores de Agregación	Dispositivos que consolidan y distribuyen el tráfico de datos dentro del Data Center. Proveen redundancia y fiabilidad a la red, permitiendo la escalabilidad de la infraestructura.
Servidores	Equipos que alojan aplicaciones y datos críticos para las operaciones del negocio. Son esenciales para procesar y almacenar información utilizada en tareas empresariales clave.

Sistemas de Almacenamiento	Sistemas que gestionan grandes volúmenes de datos, esenciales para el acceso y gestión eficiente de la información dentro del Data Center. Garantizan la disponibilidad de los datos.
Sistemas de Monitorización	Software y hardware que supervisan el estado y rendimiento de los activos tecnológicos dentro del Data Center. Permiten la detección temprana de problemas y la gestión proactiva de la infraestructura.
Conexiones de Red Externas	Enlaces de comunicación con proveedores de servicios de Internet y otras redes. Garantizan la conectividad externa del Data Center, permitiendo el acceso a los servicios desde cualquier parte.
Sistemas de Respaldo y Recuperación	Soluciones que aseguran la restauración rápida de los datos en caso de pérdida, corrupción o desastres. Garantizan la continuidad del negocio y minimizan el impacto de incidentes.

Categorización de los Datos

La categorización de los datos es esencial para garantizar que la información sea gestionada y protegida en función de su nivel de sensibilidad y criticidad. Esta clasificación asegura que los controles de seguridad aplicados sean proporcionales a la importancia de los datos dentro de las operaciones del Data Center.

- **Datos Críticos:** Estos datos son vitales para el funcionamiento de la empresa, y su pérdida o alteración podría paralizar las operaciones o causar un impacto severo en la continuidad del negocio. Requieren los niveles más altos de protección y controles de seguridad.
- **Datos Importantes:** Estos datos son necesarios para las operaciones diarias, pero su pérdida o interrupción, aunque impactante, no paralizaría completamente las operaciones

del negocio. Sin embargo, su disponibilidad y funcionalidad son esenciales para mantener la eficiencia de las operaciones.

- **Datos de Menor Importancia:** Estos datos, aunque importantes para ciertas funciones, no representan una amenaza significativa para la operación general si se ven comprometidos o pierden disponibilidad. Sin embargo, aún deben gestionarse de acuerdo con políticas de seguridad de nivel básico.

VI. Evaluación de Riesgos

Identificación de Riesgos:

Para asegurar una evaluación integral y detallada de los riesgos en el Data Center de AIRMAXTELECOM, se han identificado y analizado tanto amenazas como vulnerabilidades que podrían afectar a los activos críticos. Basándonos en la información provista, las tabla 2 resume las amenazas y vulnerabilidades percibidas en la evaluación de riesgos junto con su impacto potencial.

Tabla 2
Amenazas y Vulnerabilidades en términos de impacto potencial

ID	Amenaza	Impacto Potencial	Justificación
A001	**Incendios**	Daño físico a la infraestructura	Los incendios pueden destruir o dañar físicamente el Data Center, afectando la infraestructura crítica y la continuidad operativa de los servicios.

A002	**Terremotos**	Daño físico a la infraestructura	Los terremotos pueden generar daños estructurales severos que comprometen la operatividad de los equipos y sistemas clave del Data Center.
A003	**Inundaciones**	Daño físico a la infraestructura	Las inundaciones pueden provocar daños significativos en los sistemas eléctricos y de TI, afectando seriamente la operatividad del Data Center.
A004	**Fallos de hardware (Tier 1)**	Interrupción del servicio	Un fallo en equipos críticos como servidores y enrutadores podría detener operaciones esenciales hasta su reemplazo o reparación.
A005	**Evolución de técnicas de cibercriminales**	Compromiso de la seguridad	Las técnicas avanzadas de cibercrimen pueden vulnerar las defensas actuales, comprometiendo la confidencialidad, integridad y disponibilidad de datos.
V001	**Redundancia insuficiente en equipos**	Fallos en la red	La falta de redundancia en los equipos puede provocar fallos de conectividad, afectando la disponibilidad de servicios clave.
V002	**Ausencia de un data center espejo**	Pérdida de datos y servicio	Sin un centro de datos de respaldo, una pérdida o fallo mayor podría ser

			irreparable, afectando la continuidad operativa.
V003	**ICMP**	Fallos en la red e intrusiones	El mal uso del protocolo ICMP puede permitir ataques de denegación de servicio (DoS) o accesos no autorizados a la red, comprometiendo su seguridad.

Nota. En la tabla se puede observar las amenazas y vulnerabilidades percibidas en términos del impacto potencial al Datacenter.

Además, la tabla 3 presenta una asociación clara entre los activos críticos del Data Center de AIRMAXTELECOM y las principales amenazas y vulnerabilidades que pueden afectar su operación. Esta relación es fundamental para priorizar las medidas de mitigación, ya que permite identificar qué activos están más expuestos a riesgos específicos y cuál es el impacto potencial de dichos riesgos. Al comprender la naturaleza de cada amenaza y vulnerabilidad, es posible implementar controles y estrategias de mitigación que aseguren la protección efectiva de los recursos más valiosos.

Tabla 3

Asociación de Activos críticos con amenazas y vulnerabilidades

Activo Crítico	**Descripción**	**Amenazas**	**Vulnerabilidades**	**Impacto Potencial**
Enrutadores de Borde	Dispositivos que gestionan	Terremotos (A001),	Redundancia insuficiente (V001),	Daño físico, interrupción

	el tráfico de datos de entrada y salida del Data Center.	Inundaciones (A002), Incendios (A003), Fallos de hardware (A004), Evolución de ciberataques (A005)	ICMP (V003), Ausencia de Data Center Espejo (V002)	del servicio, compromiso de la seguridad.
Conmutadores de Agregación	Dispositivos que consolidan y distribuyen el tráfico de datos dentro del Data Center.	Terremotos (A001), Inundaciones (A002), Incendios (A003), Fallos de hardware (A004), Evolución de ciberataques (A005)	Redundancia insuficiente (V001), ICMP (V003), Ausencia de Data Center Espejo (V002)	Daño físico, interrupción del servicio, compromiso de la seguridad.
Servidores	Equipos que alojan aplicaciones y	Terremotos (A001), Inundaciones	Redundancia insuficiente (V001), Ausencia de Data	Interrupción del servicio, pérdida de

	datos críticos para las operaciones del negocio.	(A002), Incendios (A003), Fallos de hardware (A004), Evolución de ciberataques (A005)	Center Espejo (V002)	datos, exposición de información.
Sistemas de Almacenamiento (SAN/NAS)	Dispositivos y sistemas que almacenan grandes cantidades de datos.	Terremotos (A001), Inundaciones (A002), Incendios (A003), Fallos de hardware (A004), Evolución de ciberataques (A005)	Redundancia insuficiente (V001), Ausencia de Data Center Espejo (V002)	Pérdida de datos, interrupción del servicio.
Sistemas de Monitorización	Software y hardware utilizados para supervisar el	Terremotos (A001), Inundaciones (A002),	Redundancia insuficiente (V001), ICMP (V003)	Compromiso de la seguridad, pérdida de

	rendimiento y el estado del Data Center.	Incendios (A003), Evolución de ciberataques (A005)		visibilidad operativa.
Sistemas de Respaldo y Recuperación	Aseguran que los datos puedan ser restaurados en caso de pérdida o corrupción.	Terremotos (A001), Inundaciones (A002), Incendios (A003), Fallos de hardware (A004), Evolución de ciberataques (A005)	Redundancia insuficiente (V001), Ausencia de Data Center Espejo (V002)	Pérdida de datos, interrupción del servicio.
Conexiones de Red Externas	Enlaces de comunicación con proveedores de servicios de Internet y otras redes.	Terremotos (A001), Inundaciones (A002), Incendios (A003), Fallos de hardware	Redundancia insuficiente (V001), ICMP (V003)	Interrupción del servicio, compromiso de la seguridad.

	(A004), Evolución de ciberataques (A005)

Nota. En la tabla se puede observar la asociación de cada activo crítico del Datacenter junto a la vulnerabilidad que lo puede afectar.

Análisis de Riesgos:

El análisis de riesgos implica evaluar la probabilidad y el impacto de cada amenaza y vulnerabilidad identificada. Esto ayuda a priorizar los riesgos y a asignar recursos de manera efectiva para su mitigación. La tabla 4 presenta la matriz de riesgo utilizada en el análisis, basada en las guías y métodos descritos en el Apéndice I de la NIST SP 800-30.

Tabla 4

Matriz de Riesgo para AirmaxTelecom

Probabilidad		**Impacto**				
		Muy bajo	**Bajo**	**Moderado**	**Alto**	**Muy Alto**
Muy Alta		Alto	Alto	Muy Alto	Muy Alto	Muy Alto
Alta		Moderado	Alto	Alto	Muy Alto	Muy Alto
Moderado		Bajo	Moderado	Alto	Muy Alto	Muy Alto
Baja		Bajo	Bajo	Moderado	Alto	Muy Alto

Muy Baja		Bajo	Bajo	Moderado	Alto	Alto

Zona de riesgo “Baja”: Aceptar el riesgo

Zona de riesgo “Moderada”: Evaluar posibilidad de asumir riesgo

Zona de riesgo “Alta”: Implementar estrategias de mitigación para reducir el riesgo

Zona de riesgo “Crítica”: Imprescindible reducir el riesgo a través de medidas robustas de mitigación.

Nota. En la tabla se puede observar la matriz de riesgo establecida para AirmaxTelecom.

Evaluación de Riesgos:

Para entender mejor la evaluación de riesgos realizada, se presenta a continuación una tabla que resume la matriz de riesgo para los activos críticos del Data Center de AIRMAXTELECOM. Primero se define como se va a categorizar el nivel de riesgo en la tabla 5 y posterior a esto se realiza una matriz de riesgo para cada activo crítico.

Tabla 5

Escala de medición del nivel de riesgo de los activos y vulnerabilidades de AirmaxTelecom

Escala Medición Nivel de Riesgo		
Cualitativo	**Cuantitativo**	**Descripción**
Muy alto	96-100	La vulnerabilidad o amenaza está expuesta y es explotable, y su explotación podría resultar en impactos severos. No se implementa ni planifica el control de seguridad pertinente u otra

		remediación; o no se puede identificar ninguna medida de seguridad para remediar la vulnerabilidad.
Alto	80-95	La vulnerabilidad o amenaza es de alta preocupación, con base en la exposición de la vulnerabilidad y facilidad de explotación y/o en la severidad de los impactos que podrían resultar de su explotación. El control de seguridad relevante u otra remediación está planificada pero no implementada; los controles de compensación están en su lugar y son al menos mínimamente efectivos.
Moderado	21-79	La vulnerabilidad o amenaza es de preocupación moderada, con base en la exposición de la vulnerabilidad y facilidad de explotación y/o en la severidad de los impactos que podrían resultar de su explotación. El control de seguridad relevante u otra remediación se implementa parcialmente y es algo efectivo.
Bajo	5-20	La vulnerabilidad o amenaza es una preocupación menor, pero se podría mejorar la efectividad de la remediación. El control de seguridad relevante u otra remediación está completamente implementado y es algo efectivo.
Muy bajo	0-4	La vulnerabilidad o amenaza no es motivo de preocupación. El control de seguridad relevante u otra remediación se implementa, evalúa y es efectivo en su totalidad.

Cada riesgo identificado se evalúa según su **probabilidad** de ocurrencia y su **impacto** en los activos críticos. La tabla 6 presenta una **matriz de riesgo** que clasifica estos factores en una

escala de 1 a 10, donde 1 representa una probabilidad o impacto bajo, y 10 representa uno muy alto. Al realizar la multiplicación entre ambos factores se obtiene el nivel de riesgo para cada uno de los activos críticos.

Tabla 6

Matriz de Riesgo para Activos Críticos con Nivel de Riesgo para Cada Amenaza

Activo Crítico	Amenaza/ Vulnerabilidad	Probabilidad (P)	Impacto (I)	Nivel de Riesgo (P x I)	Nivel de Riesgo (Categoría)
Enrutadores de Borde	Terremotos (A001)	6	9	54	Moderado
	Inundaciones (A002)	6	8	48	Moderado
	Incendios (A003)	5	8	40	Moderado
	Fallos de hardware (A004)	5	9	45	Moderado
	Evolución de técnicas de cibercriminales (A005)	8	9	72	Alto
	Ausencia de un Data Center espejo (V002)	9	10	90	Alto
	Redundancia insuficiente (V001)	7	9	63	Alto
	ICMP (V003)	7	8	56	Moderado

Conmutadores de Agregación	Terremotos (A001)	6	9	54	Moderado
	Inundaciones (A002)	6	8	48	Moderado
	Incendios (A003)	5	8	40	Moderado
	Fallos de hardware (A004)	5	9	45	Moderado
	Evolución de técnicas de cibercriminales (A005)	8	9	72	Alto
	Ausencia de un Data Center espejo (V002)	9	10	90	Alto
	Redundancia insuficiente (V001)	7	9	63	Alto
	ICMP (V003)	7	8	56	Moderado
Servidores	Terremotos (A001)	6	9	54	Moderado
	Inundaciones (A002)	6	8	48	Moderado
	Incendios (A003)	5	8	40	Moderado
	Fallos de hardware (A004)	5	9	45	Moderado
	Evolución de técnicas de cibercriminales (A005)	8	9	72	Alto
	Ausencia de un Data Center espejo (V002)	9	10	90	Alto

	Redundancia insuficiente (V001)	7	9	63	Alto
Sistemas de Almacenamiento (SAN/NAS)	Terremotos (A001)	6	9	54	Moderado
	Inundaciones (A002)	6	8	48	Moderado
	Incendios (A003)	5	8	40	Moderado
	Fallos de hardware (A004)	5	9	45	Moderado
	Evolución de técnicas de cibercriminales (A005)	8	9	72	Alto
	Ausencia de un Data Center espejo (V002)	9	10	90	Alto
	Redundancia insuficiente (V001)	7	9	63	Alto
Sistemas de Monitorización	Terremotos (A001)	6	9	54	Moderado
	Inundaciones (A002)	6	8	48	Moderado
	Incendios (A003)	5	8	40	Moderado
	Evolución de técnicas de cibercriminales (A005)	8	9	72	Alto
	Redundancia insuficiente (V001)	7	9	63	Alto
	ICMP (V003)	7	8	56	Moderado

Sistemas de Respaldo y Recuperación	Terremotos (A001)	6	9	54	Moderado
	Inundaciones (A002)	6	8	48	Moderado
	Incendios (A003)	5	8	40	Moderado
	Fallos de hardware (A004)	5	9	45	Moderado
	Evolución de técnicas de cibercriminales (A005)	8	9	72	Alto
	Ausencia de un Data Center espejo (V002)	9	10	90	Alto
	Redundancia insuficiente (V001)	7	9	63	Alto
Conexiones de Red Externas	Terremotos (A001)	6	9	54	Moderado
	Inundaciones (A002)	6	8	48	Moderado
	Incendios (A003)	5	8	40	Moderado
	Fallos de hardware (A004)	5	9	45	Moderado
	Evolución de técnicas de cibercriminales (A005)	8	9	72	Alto
	Redundancia insuficiente (V001)	7	9	63	Alto
	ICMP (V003)	7	8	56	Moderado

VII. Estrategias de Mitigación

Las estrategias de mitigación son fundamentales para reducir la probabilidad y el impacto de los riesgos identificados en el Data Center. A continuación, se detallan las medidas específicas que deben implementarse para abordar las amenazas y vulnerabilidades detectadas.

