UNIVERSIDAD TÉCNICA DE BABAHOYO FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN SISTEMA DE INFORMACIÓN

ESTUDIANTE:

EDER SNEIDER CABRERA VITERI

TEMA:

ANALISIS DE LAS TECNOLOGIAS DE ALMACENAMIENTO EN BLOQUE EN TERMINOS DE SEGURIDAD EN LOS CENTROS DE DATOS.

TUTOR:

ING. FABIAN EDUADOR ALCOSE CANTUÑA

PROCESO DE TITULACION

ABRIL 2024- AGOSTO 2024

Resumen

El presente estudio se centra en el análisis detallado de las tecnologías de almacenamiento en bloques utilizadas en los centros de datos, con un enfoque particular en sus implicaciones de seguridad. Se exploran las arquitecturas y soluciones predominantes en el mercado, como SAN (Storage Area Network) y NAS (Network Attached Storage), evaluando sus fortalezas y debilidades en términos de protección de datos y resiliencia frente a ataques cibernéticos.

El estudio aborda aspectos clave como la encriptación de datos en reposo y en tránsito, la gestión de accesos y autenticación, la implementación de mecanismos de respaldo y recuperación ante desastres, así como la monitorización y auditoría de accesos.

Se realizan comparaciones entre tecnologías de almacenamiento tradicionales y emergentes, incluyendo el uso de soluciones basadas en la nube y tecnologías de almacenamiento. El análisis también contempla el impacto de tecnologías innovadoras como la inteligencia artificial y el aprendizaje automático en la detección y prevención de amenazas.

Palabras claves: Tecnologías de almacenamiento en bloques, Centros de datos, Seguridad de datos, SAN (Storage Area Network), NAS (Network Attached Storage), Encriptación de datos, Autenticación y gestión de accesos, Respaldo y recuperación ante desastres, Monitorización y auditoría de accesos, Almacenamiento en la nube, Protección de la información, Integridad de los datos, Confidencialidad de la información.

Abstract

This study focuses on a detailed analysis of block storage technologies used in data centers, with a particular focus on their security implications. The predominant architectures and solutions on the market, such as SAN (Storage Area Network) and NAS (Network Attached Storage), are explored, assessing their strengths and weaknesses in terms of data protection and resilience against cyber attacks.

The study addresses key aspects such as encryption of data at rest and in transit, access management and authentication, implementation of backup and disaster recovery mechanisms, as well as access monitoring and auditing.

Comparisons are made between traditional and emerging storage technologies, including the use of cloud-based solutions and storage technologies. The analysis also considers the impact of innovative technologies such as data intelligence, data protection, and data protection in the cloud.

Keywords: Block storage technologies, Data centers, Data security, SAN (Storage Area Network), NAS (Network Attached Storage), Data encryption, Authentication and access management, Backup and disaster recovery, Access monitoring and auditing, Cloud storage, Information protection, Data integrity, Information confidentiality.

INDICE

PLANTEAMIENTO DEL PROBLEMA

En el mundo digital actual, los centros de datos son el núcleo de la infraestructura corporativa, ya que almacenan mucha información sobre la información personal de la organización. La seguridad de los datos es muy importante, por lo que es importante identificar el dispositivo de bloqueo adecuado.

El almacenamiento en bloque es una forma de almacenar datos físicamente, como en un disco duro o en un centro de datos. Es importante comprender los riesgos de seguridad asociados con este tipo de almacenamiento y las formas en que se pueden mitigar para proteger la información almacenada en él.

Si bien la tecnología de almacenamiento de bloques es excelente, puede presentar una variedad de problemas, incluidos fallas de diseño, errores de configuración y errores de software. Estas vulnerabilidades podrían permitir que un atacante obtenga acceso no autorizado, corrompa datos o impida operaciones. En el entorno actual impulsado por los datos, abordar estos desafíos es fundamental para proteger los datos confidenciales, garantizar el cumplimiento y mantener la continuidad del negocio.

Este estudio tiene como objetivo resolver este problema analizando las tecnologías de almacenamiento en bloques y evaluar su efectividad en la seguridad del centro de datos. A través de este análisis, proporcionará a las organizaciones que quieran fortalecer su infraestructura de almacenamiento y proteger sus datos de posibles amenazas y ataques información valiosa para saber qué tecnología de almacenamiento en bloque es la más segura y eficiente.

JUSTIFICACION

Las amenazas a la seguridad evolucionan constantemente y surgen nuevos ataques cada vez más. Es importante que las organizaciones sean conscientes de estas amenazas y tomen las medidas necesarias para proteger sus datos. Los centros de datos contienen una gran cantidad de información, incluida información financiera, así como información personal y registros de la empresa.

La pérdida o el robo de estos datos puede tener un impacto negativo en su organización, incluido daño a la reputación, pérdida de ingresos y sanciones legales. El movimiento de estos datos puede resultar muy costoso y la seguridad de estos datos es responsabilidad de la organización.

Este análisis permitirá a las organizaciones identificar riesgos de seguridad relacionados con el centro de bloques de hardware, cuando se identifican y evalúan las amenazas y los riesgos, se puede priorizar el impacto y los riesgos para mitigarlos con las medidas de seguridad adecuadas. Al proteger los datos, las organizaciones pueden mejorar la seguridad de sus datos y reducir el riesgo de violaciones de datos.

OBJETIVOS

OBJETIVO GENERAL

- Analizar las tecnologías de almacenamiento en bloque en términos de seguridad en los centros de datos.

OBJETIVO ESPECIFICOS

1. Identificar las tecnologías de almacenamiento en bloque para determinar las amenazas de seguridad a las tecnologías de almacenamiento en bloque.
2. Comparar las diferentes tecnologías de almacenamiento en bloque en términos de seguridad.
3. Evaluar las tecnologías de almacenamiento en bloque en términos de seguridad.

LINEA DE INVESTIGACION

El presente caso de estudio se centra en la línea de investigación “Sistemas de información y comunicación, emprendimiento e innovación” ya que nos proporciona un marco teórico y metodológico para entender cómo se estructuran y gestionan los datos dentro de los centros de datos. Además, te permitirán explorar soluciones innovadoras que mejoren la seguridad de los datos, así como evaluar la viabilidad comercial de estas soluciones para startups o empresas en el sector de la tecnología.

Se relaciona con la sublínea “Redes y tecnologías inteligentes de software y hardware” debido a que se centra en la implementación de soluciones tecnológicas avanzadas que optimicen la gestión de datos y mejoren la seguridad.

MARCO TEORICO

El almacenamiento en bloques es un almacenamiento de datos que utiliza volúmenes de un entorno SAN, iSCSI y de disco local, cada bloque puede existir como una partición independiente. Un archivo de bloque es un formato de archivo que se almacena en bloques. Las empresas suelen utilizar blockchain cuando necesitan transferir datos de forma rápida, precisa y eficiente, como cuando recuperan información de una base de datos. Los sistemas operativos como Linux y Windows pueden acceder a los bloques de los siguientes métodos Fibre Channel sobre Ethernet (FCoE), Fibre Channel o iSCSI.

