



TECNICATURA SUPERIOR EN

Telecomunicaciones

Proyecto Integrador I

Almacenamiento y Seguridad

Almacenamiento y Seguridad



Almacenamiento

1) Introducción

- El objetivo de esta presentación es profundizar en el conocimiento de las bases de datos no relacionales, centrándonos específicamente en MongoDB, su implementación, uso y mejores prácticas de seguridad. Exploraremos también consideraciones éticas en el manejo de los datos y la operación de sistemas de bases de datos en servidores seguros.



Almacenamiento

Definición de una Base de Datos:

- Una base de datos es un sistema estructurado para la acumulación, recuperación y gestión de datos. Su aplicación varía desde sistemas de gestión de contenido simplificados hasta infraestructuras de IT complejas en empresas y aplicaciones a gran escala.

Tipos de Bases de Datos:

- **Relacionales:** Datos organizados en tablas interconectadas mediante claves.
- **No Relacionales (NoSQL):** Emplean modelos como documentos, clave-valor, y grafos, ofreciendo almacenamiento flexible y escalable, ideal para manejar grandes volúmenes de datos variados.



Almacenamiento

Importancia de las Bases de Datos:

- Las bases de datos son cruciales para la operación y análisis en negocios, contribuyendo significativamente a la eficiencia operacional y la capacidad analítica. Permiten:
- **Optimización de Operaciones:** Automatización y mejora de procesos internos.
- **Análisis de Datos:** Facilitan la extracción de insights para la toma de decisiones estratégicas.
- **Personalización de Servicios:** Mejoran la interacción con el usuario final basándose en análisis de datos.
- **Seguridad de la Información:** Fundamental para el manejo seguro de datos y el cumplimiento de normativas como GDPR.



Almacenamiento

2) Modelos de Datos

Definición y Tipos de Modelos de Datos

- Un **modelo de datos** es un marco teórico y conceptual utilizado para definir y organizar los datos y cómo se relacionan entre sí dentro de una base de datos. Es fundamental para entender cómo los datos son almacenados, gestionados y utilizados en sistemas de software. Dependiendo de la naturaleza de la aplicación y los requisitos del sistema, se elige un modelo de datos adecuado.



Almacenamiento

Tipos Principales de Modelos de Datos:

- **Modelo Relacional:** Los datos se organizan en tablas (o relaciones) donde cada fila representa una instancia única de un tipo de dato (entidad) y las columnas representan los atributos de esa entidad. Las tablas pueden estar relacionadas entre sí por claves primarias y foráneas.
- **Modelo Documento:** Utilizado principalmente en bases de datos NoSQL como MongoDB, los datos se representan como documentos, que generalmente se formatean en JSON o BSON. Cada documento puede contener una estructura de datos compleja que incluye arrays y subdocumentos.



Almacenamiento

- **Modelo Clave-Valor:** Cada elemento en la base de datos se almacena como un par de clave-valor. Este modelo es altamente eficiente para consultas de recuperación basadas en la clave y es adecuado para almacenar y recuperar grandes volúmenes de datos.
- **Modelo Columnar:** Organiza los datos por columnas en lugar de por filas, lo que es útil para bases de datos analíticas donde las operaciones típicamente involucran un gran volumen de datos de una o pocas columnas.
- **Modelo Grafo:** Utiliza estructuras de grafos compuestas por nodos, aristas y propiedades para representar y almacenar datos. Los nodos representan entidades, las aristas representan relaciones entre estas entidades, y las propiedades son información sobre nodos y aristas.



Almacenamiento

Comparación de Modelos de Datos Relacionales y No Relacionales

- **Modelo Relacional:**
 - **Ventajas:** Estructura bien definida, integridad de datos fuerte, lenguaje de consulta poderoso (SQL), y consistencia de transacciones.
 - **Desventajas:** Menos flexible en términos de esquema, puede no escalar horizontalmente de manera eficiente, y puede ser menos eficiente para ciertos tipos de consultas o datos no estructurados.



Almacenamiento

Comparación de Modelos de Datos Relacionales y No Relacionales

- **Modelo No Relacional:**
 - **Ventajas:** Flexibilidad de esquema (esquema dinámico), capacidad para manejar grandes volúmenes de datos y tipos de datos variados, y escalamiento horizontal eficiente.
 - **Desventajas:** Menos soporte para transacciones complejas (aunque esto ha mejorado en años recientes), y puede requerir diferentes lenguajes o formas de consulta que pueden ser menos estándares que SQL.



