Evaluación de soluciones de ciberseguridad como directrices para el aseguramiento de almacenamientos NAS y SAN

Carlos Andrés Novoa Pajarito

Asesor

Edgar Mauricio López Rojas

Universidad Nacional Abierta Y A Distancia – UNAD

Escuela De Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización En Seguridad Informática

2025

Dedicatoria

Dedico esta monografía a Dios, a mi madre y a mi esposa quienes me apoyaron y entendieron en todos los sentidos; a mis maestros, cuyos conocimientos me brindaron las herramientas para mi desarrollo personal, sin quienes mi desarrollo profesional hubiera sido imposible.

Agradecimientos

Me gustaría agradecer a los profesores de la Universidad Nacional Abierta y a Distancia por sus conocimientos, habilidades y lo más importante su paciencia al guiarme en el camino correcto para adquirir conocimientos, permitiéndome crecer profesionalmente.

Resumen

La creciente adopción de soluciones de almacenamiento en la nube y virtualización ha generado nuevos retos en el ámbito de la ciberseguridad. A pesar de estas innovaciones, la necesidad de contar con sistemas de almacenamiento locales de alta velocidad, como NAS y SAN, sigue siendo fundamental. Esto ha llevado a la implementación de estrategias de seguridad más robustas para proteger la información crítica y garantizar la continuidad de los servicios.

Por lo tanto, es importante comprender la importancia de estos dispositivos de almacenamiento y las posibles repercusiones si se ven comprometidos que va desde el robo de datos hasta la pérdida de un servicio administrado, teniendo en cuenta que además de almacenar información también se encuentran implementados entornos virtuales y su administración se debe realizar de una manera precavida para evitar accesos no autorizados a algún sistema, esto se logra mediante implementación de medidas y políticas de seguridad que nos permitan salvaguardar dicho elementos.

Esto también se debe complementar mediante la implementación adecuada de una infraestructura segura que garantice la disponibilidad, integridad y confidencialidad de la información y permita el flujo seguro de la información sin afectar los dispositivos activos de la red que transmiten la información y servicios de una compañía.

Al reconocer los riesgos se pretende obtener una mejora significativa en la protección de datos y servicios críticos garantizando su disponibilidad, integridad y confidencialidad mediante el adecuado manejo y mitigación de los riesgos identificados.

Palabras clave: Almacenamiento local, ciberseguridad, NAS, SAN, virtualización.

Abstract

The increasing adoption of cloud storage and virtualization solutions has created new challenges in the field of cybersecurity. Despite these innovations, the need for high-speed local storage systems, such as NAS and SAN, remains essential. This has led to the implementation of more robust security strategies to protect critical information and ensure the continuity of services.

Therefore, it is important to understand the importance of these storage devices and the possible repercussions if they are compromised, ranging from data theft to the loss of a managed service, taking into account that in addition to storing information, environments are also implemented. virtual and their administration must be carried out in a cautious manner to avoid unauthorized access to any system. This is achieved through the implementation of security measures and policies that allow us to safeguard said elements.

This must also be complemented by the proper implementation of a secure infrastructure that guarantees the availability, integrity and confidentiality of information and allows the secure flow of information without affecting the active network devices that transmit a company's information and services.

By recognizing risks, the goal is to significantly improve the protection of critical data and services, ensuring their availability, integrity, and confidentiality through appropriate management and mitigation of identified risks.

Keywords: Local storage, Cybersecurity, NAS, SAN, Virtualization.

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Lista de Apéndices

Introducción

Esta monografía se llevó a cabo para analizar en profundidad los distintos riesgos asociados al uso de sistemas de almacenamiento NAS y SAN, así como las estrategias para mitigar posibles ataques que pongan en peligro la información almacenada y los servicios que dependen de ellos. A través de la identificación de medidas de mejora, se busca prevenir la indisponibilidad de los datos y servicios, al mismo tiempo que se pretende detectar vulnerabilidades en la infraestructura que soporta estos sistemas y en las redes por las cuales se transmiten la información y las comunicaciones dirigidas a los clientes, tanto internos como externos.

En la actualidad, numerosas organizaciones han enfrentado incidentes relacionados con accesos no autorizados a sus sistemas de almacenamiento central. Un ejemplo destacado es el caso de la empresa IFX, donde se vulneró el almacenamiento que albergaba sus máquinas virtuales, lo que resultó en la interrupción de sus servicios debido a un presunto ataque de ransomware. Este tipo de situaciones podría haberse prevenido mediante la aplicación oportuna de actualizaciones y parches de seguridad, los cuales habrían reducido las vulnerabilidades existentes. Asimismo, la implementación de herramientas de monitoreo de red habría permitido detectar actividades sospechosas o movimientos inusuales, contribuyendo a una respuesta más rápida y efectiva ante posibles amenazas.

Esto se alcanzará mediante la creación y aplicación de políticas de seguridad integrales, dirigidas tanto al ámbito de TI como a los usuarios estándar. Estas políticas deberán abarcar todas las áreas de la empresa, promoviendo el uso de buenas prácticas y fomentando una cultura de prevención entre los empleados. Esto incluye, por ejemplo, educar a los usuarios para

identificar y manejar adecuadamente correos electrónicos sospechosos provenientes de dominios desconocidos, con el fin de reducir riesgos y fortalecer la protección general de la organización.

Planteamiento del Problema

Los ciberdelincuentes han evolucionado en la creación de ransomware diseñados para infiltrarse en todas las capas de almacenamiento de las organizaciones, incluyendo los sistemas NAS y SAN, lo que ha ocasionado graves consecuencias para numerosas empresas, estos ataques pueden pasar desapercibidos, ya que el malware se oculta en diversos tipos de archivos y opera de manera similar a un troyano, ante esta creciente amenaza, muchas organizaciones están fortaleciendo sus defensas mediante la implementación de soluciones integrales, que contemplen tanto el software como el hardware, con el objetivo de reforzar su protección y reducir la vulnerabilidad frente a los ataques de ransomware.

Por lo cual es necesario un plantear un interrogante muy importante, ¿De qué manera pueden las organizaciones optimizar sus soluciones de almacenamiento y respaldo para reducir la vulnerabilidad y mitigar el impacto de los ataques de ransomware en sus sistemas NAS y SAN? en base a esta pregunta se pretenden buscar estrategias que garanticen la continuidad operativa de los servicios y la integridad de la información en entornos informáticos cada vez más expuestos a ciberataques.

En un estudio llevado a cabo por GigaOm, los especialistas en almacenamiento y seguridad destacaron el peligro que representa el ransomware para el almacenamiento de archivos, así como cómo las tecnologías emergentes pueden reducir este riesgo, además, señalaron que los ataques de ransomware pueden afectar tanto los sistemas de cifrado como los de almacenamiento de archivos, y muchos de estos ataques logran eludir las credenciales preconfiguradas del usuario y del sistema, lo que incrementa el riesgo de gestionar toda la infraestructura, el 88% de los ataques de ransomware durante el último año estuvieron dirigidos a los sistemas de almacenamiento de copias de seguridad, de los cuales el 75% tuvo éxito, más

alarmante aún, el 44% de estos ataques fueron provocados por errores humanos, como la apertura de correos electrónicos maliciosos o el clic en enlaces que los atacantes utilizan para acceder al sistema, se estima que los ataques de ransomware tienen un impacto económico de 50.000 millones de dólares, lo que resalta la importancia de mitigar este tipo de ciberataques y tomar medidas eficaces para protegerse ante ellos, es fundamental contar con copias de seguridad de nuestros archivos en diferentes ubicaciones y actualizar y parchear el software que gestiona dichos almacenamientos (Redacción Data Center Market, 2022) .

La falta de soluciones de respaldo adecuadas puede afectar gravemente la continuidad de los servicios, especialmente en grandes empresas públicas y privadas., Juan Manuel Pascual, experto en ciberseguridad y CEO de Innovery, advierte que los informes sobre empresas que han sufrido bloqueos en sus sistemas revelan fallos en sus políticas y soluciones de continuidad de negocio, por lo tanto, las empresas deben afrontar nuevos desafíos al elegir soluciones de almacenamiento y respaldo que no solo respondan a las necesidades del mundo digital, sino que también garanticen la seguridad de la información frente a las amenazas de ransomware (Rentero, A.,2023, April 18).

Justificación

El propósito de esta monografía es comprender y destacar la importancia de proteger los dispositivos que almacenan nuestra información y servicios, ajustando todos los parámetros técnicos que podrían convertirse en puntos vulnerables para el ransomware o accesos no autorizados, lo que podría resultar en la pérdida del control y la gestión de nuestros servicios virtuales implementados.

Este objetivo solo se puede alcanzar mediante el diseño e implementación de infraestructuras seguras para nuestros sistemas de almacenamiento NAS y SAN, lo que nos permitirá proteger los activos más valiosos y no tangibles de una empresa como lo es la información, así como los servicios virtuales que allí se alojan. Si no se toman las medidas adecuadas para mitigar las posibles amenazas, podríamos ser víctimas de extorsiones para recuperar el acceso a nuestros datos, por esta razón, es crucial definir políticas y medidas de seguridad que minimicen las vulnerabilidades de nuestros sistemas de almacenamiento, a través de actualizaciones de software, instalación de parches del sistema operativo, configuración de autenticación en los servidores, entre otras; Comprender la importancia de tomar medidas preventivas nos ayudará a evitar poner en riesgo toda nuestra información. Este esfuerzo debe ser un trabajo conjunto de todas las áreas de la empresa, con la implementación de reuniones sobre ciberseguridad y la formación sobre ataques de ingeniería social, ya que, en muchos casos, estos representan un punto de entrada para los ciberdelincuentes.

No implementar medidas de seguridad adecuadas para prevenir el acceso y control de nuestros sistemas de almacenamiento NAS puede resultar en un gran impacto en la privacidad de los datos, tanto de los clientes internos y externos como de los datos empresariales, los cuales podrían ser comercializados de forma ilícita, de igual manera si no se protegen adecuadamente los servicios alojados en la arquitectura SAN, se puede generar una interrupción en la disponibilidad de los servicios proporcionados por la empresa, lo que afectaría su reputación y tendría un alto impacto económico, ya que se requeriría una reconstrucción de los servicios y la recuperación de la confianza de los clientes; Un claro ejemplo de esto fue el caso de IFX Networks, que sufrió un ciberataque de tipo ransomware que afectó la disponibilidad de los servidores virtuales y, por ende, varios de los servicios prestados a la república de Colombia, dicho ataque afectó a 34 entidades del estado, e incluso llegó a suspender los procesos judiciales y bloquear la carga de actas de defunción por parte de hospitales, impidiendo la entrega de los cuerpos a los familiares de los fallecidos, este ataque podría haberse evitado o, al menos, mitigado si se hubieran implementado las medidas adecuadas para abordar los riesgos a los que están expuestas las empresas, creando estrategias de ciberseguridad mediante análisis de riesgos, matrices y normativas, lo que permitiría obtener una visión clara de la situación actual de la empresa y, a partir de allí, desarrollar planes de acción que eliminen las amenazas a las que se pueden ver expuestas (Rentero, A, 2023, September 14).

Objetivos

Objetivo General

Establecer directrices esenciales para diseñar una infraestructura segura de almacenamiento NAS y SAN, garantizando su protección frente a posibles ataques cibernéticos y fortaleciendo la resiliencia de los sistemas.

Objetivos Específicos

Analizar las soluciones de almacenamiento SAN y NAS, identificando sus características, para evaluar su idoneidad en el aseguramiento de los datos, garantizando la integridad, disponibilidad y confidencialidad de la información en la organización.

Desarrollar configuraciones eficientes en sistemas de almacenamiento SAN Y NAS, así como el entorno de red que los soporta, y proponiendo mejoras que refuercen su protección frente a amenazas.

Diseñar una infraestructura tecnológica segura para los sistemas de almacenamiento SAN y NAS, identificando posibles vulnerabilidades y proponiendo soluciones de seguridad.

Marco Referencial

Antecedentes

Hoy en día, el almacenamiento ha experimentado un crecimiento exponencial y se ha convertido en un componente fundamental dentro de las empresas, especialmente a medida que el volumen de datos aumenta día a día; La seguridad, así como la privacidad de la información, se han vuelto aspectos cruciales para las organizaciones a medida que la economía global crece, los datos se multiplican, lo que obliga a los líderes de la industria y a los profesionales de IT a superar los límites de sus capacidades para mantenerse al día con la generación continua de información, (Media, D, 2023, February 8).

Gobernanza del Almacenamiento de Datos

Las organizaciones dependen en gran medida de los datos, el big data, los servicios y otros recursos que proporciona la información, lo que hace indispensable una gestión adecuada de estos elementos, allí surge la necesidad de establecer políticas claras de almacenamiento de datos, la gobernanza de los datos se encarga de gestionar su integridad, usabilidad, disponibilidad y seguridad, sin embargo gobernar el almacenamiento se está volviendo cada vez más complejo, ya que las organizaciones deben cumplir con un número creciente de regulaciones sobre el uso de la información y la privacidad de los datos, las iniciativas actuales de gobernanza del almacenamiento se han centrado en los datos estructurados, que se encuentran en bases de datos relacionales, no obstante también existen datos no estructurados y semiestructurados, lo que requiere el desarrollo de una solución integral para abordar todos estos tipos de información, (Media, D, 2023, February 8).

El desarrollo de una política de gobernanza de almacenamiento es el primer paso para establecer un entorno de almacenamiento seguro, sirviendo como base para definir los

procedimientos y políticas necesarios para el almacenamiento en la nube, la privacidad de la información, así como la protección y gestión de los datos. Por esta razón, es fundamental fomentar auditorías de seguridad, ya que ayudan a establecer controles sobre el uso de la información y políticas que refuerzan la seguridad informática, además estas auditorías permiten realizar análisis adecuados para tomar decisiones informadas, determinando el tipo de almacenamiento más adecuado para cada empresa.