¿Cómo funciona el almacenamiento en bloque?

Con el almacenamiento en bloques, cada bloque contiene una gran cantidad de datos (normalmente de 256 KB a 4 MB). Cada bloque representa una sección del archivo que no está organizada en un orden particular. De hecho, es posible que los datos de bloques adyacentes no tengan nada que ver entre sí. Cada bloque tiene un identificador único para distinguirlo de otros bloques. Cuando se descarga un archivo, la aplicación emite una solicitud que busca y ensambla los bloques.

Aparte del identificador, el bloque no tiene metadatos. Como no hay metadatos, el almacenamiento en bloques es muy eficiente porque casi todos los bloques contienen datos reales dentro de su capacidad de almacenamiento. No se pierde tiempo. Esto hace que el almacenamiento en bloque sea adecuado para aplicaciones que requieren un escalado vertical rápido obteniendo un rendimiento rápido de lectura y escritura.

Ventajas y Desventajas del Almacenamiento en Bloques

Como cualquier otra tecnología, el almacenamiento en bloque tiene ventajas y desventajas. Dicho esto, los beneficios del almacenamiento blockchain son claros. Esto significa que es mejor para alto rendimiento y acceso rápido a datos.

Ventajas principales del almacenamiento en bloques:

Mayor rendimiento: el almacenamiento en bloques puede lograr un mayor rendimiento que otros tipos de almacenamiento porque los usuarios pueden acceder a los datos rápidamente. Minimizar la latencia de la solicitud o el tiempo de respuesta de su aplicación es fundamental para lograr sus objetivos de rendimiento.

Modificabilidad: el almacenamiento en bloque permite modificar los archivos sin eliminar todos los datos de los archivos, como ocurre con los sistemas de archivos tradicionales. Puede realizar cambios, por ejemplo, reemplazando, eliminando o insertando bloques. Esto es útil para archivos que se actualizan con frecuencia, como archivos de bases de datos.

Mejorar la confiabilidad: bloquear el almacenamiento ayuda a garantizar que las aplicaciones importantes estén siempre disponibles.

En caso de falla, las organizaciones pueden recuperar rápida y fácilmente los datos de los informes de respaldo.

Desventajas del almacenamiento en bloques

Por supuesto, el almacenamiento en bloques también tiene sus desventajas. No se puede negar que es más caro que otros tipos de almacenamiento y puede que no sea la mejor solución para cada tarea.

Estas son algunas de las desventajas del almacenamiento en bloques:

Alto costo: el almacenamiento en bloques cuesta más que otros tipos de almacenamiento. Por ejemplo, las SAN son caras de adquirir y mantener.

Mayor complejidad: el almacenamiento en bloque es más complejo de administrar que otros tipos de almacenamiento. Por ejemplo, es posible que necesite capacitación y/o experiencia adicional para administrar de manera efectiva.

Metadatos limitados: el almacenamiento en bloques admite metadatos. Esto dificulta el seguimiento y la recuperación de datos almacenados en los sistemas de almacenamiento en bloque. (Storage, 2023)

Tipo de almacenamientos

Almacenamiento en Bloques

El almacenamiento en bloques, también conocido como almacenamiento en bloques elástico, es una secuencia de bytes de datos que contiene múltiples registros de longitud suficiente (tamaño de bloque). El proceso de almacenar datos en el registro se llama bloqueo y el proceso de recuperar datos del registro se llama apertura. Los dispositivos bloqueados generalmente se almacenan en un almacén de datos y se leen o escriben en bloques para reducir la sobrecarga y acelerar el almacenamiento de datos.

Las empresas necesitan tener bloques de datos organizados de cierta manera para que tengan sentido cuando se intenta leerlos de un registro. todo se almacena en forma de bloques. Lo más importante es cómo se organizan estos datos a nivel de bloque y cómo se accede a ellos, lo que determina su tipo de almacenamiento.

Caso de uso de almacenamiento en bloque

Por su propia naturaleza, el almacenamiento en bloque es ideal para:

- Bases de datos transaccionales: bases de datos que requieren baja latencia y alto rendimiento de IOP, como bases de datos financieras o transaccionales.
- Volúmenes RAID: los bloques se pueden almacenar en volúmenes RAID, que combinan varios discos mediante duplicación para proporcionar redundancia.
- Servidor de correo electrónico: el almacenamiento en bloque es la primera opción para el almacenamiento de correo electrónico debido a su alto rendimiento. (Qumulo, 2022)

Almacenamiento de objetos

El almacenamiento de objetos es un sistema de almacenamiento de datos que gestiona datos como objetos con identificadores únicos que contienen datos y metadatos. Estos objetos contienen subconjuntos de datos que se almacenan en una estructura plana en lugar de una jerarquía.

El almacenamiento de objetos también contiene metadatos, como características de archivos, información descriptiva o información de seguridad/herramientas. En este tipo de almacenamiento, el acceso a los datos se produce a través de API o interfaces de usuario. El almacenamiento de objetos generalmente se almacena en servidores en la nube, pero también se puede almacenar localmente.

Características del almacenamiento de objetos

Las siguientes son algunas de las características principales del almacenamiento a nivel de objetos.

- Hay varias opciones de instalación: nivel de hardware, nivel de sistema y nivel de interfaz.

- Capacidad para almacenar y gestionar grandes cantidades de datos no estructurados. Esta es una tendencia particularmente importante en campos como la inteligencia artificial y el big data.
- Capacidades mejoradas de indexación, gestión y búsqueda. Los usuarios pueden buscar y encontrar datos utilizando metadatos, contenido de objetos y otros atributos.
- Bajo rendimiento en comparación con el almacenamiento de archivos y el almacenamiento en bloques. La codificación backend (EC) agrega latencia y tiempo de procesamiento.
- La escalabilidad es buena.

Casos de uso de almacenamiento de objetos

Existen mejores casos de uso de almacenamiento, por ejemplo:

- Gestión de datos de IoT: IoT y el almacenamiento se complementan bien. El almacenamiento de objetos hace que la recopilación de datos sea fácil y permanente y garantiza que haya archivos grandes.
- Saga Intelligence: los sistemas inteligentes requieren una alta escalabilidad y pueden admitir el almacenamiento de objetos.
- Cuidado de la salud: el almacenamiento de objetos puede transferir datos de pacientes entre varios dispositivos.
- Copia de seguridad y restauración: estos conjuntos de datos no necesitan actualizarse periódicamente para admitir la copia de seguridad y la restauración. (Rahim, 2024)

Almacenamiento de archivos

El almacenamiento de archivos o almacenamiento basado en archivos es un sistema de almacenamiento de datos que organiza los datos como archivos utilizando listas de archivos, carpetas y subcarpetas. Los datos se almacenan en archivos definidos por nombre de archivo, extensión y ruta (/carpeta/subcarpeta/nombredearchivo.ext).