Almacenamiento

Consideraciones para la Elección del Modelo de Datos

- La elección entre modelos relacionales y no relacionales depende de varios factores:
 1. **Naturaleza de los Datos:** ¿Son estructurados, semi-estructurados o no estructurados?
 2. **Requisitos de Escalabilidad:** ¿Se necesita escalar horizontalmente?
 3. **Operaciones de Consulta:** ¿Qué tipo de consultas se realizarán?
 4. **Consistencia de Datos:** ¿Es crucial la consistencia transaccional?



Almacenamiento

3) Bases de Datos No Relacionales

- **Características Principales**
- Las bases de datos no relacionales, o NoSQL (Not Only SQL), se diseñaron para superar las limitaciones de las bases de datos relacionales, especialmente en contextos de big data y aplicaciones en tiempo real. Aquí están algunas de sus características más destacadas:
- **Flexibilidad de Esquema:** No requieren un esquema fijo o estructura predefinida, lo que permite a los desarrolladores crear y modificar la estructura de datos sobre la marcha.



Almacenamiento

- **Escalabilidad Horizontal:** Están diseñadas para expandirse fácilmente agregando más servidores, lo que es ideal para aplicaciones que manejan grandes volúmenes de datos y alto tráfico de usuarios.
- **Optimización de Rendimiento:** Proporcionan tiempos de respuesta rápidos incluso con grandes volúmenes de datos, gracias a su capacidad para distribuir las cargas de datos y consultas a través de múltiples nodos.
- **Manejo de Datos Diversos:** Son capaces de almacenar una variedad de tipos de datos, incluidos estructurados, semi-estructurados, y no estructurados, lo que las hace adecuadas para big data y aplicaciones web modernas.



Almacenamiento

Tipos de Bases de Datos No Relacionales

- Las bases de datos NoSQL se clasifican comúnmente en cuatro tipos, cada uno optimizado para un conjunto específico de funcionalidades y casos de uso:

1. Key-Value Stores:

- **Descripción:** Almacenan datos como una colección de pares clave-valor. Cada clave es única y se utiliza para acceder al valor correspondiente.
- **Uso:** Ideal para situaciones donde las operaciones de lectura y escritura son frecuentes y deben ser extremadamente rápidas, como en sesiones de usuarios y cachés.
- **Ejemplos:** Redis, DynamoDB.



Almacenamiento

2. Document Stores:

- **Descripción:** Almacenan datos en documentos, que son estructuras de datos más complejas que los pares clave-valor. Los documentos, que suelen estar en formatos JSON, XML o BSON, pueden contener muchos campos y datos anidados.
- **Uso:** Adecuadas para aplicaciones que manejan datos semi-estructurados y necesitan más flexibilidad que las filas y columnas tradicionales. Son especialmente útiles en CMS, plataformas de comercio electrónico y aplicaciones móviles.
- **Ejemplos:** MongoDB, CouchDB.



Almacenamiento

3. Wide-Column Stores:

- **Descripción:** Almacenan datos en tablas, filas y columnas dinámicas, pero permiten que cada fila tenga un número diferente de columnas.
- **Uso:** Excelentes para analizar grandes cantidades de datos, manejar bases de datos de series temporales, y para cualquier caso donde las filas pueden variar en el número de columnas.
- **Ejemplos:** Cassandra, HBase.



Almacenamiento

4. Graph Databases:

- **Descripción:** Utilizan estructuras de grafos para almacenar, mapear y consultar relaciones. Están compuestas por nodos (entidades) y aristas (relaciones).
- **Uso:** Ideales para analizar y visualizar datos que están interconectados y que tienen relaciones dinámicas, como redes sociales, sistemas de recomendación, y aplicaciones de detección de fraudes.
- **Ejemplos:** Neo4j, ArangoDB.



Almacenamiento

Conclusión

- Estos diferentes tipos ofrecen una gama de opciones que pueden ser seleccionadas basándose en los requisitos específicos del rendimiento, tipo de datos, y la complejidad de las relaciones dentro de los datos que una aplicación necesita gestionar.
- En la siguiente sección, nos centraremos específicamente en MongoDB, un tipo de base de datos documental, y exploraremos sus características únicas, instalación, y métodos de uso en detalle.