1. Medidas de Mitigación para Amenazas Cibernéticas

Implementación de Firewalls Avanzados y Sistemas IDS/IPS:

- Descripción: Instalar y configurar firewalls de última generación (NGFW) que ofrecen capacidades de inspección profunda de paquetes y protección contra amenazas avanzadas.

Acciones Específicas:

- Configurar políticas de seguridad estrictas que bloqueen el tráfico no autorizado.
- Actualizar automáticamente las firmas y reglas de detección de amenazas.

Actualizaciones Automatizadas de Seguridad en Hardware y Software:

Descripción: Establecer procesos automatizados para la aplicación de parches y actualizaciones en todos los sistemas y dispositivos de red.

Acciones Específicas:

- Utilizar herramientas de gestión de parches que programen actualizaciones fuera de horas pico.

- Mantener un inventario actualizado de todos los activos para asegurar que ningún dispositivo quede sin actualizar.

Segmentación de Red y Control de Accesos:

Descripción: Dividir la red en segmentos o zonas de seguridad para limitar el movimiento lateral de amenazas y controlar el acceso entre diferentes partes de la red.

Acciones Específicas:

- Implementar VLANs y aplicar políticas de acceso basadas en roles (RBAC).
- Utilizar firewalls internos para controlar el tráfico entre segmentos críticos.

Autenticación Multifactor (MFA):

Descripción: Reforzar la autenticación de usuarios mediante el uso de múltiples factores, como contraseñas, tokens físicos o aplicaciones de autenticación.

Acciones Específicas:

- Implementar MFA en sistemas críticos y accesos remotos.
- Integrar MFA con el directorio activo y sistemas de gestión de identidades.

Herramientas de Análisis de Comportamiento y SIEM:

Descripción: Utilizar sistemas de gestión de eventos e información de seguridad (SIEM) y herramientas de análisis de comportamiento para detectar actividades sospechosas o anómalas.

Acciones Específicas:

- Configurar alertas en tiempo real para actividades fuera de lo común.
- Correlacionar eventos de seguridad de diferentes fuentes para una detección más efectiva.

Capacitación Continua en Ciberseguridad:

Descripción: Establecer programas de formación y concienciación para el personal sobre las mejores prácticas en ciberseguridad.

Acciones Específicas:

- Realizar talleres y seminarios periódicos.
- Enviar boletines informativos sobre nuevas amenazas y tácticas de prevención.

2. Resiliencia de Comunicaciones y Enlaces Redundantes

Implementación de Enlaces de Comunicaciones Redundantes:

Descripción: Establecer enlaces de comunicación secundarios que entren en funcionamiento automáticamente en caso de falla del enlace principal.

Acciones Específicas:

- Contratar servicios de múltiples proveedores de internet para diversificar las rutas de acceso.
- Configurar protocolos de enrutamiento dinámico (BGP) para facilitar la conmutación automática.

Protocolos de Alta Disponibilidad:

Descripción: Utilizar protocolos como **HSRP**, **VRRP** o **GLBP** para garantizar la alta disponibilidad en dispositivos críticos de la red. También se incluyen protocolos que optimizan el rendimiento y aseguran redundancia.

Acciones Específicas:

- HSRP/VRRP/GLBP: Configurar conmutación automática entre routers, asegurando que siempre haya un dispositivo disponible en caso de falla.
- LACP: Implementar agregación de enlaces múltiples, proporcionando redundancia y mayor ancho de banda.
- MSTP/RSTP: Prevenir bucles en la red y garantizar tiempos de convergencia rápidos ante fallos de enlaces.
- Realizar pruebas de conmutación para verificar la eficacia de los protocolos en situaciones reales de fallos.

3. Estrategias de Mitigación para Fallos de Hardware

Monitoreo Predictivo de Hardware:

Descripción: Utilizar herramientas que monitoreen el estado de los componentes de hardware para predecir y prevenir fallos.

Acciones Específicas:

- Implementar sistemas de monitoreo que analicen indicadores como temperatura, uso de CPU, errores de disco, etc.
- Configurar alertas tempranas para intervenir antes de que ocurra una falla.

Mantenimiento Proactivo y Planes de Reemplazo:

Descripción: Establecer programas de mantenimiento regular y programar reemplazos de hardware antes de que alcancen el fin de su vida útil.

Acciones Específicas:

- Crear un calendario de mantenimiento preventivo.
- Mantener contratos de soporte con proveedores para garantizar reemplazos rápidos.

4. Medidas para Garantizar la Continuidad del Negocio

Desarrollo del Plan de Continuidad del Negocio (BCP):

Descripción: Documentar procedimientos y recursos necesarios para mantener las operaciones críticas durante y después de una interrupción significativa.

Acciones Específicas:

- Identificar procesos críticos y dependencias.
- Establecer estrategias de recuperación y asignar responsabilidades.

Desarrollo del Plan de Recuperación ante Desastres (DRP):

Descripción: Definir los pasos necesarios para restaurar los sistemas y servicios después de un desastre o interrupción mayor.

Acciones Específicas:

- Documentar procedimientos de restauración de datos y sistemas.
- Definir tiempos objetivo de recuperación (RTO) y puntos objetivo de recuperación (RPO).

Para definir los Tiempos Objetivo de Recuperación (RTO) y los Puntos Objetivo de Recuperación (RPO) en el plan de recuperación ante desastres, se utilizan las siguientes fórmulas:

3. **Cálculo del RTO:**

$$RTO = T_{detect} + T_{response} + T_{recover}$$

Donde:

- Tdetect: Tiempo necesario para detectar el fallo.
- Tresponse: Tiempo necesario para responder al incidente.
- Trecover : Tiempo necesario para recuperar los sistemas afectados.

Ejemplo de RTO:

Para un servidor crítico que aloja servicios empresariales esenciales:

- $T_{detect} = 10$ minutos = 10 (detección automática del fallo).
- $T_{response} = 20$ minutos (inicio de la respuesta técnica).
- $T_{recover} = 30$ minutos (restauración del sistema).

$$RTO = 10 + 20 + 30 = 60 \text{minutos} (1 \text{hora})$$

4. **Cálculo del RPO:**

$$RPO = Tbackup$$

Donde:

- Tbackup: Intervalo entre las copias de seguridad o sincronizaciones de datos.

Ejemplo de RPO:

Si las copias de seguridad se realizan cada 4 horas, el RPO sería:

$$RPO = 4horas$$

Pruebas y Simulacros Regulares:

Descripción: Realizar pruebas periódicas de los planes BCP y DRP para asegurar su efectividad y actualizar según sea necesario.

Acciones Específicas:

- Programar simulacros semestrales o anuales.
- Documentar resultados y áreas de mejora.

5. Mejoras en Seguridad Física

Control de Acceso Biométrico y Multifactor:

Descripción: Implementar sistemas de control de acceso que utilicen autenticación biométrica combinada con tarjetas de proximidad o códigos PIN.

Acciones Específicas:

- Instalar lectores de huellas dactilares o reconocimiento facial en áreas críticas.
- Establecer políticas de acceso basadas en roles y horarios.

Barreras Físicas y Seguridad Perimetral:

Descripción: Fortalecer las defensas físicas del Data Center mediante el uso de cercas, puertas reforzadas y vigilancia constante.

Acciones Específicas:

- Instalar puertas de seguridad con control de acceso en múltiples etapas (mantraps).
- Implementar rondas de vigilancia y sistemas de alarma.

Sistemas Avanzados de Detección y Extinción de Incendios:

Descripción: Utilizar sistemas de detección temprana de incendios y agentes de extinción no dañinos para equipos electrónicos (por ejemplo, gas inerte).

Acciones Específicas:

- Instalar detectores de humo de alta sensibilidad (VESDA).
- Configurar sistemas de extinción automática con gas FM-200 o similar.

Detección de Inundaciones y Control Ambiental:

Descripción: Implementar sensores de humedad y sistemas de alerta temprana para prevenir daños por agua.

Acciones Específicas:

- Colocar sensores de agua en puntos críticos.
- Configurar alarmas y protocolos de respuesta rápida.

6. Gestión de Vulnerabilidades y Actualizaciones

Escaneos Regulares de Vulnerabilidades:

Descripción: Realizar escaneos programados utilizando herramientas como Nessus y OpenVAS para identificar y corregir vulnerabilidades en el sistema.

Acciones Específicas:

- Establecer un calendario mensual o trimestral de escaneos.
- Priorizar la remediación según el nivel de criticidad de las vulnerabilidades detectadas.

Gestión de Parches y Actualizaciones:

Descripción: Implementar un proceso formal para la aplicación de parches y actualizaciones de seguridad en todos los sistemas y aplicaciones.

Acciones Específicas:

- Mantenerse informado sobre nuevas vulnerabilidades y actualizaciones a través de boletines de seguridad.
- Probar los parches en entornos controlados antes de su despliegue en producción.

7. Políticas y Procedimientos de Seguridad

Actualización y Difusión de Políticas de Seguridad:

Descripción: Revisar y actualizar periódicamente las políticas de seguridad para reflejar cambios en el entorno de amenazas y en la infraestructura tecnológica.

Acciones Específicas:

- Distribuir las políticas a todo el personal y requerir confirmación de lectura y comprensión.
- Incluir políticas sobre uso aceptable, manejo de información confidencial y protocolo de reportes.

Procedimientos de Gestión de Incidentes:

Descripción: Definir procesos claros para la identificación, reporte, escalamiento y resolución de incidentes de seguridad.

Acciones Específicas:

- Establecer un equipo de respuesta a incidentes con roles y responsabilidades definidos.
- Crear formularios y canales de comunicación específicos para el reporte de incidentes.

VIII. Estrategias de Mitigación y Protección de Activos Críticos

A continuación, se detallan las medidas de mitigación orientadas a proteger los activos críticos identificados en el Data Center de AirmaxTelecom Soluciones Tecnológicas S.A. Cada medida se ha diseñado para abordar las amenazas y vulnerabilidades previamente evaluadas, asegurando la protección integral de los recursos más valiosos.

1. **Medidas para Activos de Red (Enrutadores de Borde y Conmutadores de Agregación)**

- **Activos Críticos:**

    - Enrutadores de Borde
    - Conmutadores de Agregación

- **Amenazas:**

    - Desastres naturales
    - Fallos de hardware
    - Evolución de técnicas de cibercriminales
    - Vulnerabilidad de ICMP

- **Medidas de Mitigación:**

- Redundancia en Equipos: Implementar redundancia en los enrutadores y conmutadores para asegurar la continuidad del tráfico de datos en caso de fallos de hardware o interrupciones por desastres naturales.
- Protección Física: Reforzar la infraestructura física de los equipos ante desastres naturales, asegurando la instalación de protecciones contra incendios e inundaciones.
- Actualización Continua de Firmware: Mantener los enrutadores y conmutadores actualizados con los últimos parches y mejoras de seguridad para mitigar nuevas técnicas de ciberataques.
- Firewalls y Sistemas IDS/IPS: Implementar firewalls avanzados y sistemas de detección y prevención de intrusiones (IDS/IPS) para monitorear y filtrar el tráfico de red en tiempo real.
- Mitigación de la Vulnerabilidad de ICMP

- Restricción de ICMP en las Interfaces: Configurar listas de control de acceso (ACLs) en los enrutadores y conmutadores para permitir solo el tráfico ICMP entre dispositivos internos específicos, bloqueando todo ICMP no autorizado o proveniente de redes externas no confiables.
- Rate Limiting para ICMP: Implementar límites de tasa para el tráfico ICMP, previniendo ataques de denegación de servicio (DoS) mediante el uso excesivo de este protocolo.
- Permitir Solo ICMP Específico: Habilitar solo los tipos de mensajes ICMP necesarios, como Echo Reply y Destination Unreachable, y bloquear aquellos innecesarios o potencialmente peligrosos, como Redirect Messages.
- Monitoreo de ICMP en Firewalls y Sistemas IDS/IPS: Inspeccionar el tráfico ICMP mediante firewalls y sistemas IDS/IPS, bloqueando cualquier tráfico ICMP sospechoso o no autorizado.