La extensión depende del tipo de datos contenidos en el archivo (por ejemplo, .png para imágenes, .mp3 para audio o .doc para texto). Este es el tipo de almacenamiento más común entre los usuarios porque funciona de manera muy similar a un sistema de almacenamiento físico. Puede acceder fácilmente a los archivos utilizando el administrador de archivos o mostrando la ruta del archivo.

Las siguientes son algunas de las características principales del almacenamiento a nivel de archivos.

- Una estructura jerárquica facilita la búsqueda y administración de archivos. Tiene una interfaz sencilla para crear, editar y eliminar archivos.
- Acceder al archivo. Permiso para acceder, compartir y bloquear archivos definidos a nivel de usuario.
- La protección con contraseña también está disponible. Se puede acceder a datos no estructurados porque los metadatos son limitados.

Casos de uso del almacenamiento de archivos

El almacenamiento de archivos está diseñado para diferentes propósitos y usos, tales como:

- Sistemas de gestión de documentos.

- Compatibilidad y acceso grupal, porque se puede acceder a los archivos y modificarlos al mismo tiempo (el sistema de producción puede evitar la pérdida de datos).
- Disaster
- Recovery,
- backups y archivado.
- Analítica de datos.
- Aprendizaje automático. (Stackscale, 2023)

Centro de datos

Los centros de datos son instalaciones físicas que las organizaciones utilizan para almacenar sus aplicaciones y datos críticos. La estructura del centro de datos se basa en una red de recursos informáticos y de almacenamiento que permiten la entrega simultánea de programas y datos. Los componentes principales de la arquitectura de un centro de datos incluyen enrutadores, conmutadores, firewalls, sistemas de almacenamiento, servidores y controladores de entrega de aplicaciones.

Los centros de datos actuales son muy diferentes a los del pasado. La infraestructura ha pasado de servidores locales tradicionales a redes virtuales que admiten aplicaciones y cargas de trabajo en clústeres de infraestructura física y en entornos de múltiples nubes.

Hoy en día, los datos existen y están conectados a centros de datos, bordes y nubes públicas y privadas. Los centros de datos deben poder comunicarse entre estos sitios, tanto localmente como en la nube. Incluso una nube pública es un conjunto de centros de datos. Al alojar una aplicación en la nube, la aplicación utiliza los recursos del centro de datos del proveedor de servicios en la nube. En el mundo de la TI empresarial,

los centros de datos están diseñados para soportar aplicaciones y operaciones empresariales, incluyendo: Correo electrónico y uso compartido de archivos Aplicaciones de productividad Gestión de relaciones con el cliente (CRM) Planificación de recursos empresariales (ERP) y bases de datos. Big data, inteligencia artificial y aprendizaje automático, Escritorios virtuales, servicios de comunicación y colaboración.

Componentes clave de un centro de datos

Red de área de almacenamiento (SAN) vs. almacenamiento conectado a red (NAS)

¿Qué es un SAN?

La red de área de almacenamiento (SAN) es una red dedicada de alta velocidad que conecta servidores y dispositivos de almacenamiento, lo que permite compartir recursos de almacenamiento de red. Las SAN suelen utilizar la tecnología Fibre Channel para crear una red dedicada al almacenamiento de datos. Opera independientemente de una red de área local (LAN) y admite acceso al almacenamiento a nivel de bloque, lo que lo hace adecuado para aplicaciones que requieren datos rápidos y de bajo volumen.

¿Cómo funciona SAN?

SAN utiliza una arquitectura de red de almacenamiento única para proporcionar acceso directo y de alta velocidad a dispositivos de almacenamiento a nivel de bloque. Fibre Channel es una tecnología ampliamente utilizada en SAN, que utiliza conmutadores especializados y controladores de almacenamiento para crear conexiones entre servidores y dispositivos de almacenamiento. Las SAN suelen construirse utilizando un controlador de almacenamiento, que gestiona los discos físicos y los presenta como unidades lógicas a los servidores conectados. Los servidores pueden acceder a unidades lógicas como si

estuvieran conectados directamente a dispositivos de almacenamiento, lo que permite una transferencia de datos extremadamente rápida.

¿Qué es NAS?

El almacenamiento conectado en red (NAS) es una solución a nivel de archivos que se conecta a una red de área local y proporciona recursos de almacenamiento compartido a múltiples clientes o servidores. A diferencia de las SAN, los dispositivos NAS funcionan a través de protocolos de red estándar como Ethernet, TCP/IP y NFS o SMB/CIFS, y tienen estructuras de datos no estándar para una mayor tolerancia a fallos. Los sistemas NAS son fáciles de administrar y brindan una forma simplificada de compartir archivos y almacenar datos.

¿Cómo funciona NAS?

Por otro lado, los sistemas NAS utilizan protocolos de red estándar y actúan como servidores de archivos dedicados conectados a una LAN. Utilizan redes Ethernet e IP para comunicarse con los clientes y proporcionar acceso a datos a nivel de archivos.

Los dispositivos NAS vienen con sus propios sistemas operativos y sistemas de archivos, lo que les permite administrar el almacenamiento de archivos y realizar diversas tareas de administración de datos de forma independiente. El sistema de archivos NAS le permite almacenar y compartir archivos entre dispositivos. Los clientes pueden acceder a los archivos almacenados en un NAS utilizando protocolos como NFS (Network File System) o SMB (Server Message Block).

Casos de uso del almacenamiento conectado a red

El NAS se utiliza comúnmente para almacenamiento centralizado de archivos, uso compartido y big data por parte de PYMES, nuevas empresas y empresas que necesitan

minimizar sus costos de dispositivos de almacenamiento de estaciones de trabajo independientes.

Almacenamiento y uso compartido de archivos: Los dispositivos NAS se suelen utilizar para almacenar y compartir archivos entre varios clientes en redes domésticas, oficinas pequeñas o grupos de trabajo. Un único dispositivo NAS permite a los departamentos de TI consolidar múltiples servidores de archivos para facilitar la administración y, al mismo tiempo, ahorrar espacio y energía.

Archivos activos: NAS es útil para crear archivos activos que requieren acceso a archivos activos. Proporciona resultados de investigación a largo plazo y de bajo costo que reemplazan la cinta o el acondicionador.

Datos principales: NAS se puede utilizar para almacenar y administrar archivos grandes sin organizarlos en carpetas. Admite herramientas analíticas, ETL (consumir, transformar, cargar) e integración para la gestión y análisis de big data.

Casos prácticos de redes de área de almacenamiento

El almacenamiento de aplicaciones se utiliza a menudo en aplicaciones críticas para el negocio.

Alto rendimiento: las SAN se utilizan a menudo en áreas de informática intensiva y procesamiento de grandes datos, como investigación, ingeniería y finanzas.