Almacenamiento

4) MongoDB

- ¿Qué es MongoDB?
- MongoDB es una base de datos NoSQL orientada a documentos que fue diseñada para facilitar el desarrollo y la escalabilidad. Fue introducida en 2009 y ha ganado popularidad por su enfoque flexible y sus características potentes que la hacen ideal para manejar grandes volúmenes de datos y aplicaciones complejas.



Almacenamiento

Características Clave de MongoDB

1. Modelo de Datos Basado en Documentos:

- MongoDB almacena datos en documentos BSON (una versión binaria de JSON), lo que permite estructuras de datos ricas y profundamente anidadas con menos complejidad que las bases de datos relacionales.

2. Esquema Dinámico:

- A diferencia de las bases de datos relacionales, no requiere un esquema fijo. Esto significa que los campos pueden variar de un documento a otro y la estructura de datos puede ser modificada sin downtime.



Almacenamiento

Características Clave de MongoDB

3. Indexación Eficaz:

- Soporta índices secundarios, lo que permite una rápida recuperación de datos. Cualquier campo en un documento puede ser indexado, incluyendo los de documentos anidados y arrays.

4. Replicación y Alta Disponibilidad:

- Ofrece alta disponibilidad a través de los replica sets, que son grupos de instancias de MongoDB que mantienen el mismo conjunto de datos, proporcionando redundancia y alta disponibilidad.



Almacenamiento

Características Clave de MongoDB

5. Sharding Distribuido:

- Soporta sharding automático, lo que permite distribuir datos a través de una serie de máquinas para manejar grandes volúmenes de datos y proporcionar escalabilidad horizontal sin problemas.

6. Consistencia Eventual:

- MongoDB ofrece consistencia eventual, permitiendo un alto rendimiento y disponibilidad, especialmente en aplicaciones distribuidas a gran escala.

7. Operaciones en Tiempo Real:

- Con características como Change Streams, los desarrolladores pueden reaccionar a cambios en los datos en tiempo real, lo que es ideal para aplicaciones en tiempo real.



Almacenamiento

Ventajas de Usar MongoDB Sobre Otros Sistemas de Bases de Datos

1. Flexibilidad:

- Su esquema dinámico es ideal para aplicaciones que requieren agilidad y la capacidad de iterar rápidamente, así como para proyectos que evolucionan con el tiempo.

2. Escalabilidad:

- El sharding distribuido facilita la escalabilidad horizontal, lo que permite a MongoDB manejar aplicaciones con enormes volúmenes de tráfico y datos sin degradar el rendimiento.



Almacenamiento

Ventajas de Usar MongoDB Sobre Otros Sistemas de Bases de Datos

3. Desarrollo Rápido:

- La simplicidad del modelo basado en documentos y la amplia disponibilidad de controladores para diversos lenguajes de programación hacen que el desarrollo sea rápido y directo.

4. Comunidad y Soporte:

- Con una comunidad grande y activa, y soporte profesional disponible a través de MongoDB Inc., los desarrolladores tienen acceso a una gran cantidad de recursos y experiencia.



Almacenamiento

Ventajas de Usar MongoDB Sobre Otros Sistemas de Bases de Datos

5. Rendimiento:

- Las operaciones de lectura y escritura son extremadamente rápidas en MongoDB, especialmente en configuraciones que utilizan índices bien diseñados y técnicas de optimización adecuadas.
- MongoDB ha demostrado ser una solución robusta para una variedad de necesidades de datos, desde aplicaciones pequeñas hasta soluciones empresariales a gran escala, ofreciendo un enfoque moderno y eficiente al manejo de datos en el ecosistema digital de hoy. En la próxima sección, exploraremos cómo instalar y comenzar a utilizar MongoDB, proporcionando un camino claro para integrarlo en tus proyectos.



Almacenamiento

5) Instalación de MongoDB

Requisitos del Sistema

- Antes de instalar MongoDB, es importante asegurarse de que el sistema cumple con los requisitos mínimos necesarios para su ejecución eficiente:
- **Sistema Operativo:** Compatible con la mayoría de los sistemas operativos modernos, incluyendo varias versiones de Windows, macOS, y Linux.
- **Memoria:** Recomendado al menos 2 GB de RAM libre, aunque para entornos de producción con grandes volúmenes de datos, se recomienda mucho más.



Almacenamiento

Requisitos del Sistema

- **Espacio en Disco:** Depende del volumen de datos que se espera manejar. MongoDB utiliza archivos de mapeo de memoria para almacenar datos, por lo que el espacio en disco debe ser al menos igual al conjunto de datos.
- **Red:** Conexión de red configurada para permitir conexiones internas y, si es necesario, externas a los puertos relevantes (por defecto es el 27017 para MongoDB).