2. Medidas para Servidores y Sistemas de Almacenamiento

- **Activos Críticos:**
    - Servidores
    - Sistemas de Almacenamiento (SAN/NAS)
- **Amenazas:**
    - Fallos de hardware
    - Ausencia de un Data Center espejo

- **Medidas de Mitigación:**

➢ Backup Regular y Automatizado: Implementar copias de seguridad automatizadas y frecuentes para asegurar la replicación constante de los datos críticos.

➢ Monitoreo del Estado de los Servidores: Implementar sistemas de monitoreo en tiempo real para detectar fallos o anomalías en los servidores y sistemas de almacenamiento.

➢ Establecimiento de un Data Center Espejo: Implementar un data center espejo para replicar los datos y asegurar la continuidad operativa en caso de fallos críticos.

3. Medidas para Sistemas de Energía (UPS y Generadores de Respaldo)

- **Activos Críticos:**

  - Sistemas de Alimentación Ininterrumpida (UPS)
  - Generadores de Respaldo

- **Amenazas:**

  - Fallos de hardware

- **Medidas de Mitigación:**

➢ Pruebas Periódicas de Sistemas de Respaldo: Realizar simulacros y pruebas periódicas de los sistemas de energía de respaldo, asegurando que los UPS y generadores funcionen adecuadamente durante fallos en el suministro eléctrico.

- Redundancia en la Energía: Implementar redundancia en los sistemas de UPS y generadores, asegurando que existan fuentes alternas de energía en caso de fallos prolongados.

4. Medidas para Seguridad Física y Conexiones de Red Externas

- **Activos Críticos:**
    - Sistemas de Seguridad Física
    - Conexiones de Red Externas
- **Amenazas:**
    - Desastres naturales
    - Intrusos físicos
    - Evolución de técnicas de cibercriminales
- **Medidas de Mitigación:**

- Control de Acceso y Videovigilancia: Establecer políticas estrictas de control de acceso a las instalaciones del Data Center, implementando sistemas biométricos, CCTV y detección de intrusos.
- Simulacros de Recuperación ante Desastres: Realizar simulacros periódicos para probar la capacidad de recuperación ante desastres naturales, asegurando que el personal y los sistemas estén preparados para una respuesta eficiente.
- Monitoreo de Red Externa: Implementar un sistema de monitoreo continuo del tráfico en las conexiones de red externas para detectar comportamientos anómalos y ataques.

- Uso de VPN Seguras: Establecer conexiones VPN seguras para proteger las comunicaciones entre el Data Center y las redes externas.

IX. Estrategias de Mitigación de Riesgos

Selección de Controles:

- **Controles Preventivos:** Implementación de refuerzo estructural para proteger contra desastres naturales, mantenimiento preventivo regular de hardware, y mejora de políticas de gestión de usuarios para prevenir accesos no autorizados.
- **Controles Detectivos:** Implementación de sistemas de firewall avanzados, sistemas de detección de intrusiones (IDS), y monitoreo continuo de red para identificar actividades sospechosas de manera oportuna.
- **Controles Correctivos:** Desarrollo de planes de contingencia y recuperación ante desastres, asegurando que se puedan restaurar rápidamente las operaciones en caso de un incidente de seguridad significativo.

Implementación de Controles: Proceso detallado para la implementación de cada control seleccionado, incluyendo cronograma específico, asignación de responsabilidades y definición de recursos necesarios. Este enfoque asegura que cada medida sea implementada de manera efectiva y dentro de los plazos establecidos.

Políticas y Procedimientos: Desarrollo y actualización de políticas de seguridad y procedimientos operativos, asegurando que todas las prácticas de seguridad sean documentadas y seguidas estrictamente por todo el personal.

X. Plan de Implementación

Cronograma de Actividades

Para garantizar una efectiva mitigación de riesgos dentro de la empresa, se ha desarrollado un cronograma de actividades, que se presenta la tabla 7. Este cronograma detalla cada una de las fases críticas necesarias para la implementación de medidas de seguridad robustas, incluyendo el levantamiento de políticas de seguridad, su aprobación e implementación, así como la difusión, capacitación y la implementación de medidas tanto de ciberseguridad como de seguridad física. Cada fase cuenta con un equipo responsable y un tiempo estimado de ejecución, asegurando que las actividades se lleven a cabo de manera organizada y eficiente. El monitoreo y la revisión periódica también forman parte integral de este plan, lo que permite una evaluación continua y ajustes según sea necesario.

Tabla 7

Cronograma de Actividades

Fase	Actividad	Responsable	Fecha de Inicio	Fecha de Fin	Duración (días hábiles)	Dependencias
1	Revisión y aprobación del plan de seguridad	Alta Dirección	05/02/2025	16/02/2025	10	-

2	Revisión del manual de políticas de seguridad	Equipo de Seguridad	19/02/2025	02/03/2025	10	Fase 1
3	Aprobación de políticas	Alta Dirección	05/03/2025	18/03/2025	10	Fase 2
4	Diseño de medidas de ciberseguridad y físicas	TI y Seguridad Física	19/03/2025	01/04/2025	10	Fase 3
5	Implementación de medidas de ciberseguridad	TI	02/04/2025	30/05/2025	40	Fase 4
6	Instalación de sistemas de respaldo y energía	Mantenimiento	02/06/2025	27/06/2025	20	Fase 5
7	Mejora de seguridad física	Seguridad Física	30/06/2025	25/07/2025	20	Fase 6
8	Difusión y capacitación	Recursos Humanos	28/07/2025	22/08/2025	22	Fase 7

9	Pruebas de recuperación y simulacros	TI y Auditoría Interna	25/08/2025	05/09/2025	10	Fase 8
10	Monitoreo y revisión periódica	Auditoría Interna	08/09/2025	Continuo	Continuo	Fase 9

Nota. En la tabla se puede observar el cronograma de implementación para cada actividad y el tiempo para su ejecución.

Asignación de Recursos:

- **Personal:** TI, Seguridad, Operaciones, Recursos Humanos, Alta Dirección.
- **Equipos:** Firewalls, IDS/IPS, sistemas de UPS, generadores de respaldo, sistemas de vigilancia.
- **Presupuesto:** Para adquisición de equipos, capacitación y mantenimiento.

Planes de Monitoreo y Revisión Periódica:

Se establece un proceso de monitoreo continuo y revisión periódica para asegurar la efectividad del plan de seguridad. Esto incluye auditorías regulares, pruebas de penetración y revisiones de políticas para adaptarse a nuevas amenazas y cambios en el entorno operativo.

XI. Equipo de Trabajo

El equipo de trabajo encargado de definir y revisar las políticas de seguridad está compuesto por:

- **Director de TI:** Responsable de la supervisión general y coordinación del equipo.

- **Gerente de Seguridad:** Encargado de la implementación y monitoreo de las medidas de seguridad.
- **Analista de Riesgos:** Responsable del análisis y evaluación de riesgos.
- **Representante de la Alta Dirección:** Asegura la alineación de las políticas con los objetivos estratégicos de la empresa.
- **Especialista en Cumplimiento:** Garantiza que las políticas cumplan con los requisitos legales y normativos.
- **Representante de Recursos Humanos:** Coordina la capacitación y concienciación del personal.

XII. Programa de Formación y Concientización

Objetivo del Programa

Fortalecer la cultura de seguridad de la información dentro de la organización mediante un programa continuo de formación y concientización. Este programa tiene como fin capacitar al personal para que identifique, prevenga y responda eficazmente ante las amenazas de seguridad, asegurando que adopten las mejores prácticas y procedimientos de protección de los activos de la empresa.

Grupos de Interés

Este programa está dirigido a todos los niveles de la organización que tengan interacción con los sistemas de información, incluyendo:

- Personal de TI: Responsables de la gestión y monitoreo de los sistemas críticos.

- Gerencia: Encargados de la toma de decisiones estratégicas.
- Administración y otros departamentos: Personal que maneje información sensible o gestionen sistemas críticos.

Métodos de Entrega

Se utilizarán diversas plataformas y metodologías para impartir la formación, adaptando el contenido a las necesidades y responsabilidades de cada grupo. Estas incluyen:

1. **Talleres presenciales:**
    - Enfocados en la interacción directa y resolución de dudas.
    - Incluyen simulaciones prácticas de incidentes de seguridad.
2. **Seminarios virtuales:**
    - Facilitan el acceso remoto al contenido formativo.
    - Ideales para personal en ubicaciones descentralizadas.
3. **Módulos de e-learning:**
    - Contenido interactivo y evaluaciones al final de cada módulo.
    - Permite al personal aprender a su propio ritmo.
4. **Manuales de Usuario:**
    - Proporcionan instrucciones detalladas sobre políticas, procedimientos y herramientas de seguridad.
    - Incluyen secciones específicas como:
        - Normas generales de seguridad.
        - Uso seguro de recursos tecnológicos.
        - Gestión de incidentes de seguridad.

        - Glosario y recursos clave.

5. **Guías Prácticas:**
    - Documentos breves y específicos que explican cómo implementar medidas de seguridad en el día a día.
    - Ejemplos:
        - Creación de contraseñas seguras.
        - Identificación de correos electrónicos sospechosos.
        - Respuesta inicial a incidentes de seguridad.

Contenido del Programa

El programa abordará los siguientes temas clave:

1. **Importancia de las Políticas de Seguridad:**
    - Explicación de las políticas implementadas en la organización.
    - Relevancia de su cumplimiento para proteger los activos críticos.
2. **Mejores Prácticas de Manejo de Información:**
    - Uso seguro de contraseñas.
    - Almacenamiento adecuado de datos sensibles.
    - Reconocimiento y prevención de amenazas como phishing y malware.
3. **Procedimientos para la Gestión de Incidentes:**
    - Pasos para identificar, reportar y responder a incidentes de seguridad.
    - Simulación de escenarios de ciberataques para practicar respuestas.
4. **Implementación de Controles Preventivos y Correctivos:**
    - Uso de autenticación multifactor (MFA) para acceso seguro.

- Configuración y monitoreo de firewalls y sistemas IDS/IPS.
- Pruebas regulares de recuperación ante desastres.

5. **Manuales y Guías Prácticas:**
    - **Manual de Usuario:**
        - Instrucciones completas sobre el uso seguro de sistemas y recursos.
        - Procedimientos para reportar incidentes y aplicar controles básicos.
    - **Guías Prácticas:**
        - Documentos concisos para la aplicación inmediata de medidas de seguridad.
        - Ejemplo: Cómo responder a un correo electrónico sospechoso o restaurar datos desde un respaldo.

Simulación y Evaluación

El programa incluirá simulaciones periódicas de ciberataques y evaluaciones prácticas para medir la efectividad del aprendizaje. Además, se fomentará la retroalimentación para mejorar continuamente los materiales de formación.

Resultados Esperados

- Mayor conciencia y compromiso del personal con la seguridad de la información.
- Reducción de incidentes de seguridad por errores humanos.
- Respuesta más rápida y efectiva ante amenazas.

XIII. Monitoreo y Revisión

Métodos de Monitoreo: Técnicas utilizadas para monitorear la efectividad de los controles de seguridad, tales como el uso de sistemas de detección de intrusiones, análisis de logs y auditorías de seguridad.

Frecuencia de las Revisiones: Programación de revisiones periódicas para actualizar y mejorar el plan, asegurando que las medidas de seguridad sigan siendo efectivas frente a nuevas amenazas y cambios en el entorno.

Indicadores de Rendimiento Clave (KPIs):

- **Tiempo Medio para Detectar Incidentes (MTTD):** Medida del tiempo promedio que toma detectar un incidente de seguridad.
- **Tiempo Medio para Responder a Incidentes (MTTR):** Medida del tiempo promedio que toma responder y mitigar un incidente de seguridad.
- **Tasa de Incidentes Resueltos:** Proporción de incidentes de seguridad que han sido resueltos exitosamente.
- **Número de Incidentes de Seguridad:** Total de incidentes de seguridad reportados en un período determinado.

XIV. Mejora Continua

Feedback y Ajustes: Proceso para recibir retroalimentación y realizar ajustes necesarios, asegurando que el plan de seguridad se mantenga actualizado y efectivo.

Actualización de Políticas: Revisión y actualización regular de políticas de seguridad de acuerdo a cambios en el entorno de amenazas y avances tecnológicos.

Revisión Tecnológica Periódica: Evaluación continua de nuevas tecnologías y herramientas para mejorar la seguridad de la información, asegurando que el Data Center se beneficie de las mejores prácticas y soluciones disponibles en el mercado.

XV. Plan de Acción

Acciones Inmediatas:

- **Formación del Comité de Seguridad:** Consolidar un equipo multidisciplinario, integrado por representantes de los principales departamentos de la organización, que supervisará la implementación y mejora continua del plan de seguridad.
- **Asignación de Recursos:** Garantizar la disponibilidad de los recursos humanos, tecnológicos y financieros necesarios para ejecutar todas las fases del plan. Esto incluye la provisión de herramientas tecnológicas, capacitación especializada y soporte financiero adecuado para las iniciativas de seguridad.
- **Desarrollo de Políticas y Procedimientos (Versión Inicial Completada):** El manual de políticas de seguridad ha sido desarrollado en su primera versión. A partir de esta base, se revisarán y actualizarán los procedimientos de seguridad de manera continua, asegurando que reflejen las mejores prácticas y se ajusten a los nuevos desafíos de seguridad.
- **Capacitación Inicial:** Realizar sesiones de formación y concientización dirigidas al personal clave, con especial enfoque en las nuevas políticas de seguridad y procedimientos

establecidos. La capacitación garantizará que todos los empleados comprendan las amenazas de seguridad y estén alineados con las medidas de protección implementadas.

- **Inicio de Implementación de Medidas de Seguridad:** Comenzar con la implementación de las mejoras físicas y estructurales necesarias, así como la actualización de hardware y software, asegurando que los activos críticos estén protegidos bajo un marco sólido de seguridad.