Datos de misión crítica: las SAN brindan acceso rápido y directo a los datos, lo que las hace ideales para aplicaciones de datos de alta calidad.

Almacenamiento rápido: el almacenamiento local facilita la recuperación de datos y la recuperación ante desastres, garantiza el acceso ininterrumpido a datos críticos y reduce el tiempo de inactividad en caso de falla. (Vincent, 2023)

Diferencias entre SAN y NAS

NAS

- Un dispositivo de almacenamiento único que transfiere archivos a través de Ethernet.
- Es más barato y más fácil de configurar.
- Basado en Ethernet.
- La atención se centra en la facilidad de uso y mantenimiento.
- Escalabilidad y bajo coste (TCO).
- Los controladores comparten el almacenamiento y luego poseen el sistema de archivos.
- Un servidor Windows o UNIX/Linux es eliminado por un servidor que utiliza almacenamiento.

SAN

La red está estrechamente acoplada con múltiples dispositivos que manejan datos en bloque.

- Más caro.
- Difícil de configurar y administrar
- Ideal para aplicaciones de misión crítica y respaldo.
- Puede utilizar Ethernet y Fibre Channel
- Centrados en alto rendimiento y baja latencia

Desde la perspectiva del usuario, la mayor diferencia entre NAS y SAN es que los dispositivos NAS parecen volúmenes en un servidor de archivos y utilizan protocolos como NFS y SMB/CIFS, mientras que los discos conectados a una SAN aparecen para el usuario como discos locales.

Las debilidades de NAS se relacionan con la escala y el rendimiento. A medida que más usuarios requieren acceso, es posible que el servidor no siempre permanezca disponible, lo que requiere escalabilidad. Otra debilidad se relaciona con la naturaleza misma de Ethernet. Por diseño, Ethernet transmite datos de un lugar a otro a través de paquetes, dividiendo el origen en múltiples segmentos y enviándolos a su destino. Cualquier paquete de este tipo puede retrasarse o enviarse fuera de servicio y puede no estar disponible para el usuario hasta que todos los paquetes hayan llegado y se hayan devuelto en orden.

El desafío de una SAN se puede resumir en sus requisitos de costo y administración: tener que dedicar y mantener una red Ethernet separada para solicitudes de archivos de metadatos e implementar una red Fibre Channel puede ser una inversión significativa. Las SAN son la única forma de proporcionar un acceso a datos muy rápido a una gran cantidad de usuarios que también puede escalarse para admitir cientos de usuarios simultáneamente. Tanto el almacenamiento SAN como el NAS son métodos para administrar el almacenamiento de forma centralizada y compartirlo con múltiples hosts (servidores), ambos son seguros y pueden implementar cifrado de datos, pero se implementan de manera diferente. (KIO, 2022)

El estándar de infraestructura y diseño de centros de datos más aceptado es ANSI/TIA-942. Incluye estándares de certificación de cumplimiento ANSI/TIA-942, que brindan cumplimiento con una de cuatro categorías de niveles de centros de datos, clasificados por niveles de redundancia y resiliencia.

Nivel1: Arquitectura básica. Los centros de datos de nivel 1 brindan una protección mínima de las actividades físicas. Una fuente de alimentación y un canal de distribución no utilizado.

NIvel 2: estructura de piezas, etc. Estos datos están protegidos de la actividad física. Dispone de varios componentes electrónicos y tubería de distribución adicional.

Nivel 3: Infraestructura de instalaciones con soporte paralelo. Este centro de datos protege contra prácticamente cualquier evento físico al ofrecer componentes redundantes con múltiples rutas de propagación independientes. Cada componente se puede quitar o reemplazar sin interrumpir el servicio a los usuarios finales.

Nivel 4. Infraestructura a prueba de fallos de la instalación. Este centro de datos proporciona los niveles más altos de tolerancia a fallas y redundancia. Los componentes redundantes y las múltiples rutas de distribución independientes permiten que el mantenimiento simultáneo y las fallas únicas se propaguen por toda la instalación sin causar tiempo de inactividad. (Cisco, 2022)

Diferencias entre almacenamiento en bloques y almacenamiento de objetos

Ambas soluciones de almacenamiento son útiles según el caso de uso. El almacenamiento en bloque proporciona baja latencia y altos valores de rendimiento para una variedad de casos de uso. Sus características son principalmente útiles para el almacenamiento de bases de datos estructuradas, volúmenes de sistemas de archivos de máquinas virtuales y grandes volúmenes de operaciones de lectura y escritura. El almacenamiento de objetos se utiliza mejor para grandes volúmenes de datos no estructurados, especialmente cuando la durabilidad, el almacenamiento ilimitado, la escalabilidad y la gestión sofisticada de metadatos son factores importantes para el rendimiento general.

Diferencias entre almacenamiento en bloque y almacenamiento de archivos

Los sistemas de archivos almacenan información en áreas específicas y los sistemas de archivos se pueden integrar en muchos sistemas operativos. El almacenamiento de archivos proporciona a los usuarios finales una interfaz familiar de procesamiento de datos. Al mismo tiempo, puede agregar nuevos bloques de datos al sistema de almacenamiento en bloques sin aumentar el rendimiento. (AWS, 2023)

Elegir entre las dos opciones de almacenamiento no es fácil. Es importante comprender cómo se comparan las diferentes funciones para poder decidir qué tipo de almacenamiento en la nube se adapta mejor a sus necesidades.

Características	**Almacenamiento de objetos**	**Almacenamiento en bloque**	**Almacenamiento en archivos**
Almacenamiento de datos	Datos almacenados en objetos en una estructura de archivo plano	Datos almacenados en bloques de tamaño fijo en una estructura jerárquica	Datos almacenados en archivos
Escalabilidad	Infinitamente escalable	Escalabilidad limitada	Limitado por el sistema de archivos y la jerarquía
Rendimiento	Mejor para archivos grandes no estructurados	Adecuado para bases de datos individuales	Acceso rápido a pequeños archivos y una fácil compartición

Costo	Económico	Costoso	Muy costoso
Metadatos	Disponible	No disponible	Limitados
Confiabilidad	Muy Alta	Alta	Muy Alta
Redundancia	RAID, replicación	Replicación, dispersión geográfica	RAID, replicación de archivos
Integridad de Datos	Alta (versionado y checksum)	Depende del sistema de archivos y RAID	Depende del sistema de archivos
Proveedores	Amazon S3, Google Cloud Storage	SAN, iSCSI	NAS, NFS, SMB

Metodología

Se utilizará un enfoque mixto que me permitirá realizar un análisis profundo y riguroso de las tecnologías de almacenamiento en bloque en términos de seguridad en los centros de datos obteniendo una comprensión completa de los riesgos, desafíos y oportunidades que enfrentan las organizaciones al proteger sus datos.