Almacenamiento

Pasos para la Instalación en Diferentes Sistemas Operativos

Windows:

- 1. Descargar el Instalador:** Visita el sitio oficial de [MongoDB](https://www.mongodb.com) y descarga el instalador de MongoDB para Windows.
- 2. Ejecutar el Instalador:** Abre el archivo .msi descargado y sigue las instrucciones. Puedes elegir la instalación completa o personalizarla según tus necesidades.
- 3. Configurar el Servicio de MongoDB:** Durante la instalación, configura MongoDB como un servicio de Windows, lo que permite que MongoDB se inicie automáticamente con Windows.



Almacenamiento

macOS y Linux:

- **macOS:** MongoDB se puede instalar fácilmente utilizando Homebrew con comandos para instalar y luego iniciar MongoDB como un servicio.
- **Linux:** La instalación implica añadir el repositorio oficial de MongoDB, instalar el paquete usando el gestor de paquetes de la distribución, y configurar MongoDB para que se inicie con el sistema.



Almacenamiento

Verificación de la Instalación

- Para verificar que MongoDB está correctamente instalado:
 1. **Verificar el Servicio:** Asegúrate de que el servicio MongoDB está en ejecución, lo cual puede hacerse mediante herramientas de administración del sistema.
 2. **Conectar al Servidor de MongoDB:** Abre el shell de MongoDB ejecutando 'mongo' en la línea de comando. Si puedes interactuar con MongoDB, la instalación fue exitosa.



Almacenamiento

6) Uso de MongoDB

Estructura Básica: Databases, Collections, Documents

- MongoDB organiza sus datos en tres niveles jerárquicos fundamentales que facilitan una gestión eficiente y flexible de los datos:
1. **Databases:** Cada base de datos en MongoDB actúa como un contenedor físico para las colecciones. Cada servidor puede albergar múltiples bases de datos, cada una con su propio conjunto de datos.



Almacenamiento

Estructura Básica: Databases, Collections, Documents

- 2. Collections:** Son equivalentes a las tablas en las bases de datos relacionales, pero sin un esquema fijo. Esto significa que los documentos dentro de una misma colección pueden tener diferentes campos.
- 3. Documents:** Los documentos son el núcleo de MongoDB. Cada documento está estructurado como un objeto BSON (Binary JSON), lo que permite que almacene estructuras de datos complejas en un formato fácilmente accesible.



Almacenamiento

Operaciones CRUD Básicas

- CRUD son las operaciones básicas aplicables a los datos en cualquier sistema de gestión de bases de datos, incluyendo MongoDB:
1. **Create:** Crear o añadir nuevos documentos a una colección.
 2. **Read:** Leer o recuperar documentos. MongoDB ofrece diversas formas de consulta para acceder a los datos que necesita.
 3. **Update:** Actualizar datos existentes. MongoDB permite modificar uno o más documentos simultáneamente.
 4. **Delete:** Eliminar documentos de una colección.



Almacenamiento

Ejemplos Prácticos de Comandos MongoDB

- En la implementación en vivo, se demostrará cómo realizar operaciones CRUD utilizando la biblioteca PyMongo en un entorno de desarrollo configurado en VSCode. Se mostrarán ejemplos prácticos que incluyen:
 1. Insertar documentos en una colección.
 2. Consultar documentos utilizando diferentes filtros y métodos.
 3. Actualizar documentos específicos basándose en criterios particulares.
 4. Eliminar documentos conforme a condiciones definidas.



Seguridad y Ética en Almacenamiento de Datos

7) Seguridad en las Bases de Datos

- La seguridad de las bases de datos es crucial para proteger datos sensibles y mantener la integridad y confidencialidad de la información. En el contexto de MongoDB, existen varias prácticas y configuraciones que pueden ser implementadas para asegurar la base de datos eficazmente.

Mejores Prácticas de Seguridad en MongoDB

1. **Control de Acceso:** Implementar autenticación y autorización estrictas para limitar el acceso a la base de datos sólo a los usuarios y aplicaciones autorizadas. MongoDB soporta la autenticación basada en SCRAM, x.509 certificados, y puede integrarse con sistemas de autenticación externos como LDAP.