Crecimiento del Almacenamiento en 17,8 %

Se proyecta que para el año 2030 el almacenamiento crezca un 17,8 %, impulsado por diversos factores como el uso de la inteligencia artificial, los servicios en la nube y la expansión de las empresas. Además, el Internet de las Cosas (IoT) ha jugado un papel fundamental. Según datos de Fortune Business Insights, el mercado del almacenamiento se valoró en 217.020 millones de dólares en 2022 y se estima que alcance los 247.320 millones en 2030, el creciente énfasis de las empresas en la seguridad, fiabilidad, confidencialidad de los datos y la necesidad de infraestructuras flexibles para adaptarse a su expansión han sido determinantes para impulsar este mercado. Asimismo, el uso del IoT ha generado volúmenes masivos de información, y el auge de industrias a gran escala como la bancaria, las entidades estatales, las financieras y el comercio electrónico han hecho imprescindible invertir en el almacenamiento y gestión de datos, (Fortune Business InsightsTM, 2023).

Nube Publica para Data Storage

Con la adopción del almacenamiento híbrido, las empresas han resaltado el uso de la nube pública por su escalabilidad. Según datos de Penteo, el 71 % de las organizaciones indica contar con un modelo de nube híbrida que combina la nube pública con infraestructura tradicional. Sin embargo, solo el 32 % utiliza la nube pública para aproximadamente el 10 % de

sus necesidades de almacenamiento\2 El notable crecimiento de la nube en los últimos años ha llevado a que, en la actualidad, el 64 % de las compañías implementen soluciones de almacenamiento de datos y respaldo mediante IaaS (infraestructura como servicio). Este enfoque combina las ventajas de un cloud híbrido —que ofrece escalabilidad y flexibilidad en consecuencia, se proyecta que la cantidad de datos a nivel mundial alcance los 8,9 ZB para el año 2024, (Media, D,2023, March 13).

Marco Conceptual

SAN

Almacenamiento a nivel de bloques, red dedicada, muy rápido, para servidores (Cisco, 2025).

2FA

Es un método de autenticación que requiere que los usuarios proporcionen exactamente dos factores de verificación para obtener acceso a un sitio web, aplicación o recurso. Este tipo de autenticación multifactor requiere al menos dos formas de identificación (Seguridad de Microsoft, 2025).

Amenazas Internas

Son aquellas amenazas de seguridad que se originan con usuarios autorizados, los cuales deliberadamente, intencionalmente o de manera accidental brindan acceso legítimo a los recursos de la compañía (IBM, 2021, July 19).

Ataque DDoS

Es el intento de un ciberdelincuente de congestionar el tráfico a una aplicación o destino mediante un gran número de solicitudes para saturar el flujo de información y generar indisponibilidad (IBM, 2024, August 20).

IaaS

Es un tipo de servicio en la nube que ofrece recursos bajo demanda y permite conmutar varios factores del servicio prestado, como almacenamiento, procesamiento, redes y virtualización mediante la nube (Google Cloud, 2025).

Malware

La palabra malware es de origen inglés y es una combinación de las palabras malicious y software. Se refiere a cualquier tipo de software o servicio diseñado para dañar el dispositivo en el que se almacena, instala o accede, ya sea una computadora, teléfono móvil u otro dispositivo (Yúbal Fernández, 2020, June 2).

MFA

Multi-factor authentication es una tecnología de seguridad que requiere múltiples métodos de autenticación con el objetivo de verificar la identidad de un usuario, combinando dos o más credenciales independientes (Colaborador de TechTarget, 2021).

NAS

Almacenamiento a nivel de archivos, conectado a red común, para compartir archivos fácilmente IBM. (2025, 6 de agosto).

Phishing

El phishing es una forma de ingeniería social que busca engañar o manipular al usuario para que entregue información a personas no autorizadas. Los atacantes se aprovechan de errores humanos y generan una sensación de urgencia, haciéndose pasar por alguien en quien la víctima confía (IBM, 2024, May 17).

Puerta Trasera

Es cualquier elemento informático que permite acceder a un sistema de forma remota, anónima y sin ser detectado. Esto se presenta mediante el uso de malware, el cual puede explotar vulnerabilidades del sistema (Gómez, 2023).

Ransomware

Tipo de malware utilizado para secuestrar la información. Si el dispositivo es comprometido, congela la pantalla y oculta los datos almacenados en el disco, exigiendo un pago para su liberación (Kaspersky, 2018).

SD-WAN

Permite la administración centralizada de los dispositivos de red en la nube, mejorando los costos operativos y la gestión de los recursos de red en múltiples ubicaciones casi de forma inmediata. También permite priorizar servicios específicos dentro del tráfico de red (Intel, 2025).

Marco Teórico

Marco de Seguridad para la Red de Área de Almacenamiento (SAN)

El uso del almacenamiento SAN sumado a los múltiples riesgos de ciberseguridad han resaltado la importancia de asegurar estos elementos , la subestimación de los riesgos de los almacenamientos sumado a la poca comunicación de uso de defensas ha generado una brecha de seguridad en el almacenamiento SAN, es importante reconocer que todas las compañías se enfrentan a riesgos, en cuanto más valiosos sean sus activos mayo serán los retos que enfrentaran en su ciberseguridad, por lo cual es importante gestionar adecuadamente los riesgos mas aun cuando estos sistemas de almacenamiento carecen por si solos de funciones de seguridad , por lo cual es importante analizar las posibles vulnerabilidades a los que pueden estar expuestos, en ese sentido un almacenamiento SAN es sensible a los riesgos debido a datos y servicios que almacena , unos de los riesgos a los cuales puede estar expuesta una SAN es un ataque de hombre en el medio donde un tercero no confiable intercepta la comunicación entre dos nodos confiables , para poder asegurar la SAN ante este tipo de vulnerabilidades es necesario el uso del protocolo DH-CHAP el cual permite la autenticación por intercambio de claves ya sea de conmutador a conmutador o de host a conmutador basada en algoritmos como lo es MD5 y SHA-1 y basado en contraseñas que utilizan el algoritmo CHAP garantizando la autenticación bidireccional y unidireccional entre un iniciador y un respondedor de autenticación , este protocolo se usa para verificar periódicamente la identidad par mediante un protocolo de tres vías, la forma en que trabaja el protocolo DH-CHAP es la siguiente :

- Una vez iniciada la fase de establecimiento del enlace, el autenticador envía un mensaje de desafío al par de conexión.
- El par responde con un valor utilizando la funciona hash unidireccional.

- Luego el autenticador compara la respuesta con su propio cálculo de hash esperado, si los valores coinciden se acepta la autenticación de lo contrario se cierra la conexión del enlace.
- En intervalos aleatorio el autenticador envía un nuevo desafío al par y repite nuevamente los pasos anteriormente mencionados.

Este esquema se considera el mejor por que contempla varios ángulos de riesgos a los que se puede ver expuesta la SAN, contemplando aspectos importantes como la autenticación, el cifrado de la comunicación y la integridad de los datos, (Agbo, Ezeali, Erhunmwunsee, & Bande, 2021).

Cifrado de Información

Es un método de codificación de datos de tal manera que nadie puede acceder a ellos el cual codifica la información con el uso de una clave criptográfica, de acuerdo con el tipo de cifrado simétrico o asimétrico se generan diferentes tipos de claves pública o privada, es necesario ya que permite garantizar la integridad y confidencialidad de la información.

Esto en nuestros almacenamientos NAS es muy útil ya podemos utilizar varios tipos de cifrado y aplicarlos en nuestra información como AES de 256 bits, esto también se puede implementar a las copias de seguridad en dado caso que se presente robo de la información esta sea inaccesible, uno de los inconvenientes que tenemos cuando trabajamos con un almacenamiento de datos encriptado es que al realizar la encriptación se requiere de disponer de buenos recursos de hardware, (IBM, 2021).

Conmutación en la SAN

La conmutación aplicada en la SAN nos permite mover el tráfico de datos de almacenamiento entre grupos de almacenamiento, un conmutador interconecta varios servidores

de host los cuales están conformados por servidores de almacenamiento permitiendo una alta disponibilidad sobre estos servidores de almacenamientos se despliegan servicios virtualizados los cuales almacenan toda su información sobre los discos desplegados en la SAN (IBM. 2021, July 27).

Internet Small Computer System Interface

ISCSI es un protocolo estándar el cual está basado en IP y permite conectar dispositivos de almacenamiento en una red y trasmitir mediante los comandos SCSI mediante el uso de redes IP este protocolo permite a los clientes usar la red de almacenamiento y gestionarla es adecuado para ejecutarse en la red física, IBM. (2021, July 27).

Infraestructura de Red

La infraestructura de red son todos aquellos elementos que permiten la comunicación, entre ellos encontramos todo el hardware y software que hacen posible el flujo de datos de acuerdo a lo anterior y en base al artículo de página web redhat se reconoce que la infraestructura de red es un punto vulnerable la cual debe ser protegida y administrada de manera eficiente, la ausencia de medidas adecuadas podrían exponer nuestra red y por ende nuestros almacenamientos por eso es de vital importancia poseer una infraestructura confiable y centrada en la seguridad; Si no poseemos una infraestructura segura el atacante tendrá más herramientas para acceder a la información de nuestra compañía lo cual podría derivar en el robo de credenciales y accesos, (Infraestructura de Red Con Red Hat Y Sus Partners, 2022).

Ciberseguridad

La ciberseguridad se enfoca principalmente en la protección de los sistemas informáticos ante ataques de tipo digital, hoy en día es uno de los mayores retos para todas las compañías sobre todo aquellas del sector público de acuerdo con el articulo web channelpartner las agencias

gubernamentales que manejan información privada y brindan servicios a los ciudadanos, los convierte en blanco de ciberataques, según un informe del parlamento Europeo en 2022 se producirán más de 100.000 incidentes de ciberseguridad en la UE, afectando ámbitos como la salud, la fuerza o la movilidad, además las consecuencias de la guerra en Ucrania han aumentado el riesgo de ciberataques a las instituciones y seguridad europea (Junyi Duanmu, 2022).

Protocolo de Canal de Fibra

Es protocolo sólido y de alta velocidad el cual permite gestionar y transferir la información en una red de almacenamiento tipo SAN proporciona un transporte de tramas confiable sin perdidas y en orden los dispositivos FC también se pueden conectar a dispositivos Fibre Channel sobre Ethernet (FCoE) de igual manera tienen una velocidad de hasta 128 Gps lo cual lo hace bastante rápido para la lectura y escritura de la información, así como la trasmisión de datos, (Juniper Networks. 2024).

Equipos Activos de Red

De acuerdo con el artículo de Global, los equipos activos de red se definen como aquellos dispositivos que participan activamente en la distribución de información dentro de una red. Entre estos elementos se incluyen dispositivos como switches, routers, access points, entre otros. Estos equipos son esenciales para garantizar que los datos fluyan de manera eficiente y segura a través de la red, facilitando la comunicación entre los distintos nodos conectados (Equipo Activo de Red - Desitec, 2024).

ISO/IEC 27040:2024

La norma indica los requisitos técnicos de como las organizaciones pueden lograr un nivel adecuado de la gestión de los riesgos en el almacenamiento de datos, dicha seguridad se encuentra enfocada en la protección de los datos mientras los mismos sean almacenados en los

sistemas de tecnologías de información y a su vez se encuentre en tránsito, la seguridad de la información es relevante para aquellos administradores con responsabilidades especificas en el aseguramiento de la información y su almacenamiento por lo cual se hace necesario la creación de políticas de seguridad (ISO/IEC, 2024) .

Su implementación en las organizaciones ofrece varias ventajas , como lo es la seguridad de la información al proteger adecuadamente la información almacenada frente a las diferentes amenazas a las cuales puede estar expuesta, mejora la reputación de las organizaciones al cumplir con estándares creando un entorno de confianza para los clientes, además al prevenir incidentes de ciberseguridad en los almacenamientos se pueden evitar gastos vinculados a la recuperación de datos (Flores Miranda, 2023).

Hot Spare

Hot Spare es un dispositivo que nos permite crear un plan de respaldo en caso de que falle el componente principal, este dispositivo funciona automáticamente para recuperar un grupo de discos fallido en caso de un archivo esta herramienta es de bastante utilidad ya que nos permitirá garantizar la continuidad de los servicios suministrados en dado caso que presentemos un daño lógico o físico de nuestros dispositivos, juega un papel muy importante en el desarrollo de las NAS y SAN y su funcionamiento depende de la creación de arreglos RAID así como de los tipos de discos sin son sólidos o mecánicos, (Synology Inc., 2025).

Marco Legal

Política de Datos Personales

De acuerdo con el documento publicado por la superintendencia de industria y comercio se estableció en el artículo 15 del derecho de protección de datos personales como el derecho de toda persona para conocer, actualizar, rectificar y/o cancelar la información y datos personales que de ella se hayan recolectado y/o se traten en bases de datos públicas o privadas, esto se materializo mediante la ley 1581 del 17 de octubre de 2012, por lo anterior la superintendencia de industria y comercio ha elaborado la política para el tratamiento de datos personales lo cual aplica para todas las personas naturales y jurídicas aplicando a todas las bases de información tanto físicas como digitales las cuales posean datos personales, a lo anterior la norma clasifica los datos en varias categorías.

Dato Personal Público

Son todos aquellos datos que la norma ha definido como públicos y para recolección y tratamiento no es necesario la autorización del titular por ejemplo datos en sentencias judiciales ejecutoriadas, estado civil de las personas entre otros.

Dato Personal Semiprivado

Son todos aquellos datos que no tienen una naturaleza privada ni publica y cuya difusión puede interesar a un grupo de personas o la sociedad en general, se requiere autorización expresa del titular, como ejemplo dato crediticio.

Dato Personal privado

Es un dato personal de naturaleza reservado y el cual solo interesa al titular, requiere autorización para su tratamiento por ejemplo grado de escolaridad.

Dato Sensible

Es un dato de especial protección el cual afecta la intimidad del titular y su manejo puede generar discriminación, no puede ser objeto de tratamiento a menos que sea requerido para salvaguardar un interés del titular, ejemplo resultado de exámenes médicos.