En el presente caso de estudio para el análisis de las tecnologías de almacenamiento en bloque en términos de seguridad en los centros de datos se utilizará la investigación descriptiva comparativa que me permitirá recopilar información y entender mejor los desafíos relacionados con la seguridad en los centros de datos; así como también identificar la prevalencia de problemas de seguridad y las soluciones empleadas.

Para la recolección de datos se realizó una encuesta a expertos en seguridad y administración de centros de datos con el objetivo de recolectar información sobre las tecnologías de almacenamiento, vulnerabilidades y prácticas de seguridad. En este estudio de caso, la población es de 23 participantes, la cual estará dirigidas a 3 a expertos en seguridad que administra centros de datos y 20 personas que tienen conocimiento este campo.

RESULTADOS

Pregunta 1. ¿Cuántos años de experiencia tiene en el campo de la administración de centros de datos?

Grafica 1.

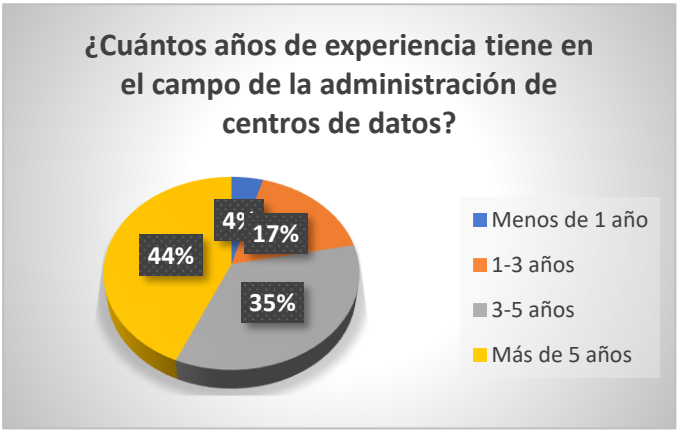

Tabla 1. Resultados de la 1 pregunta

Opción	Respuesta	Porcentaje
Menos de 1 año	1	4%
1-3 años	4	17%
3-5 años	8	35%
Más de 5 años	10	44%

Elaboración: Eder Cabrera

Fuente: Encuesta a expertos en seguridad y usuarios

Análisis:

En base a la encuesta se puede observar una distribución de experiencia diversa entre los participantes. Un pequeño grupo (4%) está en la fase inicial de aprendizaje, es decir que tiene una base mínima de conocimientos, mientras el 17% está formado por profesionales que ha comenzado a adquirir experiencia, el grupo más grande se divide con el 35% representa a personas que asumen un rol muy importante en este campo y el

44% representa a los profesionales más experimentados. Esto nos indica que existe una mezcla saludable de nuevos talentos y expertos establecidos, lo que puede ser beneficioso para el intercambio de conocimientos y el crecimiento profesional.

Pregunta 2. ¿Qué tipo de tecnologías de almacenamiento en bloque utiliza actualmente en su centro de datos?

Grafica 2.

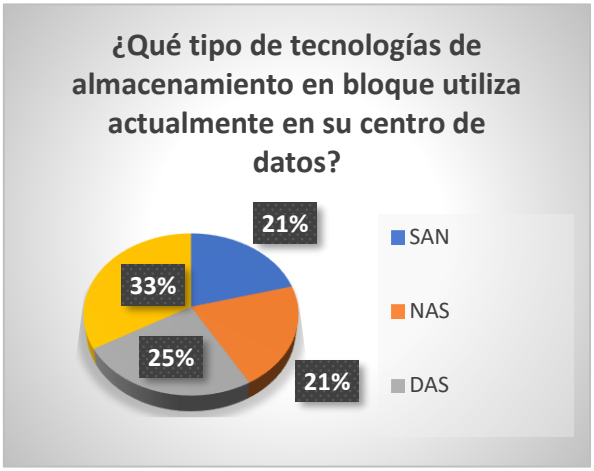

Tabla 2. Resultados de la 2 pregunta

Opción	Respuesta	Porcentaje
SAN	5	21%
NAS	5	21%
DAS	6	25%
Almacenamiento en la nube	8	33%

Elaboración: Eder Cabrera

Fuente: Encuesta a expertos en seguridad y usuarios

Análisis:

A través de la encuesta se puede analizar que el 21% utiliza SAN como tecnología de almacenamiento ya que esto permite la facilidad del acceso y la gestión centralizada de grande volumen de datos, el otro 21% indica usan NAS como solución ya que permite a los usuarios y dispositivos acceder a los datos desde un punto centralizado, el 25% utilizan DAS debido a que es una solución simple y efectiva y el 33% restante nos indica que utilizan el almacenamiento en la nube ya que permite escalabilidad y accesibilidad desde cualquier lugar y reducción de costos.

Pregunta 3. ¿Cuál es la razón principal para utilizar tecnologías de almacenamiento en bloque en su centro de datos?

Grafica 3.

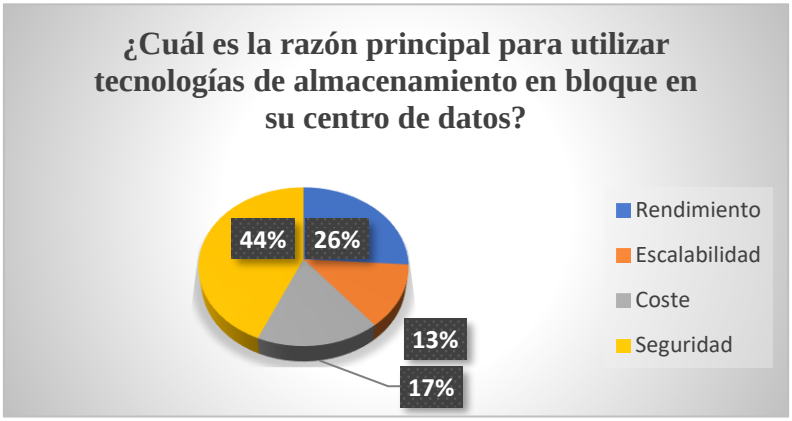

Tabla 3. Resultados de la 3 pregunta

Opción	Respuesta	Porcentaje
Rendimiento	6	26%
Escalabilidad	3	13%
Coste	4	17%
Seguridad	10	44%

Elaboración: Eder Cabrera

Fuente: Encuesta a expertos en seguridad y usuarios

Análisis:

En base a la encuesta se observa que el 26% indicaron que el rendimiento es lo principal, esto es decisivo para quienes necesitan sistemas rápidos y eficientes, para

procesar grandes volúmenes de datos o para ofrecer una experiencia de usuario fluida , el 13% mencionaron que la escalabilidad debe ser la principal razón esto se debe a que los sistemas puedan manejar una mayor carga de trabajo a medida que sus necesidades evolucionen., el 17% eligieron el coste como su razón principal debido que el costo es un factor determinante, quizás debido a restricciones presupuestarias o a la necesidad de maximizar el valor por dinero invertido y el 44% indicaron que la seguridad es la razón principal lo que indica una gran preocupación por proteger datos sensibles y asegurar que sus sistemas sean robustos frente a posibles amenazas.