Seguridad y Ética en Almacenamiento de Datos

Mejores Prácticas de Seguridad en MongoDB

- 2) **Auditoría de Seguridad:** Configurar MongoDB para auditar actividades de usuario y administrativas críticas. Esto ayuda a identificar patrones de acceso no autorizados o anómalos.
- 3) **Configuración de Red Segura:** Asegurar que MongoDB sólo escuche conexiones de interfaces de red seguras y conocidas. Utilizar firewalls para restringir el acceso al puerto de MongoDB (por defecto 27017) a sólo redes y hosts confiables.
- 4) **Actualizaciones y Parches:** Mantener MongoDB y sus dependencias actualizados con las últimas versiones y parches de seguridad para protegerse contra vulnerabilidades conocidas.



Seguridad y Ética en Almacenamiento de Datos

Cifrado de Datos en Tránsito y en Reposo

- **Cifrado en Tránsito:** MongoDB utiliza TLS/SSL (Transport Layer Security/Secure Sockets Layer) para cifrar datos en tránsito, asegurando que toda la información que se mueve entre el servidor de la base de datos y los clientes permanezca protegida contra interceptaciones.
- **Cifrado en Reposo:** A través de la función de cifrado en reposo, MongoDB ofrece la capacidad de cifrar datos en el disco, lo que garantiza que los datos almacenados no sean legibles sin las claves de cifrado adecuadas. Esto es especialmente importante para cumplir con regulaciones de privacidad y requerimientos de seguridad.



Seguridad y Ética en Almacenamiento de Datos

Configuración de Autenticación y Autorización

- **Autenticación:** MongoDB soporta múltiples mecanismos de autenticación que garantizan que sólo los usuarios autorizados puedan acceder al sistema. La configuración adecuada implica elegir un mecanismo de autenticación robusto y aplicarlo de manera consistente.
- **Autorización:** Utilizar roles y permisos para controlar el acceso a los datos en MongoDB. Definir roles específicos para diferentes usuarios y aplicar el principio de mínimo privilegio, asegurando que los usuarios tengan sólo el nivel de acceso necesario para realizar sus tareas.



Seguridad y Ética en Almacenamiento de Datos

Conclusión

- Estas medidas de seguridad no solo protegen contra accesos no autorizados y pérdida de datos, sino que también aseguran que la base de datos cumpla con las normas y regulaciones de seguridad de datos relevantes. En la próxima sección, se explorará cómo estas prácticas de seguridad se extienden más allá de la base de datos para incluir también la seguridad del servidor donde reside MongoDB.



Seguridad y Ética en Almacenamiento de Datos

8) Seguridad en los Servidores

- La seguridad en los servidores donde se alojan las bases de datos es crucial, ya que una base de datos bien asegurada puede ser comprometida si el servidor en el que opera no tiene las protecciones adecuadas. Es fundamental integrar la seguridad del servidor como parte de la estrategia de seguridad de la base de datos.
- **Importancia de la Seguridad del Servidor en la Gestión de Bases de Datos**
- Un servidor inseguro puede exponer las bases de datos a una serie de amenazas, incluyendo accesos no autorizados, ataques de inyección, y pérdida de datos críticos.



Seguridad y Ética en Almacenamiento de Datos

Asegurar el servidor ayuda a:

- 1. Proteger Datos Sensibles:** Evita que los datos críticos sean robados o alterados por actores maliciosos.
- 2. Mantener la Integridad de los Datos:** Asegura que los datos no se modifiquen de manera inapropiada.
- 3. Garantizar la Disponibilidad:** Protege contra ataques que podrían intentar interrumpir los servicios de base de datos.
- 4. Cumplir con Regulaciones:** Cumple con las regulaciones de protección de datos y privacidad, evitando sanciones legales y multas.



Seguridad y Ética en Almacenamiento de Datos

Estrategias de Seguridad para Servidores

- Implementar una estrategia de seguridad robusta para los servidores requiere una combinación de hardware, software, y políticas de seguridad adecuadas:
- 1. Actualizaciones y Mantenimiento del Sistema Operativo:**
 - Mantener el sistema operativo y el software del servidor actualizados con los últimos parches de seguridad.
 - Utilizar sólo software necesario para las operaciones de la base de datos para minimizar las vulnerabilidades potenciales.



Seguridad y Ética en Almacenamiento de Datos

Estrategias de Seguridad para Servidores

2. Control de Acceso Físico y de Red:

- Restringir el acceso físico a los servidores de bases de datos a personal autorizado.
- Configurar firewalls y otras barreras de red para limitar el acceso a los servidores de bases de datos desde redes externas e internas.