Datos Personales de Menores

Poseen una especial protección y su tratamiento se podrá ejecutar siempre y cuando no se vulneren sus derechos fundamentales y se busque proteger sus intereses y el desarrollo armónico e integral del menor.

Derechos de los Titulares

- Exponer quejas ante la entidad administrativa encargada de proteger los datos.
- Revocar la autorización supresión de sus datos personales en las bases de datos o documentos siempre y cuando no se encuentre vigentes servicios con la entidad.
- Conocer el uso de la información.
- Requerir prueba de autorización para el tratamiento de sus datos personales.
- Conocer, actualizar y corregir los datos personales.

Deberes del Responsable y Encargado del Tratamiento de Información

Responsable

Es una persona natural o jurídica de carácter público o privado que por sí misma o en asocio decide sobre la base de datos.

Encargado

Realiza el tratamiento de la información de los datos personales.

Deberes

- Tramitar las solicitudes, consultas y reclamos.
- Utilizar únicamente los datos que el titular haya autorizado.
- Respetar las condiciones de la seguridad de la información.
- Cumplir cabalmente las instrucciones y requerimientos impartidos por la autoridad administrativa competente.

Marco Contextual

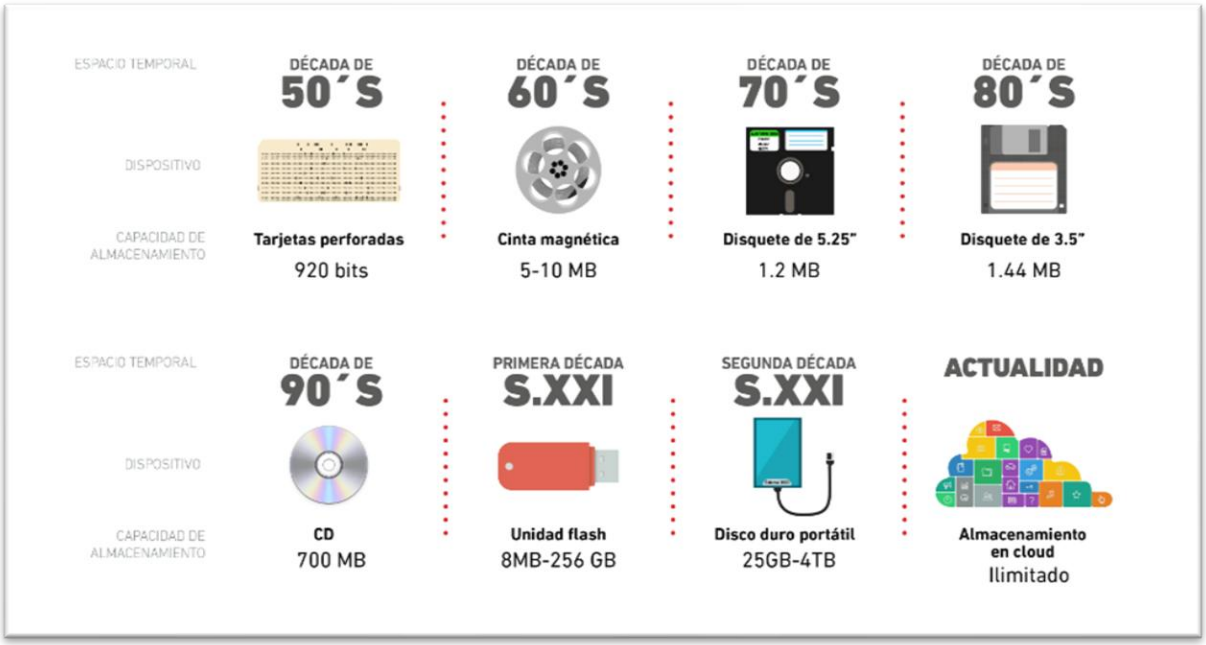
El almacenamiento ha venido evolucionando de una forma exponencial y con grandes pasos a través del tiempo reduciendo cada vez más su tamaño físico y forma de acceso y aumentando su capacidad digital, de acuerdo de la página web el observador el inicio del almacenamiento se remonta al año 1960 con las tarjetas perforadas los cuales fueron el primer medio para almacenar información dichas tarjetas estaban fabricadas con cartulina con orificios de acuerdo al código binario este método se usó hasta mediados de la década de 1970 y fue allí que aparecieron las cintas magnéticas luego de esto en los años 80 y 90 fue de gran popularidad el uso del disquete por su practicidad y bajo costo el cual fue usado comúnmente para la transferencia de datos, almacenar información y la realización de copias de seguridad de archivos de un peso moderado a pesar de uso era vulnerable a los campos magnéticos y la suciedad, pero con el paso del tiempo se lograron corregir estos temas haciéndolo más estable, poco a poco el disquete comenzó a ser reemplazado por el CD el cual fue implementado en 1985 por las empresas Sony y Philips luego de esto surgió el DVD lo cual permitía almacenar mucha más información, pero era susceptible a la perdida de información por el rayado accidental de los mismos, poco después las empresas comenzaron a aplicar de sus infraestructuras almacenamientos tipo SAN y NAS centralizando de esta manera gran parte de su información.

A mediados de la primera década del siglo XXI hizo su aparición la memoria USB o pendrive el cual usaba el puerto USB del computador para guardar información tenía muchas ventajas en comparación al DVD, ya que leía y escribía información a mayor velocidad y usaba su memoria flash para estos procesos, las primeras compañías en comercializar las USB fueron trek technology e IBM en el año 2000, el siguiente paso que tuvo el almacenamiento fue la creación de los discos duros portátiles los cuales eran capaces de almacenar grandes volúmenes

de datos a pesar de su uso hoy en día son bastante susceptibles a golpes al tener piezas mecánicas.

Figura 1

Evolución del Almacenamiento a lo Largo del Tiempo



Nota. Mesa editorial Merca2.0. (2018, April 15). Los dispositivos de almacenamiento a través del tiempo. Revista Merca2.0. https://www.merca20.com/los-dispositivos-de-almacenamiento-a-traves-del-tiempo/

Con el paso del tiempo el almacenamiento fue cambiando de forma y modo y es así como en el año 2014 el almacenamiento comenzó a ser migrado a plataformas enfocadas a internet donde encontramos hoy en día entre ellas el iCloud, Google Drive, SharePoint entre otras han migrado el almacenamiento a la nube de tal forma que los equipos físicos han pasado a un entorno virtual haciéndolos más económicos y accesibles, tal es el caso de la empresa AWS que brinda no solo almacenamiento, sino también alquila su infraestructura haciéndola escalable de

acuerdo a las necesidades actuales de acuerdo a lo anterior podemos observar el gran avance que han tenido los almacenamientos a lo largo del tiempo, pero a su vez también han surgido los riesgos y las vulnerabilidades a los que estos se ven expuestos.

Actualmente y con los avances que ha tenido el almacenamiento podemos optar por almacenar nuestra información de diferentes maneras ya sea en un sistema local, en un disco extraíble o en plataformas más robustas como lo son el SAN y NAS o en su defecto en la nube, pero para poder reconocer la mejor alternativa debemos identificar las características de cada uno de ellos y sus vulnerabilidades, por un lado, la nube brinda a las empresas espacios de almacenamientos con una alta disponibilidad, además de ser una opción muy segura al tener protocolos que controlan el tráfico haciéndola más confiable, por otro lado, su uso nos brinda cierto respaldo a nivel físico se almacenan copias en diferentes ubicaciones físicas, no obstante es vulnerable como todos los sistemas de almacenamiento y un punto de entrada para un acceso no autorizado siempre es el usuario por lo cual siempre es necesario capacitar al usuario común para evitar ataques con ingeniería social, de igual manera también tenemos el almacenamiento de discos rígidos el cual es práctico si tenemos una empresa pequeña sobre todo si no poseemos demasiado presupuesto, una gran desventaja de este tipo de almacenamientos es que puede presentar fallas físicas, ya que es un disco que posee partes mecánicas por lo cual se aconseja no almacenar información en estos discos que sea sensible para la compañía, igualmente encontramos el almacenamiento en cintas el cual consiste en guardar información digital en una cinta magnética, este tipo de almacenamiento a pesar de ser muy ambiguo se sigue usando en muchas compañías, ya que es una muy buena opción el almacenamiento de información a largo plazo, una de sus grandes ventajas es que no son afectadas por el riesgo de infectarse por un malware, dentro de sus desventajas encontramos que pueden tener daños físicos y depende en

gran parte del hardware, así mismo también encontramos el almacenamiento en medios extraíbles como USB, disco externos, DVD es en definitiva una solución temporal susceptible a daños físicos y de una capacidad de almacenamiento baja, obviamente no es recomendable para manejo de información sensible, de acuerdo con lo anterior y con base en los avances que ha tenido el almacenamiento a lo largo de la historia podemos definir que la mejor tecnología actual por su seguridad y adaptabilidad es el almacenamiento en la nube, la cual nos ofrece una alta disponibilidad accesible desde cualquier conexión hacia internet y su hardware puede ser adaptable, además de los costos de inversión.

Almacenamiento de Datos en el ADN

Actualmente se está desarrollando el almacenamiento de información en moléculas de ácido desoxirribonucleico como bien sabemos el ADN almacena nuestra información genética y es allí como varios profesionales de IT lo estudian para almacenar datos no genéticos, este proceso consiste en la codificación y decodificación de datos binarios hacia y desde las cadenas del ADN, esta investigación es bastante importante ya que como sabemos el ADN almacena toda la información biológica color de ojos, pelo, tono de la piel entre otros como la programación del cuerpo humano, estos antecedentes son importantes para reconocer el ADN como almacenamiento de datos frente a las soluciones actuales donde el almacenamiento se puede realizar en la secuencia del ADN, luego de ser secuenciado, sintetizado y copiado el ADN es bastante estable tal es su durabilidad que almacena información de fósiles que habitaron hace 500000 millones de años, (KIO, 2021).

Los investigadores de la universidad de Washington y Microsoft han logrado desarrollar un sistema automatizado para escribir, leer y guardar información en el ADN, el proceso de almacenamiento de un dato digital como por ejemplo una foto consiste en la conversión de bits o

código binario sea escrito en el ADN tal como si se realizara con una impresora de inyección esos datos binarios son almacenados en las 4 bases del ADN adenina timina, citosina y guanina y para recuperar dicha información simplemente tendría que secuenciarse, este desarrollo permitirá almacenar grandes volúmenes de información y su durabilidad y estabilidad se destacarán.

La Regla del 3-2-1

Con el desarrollo tecnológico en el almacenamiento ha crecido a su vez los riesgos a los que estos se ven expuestos, realizar copias de la información se ha convertido en una prioridad para garantizar el flujo continuo de los datos así como de su consulta y mitigar daños causados por ataques cibernéticos o daños de hardware para ello se implementó la regla 3-2-1 la cual nos recomienda la creación de copias de seguridad que mantiene y diversifica el lugar donde se almacenan las copias de seguridad esta regla estable que se deben poseer al menos tres copias de los datos almacenados de las cuales dos de las copias deben encontrarse en diferentes tipos de medios y al menos una copia debe estar almacenada fuera del sitio o en el cloud, el objetivo principal de esta regla es garantizar la disponibilidad de la información asegurando el respaldo de la misma en dado caso que una de ellas falle dentro de las ventajas de esta estrategia podemos destacar que la distribución de las copias en diferentes ubicaciones garantiza que un daño físico o local acabe con toda la información, también podemos resaltar que no se depende únicamente de una sola copia de seguridad, también se considera un modelo seguro, ya que en dado caso de ser infectados por un malware solo se dañara dicha información y las demás copias se encontraran aisladas, a pesar de que es una buena solución de respaldo no es aplicable a todas las empresas, ya que depende en gran parte del modelo de infraestructura implementado.

Servicios de Almacenamiento Gestionado De Netapp y Google

La empresa NetApp ha anunciado una asociación con Google cloud los cuales ofrecerán nuevos niveles de almacenamiento combinados con el cloud, lo cual se agrupa con el servicio Google Cloud NetApp Volumes el cual es un servicio de archivos administrado 100 % en la nube lo cual permitirá la adecuada administración de datos empresariales y el despliegue rápido y seguro de las cargas de información empresariales con herramientas como Google cloud, este servicio está basado en la nube y el software de administración de datos de NetApp ONTAP permitiendo en la actualidad ampliar las cargas de trabajo de Google cloud mediante un servicio de almacenamiento automatizado ofreciendo seguridad de los datos, continuidad del negocio de acuerdo a las cargas de trabajo, esto beneficia en gran parte las cargas de trabajo de los servicios que sustentan plataformas como SAP, VMware, Linux entre otros,(Media, D. 2023, August 28).

Analizar Las Soluciones De Almacenamiento SAN Y NAS, Identificando Sus Características, Para Evaluar Su Idoneidad En El Aseguramiento De Los Datos, Garantizando La Integridad, Disponibilidad Y Confidencialidad De La Información En La Organización

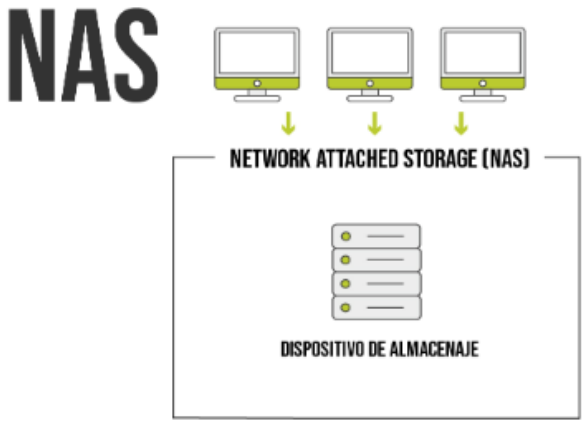
Para poder comprender como diseñar una infraestructura tecnológica segura es importante reconocer cada uno de los elementos que la conforma, así como sus ventajas y desventajas, Este tipo de implementaciones suele aplicarse en ambientes empresariales donde su función principal es proteger la infraestructura de red mediante la ejecución de medidas preventivas con objetivo principal de blindarse contra la modificación de datos y recursos no autorizados, y es apoyada en varios recursos entre los cuales encontramos firewalls, redes VPN, software para análisis de comportamiento, sistemas de detección entre otros, todo esto nos permitirá lograr que nuestros datos viajen de manera segura desde su origen hacia el destino evitando vulnerabilidades las cuales podrían ser aprovechadas por un intruso.