Mediano Plazo (6-12 meses):

- **Fortalecimiento de la Ciberseguridad:** Desplegar sistemas avanzados de ciberseguridad y actualizar las políticas de seguridad previamente diseñadas. Se implementarán controles como firewalls avanzados, IDS/IPS (sistemas de detección y prevención de intrusiones) y autenticación multifactor (MFA) para asegurar una protección robusta ante amenazas cibernéticas.
- **Simulacros de Recuperación ante Desastres:** Ejecutar simulacros de recuperación periódicos para poner a prueba la efectividad del plan de recuperación ante desastres y la continuidad del negocio. Estos ejercicios ayudarán a identificar posibles áreas de mejora en los procedimientos de respuesta.
- **Monitoreo Continuo de Seguridad:** Establecer sistemas de monitoreo en tiempo real para la detección proactiva de incidentes de seguridad. Se implementarán herramientas para la supervisión continua de logs y redes, lo que permitirá detectar amenazas antes de que se conviertan en problemas críticos.
- **Auditorías y Evaluaciones Regulares:** Realizar auditorías trimestrales y evaluaciones continuas de la infraestructura de seguridad para identificar vulnerabilidades y riesgos. Las

auditorías se enfocarán en verificar la efectividad de las medidas implementadas y en realizar ajustes necesarios según las nuevas amenazas emergentes.

Largo Plazo (12-24 meses):

- **Establecimiento del Data Center Espejo:** Completar la implementación del Data Center espejo, que permitirá una replicación de datos crítica para asegurar la continuidad del servicio en caso de fallos mayores o desastres. El objetivo es reducir al mínimo los tiempos de inactividad en situaciones críticas.
- **Revisiones Periódicas del Plan de Seguridad:** Mantener un ciclo de revisión continua del plan de seguridad, ajustándolo a las nuevas amenazas, tendencias tecnológicas y mejores prácticas del sector. Esto incluirá la actualización de políticas y procedimientos, basándose en auditorías y análisis de incidentes previos.
- **Sostenimiento del Programa de Formación Continua:** Mantener y actualizar el programa de formación y concientización para todos los empleados, asegurando que se adapten a las nuevas amenazas cibernéticas y a los cambios en las tecnologías. El contenido del programa será revisado y actualizado anualmente.
- **Mejora Continua:** Implementar mejoras continuas basadas en el feedback recibido de auditorías internas y simulacros, asegurando que el Data Center esté alineado con las mejores soluciones tecnológicas y operativas disponibles. Esta fase garantizará que las soluciones implementadas evolucionen conforme a los desafíos del entorno digital.

XVI. Cumplimiento Legal y Normativo

El plan de seguridad del Data Center de AirmaxTelecom Soluciones Tecnológicas S.A. se fundamenta en el estricto cumplimiento de las leyes y normativas locales e internacionales aplicables al manejo, protección y procesamiento de la información, así como en el uso y operación de la infraestructura tecnológica crítica. A continuación, se detallan los principales marcos legales y normativos que este plan aborda para garantizar la conformidad regulatoria:

Ley Orgánica de Protección de Datos Personales

En cumplimiento con la Ley Orgánica de Protección de Datos Personales de Ecuador, el plan de seguridad garantiza la protección de los datos personales almacenados y procesados en el Data Center. Las medidas implementadas aseguran que los datos sensibles sean manejados bajo estrictos controles de confidencialidad y solo sean accesibles por personal autorizado.

- **Principios Claves:**
    - Confidencialidad y Protección de Datos: Implementación de controles de acceso rigurosos, encriptación de datos, y monitoreo constante para prevenir accesos no autorizados.
    - Derechos de los Titulares: El Data Center está preparado para responder de manera oportuna a solicitudes de acceso, modificación o eliminación de datos personales, garantizando los derechos de los titulares.

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos

El plan asegura que la información transmitida y almacenada electrónicamente cumpla con los requisitos de autenticidad, integridad y no repudio establecidos en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

- **Implementaciones Claves:**
    - Autenticación y No Repudio: Uso de tecnologías de autenticación avanzada y verificación de firmas electrónicas para asegurar la validez y la integridad de los datos.
    - Protección de Mensajes de Datos: Encriptación de mensajes durante su transmisión para garantizar la confidencialidad de las comunicaciones electrónicas.

Normativa de la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL)

El Data Center se rige por las regulaciones establecidas por ARCOTEL, asegurando el cumplimiento de los estándares técnicos y operacionales para el correcto funcionamiento de la infraestructura crítica de telecomunicaciones.

- **Cumplimiento Específico:**
    - Regulación de Infraestructura Crítica: Implementación de medidas para garantizar la continuidad operativa de los servicios de telecomunicaciones, minimizando riesgos de interrupciones.
    - Revisión Técnica: Se realizan revisiones técnicas periódicas para asegurar que todos los equipos del Data Center cumplen con los requisitos operativos establecidos por ARCOTEL.

Código Orgánico Integral Penal (COIP)

El plan también se ajusta al Código Orgánico Integral Penal (COIP), que penaliza los delitos informáticos y las infracciones relacionadas con la manipulación indebida de información. El plan establece controles de seguridad para evitar violaciones de la ley, protegiendo tanto los sistemas como los datos que gestiona el Data Center.

- **Cumplimiento con el COIP:**
    - Prevención de Delitos Informáticos: Implementación de controles avanzados, como sistemas de detección de intrusiones (IDS/IPS) y firewalls, para prevenir accesos no autorizados y ciberataques.
    - Monitoreo de Actividades Sospechosas: Supervisión continua de la infraestructura de TI para detectar cualquier actividad irregular o intento de ataque cibernético.

Ley Orgánica de Telecomunicaciones

En conformidad con la Ley Orgánica de Telecomunicaciones, el Data Center asegura que los servicios de telecomunicaciones se presten de manera segura y eficiente, cumpliendo con los estándares de calidad y operatividad requeridos para garantizar la disponibilidad continua de los servicios.

- **Cumplimiento Específico:**
    - Gestión de la Continuidad Operativa: Implementación de medidas que garantizan la disponibilidad de los servicios de telecomunicaciones, minimizando los tiempos de inactividad y asegurando la calidad del servicio.

- Cumplimiento Técnico: Asegurar que las operaciones del Data Center están alineadas con los estándares técnicos y normativos establecidos por las autoridades competentes en el sector de telecomunicaciones.

Proceso de Implementación de la Norma ISO/IEC 27001

AirmaxTelecom Soluciones Tecnológicas S.A. se encuentra en proceso de implementar la norma ISO/IEC 27001, que proporciona un marco internacionalmente reconocido para la gestión de la seguridad de la información. Este estándar garantiza la protección de la confidencialidad, integridad y disponibilidad de los datos críticos de la empresa.

- **Avances en la Implementación:**
  - Análisis de Brechas: Se ha realizado un análisis preliminar para identificar áreas de mejora que permitan cumplir con los requisitos de la norma.
  - Formalización de Políticas y Procedimientos: Se están definiendo políticas y procedimientos que aseguren el cumplimiento con los controles establecidos por la ISO/IEC 27001.
  - Auditoría y Certificación: Una vez implementados los controles, la empresa someterá su infraestructura a auditorías externas con el fin de obtener la certificación.

Normativa NIST SP 800-30

El plan de seguridad también sigue las directrices de la NIST SP 800-30, una guía internacionalmente reconocida para la gestión de riesgos en sistemas de información. Este marco

garantiza que todas las amenazas y vulnerabilidades en la infraestructura del Data Center se identifiquen y mitiguen de manera efectiva.

- **Cumplimiento con NIST SP 800-30:**
    - Identificación y Evaluación de Riesgos: Evaluación completa de los riesgos asociados con la infraestructura tecnológica y la implementación de medidas de mitigación.
    - Plan de Respuesta ante Incidentes: Desarrollo de un plan de respuesta basado en la metodología NIST para asegurar una reacción rápida y efectiva ante cualquier violación de seguridad.
    - Cumplimiento con Normas Relacionadas con la Continuidad del Negocio
    - El plan de seguridad también se alinea con estándares internacionales de continuidad del negocio, asegurando que los servicios críticos se mantengan operativos en caso de incidentes o desastres.
- **Principios de Continuidad:**
    - Planes de Recuperación ante Desastres (DRP): Desarrollo, implementación y pruebas regulares de los planes de recuperación para asegurar la restauración rápida de los sistemas críticos.
    - Simulacros Regulares: Ejecución periódica de simulacros para validar la eficacia de los planes de recuperación y continuidad operativa.

Plan de Cumplimiento y Auditoría

El cumplimiento de todas las normativas mencionadas se evalúa mediante auditorías internas y externas periódicas. AirmaxTelecom se compromete a la mejora continua de sus políticas y

procedimientos, asegurando que su infraestructura cumpla con los requisitos legales y regulatorios vigentes, tanto a nivel local como internacional.

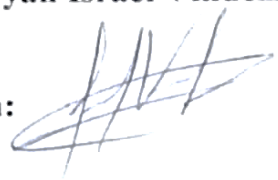
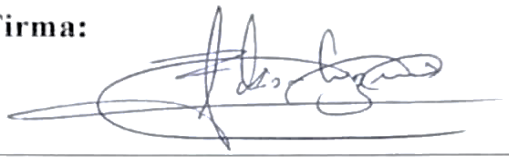
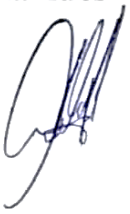
AIRMAXTELECOM

SOLUCIONES TECNOLÓGICAS S.A.

MANUAL DE POLÍTICAS DE SEGURIDAD

DATA CENTER

VERSIÓN 1.0

Versión	**1.0**
Elaborado por:	**Sr. Bryan Israel Vinueza Bedoya** **Firma:**  **MSc. Fabián Cuzme Rodríguez** **Firma:** 
Fecha de elaboración:	**15/11/2024**
Revisado por:	**Ing. Andrés Benavides** **Firma:** 
Fecha de revisión:	**14/01/2025**
Aprobado por:	
Fecha de aprobación:	

Contenido

Manual de Políticas de Seguridad

1. Objetivo del Manual

El objetivo de este manual es establecer un conjunto de políticas de seguridad que proporcionen directrices claras para la protección de los activos críticos del Data Center de AIRMAXTELECOM. Estas políticas están diseñadas para mitigar riesgos, garantizar la continuidad operativa, y proteger la confidencialidad, integridad y disponibilidad de la información.

2. Alcance

Este manual aplica a todos los empleados, contratistas y proveedores de AIRMAXTELECOM que tengan acceso a los sistemas, datos, infraestructura y servicios del Data Center. Cubre aspectos relacionados con la seguridad física, seguridad lógica, gestión de incidentes, control de acceso y manejo de la información, entre otros.

3. Introducción a la NIST SP 800-30

Este manual de políticas se fundamenta en las directrices de la **NIST SP 800-30,** un estándar internacionalmente reconocido que establece un marco para la evaluación y gestión de riesgos en sistemas de información. La metodología de la NIST SP 800-30 permite identificar, analizar y responder a los riesgos asociados con la seguridad, garantizando un enfoque sistemático y proactivo para la protección de los activos de información.

4. Políticas de Seguridad

4.1 Política de Gestión de Accesos

Objetivo

Controlar el acceso a los recursos del Data Center para asegurar que solo el personal autorizado tenga acceso a la información y los sistemas.

Alcance

Aplica a todos los sistemas de información, dispositivos de red, aplicaciones y datos del Data Center.

Políticas:

- **Autenticación Multifactor (MFA)**: Todo acceso a sistemas críticos debe utilizar autenticación multifactor para protegerse contra accesos no autorizados.
- **Control de Accesos Basado en Roles (RBAC)**: Los permisos de acceso a sistemas, aplicaciones y datos deben ser asignados en función de los roles laborales.
- **Revisión Periódica de Accesos**: Los accesos a sistemas deben ser revisados trimestralmente para asegurar que sean apropiados y vigentes según las responsabilidades de cada empleado.
- **Acceso Físico Restringido**: El acceso físico al Data Center solo se permite a personal autorizado. Se debe utilizar control biométrico y doble autenticación en zonas sensibles.

Medidas de Cumplimiento

- **Auditorías de accesos semestrales:**

- **Indicador de cumplimiento:** Porcentaje de auditorías de accesos realizadas según el cronograma semestral.
- **Meta mínima: 100% de las auditorías de accesos programadas deben completarse dentro del periodo establecido.**
- **Verificación:** Documentación que incluya:
    - Registro de accesos revisados.
    - Usuarios con accesos no autorizados identificados.
    - Acciones correctivas implementadas tras cada auditoría.

- **Implementación de registros de acceso en sistemas clave:**

- **Indicador de cumplimiento:** Porcentaje de sistemas clave que generan y almacenan registros de acceso de manera adecuada.
- **Meta mínima: 95% de los sistemas clave deben tener registros activos y cumplir con políticas de retención.**
- **Verificación:** Auditorías trimestrales para revisar:
    - Actividad de registro.
    - Configuración y seguridad de los logs de acceso.
- **Evaluación adicional:** Reducción de incidentes relacionados con accesos no registrados.

- **Capacitación del personal sobre la importancia de la gestión de accesos:**

- **Indicador de cumplimiento:** Porcentaje de empleados clave que completan la capacitación anual obligatoria sobre gestión de accesos.
- **Meta mínima: 95% del personal clave debe completar y aprobar la capacitación.**

- **Verificación:** Registro detallado de las sesiones de capacitación realizadas, lista de asistentes, resultados de evaluaciones y porcentaje de participantes que alcanzan una puntuación mínima del 80%.

4.2 Política de Protección de Datos

Objetivo

Asegurar la protección de los datos sensibles y críticos almacenados, procesados o transmitidos por los sistemas del Data Center.

Alcance

Incluye todos los datos operativos, financieros y de clientes almacenados en los sistemas del Data Center.