Pregunta 4. ¿Qué medidas de seguridad utiliza para proteger los datos almacenados en bloque?

Grafica 4.

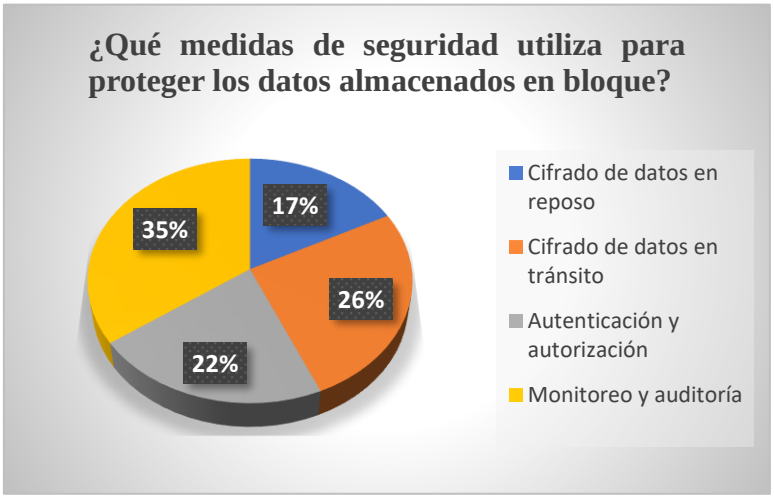

Tabla 4. Resultados de la 4 pregunta

Opción	Respuesta	Porcentaje
Cifrado de datos en reposo	4	17%
Cifrado de datos en tránsito	6	26%
Autenticación y autorización	5	22%
Monitoreo y auditoría	8	35%

Elaboración: Eder Cabrera

Fuente: Encuesta a expertos en seguridad y usuarios

Análisis:

A través de la encuesta el 35% nos indica que es el monitoreo y auditoria es la media más importante esto se debe a que estas prácticas permiten detectar actividades sospechosas y anomalías, lo cual es crucial para identificar y responder rápidamente a posibles amenazas de seguridad, mientras que el 26% prefieren el cifrado de datos debido a que asegura que los datos sean ilegibles para cualquiera que no tenga la clave de cifrado, protegiendo así la información confidencial, el 22% eligen la autenticación y autorización ya que estas medidas garantizan que solo los usuarios y sistemas autorizados puedan acceder a los datos, lo que es esencial para evitar accesos no autorizados y proteger la integridad de la información y el 17% restante eligen el cifrado de datos en tránsito ya que se enfoca en proteger los datos mientras se trasladan entre sistemas, asegurando que no sean interceptados o manipulados durante la transmisión.

Pregunta 5. ¿Ha experimentado alguna brecha de seguridad relacionada con su almacenamiento en bloque en los últimos 12 meses?

Grafica 5.

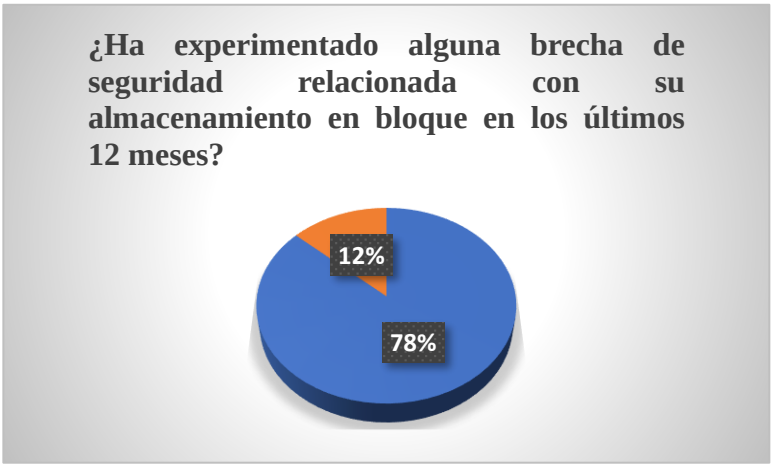

Tabla 5. Resultados de la 5 pregunta

Opción	Respuesta	Porcentaje
NO	18	78%
SI	5	12%

Elaboración: Eder Cabrera

Fuente: Encuesta a expertos en seguridad y usuarios

Análisis:

En base a la encuesta el 78% nos dicen que no han experimentado alguna brecha de seguridad relacionada con su almacenamiento en bloque en los últimos 12 meses esto se debe a que cuentan con medidas de seguridad robustas y tienen capacitación continua del personal en temas de seguridad y 12% restante nos dicen que si han experimentado alguna brecha de seguridad relacionada con su almacenamiento en bloque en los últimos 12 meses ya que pueden haber sido objetivos de ataques específicos y sofisticados que lograron superar las defensas establecidas..

Pregunta 6. ¿Qué tan seguro considera que es su almacenamiento en bloque actualmente?

Grafica 6.

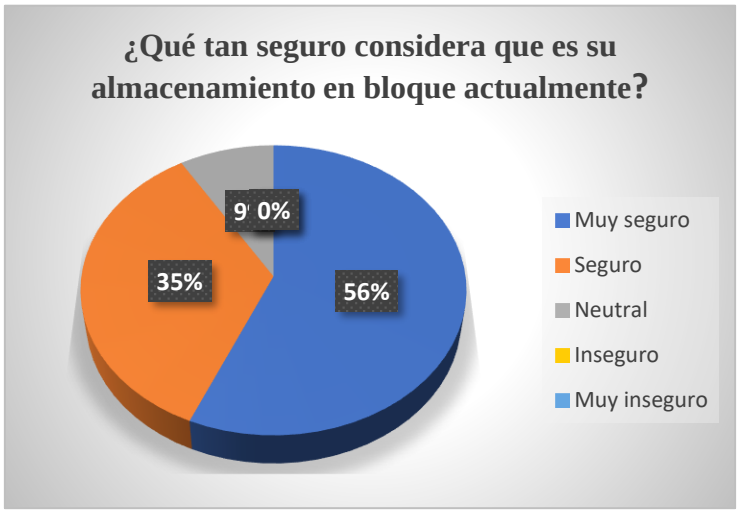

Tabla 6. Resultados de la 6 pregunta

Opción	Respuesta	Porcentaje
Muy seguro	13	56%
Seguro	8	35%
Neutral	2	9%
Inseguro	0	0%
Muy inseguro	0	0%

Elaboración: Eder Cabrera

Fuente: Encuesta a expertos en seguridad y usuarios

Análisis:

A través de la encuesta se puede observar que la seguridad de almacenamiento es muy positiva con el 91% nos afirman que no han tenido problemas y lo califican como muy seguro y seguro esto se deben que pueden confiar en la reputación y las garantías ofrecidas por los proveedores de almacenamiento, lo que contribuye a su sensación de seguridad, mientras que el 9% mantiene una postura neutral sin opiniones negativas.