NAS (Network Attached Storage)

Una NAS es un sistema de almacenamiento conectado a la red el cual combina dos factores el hardware y el software lo cual lo hace bastante beneficioso en temas de seguridad, permiten almacenar archivos en la red bajo el protocolo de trasmisión TCP como lo podemos evidenciar en la siguiente figura.

Figura 2

Infraestructura NAS



Nota. Adrià Miralvés. (2023, April 21). SAN vs NAS: comparativa de redes | OnWork IT & Cloud. OnWork. https://onwork.cloud/san-vs-nas/.

Una NAS está compuesta por varios elementos entre los cuales encontramos el almacenamiento, que puede estar conformada por más de 2 discos los cuales pueden ser configurables en arreglos (RAID) haciéndolos redundantes según las necesidades presentadas, por otro lado posee una CPU permitiéndole manejar una alta carga transaccional de datos complementándose con un sistema operativo embebido que resulta práctico en su administración con herramientas diseñadas para reforzar la seguridad de la información.

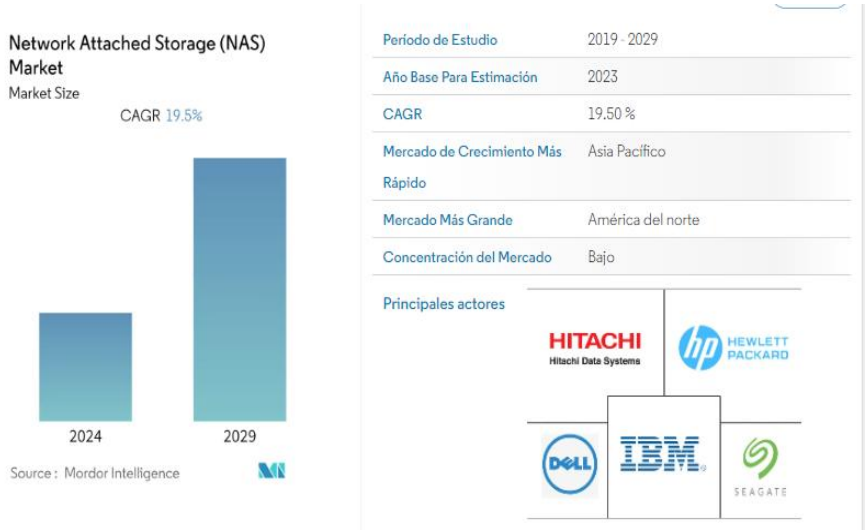
La conexión utilizada para la NAS es de tipo ethernet lo cual lo hace adaptable a sistemas LAN además de funcionar como un almacenamiento de red, una NAS también autentica los clientes, gestiona los archivos y posee herramientas que facilitan la protección de los datos, son útiles para almacenar copias de seguridad no solo de archivos sino también de entornos virtuales como vmware y hyper-v entre otros, por su tipo de conexión ethernet y su facilidad de integración, es una solución adecuada para pequeñas y medianas empresas., (AWS. 2021).

Características de la NAS

- Capacidad de almacenamiento de archivos, así como su facilidad en su configuración y uso permitiendo el acceso simultaneo de usuarios a la información almacenada.
- Adaptabilidad mediante el manejo de protocolos estándar como NFS, CIFS o SMB permitiendo su integración con diferentes sistemas operativos como Linux, Windows o macOS.
- Disponibilidad de los datos mediante funcionalidades de RAID sobre sus discos permitiendo la tolerancia a fallos.
- Asegurabilidad de la información mediante la implementación de cifrado, control de accesos y la utilización de autenticación multifactor (MFA).

Figura 3

Mercado de Almacenamiento NAS



Nota. Almacenamiento conectado a la red (NAS) Volumen del mercado | Mordor Intelligence. (2024). Mordorintelligence.com. https://www.mordorintelligence.com/es/industry-reports/network-attached-storage-nas-market.

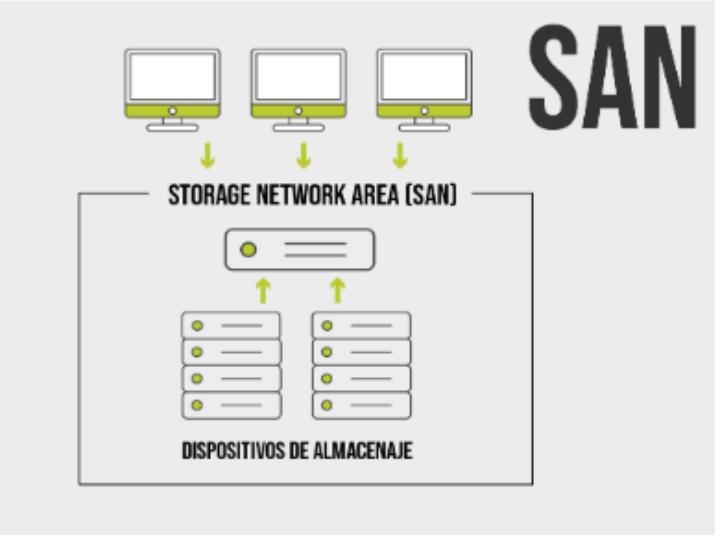
Se estima que el mercado de los almacenamientos NAS crecerá a una tasa del 19.5 % anual y se espera un crecimiento aun mayor para el año 2029, siendo el covid-19 el detonador para el crecimiento de uso de datos por lo cual las compañías buscan cada vez más soluciones de almacenamiento de datos seguros, el creciente uso de almacenamientos NAS en las compañías ha llevado a los proveedores desarrollar soluciones de almacenamiento personalizadas para una gestión integral de datos, esta es una solución de almacenamiento atractiva por su bajo costo y su capacidad de administración de datos, sin embargo dicho crecimiento puede verse afectado por el uso de almacenamiento en la nube el cual ofrece una administración centralizada a través de proveedores SaaS, a pesar de ello se prevé que NAS evolucione hacia un modelo híbrido con la nube, asegurando un respaldo adecuado de la información, (Almacenamiento Conectado a La Red (NAS) Tamaño Del Mercado | Mordor Intelligence, 2024).

SAN (Storage Area Network)

Se define como un sistema de almacenamiento el cual facilita la interconexión de servidores creando así un depósito de almacenamiento común usadas principalmente para aplicaciones críticas de una compañía garantizando una alta disponibilidad y baja latencia en el acceso a los servicios.

Figura 4

Infraestructura SAN



Nota. Adrià Miralvés. (2023, April 21). SAN vs NAS: comparativa de redes | OnWork IT & Cloud. OnWork. https://onwork.cloud/san-vs-nas/.

Un almacenamiento SAN se basa en una estructura de bloques (iSCSI) con una arquitectura de alta velocidad el cual permite el despliegue de aplicaciones en unidades de disco lógicas definidas como LUN, estos almacenamientos están conformados por tres capas fundamentales, (Content Studio. 2022, January 19).

Capa Host

Está compuesta por los servidores que se encuentran conectados a la SAN los cuales realizan cargas de trabajo altas, estas conexiones a la SAN son dedicas y se realizan mediante adaptadores de bus de host (HBA).

Capa De Estructura

Esta capa comprende el cableado y los elementos de red que permiten la conexión entre los servidores y el almacenamiento SAN donde podemos encontrar varios elementos como switches, routers, hubs y todos aquellos elementos activos de la red que permiten la *comunicación.*

Capa De Almacenamiento

Se compone por todos los elementos de almacenamiento como discos duros que conforman la SAN los cuales pueden ser estructurados bajo RAID mejorando así la disponibilidad y el respaldo de la información.

A diferencia de una NAS un almacenamiento SAN puede utilizar varios protocolos en donde podemos encontrar el protocolo de canal de fibra (FCP) utilizado para servicios que requieren alto rendimiento y velocidad, por otro lado, encontramos el iSCSI el cual básicamente permite la conexión mediante TCP/IP y por último tenemos el canal de fibra por ethernet (FCoE) el cual permite que las conexiones (FC) se realicen sobre ethernet.

Características de la SAN

- Disponibilidad de los servicios desplegados en sus discos mediante herramientas de replicación de datos como snapshots y copias de seguridad garantizando de esta manera la integridad, continuidad y disponibilidad del negocio.
- Administración centralizada y segmentación de tráfico lo cual permite el control de la seguridad de los volúmenes de almacenamiento.
- Alta disponibilidad mediante el uso de múltiples rutas de datos y sistemas RAID con el fin de garantizar la tolerancia a fallos.

En base al análisis y características de los almacenamientos NAS y SAN es necesario evaluar criterios que garanticen la integridad, disponibilidad y confidencialidad de los datos y servicios, por lo cual se propone una lista de verificación de requisitos contemplando cada una de estas variables.

Tabla 1

Evaluación de Integridad, Disponibilidad y Confidencialidad en NAS y SAN

Aspecto	Criterio a evaluar	Sí	No	Observaciones
Integridad	El sistema soporta sistemas de archivos robustos como ZFS y EXT4			
	Implementa mecanismos de protección contra corrupción de datos como checksum y RAID.			
	Permite la creación de snapshots o versiones de los datos			
	Registra auditorías de acceso y modificaciones			
Disponibilidad	Cuenta con hardware redundante (discos, fuentes de poder)			
	Soporta failover o clustering para continuidad del servicio			
	Tiene capacidad para replicar datos en diferentes ubicaciones			
	Dispone de balanceo de carga o multipathing (SAN)			

Aspecto	Criterio a evaluar	Sí	No	Observaciones
	Monitoriza la salud del sistema y realiza mantenimiento preventivo			
	Controla accesos mediante autenticación basada en usuarios y grupos			
	Integra sistemas de autenticación (LDAP, Active Directory)			
Confidencialidad	Implementa cifrado de datos en reposo y en tránsito			
	Aplica políticas estrictas de permisos de acceso			
	Segmenta la red para limitar accesos (zoning en SAN)			
	Realiza auditorías y alertas sobre accesos sospechosos			

Nota. Esta table permite evaluar las condiciones actuales de la NAS y SAN respecto a parámetros de seguridad que garantizan la disponibilidad integridad y confidencialidad de datos y servicios.

Desarrollar Configuraciones Eficientes en Sistemas de Almacenamiento SAN y NAS, así como el Entorno de Red que los Soporta, y Proponiendo Mejoras que Refuercen Su Protección Frente a Amenazas

Una vez comprendido el funcionamiento de los sistemas de almacenamiento SAN y NAS, es necesario detallar las medidas de seguridad que debemos implementar para garantizar la integridad,disponibilidad y confidencialidad de nuestros datos.

Aseguramiento de NAS

Actualmente muchas compañías utilizan soluciones de almacenamiento NAS convirtiéndolas en un objetivo atractivo para los ciberdelincuentes por ello es necesario asegurar estos dispositivos implementado configuraciones adecuadas que permitirán la protección de los mismos, es fundamental implementar las siguientes medidas las cuales, aunque no se apliquen de manera uniforme en todos los fabricantes, suelen estar disponibles a través de actualizaciones de software en estos sistemas (Kaspersky Security for Storage | Kaspersky, 2025).

- Desactive el acceso web mediante una dirección publica, ya que tenerlo en la web representa un riesgo latente a un ciberataque y robo de datos.
- Debido a que SMB ha sido blanco de ataques constantes se recomienda mantenerlo desactivado.
- Habilite los puertos que requiera para servicios específicos, el no tener una adecuada gestión de los mismo puede generar brechas de seguridad.
- Cifre las carpetas que compartidas en una NAS y establezca claves para evitar su borrado o accesos no autorizados.
- Defina un tiempo de renovación de claves de los usuarios que ingresan al almacenamiento, asegurando la actualización regular de claves.

- Enmascare la IP del servidor NAS y use un registro DNS para su acceso.
- Habilite 2FA para el acceso lo cual proporcionara una capa de seguridad adicional.

Las anteriores medidas permitirán una protección esencial de los almacenamientos NAS, el no aplicarlas podrían ocasionar perdida de nuestros datos, un ejemplo claro de ello ocurrió en mayo de 2017, cuando se propagó el troyano WannaCry, responsable de 45.000 ataques en un solo día, países como rusia, ucrania, la india y Taiwán fueron especialmente afectados; Este malware inyecta un exploit el cual se encarga de infectar el ordenador luego de esto un cifrador, encripta los archivos y posteriormente los delincuentes solicitan un rescate para desencriptar dichos datos y que puedan ser restaurados, si dicha información ya hubiese estado cifrada por una herramienta como lo es BitLocker al atacante no hubiera podido realizar dicho ataque de manera exitosa, (Perekalin, A. 2017, May 13).

Aseguramiento de SAN

El almacenamiento SAN se ha convertido en una solución de alto rendimiento para entornos virtualizados debido a su alta disponibilidad y velocidad de acceso a los datos, protegerla adecuadamente permitirá la continuidad de los servicios que se alojen en dicho almacenamiento.

- Enmascarar todas las direcciones IP incluidas las de administración de la SAN.
- Definir un puerto TCP/IP de acceso especifico y evitando usar el establecido de fábrica.
- Establezca roles y responsabilidades para la administración de la SAN, garantizando el cumplimiento de políticas de seguridad.

- Implemente cifrados de datos solidos como AES o RSA para aquellos datos estáticos y dinámicos almacenados.

Seguridad de la Infraestructura

La seguridad en la infraestructura requiere una perspectiva global que abarque todos los procesos tecnológicos que se ejecutan dentro de una compañía es por ello que la agencia de seguridad de infraestructura y seguridad (CISA) recomienda definir los puntos de partida de la creación de una infraestructura segura con el objetivo de identificar vulnerabilidades, al priorizar la ciberseguridad, las compañías pueden tomar conciencia de las amenazas informáticas a las que están expuestas y adoptar medidas efectivas para proteger la información. De acuerdo con lo anterior, se definirán los parámetros que desempeñan un papel crucial en la red, (CISA, 2024).