Políticas

- **Categorización de Datos**: Todos los datos deben categorizarse en niveles de sensibilidad (Confidencial, Sensible, Público) y protegerse en consecuencia.
- **Encriptación Obligatoria**: Todos los datos sensibles deben estar encriptados tanto en tránsito como en reposo. Se utilizará encriptación de alta seguridad como **AES-256**. Adicionalmente, se consideran los siguientes algoritmos según las recomendaciones del NIST:

  Encriptación simétrica:

- AES (Advanced Encryption Standard): Versiones AES-128, AES-192 y AES-256, aprobadas en FIPS 197, son estándares recomendados para la protección de datos en reposo y en tránsito.
- Triple DES (3DES): Aunque aceptable en sistemas legados, está desaprobado para nuevas implementaciones según la NIST SP 800-131A.

Encriptación asimétrica:

- RSA (Rivest-Shamir-Adleman): Longitudes de clave de al menos 2048 bits para seguridad básica o 3072 bits para mayor robustez.
- ECC (Elliptic Curve Cryptography): Incluye algoritmos como ECDH para el intercambio de claves y ECDSA para firmas digitales, recomendados por NIST SP 800-56A Rev. 3.

Algoritmos de hash:

- SHA-2 (Secure Hash Algorithm 2): Versiones SHA-224, SHA-256, SHA-384 y SHA-512, como definidas en FIPS 180-4, para garantizar la integridad de los datos.
- SHA-3: Recomendado para aplicaciones que requieren mayor resistencia criptográfica (FIPS 202).

Intercambio de claves:

- Diffie-Hellman (DH) y Elliptic Curve Diffie-Hellman (ECDH): Métodos robustos para establecer claves compartidas, como se describe en NIST SP 800-56A Rev. 3.

Firma digital:

  - RSA: Para garantizar la autenticidad de datos y mensajes.
  - ECDSA: Firma digital basada en curvas elípticas, que ofrece mayor eficiencia con claves más pequeñas.
  - EdDSA (Edwards-Curve Digital Signature Algorithm): Algoritmo moderno basado en curvas como Ed25519, recomendado para escenarios que requieren alta velocidad y seguridad.

- **Copia de Seguridad y Retención de Datos**: Se realizarán copias de seguridad automáticas de los datos críticos diariamente, y estas copias deben ser almacenadas en un **Data Center espejo u otra ubicación distinta** para asegurar su disponibilidad en caso de desastre.
- **Gestión de la Eliminación de Datos**: Los datos que ya no sean necesarios deben ser eliminados de forma segura utilizando métodos aprobados como **borrado seguro** o destrucción física.

Medidas de Cumplimiento

- **Auditorías trimestrales de datos sensibles:**
  - **Indicador de cumplimiento:** Porcentaje de auditorías trimestrales completadas según el cronograma establecido por la empresa.
  - **Meta mínima: 80% de las auditorías programadas deben completarse trimestralmente.**
  - **Verificación:** Reportes documentados que incluyan el análisis de los datos sensibles revisados, hallazgos y acciones correctivas implementadas.
- **Verificación periódica de la correcta encriptación de datos en tránsito y en reposo:**

- **Indicador de cumplimiento:** Porcentaje de sistemas críticos verificados con configuraciones de encriptación adecuadas.
- **Meta mínima: 95% de los sistemas críticos deben cumplir con las normas de encriptación establecidas.**
- **Verificación:** Auditorías trimestrales que evalúen los sistemas de encriptación en uso y las políticas implementadas.

- **Políticas de retención de datos revisadas anualmente:**
  - **Indicador de cumplimiento:** Porcentaje de políticas de retención evaluadas y aprobadas durante la revisión anual.
  - **Meta mínima: 100% de las políticas de retención deben ser revisadas y actualizadas anualmente.**
  - **Verificación:** Registro de revisiones realizadas, fecha de actualización, responsables y aprobaciones correspondientes.

4.3 Política de Gestión de Incidentes

Objetivo

Definir el proceso para la identificación, respuesta y resolución de incidentes de seguridad que puedan afectar los activos del Data Center.

Alcance

Esta política aplica a todos los incidentes relacionados con la seguridad de la información, incluidas violaciones de datos, ataques cibernéticos y fallos críticos de hardware o software.

Políticas

- **Equipo de Respuesta a Incidentes (ERI)**: Se establecerá un equipo especializado encargado de gestionar y resolver los incidentes de seguridad. Este equipo debe estar disponible 24/7.
- **Reporte Inmediato de Incidentes**: Todo incidente de seguridad debe ser reportado inmediatamente al **Equipo de Respuesta a Incidentes**.
- **Procedimientos de Gestión de Incidentes**: Se deben seguir procedimientos claros para contener, erradicar, recuperar y analizar los incidentes.
- **Registro y Análisis de Incidentes**: Todos los incidentes deben registrarse y documentarse para análisis post-incidente, permitiendo aprender y mejorar las defensas.

Medidas de Cumplimiento

- **Auditoría de incidentes semestral:**
    - **Indicador de cumplimiento:** Porcentaje de auditorías de incidentes realizadas según el cronograma semestral.
    - **Meta mínima: 100% de las auditorías programadas deben completarse semestralmente.**
    - **Verificación:**
        - Informes detallados de auditoría que incluyan análisis de incidentes registrados, tiempo de resolución y acciones de mejora implementadas.
        - Seguimiento de hallazgos y cumplimiento de las recomendaciones.
- **Simulacros de respuesta a incidentes realizados trimestralmente:**

- **Indicador de cumplimiento:** Porcentaje de simulacros completados dentro del periodo trimestral planificado.
- **Meta mínima: 95% de los simulacros programados deben realizarse de manera efectiva cada trimestre.**
- **Verificación:**
  - Registro de simulacros con detalles como fecha, escenarios probados, participantes y evaluación de desempeño.
  - Reporte de resultados con indicadores como tiempo de respuesta promedio y efectividad en la contención de incidentes simulados.
- **KPI adicional:** Identificación y reducción de brechas detectadas durante los simulacros.

- **Revisión y actualización de los procedimientos de respuesta a incidentes de forma anual:**
  - **Indicador de cumplimiento:** Porcentaje de procedimientos revisados y actualizados al menos una vez al año.
  - **Meta mínima: 100% de los procedimientos de respuesta a incidentes deben ser revisados y aprobados anualmente.**
  - **Verificación:**
    - Registro de revisiones realizadas, incluyendo responsables, fecha de actualización y aprobación final.
    - Comparación con estándares de la industria para identificar mejoras necesarias.

- **Evaluación adicional:** Incorporación de lecciones aprendidas de incidentes pasados y simulacros en los procedimientos actualizados.

4.4 Política de Continuidad del Negocio

Objetivo

Asegurar que los sistemas críticos del Data Center puedan seguir operando ante eventos adversos o desastres, minimizando el impacto en las operaciones del negocio.

Alcance

Esta política aplica a todos los sistemas críticos, incluidos servidores, bases de datos, redes y aplicaciones esenciales.

Políticas

- **Desarrollo y Prueba de Plan de Continuidad del Negocio (BCP)**: Se debe desarrollar un plan de continuidad del negocio que identifique los sistemas críticos y defina los procedimientos para su recuperación ante desastres.
- **Plan de Recuperación ante Desastres (DRP)**: El DRP debe incluir pasos detallados para la restauración de sistemas críticos, con un enfoque en minimizar los tiempos de recuperación (RTO) y los puntos de recuperación (RPO).
- **Pruebas de Continuidad**: El plan de continuidad del negocio debe ser probado al menos dos veces al año mediante simulacros de desastres.

Medidas de Cumplimiento

- Simulacros anuales de recuperación ante desastres.
- Auditorías anuales del plan de continuidad y recuperación.
- Revisión y actualización continua del BCP y DRP.

- **Simulacros anuales de recuperación ante desastres:**

  - **Indicador de cumplimiento:** Porcentaje de simulacros realizados dentro del calendario anual establecido.
  - **Meta mínima: 100% de los simulacros anuales planificados deben ejecutarse.**
  - **Verificación:**
    - Registro detallado de simulacros, incluyendo:
      - Fecha y hora de ejecución.
      - Sistemas y procesos probados.
      - Tiempo de recuperación logrado en comparación con los objetivos de recuperación (RTO y RPO).
      - Brechas detectadas y acciones correctivas.
  - **KPI adicional:** Reducción del tiempo promedio de recuperación en cada simulacro.

- **Auditorías anuales del plan de continuidad y recuperación:**

  - **Indicador de cumplimiento:** Porcentaje de auditorías del plan de continuidad (BCP) y recuperación ante desastres (DRP) realizadas según el cronograma anual.
  - **Meta mínima: 100% de las auditorías programadas deben completarse anualmente.**
  - **Verificación:**

- Informes de auditoría que evalúen:
  - Actualización de los planes.
  - Eficiencia de los procedimientos descritos.
  - Conformidad con estándares regulatorios y mejores prácticas.
- Registro de acciones correctivas implementadas tras la auditoría.

- **Revisión y actualización continua del BCP y DRP:**

- **Indicador de cumplimiento:** Porcentaje de revisiones y actualizaciones realizadas en comparación con los cambios detectados en el entorno tecnológico, operativo o regulatorio.
- **Meta mínima: 95% de los cambios relevantes deben reflejarse en actualizaciones del BCP y DRP en un plazo máximo de 30 días.**
- **Verificación:**
  - Registro de revisiones realizadas, con detalle de las áreas modificadas, responsables y fecha de aprobación.
  - Incorporación de lecciones aprendidas tras simulacros, auditorías y eventos reales.
- **KPI adicional:** Aumento en la eficacia de los planes medido por la mejora en los tiempos y calidad de recuperación.

4.5 Política de Gestión de Vulnerabilidades

Objetivo

Establecer un proceso continuo para la identificación, evaluación y mitigación de vulnerabilidades en los sistemas del Data Center.

Alcance

Aplica a todos los sistemas de TI, incluyendo hardware, software y redes.

Políticas

- **Escaneos Regulares de Vulnerabilidades**: Se realizarán escaneos mensuales con herramientas como **Nessus** y **OpenVAS** para identificar vulnerabilidades en los sistemas críticos.
- **Gestión de Parches**: Los parches de seguridad deben ser aplicados de manera oportuna, según las directrices de seguridad y los resultados de los escaneos.
- **Priorización de Vulnerabilidades**: Las vulnerabilidades deben priorizarse según su criticidad, basándose en el impacto potencial y la probabilidad de explotación.

Medidas de Cumplimiento

- Auditoría trimestral de vulnerabilidades detectadas y mitigadas.
- Verificación periódica de la aplicación de parches de seguridad.
- Revisión y actualización anual de las políticas de gestión de vulnerabilidades.

4.6 Política de Seguridad Física

Objetivo

Proteger el acceso físico a las instalaciones del Data Center para evitar el acceso no autorizado y la manipulación física de los activos.

Alcance

Aplica a todos los puntos de acceso al Data Center y las áreas que contienen equipos críticos.

Políticas

- **Control de Acceso Biométrico**: Todo acceso al Data Center debe ser controlado mediante autenticación biométrica combinada con tarjetas de proximidad.
- **Monitorización 24/7**: Cámaras de vigilancia y sistemas de monitoreo deben estar operativos las 24 horas del día, con almacenamiento de grabaciones por un mínimo de 90 días.
- **Sistemas de Seguridad Redundantes**: Se deben implementar sistemas de detección de intrusos y alarmas contra incendios y otras amenazas físicas.

Medidas de Cumplimiento

- **Auditoría semestral de la seguridad física:**

- **Indicador de cumplimiento:** Porcentaje de auditorías de seguridad física completadas según el cronograma semestral.
- **Meta mínima: 100% de las auditorías planificadas deben realizarse semestralmente.**
- **Verificación:**
    - Informes detallados de auditoría que incluyan:
        - Evaluación de puntos de acceso, sistemas biométricos y controles de acceso.
        - Identificación de vulnerabilidades físicas y plan de mitigación.
        - Acciones correctivas implementadas y su estado de cumplimiento.

- **Pruebas periódicas de los sistemas de seguridad física, incluidas las alarmas y cámaras:**

  - **Indicador de cumplimiento:** Porcentaje de sistemas críticos (alarmas, cámaras, controles de acceso) probados dentro del plazo establecido.
  - **Meta mínima: 95% de los sistemas de seguridad deben ser probados trimestralmente para garantizar su operatividad.**
  - **Verificación:**
    - Registro de pruebas realizadas, con detalle de:
      - Fecha y hora de ejecución.
      - Sistemas probados y resultados de las pruebas.
      - Fallos detectados y tiempo promedio de resolución.
  - **KPI adicional:** Reducción del tiempo de inactividad de los sistemas de seguridad tras la identificación de fallos.

5. Cumplimiento y Auditoría

El cumplimiento de estas políticas será revisado mediante auditorías internas y externas periódicas. El **Departamento de Seguridad** será responsable de llevar a cabo auditorías anuales y pruebas regulares de cumplimiento para garantizar que estas políticas se implementen y sigan adecuadamente.

6. Revisión y Actualización

Este manual será revisado de manera anual, o cuando sea necesario debido a cambios en el entorno tecnológico o regulatorio. Cualquier modificación deberá ser aprobada por la **Alta Dirección** y comunicada a todo el personal relevante.

CONCLUSIONES

- La aplicación de la metodología NIST SP 800-30 en el data center permitió identificar y priorizar los riesgos más críticos asociados a la infraestructura tecnológica. Este enfoque integral de gestión de riesgos ha sentado las bases para una mejora significativa en la seguridad operativa, logrando mitigar amenazas tanto internas como externas de manera estratégica.
- Los activos clave, como enrutadores de borde, servidores de almacenamiento y sistemas eléctricos redundantes, fueron reconocidos como esenciales para la continuidad del negocio. La protección adecuada de estos elementos críticos, a través de medidas técnicas y organizativas, ha demostrado reducir significativamente el impacto de fallos o ataques. Según análisis comparativos con estudios similares, la seguridad del data center se estimaba en un 65% antes de la implementación del plan de seguridad, aumentando hasta un 90% tras la aplicación de las estrategias propuestas.
- Herramientas avanzadas como Nessus, OpenVAS y honeynet desempeñaron un papel fundamental en la detección de vulnerabilidades, proporcionando información técnica precisa para diseñar medidas específicas. Este análisis técnico se complementó con encuestas y entrevistas al personal, lo que permitió identificar áreas de mejora en las prácticas operativas y promover una cultura organizacional orientada a la seguridad.
- La implementación de estrategias como un data center espejo y mejoras en la redundancia de equipos destacan como soluciones críticas para garantizar la resiliencia frente a desastres naturales y fallos técnicos. Estas acciones no solo aseguran la continuidad operativa, sino que también aumentan la confianza en la infraestructura tecnológica.