Pregunta 7. ¿Qué mejoras cree que serían necesarias para aumentar la seguridad de su almacenamiento en bloque?

Grafica 7.

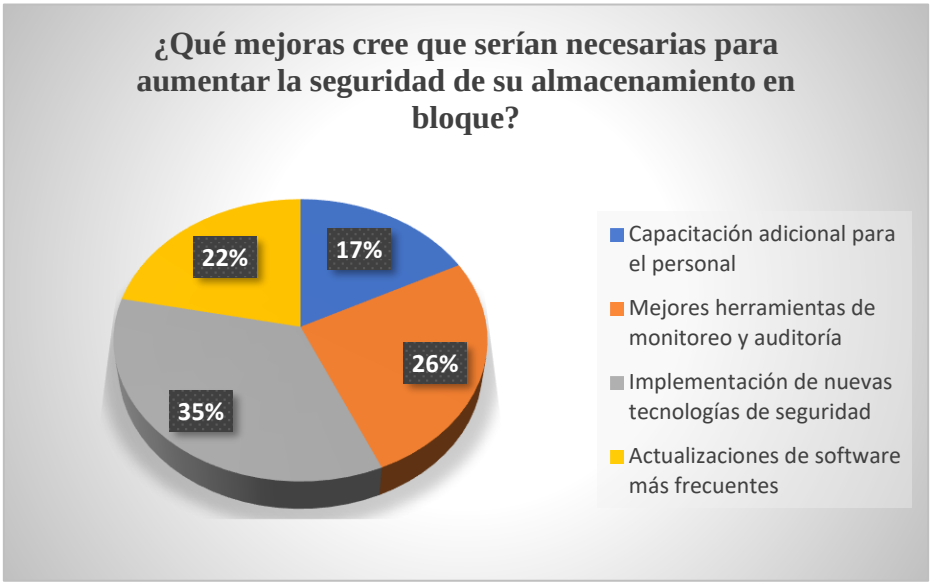

Tabla 7. Resultados de la 7 pregunta

Opción	Respuesta	Porcentaje
Capacitación adicional para el personal	4	17%
Mejores herramientas de monitoreo y auditoría	6	26%
Implementación de nuevas tecnologías de seguridad	8	35%
Actualizaciones de software más frecuentes	5	22%

Elaboración: Eder Cabrera

Fuente: Encuesta a expertos en seguridad y usuarios

Análisis:

En base a la encuesta se observa que el 17% considera que mejorar la capacitación del personal es crucial para aumentar la seguridad porque al capacitar adecuadamente al personal, se reducen los errores humanos, se mejora la comprensión de las políticas de seguridad y se fortalecen las prácticas de gestión de datos, el 26% destaca que es importante tener herramientas para monitorear y auditoría el sistema de almacenamiento ya que estas herramientas son fundamentales para detectar y responder a actividades sospechosas o inusuales., el 35% sugiere que la implementación de nuevas tecnologías de seguridad es esencial para mejorar la seguridad del almacenamiento esto se debe a que las tecnologías de seguridad están en constante evolución, y nuevas soluciones pueden ofrecer mejores niveles de protección y el 22% restante considera que las actualizaciones de software son necesarias para mantener la seguridad del sistema para parchear vulnerabilidades conocidas y asegurar que el sistema esté protegido contra los ataques más recientes.

Pregunta 8. ¿Cuáles son las principales barreras que enfrenta para mejorar la seguridad del almacenamiento en bloque en su organización?

Grafica 8.

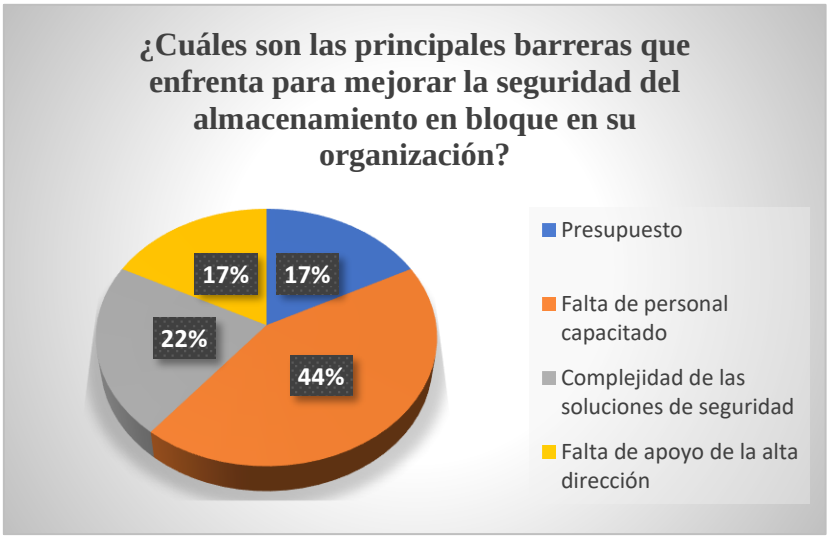

Tabla 8. Resultados de la 8 pregunta

Opción	Respuesta	Porcentaje
Presupuesto	4	17%
Falta de personal capacitado	10	44%
Complejidad de las soluciones de seguridad	5	22%
Falta de apoyo de la alta dirección	4	17%

Elaboración: Eder Cabrera

Fuente: Encuesta a expertos en seguridad y usuarios

Análisis:

Mediante la encuesta nos indica que la principal barrera para mejorar la seguridad de almacenamiento es la falta de personal capacitado con el 44%, el 22% nos dicen que la complejidad de soluciones de seguridad es la segunda barrera, con un 17% la falta de apoyo representa otra babera para la seguridad y el 17% restante nos afirma que el presupuesto es una barrera insignificantica para la seguridad.

DISCUSION DE LOS RESULTADOS

En nuestro caso de estudio, la mayoría de los encuestados , con el 44%, tienen más de 5 años de experiencia en su campo, lo que indica un alto nivel de conocimiento y competencia. Un 35% tienen entre 3 y 5 años de experiencia, lo que también refleja una sólida base de experiencia. Un 17% de los encuestados cuentan con 1 a 3 años de experiencia, mientras que solo un 4% tiene menos de 1 año en el área.

La encuesta muestra una distribución positiva de expertos en diferentes experiencias, esto indica un campo de crecimiento con un fututo prometedor. Es importante promover aún más la capacitación y el desarrollo vocacional para garantizar que el área continue progresando para satisfacer las necesidades del equipo de trabajo.

La encuesta nos proporciona las preferencias tecnológicas de almacenamiento en bloque entre los usuarios y la elección de esto depende de los requisitos y necesidades de cada usuario. Se debe considerar factores como la escalabilidad, el rendimiento, el costo, la rentabilidad y el acceso simple es importante para tomar una decisión bien fundada.