Segmentación de Redes y Funciones

Debemos prestar especial atención al diseño de una infraestructura de red, procurando la segmentación de la red mediante el uso de VLANs haciéndola un mecanismo de seguridad eficiente, limitando la propagación de posibles incidentes de seguridad hacia otras áreas de la red, para lograrlo, se recomienda emplear routers junto con la implementación de VLANs que dividan el tráfico o, en caso de detectar un posible ataque, desactivar el flujo en puertos específicos.

Restricción de las Comunicaciones

Se debe filtrar y monitorear la comunicación tanto interna como externa de lo contario podríamos enfrentarnos a intrusos que merodeen nuestra red local permitiendo la persistencia del atacante en la red mediante la generación de puertas traseras o instalación de software que monitoree nuestro tráfico.

Reforzar los Dispositivos de Red

El refuerzo de nuestros dispositivos activos de red es la mejor manera de garantizar la seguridad de la infraestructura de red esto se logra mediante el desarrollo de políticas de seguridad que aborden aspectos como el cifrado de la red, la protección del accesos mediante el uso de contraseñas seguras, la protección de switches, routers,firewalls y la implementación de medidas de seguridad de acceso físico como biométricos para restringir el acceso a áreas sensibles de la compañía donde se alojan los servidores de almacenamiento y servicios, así como realizar revisiones y actualizaciones periódicas de seguridad.

Proteger el Acceso a los Dispositivos de la Infraestructura

Se deben definir los roles y permisos para determinar que personal de confianza pueden acceder a nuestros recursos de red ya sea nivel físico o lógico con el fin de garantizar de esta manera la autenticidad de los usuarios mediante la implementación de servicios de autenticación como MFA o 2FA donde se gestione el acceso y los privilegios.

Administración de Red Fuera de Banda (OOB)

La administración fuera de banda nos permitirá gestionar de manera remota los equipos críticos de la red mediante una conexión segundaria que se encuentra separada de la conexión de red principal, esto no solo incrementa la seguridad general, sino que también posibilita el acceso y la administración remota durante fallos, ya que se aísla el tráfico de administración del tráfico de los usuarios.

Verificación de la Integridad del Hardware y Software

Se deben verificar que todos los dispositivos cuenten con licenciamiento legítimo, el uso de software sin licenciamiento o parcheado con licencias ilegitimas nos expone a riesgos en nuestra red ya que no cuentan con actualizaciones de seguridad que mitiguen vulnerabilidades.

Ventajas de una Infraestructura Segura Red

Implementar adecuadamente una infraestructura de red segura permitirá a las compañías brindar una tranquilidad y confianza tanto a sus clientes internos, impulsando el desarrollo de las tecnologías de la información, a continuación, se destacan las ventajas más relevantes de contar con una infraestructura segura.

Administración Adecuada de Recursos

La implementación de medidas de seguridad adecuadas permitirá aprovechar al máximo la capacidad de la red sin que suponga un riesgo para los usuarios, contribuyendo en la reducción de costos operativos.

Mejoramiento De La Productividad

Al desarrollarse el flujo de datos en un ambiente controlado los usuarios pueden compartir información en la red local de la compañía.

Protección de datos

La implementación de políticas de segura y el uso de copias de seguridad garantizan el aseguramiento de la propiedad intelectual que constituye toda la información de la compañía convirtiéndose en el activo no tangible más importante.

Tipos de Seguridad de Infraestructura de Red

De acuerdo con el enfoque de deseemos brindar a nuestra infraestructura podemos optar por diferentes tipos de seguridad de acuerdo con las necesidades de nuestra compañía.

Controles de Acceso

El control de acceso es fundamental en la seguridad de nuestra red ya que define quien posee los permisos para acceder a determinados recursos y en que escenarios, el uso de sistemas biométricos protege los espacios físicos mientras que las directivas de control protegen los datos

digitales, la implementación de este tipo de seguridad reduce el riesgo de filtrado de datos por parte de los empleados de la compañía y mantiene segura la red.

Seguridad de las Aplicaciones

Este tipo de seguridad nos permite a desarrollar características dentro del software para prevenir vulnerabilidades, su intervención es esencial ya que las aplicaciones suelen estar disponibles mediante varias redes tipo cloud lo cual aumenta las posibilidades de un ataque, por ello es necesario realizar pruebas de seguridad en las aplicaciones para identificar posibles puntos de mejora.

Redes VPN

Utilizar una VPN para el flujo de datos e información resulta sumamente beneficioso, ya que cifra la conexión entre dos puntos y establece un canal seguro, además de esto oculta el direccionamiento IP lo cual dificulta el monitoreo del tráfico.

Análisis de Comportamiento

El análisis de comportamiento utiliza el aprendizaje automático para identificar comportamientos inusuales o maliciosos esto se realiza mediante el análisis y comparación de las actividades cotidianas y trafico usual de la red, este tipo de seguridad es bastante provechoso ya que cada malware se comportan de una manera distinta en la red, estas herramientas usan volúmenes masivos de datos para determinar cuál es el comportamiento usual de los usuarios y, a partir de ahí, identificar eventos, tendencias y patrones, tanto en tiempo real como de forma histórica, VMware by Broadcom - Cloud Computing for the Enterprise. (2024).

Seguridad Inalámbrica

Es un elemento sensible y menos seguro que la red cableada por eso es importante que los protocolos de seguridad se encuentren actualizados lo cual es algo propiamente del fabricante mediante las actualizaciones firmware.

Propuestas de Mejoras para la Protección de SAN Y NAS Frente a Amenazas

- Poner en marcha tácticas automatizadas que garanticen la implementación adecuada de actualizaciones de seguridad en los dispositivos de almacenamiento, previniendo de esta manera que sean infraccionados.
- Implementar tecnologías que supervisen en tiempo real el tráfico de red de los almacenamientos, detectando de esta manera accesos no permitidos o acciones sospechosas para atención inmediata.
- Asegurar la protección de los datos guardados a través de cifrados sólidos, así como la comunicación de estos aparatos a través de vías seguras.
- Incrementar la implementación de autenticación multifactor en todos los accesos de los usuarios a la información guardada • Incrementar la utilización de autenticación multifactor para todos los accesos de los usuarios a la información guardada
- Aplicar políticas de respaldo que definan la repartición de copias en distintos lugares físicos y lógicos, asegurando de esta manera una recuperación eficaz frente a incidentes.

Diseñar una Infraestructura Tecnológica Segura para los Sistemas de Almacenamiento SAN Y NAS, Identificando Posibles Vulnerabilidades y Proponiendo Soluciones de Seguridad

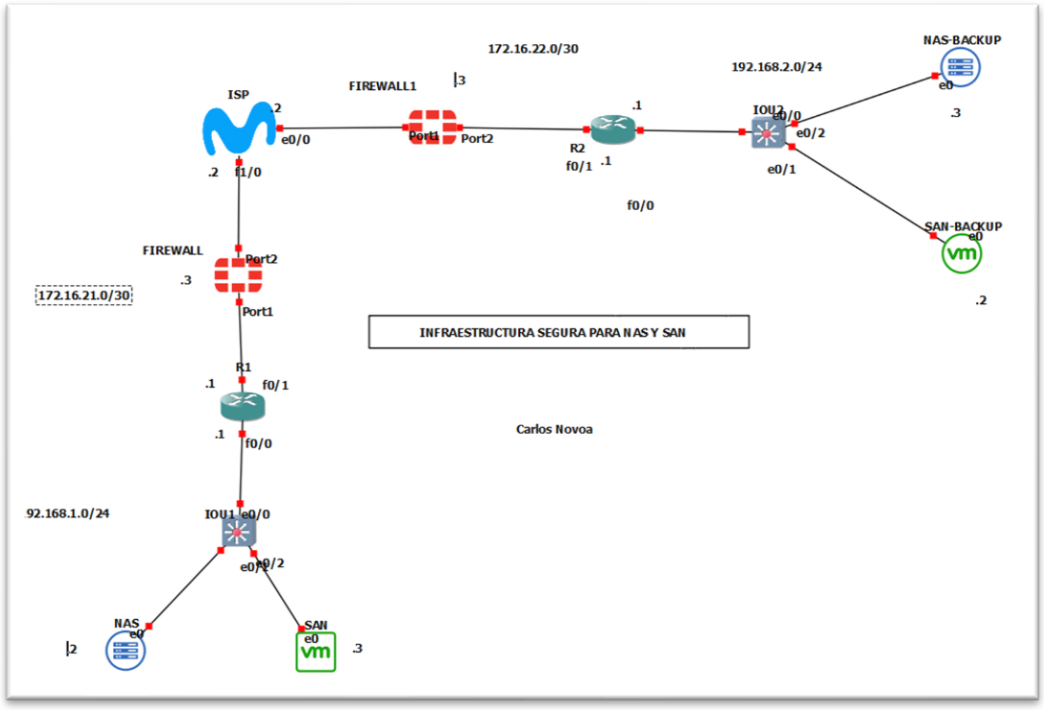
Es necesario diseñar mediante el software GNS3 los diversos elementos que intervienen en la creación de una red segura, por lo cual mediante esta herramienta podremos emular diferentes redes y elementos como switches, routers, firewalls, servidores entre otros, otra de las grandes ventajas de esta herramienta es que es gratuita y es capaz de simular varios tipos de equipos y marcas lo cual es bastante beneficioso si queremos realizar pruebas en un entorno controlado y seguro, sin embargo requiere de buenas capacidades de hardware adecuados para la cantidad de dispositivos a simular, dicho lo anterior se propone un prototipo de red que cumpla con las condiciones adecuadas para poder proteger nuestros almacenamientos NAS y SAN, este diseño incluye routers, switches de capa 3 con la posibilidad de crear VLANs, un firewall fortinet para el control del tráfico y la implementación de túneles VPN, así como copias de seguridad de los almacenamientos SAN y NAS distribuidas en diferentes ubicaciones físicas de la red.

Para lograr proteger toda nuestra infraestructura de red y los elementos que la conforman se hace necesario la implementación de soluciones que nos permitan atender y mitigar los incidentes de seguridad, en la actualidad los ataques cibernéticos se encuentran enfocados hacia los sistemas operativos y todos los elementos que facilitan su comunicación hacia internet ya que representan una parte fundamental para obtener el control de un sistema informático en una compañía pero no solo los ataques han sido desarrollados para acceder de manera física o lógica

a los elementos de la red sino que los ciberdelincuentes han implementado estrategias de ingeniería social para acceder de manera no autorizada a estos sistemas con ayuda del usuario; El crecimiento exponencial de los ciberataques a nivel mundial ha generado un impacto directo en las empresas, ya sea mediante el robo de información o la denegación de servicios, estos ataques no solo provocan pérdidas económicas, sino que también afectan la reputación de las organizaciones ante sus clientes, si bien aunque no hay medidas 100 % efectivas debido al desarrollo creciente de vulnerabilidades de seguridad si podemos mitigar gran parte de las mismas y por ende el acceso no autorizado a información confidencial y servicios, (Toledo, R. 2022, 24 de mayo).

Figura 5

Diseño de infraestructura Segura



Nota. Propuesta de una infraestructura segura para almacenamientos NAS y SAN

De acuerdo con la figura 2 se puede observar claramente todos elementos de red que interactúan con los almacenamientos NAS y SAN en donde se visualizan firewalls, routers y switches por lo cual si se desea una solución efectiva debemos identificar y mitigar las posibles vulnerabilidades a los que está expuesto de cada uno de estos elementos, teniendo en cuenta que aunque los elementos existen dentro de la red sino se configuran adecuadamente pueden no tener efecto alguno en la protección de la red, dentro de las vulnerabilidades que se pueden presentar en los dispositivos de red encontramos :

- Falta de filtrado de trafico
- Usuarios de administración y contraseñas no cambiados
- Ausencia de ACLs o mal configuradas
- Falta de configuración de puertos
- No uso de segmentación (VLANs)

A continuación, se relacionarán medidas efectivas que contribuirán a al aseguramiento de los dispositivos de red y por ende a los datos y servicios de acuerdo con las vulnerabilidades mencionadas

Aseguramiento de Dispositivos Activos De Red

Es fundamental proteger todos los dispositivos por donde se transportan los datos, así como implementar acciones rápidas que mitiguen posibles brechas de seguridad, a continuación, se presentarán estrategias que fortalecerán la seguridad de la red, considerando los elementos definidos en el diseño propuesto, los cuales interactúan de manera directa e indirecta con los sistemas de almacenamiento NAS y SAN.

Firewall

Una herramienta bastante útil a la hora de proteger nuestra red es el uso de un firewall el cual establece un límite entre nuestra red interna hacia una red externa como internet, sin embargo, su uso por sí solo no es suficiente para garantizar la seguridad, la implementación de protocolos seguros, generación de políticas de autenticación como MFA contribuirán al alcanzar el objetivo de tener una red segura, los firewalls han sido un aliados estratégicos en la seguridad de la información ya que controlan el tráfico y deniegan servicios no autorizados, esto se realiza mediante la implementación de varios filtros, entre los que encontramos:

Filtrado de Paquetes

Esto nos permite denegar o permitir el acceso a la red a equipos de acuerdo con una IP especifica o MAC.

Filtrado de Aplicaciones

Permite o deniega acceso a aplicaciones de acuerdo con el puerto y protocolo.

Filtrado de URL

Permite o deniega acceso a sitios web de acuerdo con una URL especifica.

Inspección de Paquetes con Estado

Todo paquete que ingrese debe representar una respuesta legitima a una solicitud de un host internos, aquellos que no generen una solicitud se consideraran como ilegítimos y se bloquearan, esto es muy útil cuando se presentan ataques de DDoS, además, según el fabricante, pueden incorporarse capacidades avanzadas de filtrado y servicios adicionales que refuercen la seguridad de la información, por ello, es fundamental considerar el Cuadrante Mágico de Gartner, que permite evaluar y seleccionar las mejores soluciones disponibles en el mercado.