- Finalmente, se concluye que las medidas técnicas deben ser respaldadas por programas de capacitación continua para el personal y políticas de seguridad claras. Esto fomenta la prevención y asegura una respuesta oportuna y efectiva ante incidentes, consolidando un entorno seguro y confiable en un panorama de amenazas en constante evolución.

RECOMENDACIONES

- Se recomienda realizar mejoras estructurales en el Data Center**,** tales como sistemas avanzados de protección contra incendios, instalación de mecanismos de drenaje ante inundaciones, y medidas de resistencia ante desastres naturales. Además, es imperativo implementar un mantenimiento preventivo continuo para el hardware crítico, asegurando la disponibilidad constante de los servicios.
- Se sugiere la implementación de sistemas avanzados de detección y respuesta a incidentes (IDS/IPS) y la capacitación constante del personal en prácticas de ciberseguridad. La creación de un Data Center espejo permitirá la replicación en tiempo real de los datos, garantizando la continuidad operativa incluso ante ataques o fallos graves, mejorando así la resiliencia ante ciberataques.
- Es crucial actualizar las políticas de seguridad para que cubran todos los aspectos operativos del Data Center, desde la gestión de accesos hasta la protección de datos sensibles. Además, se deben formalizar procedimientos claros para la recuperación ante desastres (DRP) y la continuidad del negocio (BCP), probándolos regularmente mediante simulacros semestrales para garantizar su efectividad y realizar ajustes necesarios.
- Para asegurar la efectividad del plan a largo plazo**,** es necesario implementar un sistema robusto de monitoreo, basado en KPIs como el Tiempo Medio para Detectar (MTTD) y el Tiempo Medio para Responder (MTTR) a incidentes. Además, se recomienda realizar auditorías de seguridad y evaluaciones de vulnerabilidades periódicas, con el fin de identificar áreas de mejora y ajustar el plan de seguridad ante nuevas amenazas y tecnologías emergentes.

REFERENCIAS

Asamblea Nacional. (2011). *CONSTITUCION DE LA REPUBLICA DEL ECUADOR 2008 Decreto Legislativo 0 Registro Oficial*. www.lexis.com.ec

Asamblea Nacional. (2021). *LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES*. www.lexis.com.ec

Benalcázar Gladys. (2019). *Implementación de una infraestructura de IT virtual para el data center de la facultad de ingeniería en Ciencias Aplicadas, en la Universidad Técnica del Norte*. http://repositorio.utn.edu.ec/handle/123456789/9560

Blank, R. M., & Gallagher, P. D. (2012). *Guide for conducting risk assessments*. https://doi.org/10.6028/NIST.SP.800-30r1

Cauja Altamirano, M. J. (2024). *Metodología de un sistema DLP (Data Loss Prevention) para la entidad financiera "Cooperativa de Ahorro y Crédito Santa Anita Ltda." basada en la norma ISO/IEC 27002:2022, sección 5.12 y 8.12*. https://repositorio.utn.edu.ec/handle/123456789/15625

Cisco. (2023). *¿Qué es un centro de datos? - Cisco*. https://www.cisco.com/c/es_mx/solutions/data-center-virtualization/what-is-a-data-center.html

COIP. (2021). *CÓDIGO ORGÁNICO INTEGRAL PENAL*. https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

Congreso Nacional. (2018). *LEY DE COMERCIO ELECTRONICO, FIRMAS Y MENSAJES DE DATOS*. www.lexis.com.ec

Figueroa, J., Rodriguez, R., Bone, C., & Saltos, J. (2017). *La seguridad informática y la seguridad de la información*. https://polodelconocimiento.com/ojs/index.php/es/article/view/420/pdf

Lawrence Andy. (2018). *Uptime Data*.

Li, Y. J., & Hoffman, E. (2023). Designing an incentive mechanism for information security policy compliance: An experiment. *Journal of Economic Behavior & Organization*, *212*, 138–159. https://doi.org/10.1016/J.JEBO.2023.05.033

Louis, B. (2018). *Targeted Attack Detection by Means of Free and Open Source Solutions*. https://www.researchgate.net/profile/Louis-Bernardo/publication/332409647_Targeted_Attack_Detection_by_Means_of_Free_and_Open_Source_Solutions/links/5cb79fc692851c8d22f2d838/Targeted-Attack-Detection-by-Means-of-Free-and-Open-Source-Solutions.pdf

MINTEL. (2021). *LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES*. https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

MINTEL. (2022). *Plan Estratégico Institucional*. https://www.telecomunicaciones.gob.ec/wp-content/uploads/2022/08/Plan-Estrategico-Institucional.pdf

Noheli, J., & Jiménez, M. (2021). *UNIVERSIDAD POLITÉCNICA SALESIANA SEDE GUAYAQUIL TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE: INGENIERA DE SISTEMAS CARRERA: INGENIERÍA DE SISTEMAS*.

Ramírez Castro, A., & Ortiz Bayona, Z. (2011). Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. *Ingeniería, ISSN-e 2344-8393, ISSN 0121-750X, Vol. 16, Nº. 2, 2011, Págs. 56-66*, *16*(2), 56–66. https://dialnet.unirioja.es/servlet/articulo?codigo=4797252&info=resumen&idioma=SPA

Ramon Hurtado, S. (2023). Implementación de un sistema de virtualización centralizado basado en PROXMOX para optimizar la gestión de recursos informáticos del Data Center del Gobierno Regional Pasco, 2022. *Universidad Nacional Daniel Alcides Carrión*. http://repositorio.undac.edu.pe/handle/undac/3325

Regina Baena, G., Mendoza Mendez, R. V., & Joel Coronado, E. dorantes. (2019). Importancia de la norma ISO/EIC 27000 en la implementación de un sistema de gestión de la seguridad de la información. *Contribuciones a La Economía*, *junio*.

Ruben, J., Yupanqui, A., & Oré, S. B. (2017). *Políticas de Seguridad de la Información: Revisión Sistemática de las Teorías que Explican su Cumplimiento*. *25*, 112. https://doi.org/10.17013/risti.25.112-134

Secretaría Nacional de Planificación. (2021). *Plan de Creación de Oportunidades 2021-2025* . https://www.planificacion.gob.ec/plan-de-creacion-de-oportunidades-2021-2025/

Supriyadi, Y., & Hardani, C. W. (2018). Information system risk scenario using COBIT 5 for risk and NIST SP 800-30 Rev. 1 a case study. *Proceedings - 2018 3rd International*

Conference on Information Technology, Information Systems and Electrical Engineering, ICITISEE 2018, 287–291. https://doi.org/10.1109/ICITISEE.2018.8721034

Torres, G. (2015). *Estudio comparativo entre las metodologías MAGERIT y CRAMM, utilizadas para Análisis y Gestión de Riesgos de Seguridad de la Información*.

Vmware. (2023). *¿Qué es la seguridad del centro de datos? | Glosario de VMware | ES*. https://www.vmware.com/es/topics/glossary/content/data-center-security.html

ANEXOS

ANEXO A Entrevista levantamiento de información

	UNIVERSIDAD TÉCNICA DEL NORTE **CARRERA DE INGENIERÍA EN TELECOMUNICACIONES**
PROYECTO: PLAN DE SEGURIDAD PARA LA GESTIÓN DE RIESGOS UTILIZANDO METODOLOGÍA NIST SP 800-30 PARA EL DATA CENTER DE LA EMPRESA AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A.	
Fecha de Realización:	15/04/2024
Organización:	AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A.
Encuestado/a:	**Carlos Andrés Benavides**
Cargo:	**Jefe de Networking**

INTRODUCCIÓN

La siguiente entrevista pretende obtener los datos necesarios sobre la infraestructura tecnológica y la gestión de riesgos en el Data Center de AirmaxTelecom Soluciones Tecnológicas S.A. Esta información es crucial para completar la evaluación de riesgos y fortalecer la seguridad del data center.

Objetivo: Obtener información detallada sobre la infraestructura tecnológica actual y las prácticas de gestión de riesgos en el Data Center de AirmaxTelecom Soluciones Tecnológicas S.A.

Información General

1. ¿Qué tipos de servicios se proporcionan desde el Data Center?
2. ¿Cuántas personas trabajan en la operación y mantenimiento del Data Center?

Infraestructura Física y Tecnológica

4. ¿Cuáles son los principales equipos de red utilizados en el Data Center? (Marcas y modelos)
5. ¿Qué tipo de sistemas de refrigeración se utilizan en el Data Center?

6. ¿Existen sistemas de energía de respaldo y protección contra fallos eléctricos? Detalle las especificaciones.

Gestión de Hardware y Mantenimiento

7. ¿Cuál es el procedimiento para la adquisición y renovación de hardware en el Data Center?
8. ¿Con qué frecuencia se realizan auditorías de hardware y software?

Seguridad Cibernética

9. ¿Qué tipos de firewalls y sistemas IDS/IPS están implementados en el Data Center?
10. ¿Se realizan pruebas de penetración periódicas? ¿Con qué frecuencia?
11. ¿Qué soluciones de software de seguridad están desplegadas (antivirus, antimalware, acls, iptables, vlans, etc.)?

Gestión de Datos y Políticas de Seguridad

12. ¿Qué políticas existen para el manejo y almacenamiento de datos sensibles
13. ¿Cómo se maneja la encriptación de datos en tránsito y en reposo?

Evaluación y Gestión de Riesgos

14. ¿Se han desarrollado capacitaciones sobre la gestión de riesgos y seguridad de TI para el personal? Describa brevemente

Cumplimiento y Obligaciones Legales

15. ¿Cómo se asegura el cumplimiento de las normativas y estándares internacionales de seguridad?

ANEXO B Encuesta para levantamiento de información

	UNIVERSIDAD TÉCNICA DEL NORTE **CARRERA DE INGENIERÍA EN TELECOMUNICACIONES**
PROYECTO: PLAN DE SEGURIDAD PARA LA GESTIÓN DE RIESGOS UTILIZANDO METODOLOGÍA NIST SP 800-30 PARA EL DATA CENTER DE LA EMPRESA AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A.	
Fecha de Realización:	15/04/2024
Organización:	AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A.
Encuestado/a:	**Carlos Andrés Benavides**
Cargo:	**Jefe de Networking**

INTRODUCCIÓN

La siguiente entrevista pretende obtener los datos necesarios sobre la infraestructura tecnológica y la gestión de riesgos en el Data Center de AirmaxTelecom Soluciones Tecnológicas S.A. Esta información es crucial para completar la evaluación de riesgos y fortalecer la seguridad del data center.

Objetivo: Obtener información detallada sobre la infraestructura tecnológica actual y las prácticas de gestión de riesgos en el Data Center de AirmaxTelecom Soluciones Tecnológicas S.A.

Información General

3. **¿Qué tipos de servicios se proporcionan desde el Data Center?**
4. **¿Cuántas personas trabajan en la operación y mantenimiento del Data Center?**

Infraestructura Física y Tecnológica

7. **¿Cuáles son los principales equipos de red utilizados en el Data Center? (Marcas y modelos)**
8. **¿Qué tipo de sistemas de refrigeración se utilizan en el Data Center?**

9. **¿Existen sistemas de energía de respaldo y protección contra fallos eléctricos? Detalle las especificaciones.**

Gestión de Hardware y Mantenimiento

9. ¿Cuál es el procedimiento para la adquisición y renovación de hardware en el Data Center?

10. ¿Con qué frecuencia se realizan auditorías de hardware y software?

Seguridad Cibernética

12. ¿Qué tipos de firewalls y sistemas IDS/IPS están implementados en el Data Center?

13. ¿Se realizan pruebas de penetración periódicas? ¿Con qué frecuencia?

14. ¿Qué soluciones de software de seguridad están desplegadas (antivirus, antimalware, acls, iptables, vlans, etc.)?

Gestión de Datos y Políticas de Seguridad

14. ¿Qué políticas existen para el manejo y almacenamiento de datos sensibles?

15. ¿Cómo se maneja la encriptación de datos en tránsito y en reposo?

Evaluación y Gestión de Riesgos

15. ¿Se han desarrollado capacitaciones sobre la gestión de riesgos y seguridad de TI para el personal? Describa brevemente.

Cumplimiento y Obligaciones Legales

16. ¿Cómo se asegura el cumplimiento de las normativas y estándares internacionales de seguridad?

AIRMAXTELECOM

SOLUCIONES TECNOLÓGICAS S.A.

MANUAL DE INSTALACIÓN
HERRAMIENTAS NESSUS Y OPENVAS

ANEXO C Manual de Instalación de Nessus y OpenVAS en Kali Linux Virtualizado en VirtualBox

Índice

1. Preparativos

Instalación de Kali Linux en VirtualBox

Paso 1: Descargue e instale VirtualBox desde el sitio web oficial.

Paso 2: Descargue la imagen ISO de Kali Linux desde el sitio web oficial.

Paso 3: Cree una nueva máquina virtual en VirtualBox:

- Asigne un nombre y seleccione "Linux" como tipo y "Debian (64-bit)" como versión.
- Asigne al menos 2 GB de RAM y 20 GB de espacio en disco

Paso 4: Monte la imagen ISO de Kali Linux y comience la instalación. Siga las instrucciones en pantalla para completar la instalación.