La escalabilidad se destaca como la principal prioridad para los participantes, con un 44% eligiéndola como su principal preocupación. Le siguen el rendimiento con un 26%, el coste con un 17% y la escalabilidad con un 13%. Estos resultados subrayan que, aunque otros factores como el rendimiento y el coste son importantes, la protección de los datos es el aspecto más crucial para la mayoría de los encuestados. Esto sugiere que cualquier estrategia o decisión tecnológica debería priorizar medidas robustas de seguridad para satisfacer las expectativas y necesidades de la mayoría de los usuarios.

También nos indica que el enfoque de seguridad solidad para proteger los datos deber cubrir medidas de seguridad como el monitoreo y la auditoria ya que permite detectar posibles amenazas, mientras que le cifrado de datos garantiza que los datos no

estén disponibles, incluso si se interceptan. En cambio, la autenticación y autorización garantiza que solos los usuarios puedan acceder a los datos y el cifrado en transito protege los datos durante la transmisión. Al implementar estas medidas de seguridad las empresas pueden proteger sus datos.

CONCLUSION

Se identificaron varias tecnologías para almacenar bloques, cada una de las cuales con sus propias características y uso. Gracias a un análisis exhaustivo, se determinaron las principales amenazas de seguridad relacionadas con estas tecnologías. Esto incluye vulnerabilidades, como acceso no autorizado, ataques de ataque y la posibilidad de corrupción de datos. Comprender estas amenazas es importante para la implementación de medidas de protección adecuadas.

Al comparar diferentes tecnologías de almacenamiento de bloques, se han llevado a cabo evaluaciones detalladas de sus fortalezas y debilidades en términos de seguridad. Este análisis comparativo ha permitido identificar qué tecnología ofrece un mayor nivel de protección contra amenazas específicas. Se han considerado factores como el cifrado, la redundancia de datos y los mecanismos de autenticación para determinar la resistencia de cada tecnología sobre la posibilidad de ataques.

La evaluación tecnológica se ha convertido en la clave para comprender su efectividad en el entorno real. A través de pruebas prácticas y análisis teóricos, la capacidad de cada tecnología se ha evaluado para resistir las amenazas de seguridad. Esta evaluación ha proporcionado una visión clara de qué tecnología es más segura y que requiere una mejora o renovación para cumplir con los estándares de seguridad actuales. Esta comprensión es muy importante para la toma de decisiones que se informa al elegir la tecnología de almacenamiento de bloque que es adecuada para diferentes aplicaciones.

RECOMENDACIONES

Se recomienda investigar sobre las tecnologías de almacenamiento en bloque como SAN, NAS y SCS lo cual se debe analizar sus vulnerabilidades e identificar sus amenazas para identificar cual se adapte a tus necesidades e implementar medidas adecuadas para mitigar estos riesgos y proteger los datos críticos.

Se recomienda realizar una comparación con las diferentes tecnologías de almacenamiento en bloque en términos de seguridad evaluando múltiples criterios tanto como sus ventajas y desventajas, esta comparación permitirá tomar decisiones adecuadas según las necesidades.

Se recomienda implementar una política estricta de control de acceso que determine quién puede acceder a los datos y en qué condiciones, además de tener una herramienta de monitoreo que advierte el acceso no autorizado o la actividad sospechosa y brinda capacitación regular al personal sobre las mejores prácticas de seguridad y cómo manejar Datos sobre datos sensibles.

ANEXOS

Cuestionario de Encuesta

1. ¿Cuántos años de experiencia tiene en el campo de la administración de centros de datos?

a) Menos de 1 año

b) 1-3 años

c) 3-5 años

d) Más de 5 años

2. ¿Qué tipo de tecnologías de almacenamiento en bloque utiliza actualmente en su centro de datos? (Seleccione todas las que apliquen)

a) SAN (Storage Area Network)

b) NAS (Network Attached Storage)

c) DAS (Direct Attached Storage)

d) Almacenamiento en la nube

3. ¿Cuál es la razón principal para utilizar tecnologías de almacenamiento en bloque en su centro de datos?

a) Rendimiento

b) Escalabilidad

c) Coste

d) Seguridad

4. ¿Qué medidas de seguridad utiliza para proteger los datos almacenados en bloque?

a) Cifrado de datos en reposo

b) Cifrado de datos en tránsito

c) Autenticación y autorización

d) Monitoreo y auditoría

5. ¿Ha experimentado alguna brecha de seguridad relacionada con su almacenamiento en bloque en los últimos 12 meses?

a) Sí

b) No

6. ¿Qué tan seguro considera que es su almacenamiento en bloque actualmente?

a) Muy seguro

b) Seguro

c) Neutral

d) Inseguro

e) Muy inseguro

7. ¿Qué mejoras cree que serían necesarias para aumentar la seguridad de su almacenamiento en bloque?

a) Actualizaciones de software más frecuentes

b) Capacitación adicional para el personal

c) Mejores herramientas de monitoreo y auditoría

d) Implementación de nuevas tecnologías de seguridad

8. ¿Cuáles son las principales barreras que enfrenta para mejorar la seguridad del almacenamiento en bloque en su organización?

a) Presupuesto

b) Falta de personal capacitado

c) Complejidad de las soluciones de seguridad

d) Falta de apoyo de la alta dirección

Bibliografía

AWS. (2023). Obtenido de https://aws.amazon.com/es/what-is/block-storage/

AWS. (2023). Obtenido de https://aws.amazon.com/es/what-is/block-storage/

Cisco. (2022). Obtenido de https://www.cisco.com/c/es_mx/solutions/data-center-virtualization/what-is-a-data-center.html

KIO. (2022). Obtenido de https://www.kio.tech/blog/data-center/almacenamiento-nas-y-san

Mecalux. (09 de Septiembre de 2020). *Mecalux*. Obtenido de https://www.mecalux.es/blog/almacenamiento-en-bloque

Qumulo, E. (1 de Febrero de 2022). *Qumulo*. Obtenido de https://qumulo.com/es/blog/block-storage-vs-object-storage-vs-file-storage/

Rahim, J. (27 de Mayo de 2024). *Astera*. Obtenido de https://www.astera.com/es/type/blog/cloud-storage/

Stackscale. (22 de marzo de 2023). Obtenido de https://www.stackscale.com/es/blog/tipos-de-almacenamiento/

Storage, P. (2023). *Pure Storage*. Obtenido de https://www.purestorage.com/es/knowledge/what-is-block-storage.html#:~:text=Un%20archivo%20de%20bloque%20es,de%20una%20base%20de%20datos.

Vincent. (20 de Julio de 2023). *FS*. Obtenido de https://community.fs.com/es/article/storage-area-network-san-vs-network-attached-storage-nas.html