Figura 6

Cuadrante de Gartner firewalls 2022

Notas. Belen. (2022, December 28). Firewall de Red - Cuadrante Mágico de Gartner 2022 - tecnozero. Tecnozero Soluciones Informaticas. https://www.tecnozero.com/blog/cuadrante-magico-de-gartner-para-firewalls-de-red-2022/

De acuerdo con lo anterior se pueden observar tres marcas de firewalls principales en primer lugar, fortinet se destaca por su tecnología SD-WAN la cual centraliza varios servicios y algo muy importante y es que está enfocándose a servicios en la nube como AWS, por otro lado podemos observar que los firewalls palo alto que con su actualización de firmware en el 2022 han mejorado notablemente el filtrado URL, seguridad de DNS y ha enfocado sus servicios hacia IoT, finalmente encontramos el check point el cual lanzo productos para medianas empresas lo cual es bastante beneficioso entendiendo que muchas empresas no cuentan con el musculo financiero para invertir en equipos especializados,(Belen. 2022, December 28).

Routers

Es importante garantizar la seguridad de la red cerrando todas las posibles brechas, especialmente en los routers, que controlan el tráfico de datos, si un router es comprometido, se podría perder el control de toda la infraestructura de red y la información de acceso a servicios, por ello, es crucial implementar medidas de protección efectivas, como las que se mencionarán a continuación, (Prestigia Seguridad 2022, February 8).

Contraseñas

Es fundamental cambiar contraseñas predeterminadas en estos dispositivos, ya que suelen ser una puerta de entrada de los ciberdelincuentes, se deben establecer claves seguras con altos parámetros de complejidad combinando mayúsculas, minúsculas, números y caracteres especiales, es recomendable definir usuarios y roles dentro de la configuración del dispositivo para restringir el acceso y mejorar la seguridad.

Listas de Control de Acceso

Las listas de control de acceso son bastante efectivas, ya que blindan la red de una manera robusta sin embargo si no se establecen reglas específicas pueden generar acceso no autorizados, por lo cual se deben definir de manera específica que elementos pueden generar tráfico dentro de la red, para ello, se deben establecer qué puertos de entrada y salida están permitidos y qué aplicaciones pueden generar y solicitar determinados servicios.

Actualización de Firmware

Se deben hacer revisiones periódicas de actualizaciones de software disponibles por parte del fabricante para el dispositivo con el fin de mitigar posibles vulnerabilidades que puedan comprometer el control del router y poder solventarlas de manera temprana, un claro ejemplo de la importancia de estas actualizaciones fue el ataque de malware sufrido por la compañía

windstream el cual afecto 600,000 routers, provocando la indisponibilidad de los servicios y dejando a miles usuarios sin conexión a internet, este malware exploto vulnerabilidades de 179,000 equipos de actiontec y 480,000 de sagecom lo cual dejo inutilizable estos elementos, dicho malware sobrescribió el firmware complicando aún más el proceso de recuperación, (Ilan Cherre. 2024, May 30).

Switches

Este elemento facilita la interconexión de los elementos que conforman de la red, como estaciones de trabajo, servidores, cámaras, teléfonos entre otros, por lo cual es fundamental establecer medidas de seguridad que protejan estos dispositivos contra accesos no autorizados, garantizando la integridad y disponibilidad de la red., (Comunidad FS,2023).

Seguridad de Puertos

Se deben establecer funciones de seguridad en la red con el fin de restringir el acceso no autorizado mediante reglas de MAC que limiten la conexión a un determinado puerto, además se deben desactivar aquellos puertos que no están siendo utilizados por alguna estación de trabajo reduciendo así posibles puntos de vulnerabilidad y fortaleciendo la seguridad de la infraestructura de red, el uso de este tipo de configuraciones son útiles ya que bloquea usuarios que pretendan conectarse a nuestra red de manera indebida,

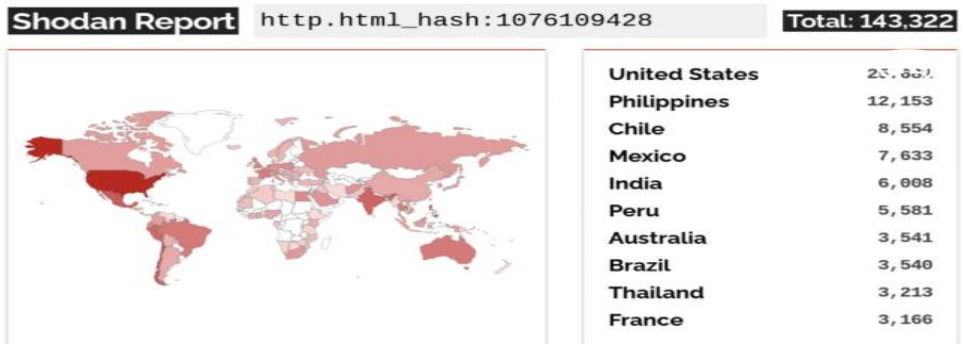
Implementar VLANs

Se debe segmentar la red mediante VLANs para minimizar el impacto de posibles vulnerabilidades, permitiendo el aislamiento de estaciones de trabajo y servidores principales, esta práctica es especialmente útil en redes de gran tamaño, ya que mejora la seguridad, optimiza el tráfico de datos y dificulta el movimiento lateral de amenazas dentro de la infraestructura.

La efectividad de las medidas depende en gran medida del administrador de la red,por lo cual es necesario implementar planes de trabajo y revisiones que mitiguen las vulnerabilidades las cuales pueden ser corregidas con actualizaciones o configuraciones específicas, incluso cuando se dispone de una infraestructura de red compuesta por equipos de última generación, nunca serán excesivas las medidas adoptadas para garantizar la protección de la información, un claro ejemplo de la importancia de estas prácticas es el caso reportado por el blog EHC Group, donde más de 10,000 dispositivos Cisco con IOS XE fueron vulnerados a través de su interfaz de usuario web, donde los atacantes no autenticados explotaron la vulnerabilidad CVE-2023-20198, obteniendo acceso al dispositivo, creando cuentas locales y posteriormente elevando privilegios a usuario root,la facilidad con la que lograron comprometer estos dispositivos se debió a que la interfaz web estaba habilitada, lo que resalta la importancia de desactivar funciones innecesarias y aplicar configuraciones seguras (IOS XE, 2023, October 18).

Figura 7

Dispositivos vulnerables cisco IOS XE



Nota. Shodan. (2024). Shodan. https://www.shodan.io/

De acuerdo con una búsqueda realizada en shodan en su momento se identificaron más de 140,000 dispositivos con su interfaz web habilitada expuestos a internet, esta vulnerabilidad

podría haber tenido un impacto aún mayor si cisco no hubiera tomado las medidas necesarias para mitigarla, de allí la importancia de mantener el firmware actualizado, ya que las actualizaciones suelen corregir fallos de seguridad que podrían ser explotados por atacantes, poniendo en riesgo la infraestructura de red y la información crítica.

Medición del Riesgo para una Infraestructura de Red

La efectividad de las medidas adoptadas pueden evaluarse mediante un adecuado análisis de riesgo, el cual permite reconocer las amenazas a las que pueden estar expuestos los activos tecnológicos críticos de una compañía que pudiesen comprometer la disponibilidad, integridad y confidencialidad de los servicios y datos, identificar los riesgos a los que está expuesta una organización facilita su gestión, permitiendo evaluar y reducir amenazas mientras se desarrollan estrategias de mejora continua para contrarrestar ataques cibernéticos, por consiguiente para llevar a cabo un análisis de riesgos efectivo, es fundamental aplicar metodologías estructuradas que aborden aspectos clave como la identificación de amenazas, cálculo de riesgos, impacto y probabilidad de ocurrencia y activos tecnológicos cruciales para la operación de la organización, definidas e identificadas las amenazas podremos diseñar un plan de gestión de riesgos y comenzar a mitigar cada una de ellas según sea el caso, tomando medidas que contribuyan a la reducción de incidentes de ciberseguridad, como por ejemplo la implementación de políticas de seguridad, despliegue de antivirus, implementación de inteligencia artificial entre otras, 2024 ha sido un año de muchos retos para las compañías en cuanto a ciberseguridad con una proyección de costos del cibercrimen de unos US 9.5 millones además se estima una mayor actividad de los ciberdelincuentes enfocados en ataques de DDoS, extorsión, phishing entre otros, aunque los análisis de riesgos ayudan mitigar gran parte de estas amenazas en una compañía es importante resaltar que un alto porcentaje de los ataques se dirige al factor humano, donde los atacantes

persuaden a los usuarios para obtener acceso no autorizado, y es allí donde es crucial enfocar gran parte de los esfuerzos en capacitaciones a los usuarios que les permitan reconocer si están o no frente a un ciberdelincuente, si reconocemos el impacto económico y reputacional de un ciberataque podemos comprender la importancia de los análisis de riesgos los cuales nos permitirán tomar medidas tempranas,aunque un análisis de riesgos no garantiza una seguridad informática al 100 % si minimiza las brechas de seguridad que se pueden tener y minimiza el impacto de un ataque con los planes de recuperación que se halla diseñado para cada caso.

Incidentes de Ciberseguridad

Para poder implementar de manera asertiva soluciones de seguridad es necesario reconocer los incidentes de seguridad, un incidente se presenta cuando una persona intenta acceder a nuestra infraestructura de manera no autorizada poniendo en riesgo toda nuestra información confidencial, esto implica una amenaza para las empresas por que pueden explotar cualquier tipo de vulnerabilidad en la infraestructura de red, actualmente los incidentes de seguridad más comunes son el malware, phishing, ransomware, DDoS y las amenazas internas.

Reconocer los incidentes de ciberseguridad es fundamental, ya que tienen un impacto notable en los objetivos empresariales, de acuerdo con el artículo de la revista cloud computing las pymes españolas se enfrentan día a día a incidentes de ciberseguridad en donde encuentran muchos factores que contribuyen en la falta de protección cibernética como lo son, presupuestos limitados, capacidad para formar a sus empleados en temas de ciberseguridad y la falta de orientación y asesoramiento, aunque muchas pymes son conscientes de la importancia de la ciberseguridad, a menudo desconocen cómo gestionarla de manera efectiva, es importante resaltar que casi la mitad de las pymes a nivel global (48%) ha sufrido un incidente de ciberseguridad en el último año por los cual es importante para estos pequeños y medianos

negocios identificar por donde se debe empezar para superar las barreras de inversión en este aspecto reconociendo su impacto y sus beneficios si se maneja de una manera adecuada.

Logs de Datos de Seguridad

Un incidente de seguridad puede ser identificado mediante la recopilación de datos de registro de todos los equipos activos y pasivos que conforman la red, así como de los servicios en ejecución, al tener estos registros de manera centralizada podemos detectar eventos de seguridad por lo cual es importante recolectar los registros de los siguientes elementos y servicios de la red, IBM. (2024, August 20).

Datos Internos

- Firewalls.
- Routers.
- Sistemas de flujo de red.
- Proxys.
- Access Point.
- Filtros web.
- Sistemas de seguridad física.
- Sistema de prevención de perdida de datos.

Pero no solo podemos basarnos en los registros de información local también importante la obtención de información externa que nos oriente a reconocer si existen vulnerabilidades y como corregirlas.

Datos Externos

- Alertas de seguridad del proveedor de nuestros equipos, sus avisos de seguridad nos advierten sobre las amenazas y la manera de mitigarlos mediante actualizaciones o parches de seguridad.
- Alertas de seguridad de código abierto, varias organizaciones como secunia y MITRE publican información sobre amenazas mucho antes de que lo haga el proveedor oficial.

Plan de Respuesta a Incidentes de Ciberseguridad

El plan de incidentes de ciberseguridad es fundamental ya que nos orienta en la manera de reaccionar ante un ataque el cual nos permitirá definir los procedimientos para poder mitigar el impacto y tomar decisiones adecuadas para superar el incidente presentado, por lo cual es necesario seguir las siguientes pautas para poder obtener un plan de respuesta a incidentes exitoso, (ciberseg1922. 2020, May 11).

Preparación

Es la clave para poder tener una respuesta oportuna a los incidentes de ciberseguridad, por lo cual se debe crear un plan solido para abordar de manera adecuada cada novedad presentada, en donde se deben desarrollar políticas de respuesta a los incidentes, de igual manera se deben definir pautas de comunicación para que esta sea fluida durante y después de un incidente de ciberseguridad, otra herramienta esencial es la realización de ejercicios de test de seguridad esto nos permitirá identificar amenazas y actuar de manera previa a un ataque real, además debemos evaluar la capacidad de detección de amenazas.

Identificación e Informes

Es importante monitorear los eventos de seguridad lo cual permitirá identificar y corregir a tiempo posibles incidentes de ciberseguridad por lo cual debemos:

Supervisar

Se monitorea los eventos de ciberseguridad mediante el uso de herramientas como firewalls, sistemas de detección de instrucciones y prevención de perdida de información.

Detectar

Identifica posibles incidentes de ciberseguridad, para ello podemos usar herramientas como SIEM.

Alerta

Los encargados de IT crean un ticket del incidente presentado, documentan de manera adecuada los hallazgos y asignan una clasificación al incidente.

Informar

Se crean informes reglamentarios donde se evidencie la trazabilidad y acciones a tomar sobre el incidente.

Análisis

Se deben emplear de manera eficiente los recursos disponibles para recolectar datos significativos, los cuales permitirán llevar a cabo un análisis completo que incluya el análisis forense, el estudio de la memoria y la evaluación de malware, a medida que se desarrolla la obtención de información es necesario contemplar tres puntos esenciales:

Análisis De Punto Final

En este punto se determina los rastros o huellas que haya podido haber dejado el atacante, asimismo como la construcción de una línea de tiempo de actividades, es analizar una copia bit a bit de los sistemas afectados y capturar la memoria RAM, lo que permite detectar posibles detonantes del incidente y comprender su origen.