Configuración de la máquina virtual

Paso 5: Después de instalar Kali Linux, inicie la máquina virtual y asegúrese de que tenga acceso a internet. Puede hacerlo configurando la red de la máquina virtual en "NAT" o "Bridged Adapter".

2. Instalación de Nessus

Requisitos previos

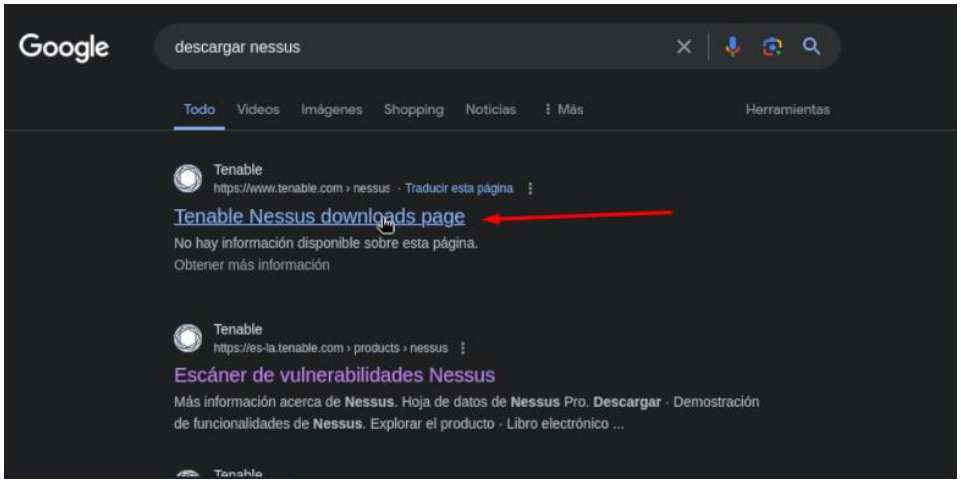
- Kali Linux instalado y actualizado
- Acceso a internet
- Privilegios de root

Descarga e instalación

Paso 1: Descargar Nessus desde el sitio web oficial de Tenable ingresando al navegador de la máquina Kali Linux.

Figura 1

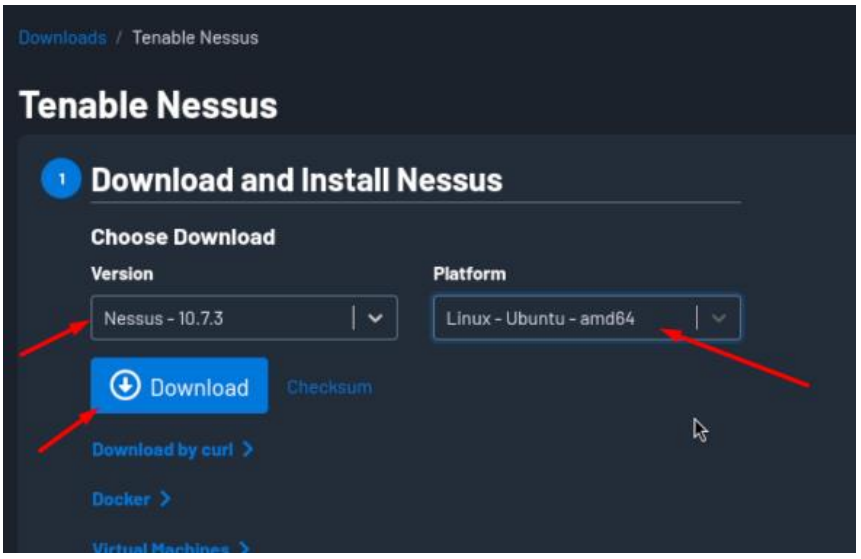
Sitio Web de Nessus



Paso 2: Seleccionar la versión de Nessus y la plataforma Linux Ubuntu amd64

Figura 2

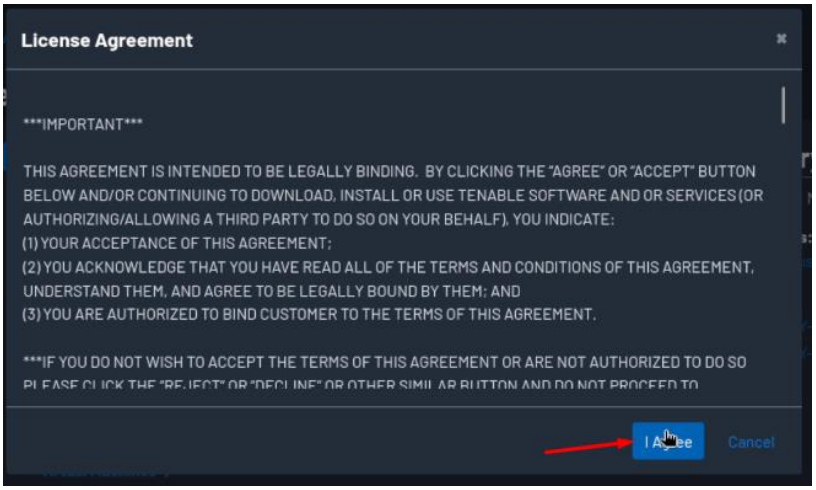
Descarga Nessus para Linux



Paso 3: Aceptar los términos y condiciones para empezar con la descarga.

Figura 3

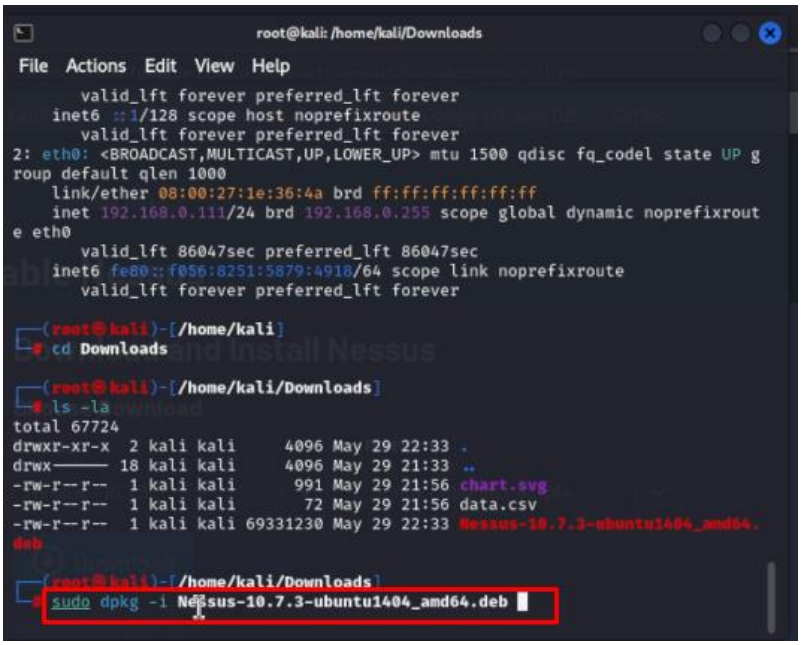
Términos y Condiciones



Paso 4: Instalar el paquete descargado abriendo un terminal y dirigiéndose a la carpeta en donde se encuentra el archivo descargado. Una vez en la carpeta utilice el comando sudo dpkg -i con el nombre del archivo descargado.

Figura 4

Comando para instalar Nessus desde la carpeta de descargas.



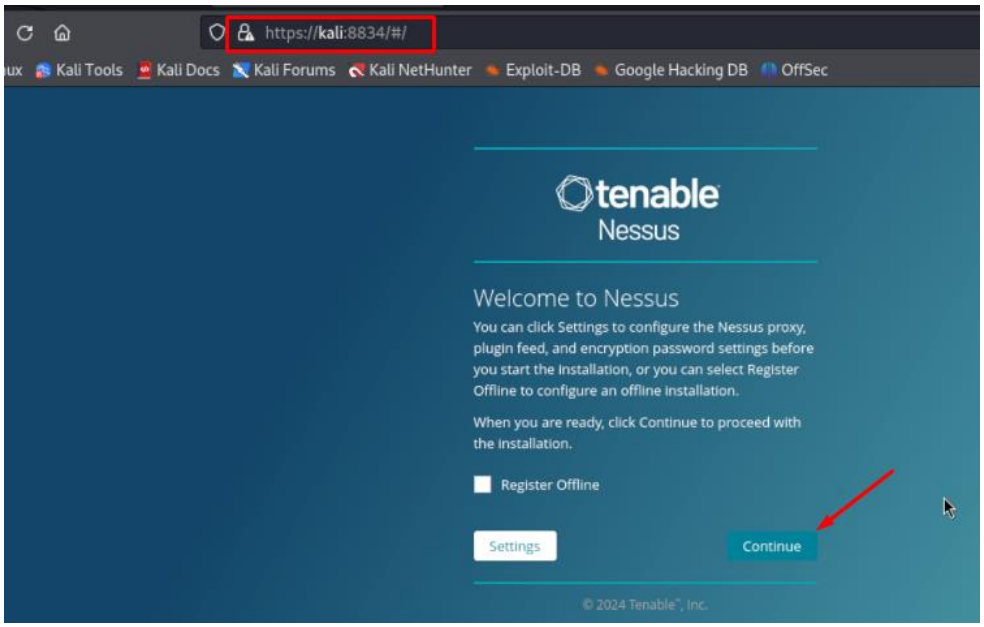
Paso 5: Verificar e Iniciar el servicio de Nessus con los comandos systemctl status Nessus.d y systemctl start Nessus.d

Configuración inicial

Paso 6: Dirigirse al navegador dentro de Kali y digitar https://localhost:8834 para acceder a la interfaz web de Nessus.

Figura 5

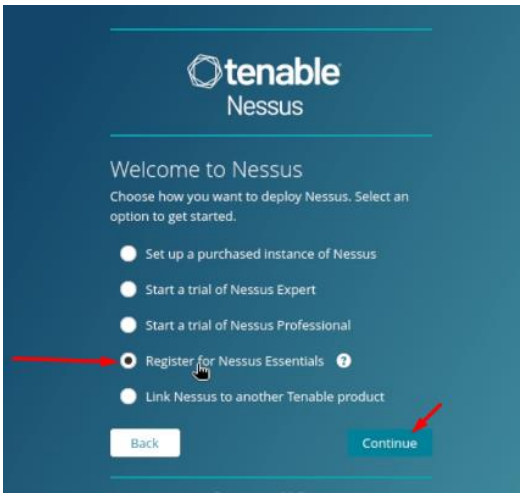
Nessus abierto a través del navegador web usando https://localhost:8834.



Paso 7: Seleccionar el botón continuar como se muestra en la figura 7 y realizar el registro para Nessus essentials.

Figura 6

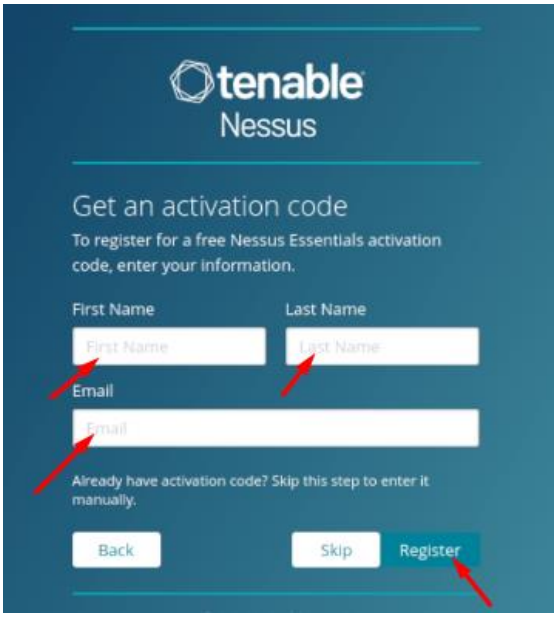
Registro para Nessus Essentials.



Paso 8: Configurar para crear una cuenta con usuario, contraseña y una dirección de correo para acceder a la interfaz de Nessus.

Figura 7

Registro usuario, contraseña y correo.

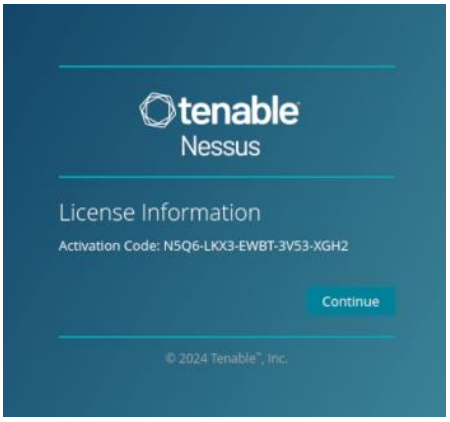


Activación y actualización

Paso 9: Copiar la clave de activación proporcionada por Tenable en caso de que se requiera para algún paso posterior.

Figura 8

Código de activación



Paso 10: Crear un usuario y una contraseña para acceder a Nessus

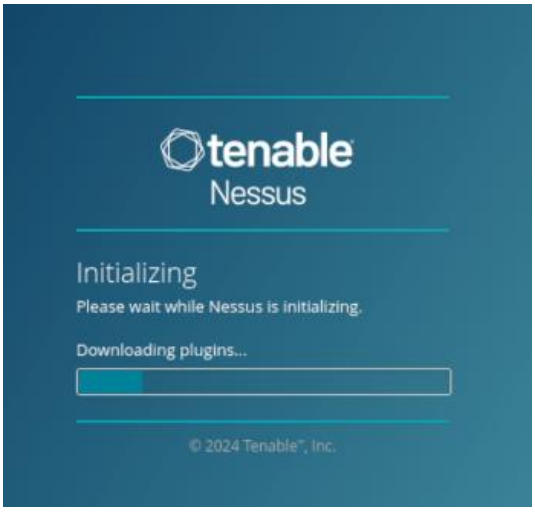
Figura 9

Creación de Usuario y Contraseña

Paso 11: Esperar mientras se actualizan los plugins para asegurar que Nessus tenga las últimas definiciones de vulnerabilidades.

Figura 10

Proceso de descarga de plugins

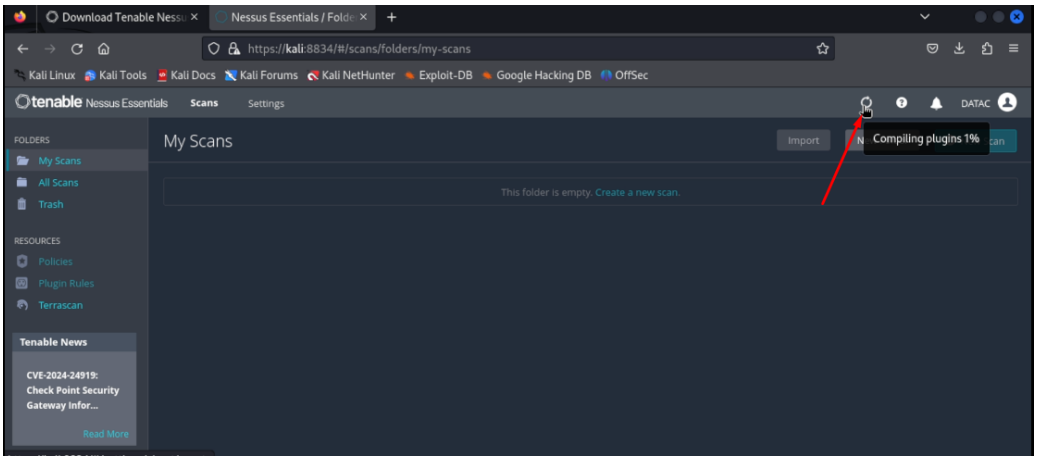


Realización del primer escaneo

Paso 12: Una vez se inicia esperar a que se compilen todos los plugins al 100%

Figura 11

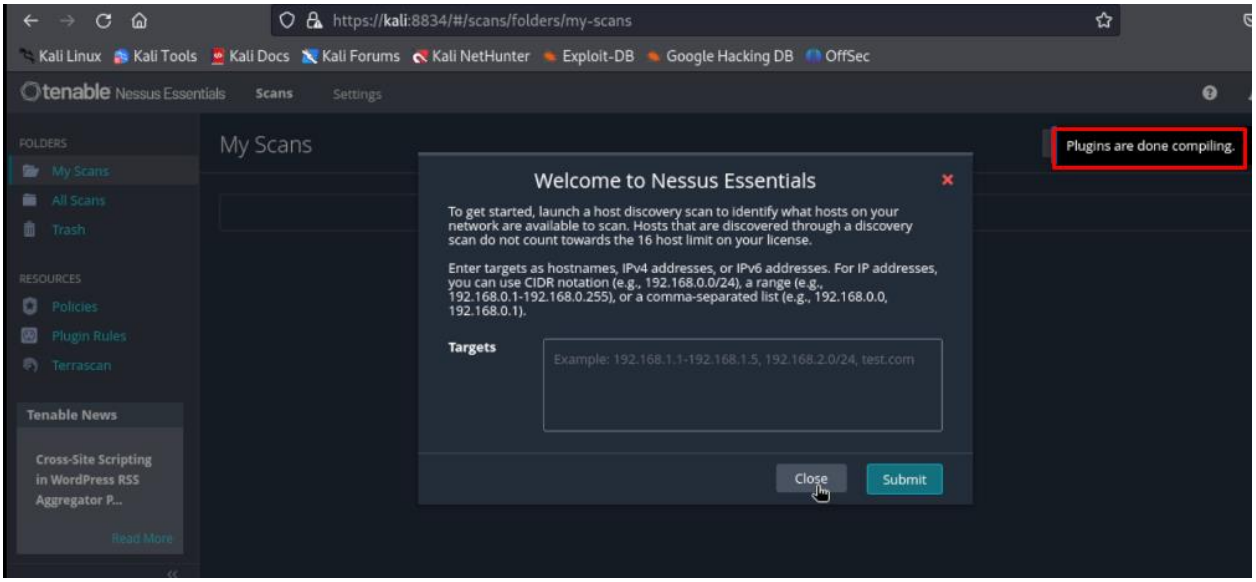
Proceso de compilación de plugins.



Paso 13: Cuando se complete el paso anterior ya se puede ejecutar un escaneo a la red y revisar los resultados una vez completado.

Figura 12

Interfaz de Nessus una vez se compilan todos los plugins



3. Instalación de OpenVAS

Requisitos previos

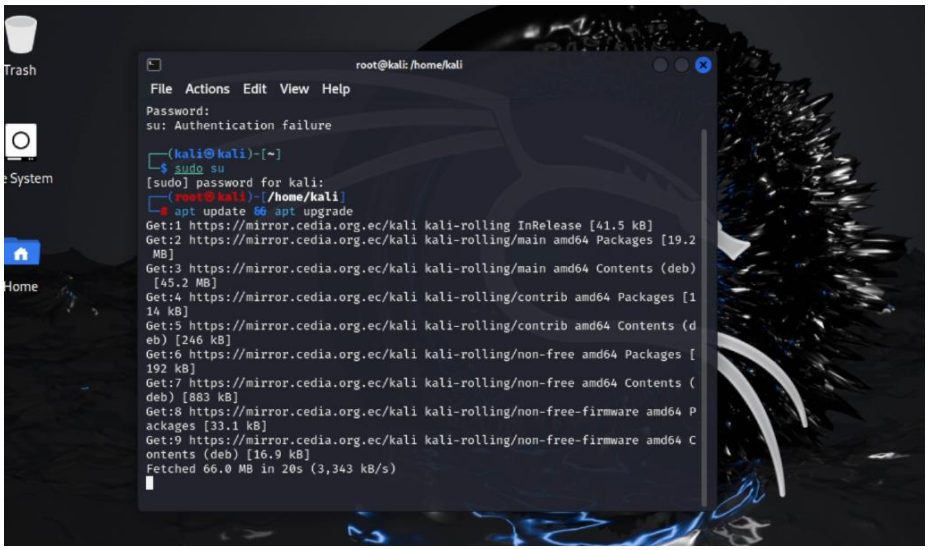
- Kali Linux instalado y actualizado
- Acceso a internet
- Privilegios de root

Descarga e instalación

Paso 1: Actualizar los repositorios del sistema con los comandos sudo apt update && upgrade

Figura 13

Actualización del sistema



Paso 2: Instalar OpenVAS usando el siguiente comando: apt install openvas

Figura 14

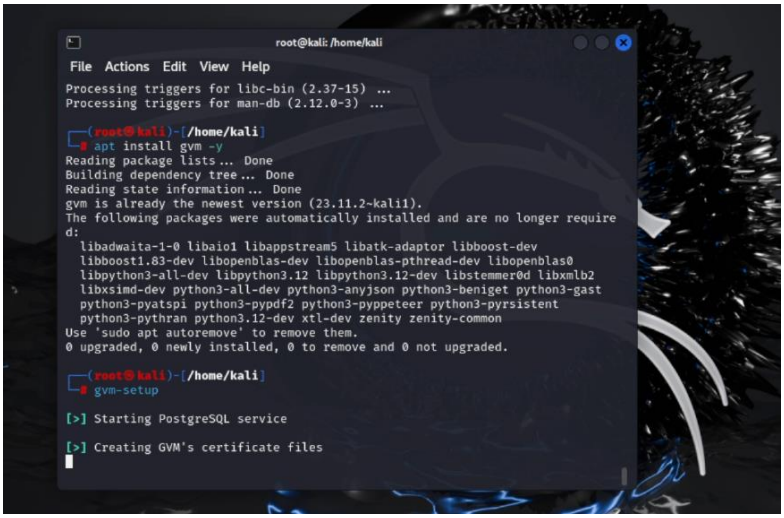
Proceso de instalación Openvas

Configuración inicial

Paso 3: Instalar Greenbone Vulnerability Management (GVM) – Pieza intermedia entre OpenVAS y la interfaz web que gestiona la configuración y los resultados de los escaneos. Usando el siguiente comando: apt install gvm -y, y para iniciar el servicio digitar gvm-setup.

Figura 15

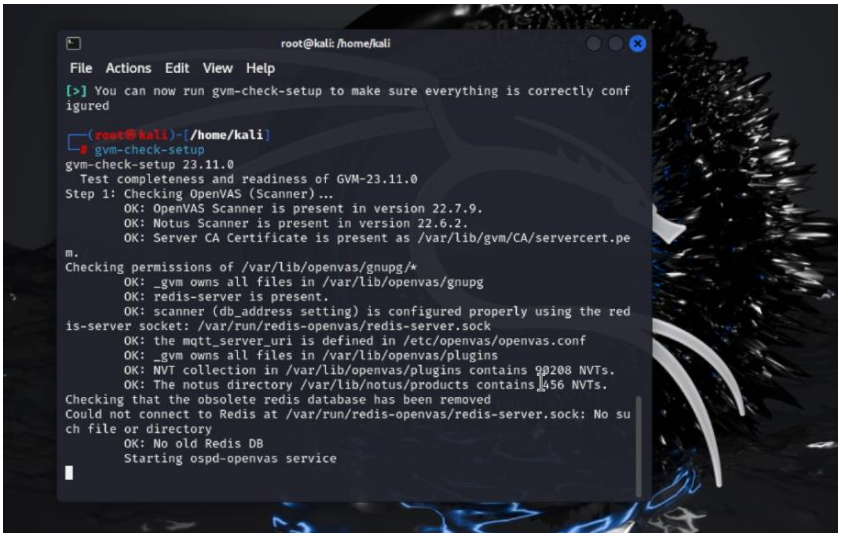
Instalación e Inicio de GVM



Paso 4: Verificar la instalación de gvm con el siguiente comando gvm-check-stup

Figura 16

Verificación completada de GVM



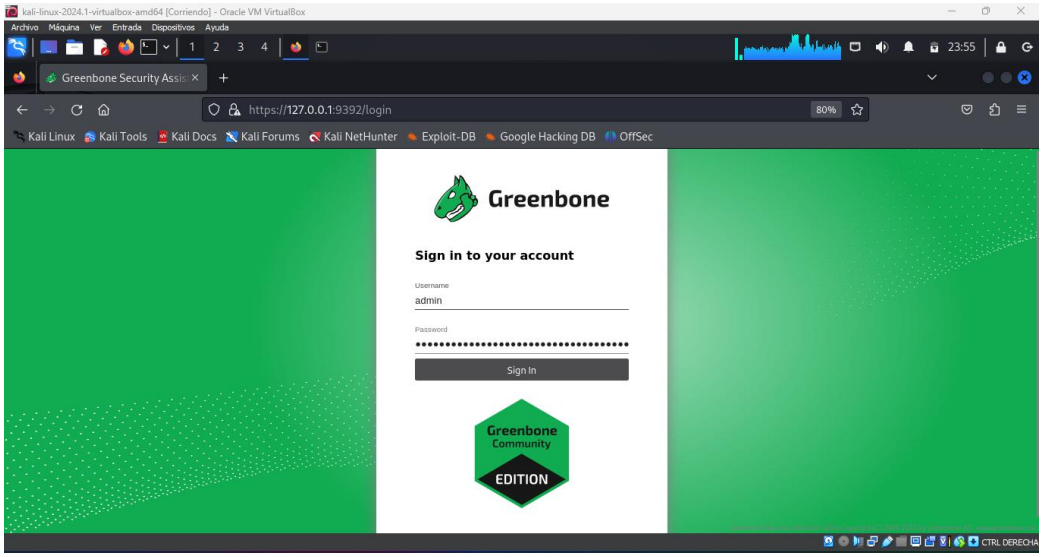
Paso 6: Una vez se verifican todos los pasos sin errores la instalación ha sido completada y se puede acceder a su interfaz gráfica desde el navegador.

Realización del primer escaneo

Paso 7: Acceder a la interfaz web de OpenVAS usando https://localhost:9392, ingresar el usuario y contraseña que viene por defecto para administrador.

Figura 17

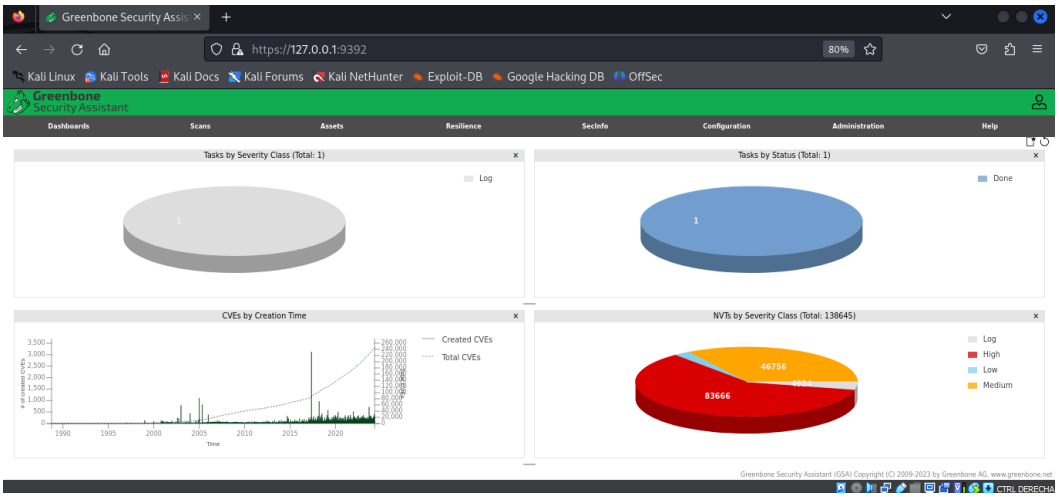
Interfaz Web Nessus.



Paso 7: Crear un nuevo escaneo y configurar los parámetros necesarios para poder utilizar OpenVAS.

Figura 18

Pantalla principal OpenVAS



Paso 8: Ejecutar el escaneo y revisar los resultados una vez completados.