Análisis Binario

Nos permite analizar los binarios maliciosos los cuales pudieron haber sido aprovechados por el ciberdelincuente, esto lo podemos realizar de dos maneras una de ellas es analizar el comportamiento del programa malicioso en un entorno controlado, otra manera es mediante el análisis estático en donde se intenta identificar mediante ingeniería inversa toda la funcionalidad del software malicioso.

Caza Empresarial

Permite analizar los sistemas existentes de registro de eventos para así determinar el alcance del incidente de ciberseguridad, de igual manera se deben documentar todos los equipos y servicios afectados para poder realizar adecuadamente una neutralización efectiva.

Contención

Se deben crear estrategias de contención al incidente presentado de acuerdo con el análisis realizado para evitar mayores afectaciones por lo cual es necesario realizar lo siguiente:

Apagado Controlado

Una vez identificado los equipos y servicios afectados estos deben ser apagados de manera controlada de tal modo que no se pierda la información allí alojada dicho apagado debe ser coordinado con todos los involucrados.

Depurar y Reparar

Se debe hacer una limpieza de los equipos infectados e instalación de cero del SO base, en donde se deben cambiar las credenciales que pudieron haberse visto comprometidas.

Mitigación de Amenazas

Si se identifica que hay comprometidas IPs o dominios se deben generar solicitudes de mitigación que aíslen la comunicación de salida dichos sitios.

Acciones Posteriores al Incidente

Luego de que se identificó que se presentó un incidente y se logró mitigar debemos documentar adecuadamente cada aspecto relacionado al mismo para aplicar mejoras y evitar de esta manera más incidentes de seguridad por lo cual es necesario seguir las siguientes pautas:

Generar Un Informe de Incidentes

Se debe documentar de manera detallada el incidente el cual será la base para implementar mejoras al plan de respuesta y servirá para ejecutar acciones en pro a la seguridad informática de la compañía.

Monitoreo Luego del Incidente

Permite hacer un seguimiento a las actividades posteriores al incidente con el fin de que la amenaza no se presente de nuevamente, por lo cual es conveniente el uso de un visor de registro de seguridad el cual analizara los datos del sistema SIEM.

Identificar Medidas Preventivas

Nos permite generar nuevas iniciativas de seguridad las cuales contribuyan a evitar futuros incidentes de ciberseguridad, están iniciativas deben ir enfocadas hacia todas las áreas de la compañía.

Los anteriores elementos nos permitirán actuar de una manera efectiva ante un incidente cibernético y poder generar las medidas adecuadas para evitarlos, de acuerdo con la revista el economista el sector privado está reconociendo la importancia de la ciberseguridad ya que muchas compañías han migrado gran parte de sus servicios y almacenamientos a la nube por lo cual han comenzado a tomar medidas necesarias para garantizar la seguridad e integridad de su información y servicios, pero no solo las compañías privadas se han visto afectadas con incidentes de seguridad también se han presentado ataques a hospitales públicos en donde se ha

presentado el robo de información de los cuales en México se han presentado 12 incidentes, todos estos riesgos que ha tenido el sector tecnológico ha creado la necesidad en los diferentes mercados de enforcar gran parte de sus recursos al área tecnológica con el fin de garantizar la continuidad de sus operaciones y generar una buena reputación de la protección de sus datos ante sus clientes, (Riquelme, R. 2023, November 12).

Soluciones de Ciberseguridad Frente Amenazas

Luego de reconocer como actuar ante un incidente de ciberseguridad es importante identificar las diferentes herramientas que nos permitirán actuar de una manera efectiva, de acuerdo con el artículo del sitio web enfasys las empresas especializadas en respaldo de almacenamiento y recuperación de servicios como lo es Acronis están invirtiendo en inteligencia artificial y de esta manera ser más efectivos ante las amenazas de ciberseguridad, sin embargo también es importante evaluar comprender que el cambio se comienza si generamos una conciencia del impacto que puede llegar a ocasionar un ciberataque, los empleados representan el eslabón más débil en la ciberseguridad de una compañía por lo que es clave implementar capacitaciones que fomenten una cultura corporativa en torno a la ciberseguridad, iniciando por la alta dirección, ya que muchos líderes empresariales aún desconocen los riesgos e implicaciones de la seguridad informática., (Matias D'Ambrosio. 2023, November 21).

Protección de Cargas de Trabajo en la Nube

La protección de cargas de trabajo y servicios en la nube es un proceso clave para garantizar el correcto funcionamiento de las aplicaciones y el almacenamiento en entornos cloud, por lo cual para que una aplicación o servicio funcione adecuadamente se deben garantizar que todas las cargas de trabajo funcionen adecuadamente, con los pasos agigantados que ha tenido la tecnología también han surgido nuevos retos en ciberseguridad, en donde los ciberdelincuentes

están ejecutando cada vez más ataques con programas de robo de información por ello se hace necesario buscar estrategias de seguridad que se basen en proteger las terminales de forma preventiva, de acuerdo a lo anterior las empresas que utilizan nubes privadas deben enfocar sus esfuerzos en mitigar los riesgos y salvaguardar sus cargas de trabajo ante posibles amenazas, (VMware. 2024).

Solución de Blindaje de Cargas de Trabajo

Una solución altamente recomendada por Gartner para la protección de cargas de trabajo en la nube es Cloud Workload Protection Platform (CWPP), esta tecnología se especializa en garantizar la seguridad de los servidores en entornos de nube pública para ello CWPP tiene dos maneras de proteger las cargas de trabajo:

Microsegmentación

Una de ellas es la microsegmentación, una técnica de seguridad de red que consiste en dividir el centro de datos en múltiples segmentos de seguridad, llegando hasta el nivel individual de cada carga de trabajo. Al tratarse de un entorno virtualizado, este método permite establecer políticas de seguridad flexibles que aíslan y protegen las cargas de trabajo, esto impide que los programas maliciosos se trasladen de un servidor a otro.

Hipervisor Bare Metal

Otra forma de proteger las cargas de trabajo mediante el uso del hipervisor bare metal un software de virtualización que permite crear y administrar máquinas virtuales al separar el software del hardware del sistema, esta solución se instala directamente en el hardware de la maquina y se gestiona entre el hardware y el SO, esto permite aislar las máquinas virtuales si son atacadas garantizando las cargas de trabajo, esta solución es bastante adecuada ya que permite proteger toda nuestra infraestructura ante un incidente de seguridad.

Sistema de Detección de Intrusiones (IDS)

Dentro de los elementos que pueden contribuir al aseguramiento de la información podemos encontrar los sistemas de detección de intrusiones (IDS) los cuales monitorean en tiempo real el tráfico y los dispositivos que se encuentran en la red con el fin de encontrar actividades sospechosas, por lo cual es necesario evaluar qué sistema es el más adecuado para nuestros almacenamientos SAN y NAS de acuerdo con sus características en donde podemos encontrar dos tipos de sistemas de intrusión, (IBM. 2023, April 19).

Basado En Host (HIDS)

Es un software el cual está enfocado en analizar un determinado host, examinando cada uno de los registros del sistema, la actividad de los usuarios, la integridad de los archivos y las conexiones de red que se efectúan a dicho host, es desplegado mediante instalación de agentes el cual es instalado en el cliente, los eventos que monitorea son comparados con una base de datos de ataques o patrones registrados, al generarse alguna actividad inusual, envía alertas y notificaciones a los administradores de la red.

Basado en Red (NIDS)

Este sistema de detección está diseñada para analizar el tráfico de la red en busca de actividades sospechas que pueden inferir en un posible ataque cibernético, funciona de manera pasiva analizando los paquetes de datos de la red que se transportan en tiempo real, estos paquetes son analizados mediante el uso de técnicas como la detección basada en firmas y anomalías en los cuales compara con bases de datos de firmas de ataques conocidas, si encuentra una coincidencia genera una alerta, por otro lado la detección basada en anomalías reconoce desviaciones del comportamiento normal de una red e informa cualquier actividad sospechosa,

dándole al administrador de la red una herramienta adecuada para mitigar ataques mediante bloqueo de tráfico.

Aunque los IDS son herramientas bastante útiles no son infalibles y tienen debilidades, donde se pueden encontrar ataques que no pueden ser detectados sino se encuentran en firmas conocidas y generando falsos positivos, aunque tienen limitaciones son herramientas esenciales para el aseguramiento de la información y `pueden ser fortalecidos junto con otras medidas de seguridad, como firewalls, antivirus, políticas de seguridad entre otros, de acuerdo a lo anterior la solución más conveniente para nuestros almacenamientos SAN y NAS son aquellos basados en host (HIDS) los cuales se dedicaran de manera permanente a monitorear todas las actividades de estos dos elementos tan esenciales en nuestra red.

Sistema de Prevención de Intrusiones (IPS)

Los sistemas de prevención de intrusiones (IPS) surgieron como una evolución de los sistemas de detección de intrusos (IDS), que únicamente logran identificar e informar acerca de las amenazas, por lo tanto, un IPS realiza las mismas tareas que un IDS, pero además tiene la capacidad de bloquear el tráfico perjudicial, lo que disminuye la carga de trabajo de los equipos de seguridad y de los centros de operaciones de ciberseguridad (SOC),los IPS también facilitan la implementación de las políticas de seguridad de la red al impedir actividades no autorizadas, incluso de usuarios legítimos, estos sistemas de prevención de intrusiones emplean tres técnicas fundamentales para examinar el flujo de datos, ya sea de manera aislada o en conjunto como lo son:

Concientización del Usuario

Aunque todas las medidas anteriormente mencionadas contribuyen de manera significativa en el aseguramiento de la red, pueden ser obsoletas sino se capacita adecuadamente a los usuarios, los cuales juegan un papel crucial en la ciberseguridad de una compañía siendo el usuario el eslabón más débil en la cadena de seguridad informática, ya que, aunque se implementen políticas de seguridad y tecnologías un solo error humano puede comprometer toda la infraestructura de una empresa, un usuario capacitado en ciberseguridad tiene un impacto positivo significativo, entre los cuales se pueden destacar:

Reduce el Riesgo de Ciberataques

Cuando los usuarios están bien informados sobre las amenazas cibernéticas, como la ingeniería social y el phishing son menos propensos a caer en trampas que puedan comprometer la seguridad de la empresa como, por ejemplo, si un empleado recibe un correo electrónico sospechoso que solicita información confidencial, su conocimiento sobre phishing le permitirá identificar la amenaza y evitar hacer clic en enlaces o descargar archivos adjuntos maliciosos.

Fortalece las Políticas de Seguridad

Las políticas de seguridad son más efectivas cuando los usuarios las comprenden y las siguen, la concienciación ayuda a los empleados a entender la importancia de estas políticas y a aplicarlas en su trabajo diario lo cual puede incluir el uso de contraseñas seguras, la actualización regular del software y la denuncia de cualquier actividad sospechosa.

Protege la Información Confidencial

Los datos son uno de los activos más valiosos de una empresa, los usuarios conscientes de la importancia de la seguridad de la información son más propensos a manejarla con cuidado

y a seguir los protocolos de seguridad para protegerla, esto incluye el almacenamiento seguro de datos, el uso de cifrado y la eliminación adecuada de información confidencial.

Minimiza las Pérdidas Financieras

Los ataques cibernéticos pueden provocar un efecto económico considerable en las empresas, abarcando los gastos de restauración de datos, las sanciones por incumplimiento de las normativas y la disminución de ingresos como consecuencia de la interrupción de las operaciones, la sensibilización de los usuarios puede contribuir a evitar estos ataques y a mitigar las pérdidas económicas relacionadas.

Mejora la Reputación de la Empresa

Un ciberataque exitoso puede afectar la reputación de una compañía y perjudicar la confianza de sus clientes, al fomentar una cultura de concienciación en ciberseguridad, las empresas pueden demostrar su compromiso con la protección de la información y fortalecer la confianza de sus clientes.

La concienciación del usuario es clave para la ciberseguridad empresarial educando al personal interno y terceros que colaboren con la compañía sobre las amenazas y las mejores prácticas de seguridad, fomentando una cultura de protección sólida ayudando a defender las organizaciones frente a ciberataques y a garantizar que opere de manera segura y eficiente.

Conclusiones

Las soluciones de almacenamiento SAN y NAS juegan un papel esencial en la protección de los datos y servicios al brindar mecanismos que garantizan la integridad, disponibilidad y confidencialidad de la información por un lado la NAS brinda capacidades de autenticación de cifrado y control de accesos fortaleciendo así la seguridad de la red interna , por otro lado la SAN proporciona alta disponibilidad y segmentación de tráfico y replicación de datos lo cual minimiza riesgos ante ataques y contribuyen a un plan de recuperación, siendo ambas tecnologías de almacenamiento herramientas que contribuyen a la seguridad de la organización.

La protección adecuada de los sistemas de almacenamiento SAN y NAS requieren el desarrollo de estrategias integrales que contemplen tanto la configuración segura de los dispositivos como el aseguramiento de la infraestructura de red que la soporta, la adopción de buenas prácticas como la segmentación de redes, el control estricto de accesos y cifrado de datos es vital para minimizar la superficie de ataque y los riesgos que comprometan la información crítica.

El diseño de una infraestructura para los sistemas de almacenamiento SAN y NAS implica garantizar que todos los dispositivos de red como firewalls, routers y switches se encuentre configurados adecuadamente para mitigar vulnerabilidades comunes , la ausencia de configuraciones de seguridad representan riesgos significativos que pueden facilitar los ataques de los ciberdelincuentes, es por ello que una seguridad efectiva requiere de una gestión integral y continua de todos los elementos que interactúan con los sistemas de almacenamiento, teniendo en cuenta los aspectos técnicos como humanos.

Las organizaciones pueden optimizar sus almacenamientos NAS y SAN implementando estrategias integrales que aborden tanto la fortificación de la infraestructura de red que las

soportan como la configuración técnica de los dispositivos, esto sumado a políticas robustas de respaldo distribuido y monitoreo continuo, las compañías reducen significativamente su exposición a ciberataques preservando de esta manera la integridad, disponibilidad y confidencialidad de los datos y servicios críticos.

Recomendaciones

Para asegurar un entorno de almacenamiento seguro es necesario implementar medidas integrales como controles de acceso , autenticación multifactor (MFA),cifrados de datos en transito y reposo , así como medidas que garanticen la replicación de datos , además se deben evaluar de manera periódica las infraestructuras de almacenamiento con listas de verificación que contemplen aspectos de seguridad específicos tanto para las NAS como la SAN, asegurando de esta manera detección y mitigación de vulnerabilidades.

Es indispensable implementar medidas continuas de gestión de la seguridad donde se contemplen auditorias regulares de configuración, monitoreo de tráfico y detección de anomalías para los almacenamientos SAN y NAS, de la mano de capacitaciones del personal en practicas de seguridad que garanticen el cumplimiento de las políticas internas con el objetivo de reducir errores humanos que puedan ocasionar vulnerabilidades.

Se recomienda implementar un estricto programa de aseguramiento de dispositivos de red que contemple la actualización constante de firmware, el robustecimiento de uso de contraseñas, así como la gestión de usuarios con roles específicos, es vital emplear firewalls con políticas de filtrado avanzado que incluyan la inspección de paquetes con estado, además se debe promover revisiones periódicas y pruebas de vulnerabilidades para anticipar y mitigar posibles ataques.

Las organizaciones deben adoptar un enfoque multidimensional para proteger sus sistemas NAS y SAN, integrando tecnologías avanzadas como análisis de comportamiento y detección de anomalías para identificar rápidamente actividades sospechosas, es fundamental implementar un esquema de gestión de parches automatizado para asegurar que todos los dispositivos estén protegidos contra vulnerabilidades conocidas, finalmente se debe promover

una cultura organizacional orientada a la ciberseguridad con formación continúan y simulacros de respuesta ante incidentes reforzando de esta manera la infraestructura de los almacenamientos ante las diferentes amenazas.

Referencias Bibliográficas

Almacenamiento conectado a la red (NAS) volumen del mercado | Mordor Intelligence. (2024). Mordor Intelligence. https://www.mordorintelligence.com/es/industry-reports/network-attached-storage-nas-market

Agbo, J. C., Ezeali, P. C., Erhunmwunsee, D. O., & Bande, P. S. (2021). Security Framework for Storage Area Network (SAN). International Journal of Progressive Sciences and Technologies, 27(2), 267 Universidad de Nigeria.

Amazon Web Services, Inc. (2021). ¿Qué es el NAS? - Explicación del almacenamiento conectado a la red. AWS. https://aws.amazon.com/es/what-is/nas/#:~:text=La%20unidad%20NAS%20se%20conecta,otros%20dispositivos%20al%20dispositivo%20NAS

Aragón, D. (2016, noviembre 18). Encriptar archivos en servidores NAS para mejorar la seguridad. Qloudea Blog: Especialistas en Servidores NAS. https://qloudea.com/blog/encriptar-archivos-servidores-nas/

Augusto, G., Luz, A., & Enrique, L. (2024). Aproximación al ciberdelincuente desde la perspectiva del control social. Revista Criminalidad, 65(3), 81–95. https://doi.org/10.47741/17943108.508

Bracci, F. (s.f.). Mapeo sectorial. CAMTIC. https://www.camtic.org/wp-content/uploads/2017/06/CAMTIC-Mapeo-Sectorial.pdf

Ciberseg1922. (2020, mayo 11). Plan de respuesta a incidentes de seguridad. Ciberseguridad. https://ciberseguridad.com/normativa/espana/medidas/plan-respuesta-incidentes-seguridad/

Colaborador de TechTarget. (2021). Autenticación multifactor o MFA. ComputerWeekly.es. https://www.computerweekly.com/es/definicion/Autenticacion-multifactor-o-MFA

Container and Kubernetes security. (2024, octubre). Sysdig. https://sysdig.com/solutions/container-and-kubernetes-security/

Cybersecurity and Infrastructure Security Agency (CISA). (2024). Resumen de CISA ChemLock. https://www.cisa.gov/resources-tools/resources/resumen-de-cisa-chemlock

Cisco. (2025). ¿Qué es una red de área de almacenamiento (SAN)? https://www.cisco.com/site/us/en/learn/topics/computing/what-is-storage-area-networking.html

Chukry, S., & Sbeyti, H. (2019). Security enhancement in storage area network. En Proceedings of the 2019 7th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1–5). IEEE. https://doi.org/10.1109/ISDFS.2019.8757492

Digi.com. (2015). Gestión fuera de banda y resistencia de la red. https://es.digi.com/solutions/by-technology/out-of-band-management

Flores Miranda, M. (2023, 4 de septiembre). La norma ISO 27040 y su rol en el almacenamiento seguro de la información. Delete Technology. Recuperado de https://www.deletetechnology.com/blog/la-norma-iso-27040-y-su-rol-en-el-almacenamiento-seguro-de-la-informacion

FS Community. (2023). Explicación de los conceptos básicos de seguridad del switch. Knowledge. https://community.fs.com/es/article/basic-switch-security-concepts-explained.html

Gallardo, I., Bazán, P., & Venosa, P. (2019). Arquitectura de certificados digitales: De una arquitectura jerárquica y centralizada a una distribuida y descentralizada. Revista Ibérica de Sistemas e Tecnologias de Informação, 32, 49–66. https://doi.org/10.17013/risti.32.49-66

Google Cloud. (2024). ¿Qué es IaaS (infraestructura como servicio)?. https://cloud.google.com/learn/what-is-iaas?hl=es

Grupo Atico34. (2023, junio 14). Integridad informática: ¿Qué es y cómo proteger los datos? https://protecciondatos-lopd.com/empresas/integridad-informatica/

Gutiérrez, J. (2023, septiembre 14). El ataque de ransomware a IFX Telecomunicaciones. ESoft LATAM. https://esoft.com.co/blog/2023/09/14/ataque-de-ransomware-ifx-entidades-publicas-colombia/

Hacker vs. ciberdelincuente. (2021). INCIBE. https://www.incibe.es/aprendeciberseguridad/hacker-vs-ciberdelincuente

Hernández, Y. (2022, abril 18). ¿Qué es una amenaza en seguridad informática y cómo prevenirla? Tutoriales Dongee. https://www.dongee.com/tutoriales/que-es-una-amenaza-en-seguridad/

IBM. (2016). Introduction to storage area networks. IBM Redbooks. https://www.redbooks.ibm.com/redbooks/pdfs/sg245470.pdf

IBM. (2021, julio 19). Amenazas internas. https://www.ibm.com/mx-es/topics/insider-threats

IBM. (2021, julio 27). Storage area network. https://www.ibm.com/mx-es/topics/storage-area-network

IBM. (2024, mayo 17). Phishing. https://www.ibm.com/es-es/topics/phishing

IBM. (2024, agosto 20). Respuesta a incidencias. https://www.ibm.com/mx-es/topics/incident-response

IBM. (2025, 6 de agosto). ¿Qué es el almacenamiento conectado en red (NAS)? https://www.ibm.com/think/topics/network-attached-storage

International Organization for Standardization. (2024). ISO/IEC 27040:2024 Information technology — Security techniques — Storage security (2nd ed.). ISO. https://www.iso.org/standard/80194.html

Infordisa. (2016, diciembre). Comparativa SAN vs. NAS. https://www.infordisa.com/es/comparativa-san-vs-nas/

ISO/IEC. (2024). Information technology — Security techniques — Storage security (ISO/IEC 27040:2024, Edición 2). International Organization for Standardization. https://www.iso.org/standard/80194.html

Juniper Networks. (2024). Fibre Channel overview. https://www.juniper.net/documentation/mx/es/software/junos/storage/topics/concept/fibre-channel-overview.html

Kaspersky, L. G. (2017, diciembre 12). Cómo proteger los equipos NAS del malware. Kaspersky.es. https://www.kaspersky.es/blog/nas-security/14996/

Kaspersky, P. A. (2017, mayo 13). WannaCry: ¿estás a salvo? Kaspersky.es. https://www.kaspersky.es/blog/wannacry-ransomware/10503/

KIO. (2021). Almacenamiento de datos digitales en el ADN. https://www.kio.tech/blog/data-center/almacenamiento-de-datos-digitales-en-el-adn

La regla de las copias de seguridad 3-2-1 explicada. (2024, marzo 18). NinjaOne. https://www.ninjaone.com/es/blog/3-2-1-respaldo-de-seguridad-explicado/#:~:text=La%20norma%20establece%20que%20debes,sitio%20o%20en%20la%20nube

Ley 1581 de 2012 Protección de Datos Personales. (2016). Prezi.com. https://prezi.com/umhfwxljovd6/ley-1581-de-2012-proteccion-de-datos-personales/

Media, D. (2022, septiembre 22). Protección contra el ransomware en los sistemas de almacenamiento NAS. Ituser.es. https://almacenamientoit.ituser.es/noticias-y-actualidad/2022/09/proteccion-contra-el-ransomware-en-los-sistemas-de-almacenamiento-nas

Media, D. (2023, agosto 28). NetApp y Google Cloud introducen servicios de almacenamiento gestionado. Ituser.es. https://www.ituser.es/actualidad/2023/08/netapp-y-google-cloud-introducen-servicios-de-almacenamiento-gestionado

Mesa editorial Merca2.0. (2018, abril 15). Los dispositivos de almacenamiento a través del tiempo. Revista Merca2.0. https://www.merca20.com/los-dispositivos-de-almacenamiento-a-traves-del-tiempo/

Ortega, R. (2023, julio 17). Acceso, gestión y seguridad en entornos híbridos de almacenamiento para PyMEs: Los nuevos retos del canal. ESemanal - Noticias del Canal. https://esemanal.mx/2023/07/acceso-gestion-y-seguridad-en-entornos-hibridos-de-almacenamiento-para-pymes-los-nuevos-retos-del-canal/

Prestigia Seguridad. (2022, febrero 8). Seguridad en routers corporativos. https://seguridad.prestigia.es/seguridad-en-routers-corporativos/

Rentero, A. (2023, abril 18). Los backup, nuevo objetivo para los ciberdelincuentes. Silicon. https://www.silicon.es/los-backup-nuevo-objetivo-para-los-ciberdelincuentes-2476918

Redacción Data Center Market. (2022, julio 29). El 88% de ataques de ransomware intentaron afectar los repositorios de backup. Data Center Market. https://www.datacentermarket.es/tendencias-ti/el-88-de-ataques-de-ransomware-intentaron-afectar-los-repositorios-de-backup/

Riquelme, R. (2023, noviembre 12). Empresas empiezan a tener compromiso en ciberseguridad, pero falta mucho por hacer: Industria. El Economista. https://www.eleconomista.com.mx/empresas/Empresas-empiezan-a-tener-compromiso-en-ciberseguridad-pero-falta-mucho-por-hacer-industria-20231111-0020.html

Synology Inc. (2025). Hot Spare | DSM [Base de conocimiento, versión 7]. Centro de conocimientos de Synology. https://kb.synology.com/es-es/DSM/help/DSM/StorageManager/hotspare?version=7

TEAM, A. (2022). Diferencias entre amenaza, vulnerabilidad y riesgo. Ambit-Bst.com. https://www.ambit-bst.com/blog/diferencias-entre-amenaza-vulnerabilidad-y-riesgo

Tecnozero Soluciones Informáticas. (2022, diciembre 28). Firewall de red: Cuadrante Mágico de Gartner 2022. Tecnozero. https://www.tecnozero.com/blog/cuadrante-magico-de-gartner-para-firewalls-de-red-2022/

Varguez, C. (2021, junio 23). La guía de fiabilidad del ingeniero para entender la seguridad en dispositivos IoT, LAN y WAN. ERBESSD Instruments. https://www.erbessd-instruments.com/es/articulos/la-guia-de-fiabilidad-del-ingeniero-para-entender-la-seguridad-en-dispositivos-iot-lan-y-wan/#:~:text=SEGURIDAD%20DE%20RED%20LAN/WAN,-Un%20cortafuegos%20o

Vive UNIR. (2021, marzo 31). Confidencialidad en seguridad informática: Claves para garantizarla. UNIR. https://www.unir.net/revista/ingenieria/confidencialidad-seguridad-informatica/

Walton, A. (2018, febrero 10). Cómo mantener la seguridad de la red. CCNA desde Cero. https://ccnadesdecero.es/seguridad-red-lan/

Yúbal Fernández. (2020, junio 2). Malware: Qué es, qué tipos hay y cómo evitarlos. Xataka Basics. https://www.xataka.com/basics/malware-que-que-tipos-hay-como-evitarlos

Apéndices

Apendice A

Glosario

Amenaza. Se define como la explotación de una vulnerabilidad o fallo el cual es usado para afectar la operación de un sistema (Hernández, 2022, 18 de abril).

Confidencialidad. Permite garantizar que la información solo puede ser accedida por los usuarios autorizados (Vive UNIR, 2021, 31 de marzo).

Conmutar. Permite conectar varios servidores al dispositivo de almacenamiento compartido.

Cloud. Es la disponibilidad bajo demanda de los recursos de computación a través de internet, evitando que las compañías se encarguen del aprovisionamiento de los recursos.

Ciberdelincuente. Persona que busca sacar provecho de problemas o fallos de seguridad mediante herramientas de ingeniería social o malware (INCIBE, 2021).

Disponibilidad. Permite asegurar el acceso oportuno a los datos y los recursos a los usuarios autorizados.

Ingeniería social. Son las diferentes técnicas que usa un delincuente para obtener información confidencial de los usuarios engañando a sus víctimas y utilizando como herramientas correos falsos, mensajes de texto, llamadas telefónicas, entre otros.

Integridad. Garantiza que los datos no hayan sido manipulados o corrompidos, por lo cual deben ser confiables (Grupo Atico34, 2023, 14 de junio).

Riesgo. Es la posibilidad de que un sistema presente una anomalía a nivel de seguridad y que una amenaza se materialice (Team A, 2022).

Vulnerabilidad. Es una debilidad de un sistema el cual puede ser atacado y recibir un daño.