3. Seguridad en la Configuración:

- Asegurarse de que todas las configuraciones del servidor y de la base de datos sigan las mejores prácticas de seguridad, como la desactivación de servicios no utilizados y la configuración adecuada de los permisos de usuario.
- Implementar el principio de mínimo privilegio, asegurando que los usuarios y aplicaciones tengan sólo los permisos necesarios para su función.



Seguridad y Ética en Almacenamiento de Datos

Estrategias de Seguridad para Servidores

4. Monitorización y Respuesta a Incidentes:

- Implementar herramientas de monitorización para detectar y registrar actividad sospechosa o no autorizada en tiempo real.
- Establecer un plan de respuesta a incidentes para abordar y mitigar rápidamente cualquier brecha de seguridad.

5. Cifrado y Backup de Datos:

- Utilizar cifrado para proteger los datos almacenados y transmitidos desde y hacia el servidor de bases de datos.
- Asegurar que existan políticas de backup y recuperación de desastres para recuperar los datos en caso de pérdida o corrupción.



Seguridad y Ética en Almacenamiento de Datos

Estrategias de Seguridad para Servidores

Estas estrategias de seguridad son importantes para proteger los servidores que alojan bases de datos y deben ser evaluadas y ajustadas regularmente para adaptarse a las amenazas y requisitos de seguridad. En la próxima sección, se explorará el sistema operativo Linux y cómo Ubuntu Server puede ser una plataforma eficaz para gestionar bases de datos de forma segura



Seguridad y Ética en Almacenamiento de Datos

9) El Sistema Operativo Linux

Por Qué Usar Linux para Servidores

- Linux es ampliamente reconocido y utilizado en entornos de servidores por varias razones clave:
- **Estabilidad y Fiabilidad:** Linux es conocido por su robustez y estabilidad en operaciones a largo plazo, lo que es esencial para servidores que requieren alta disponibilidad.
- **Seguridad:** Ofrece excelentes características de seguridad, que pueden ser ampliadas y personalizadas para proteger aún más el sistema contra amenazas externas e internas.



Seguridad y Ética en Almacenamiento de Datos

Por Qué Usar Linux para Servidores

- **Costo-Efectividad:** Al ser un sistema operativo de código abierto, Linux reduce los costos asociados con licencias de software, lo que lo hace una opción económica para muchas organizaciones.
- **Flexibilidad y Personalización:** Los administradores pueden modificar el sistema para que se ajuste exactamente a sus necesidades, optimizando el rendimiento y la seguridad.



Seguridad y Ética en Almacenamiento de Datos

Beneficios y Características de Seguridad de Linux

- Linux ofrece diversas funcionalidades que lo hacen ideal para gestionar entornos seguros:
- **Control de Acceso Discrecional y Obligatorio (DAC y MAC):** Linux implementa políticas de control de acceso que permiten a los administradores controlar quién puede ver y modificar archivos o procesos.
- **SELinux y AppArmor:** Proporcionan herramientas para gestionar políticas de seguridad que ayudan a limitar las capacidades de los programas y servicios, mejorando significativamente la seguridad del servidor.



Seguridad y Ética en Almacenamiento de Datos

Beneficios y Características de Seguridad de Linux

- **Firewall Integrado (iptables, nftables):** Facilita la configuración de reglas de firewall para proteger el servidor contra accesos no autorizados.
- **Parches y Actualizaciones Regulares:** La comunidad de Linux proporciona actualizaciones constantes que incluyen parches de seguridad, lo que ayuda a mantener el sistema protegido contra vulnerabilidades recién descubiertas.



Seguridad y Ética en Almacenamiento de Datos

10) Ubuntu Server

Ventajas de Usar Ubuntu Server para Bases de Datos

- Ubuntu Server es una distribución de Linux que se ha ganado la confianza de los desarrolladores y administradores de sistemas por sus múltiples ventajas para manejar bases de datos:
- **Soporte a Largo Plazo (LTS):** Las versiones LTS de Ubuntu reciben cinco años de soporte y actualizaciones de seguridad, lo que garantiza estabilidad y seguridad a largo plazo.



Seguridad y Ética en Almacenamiento de Datos

- **Ventajas de Usar Ubuntu Server para Bases de Datos**
- **Amplia Compatibilidad con Software de Bases de Datos:** Ubuntu es compatible con la mayoría de los sistemas de gestión de bases de datos, incluyendo MongoDB, MySQL, PostgreSQL, entre otros, lo que permite una fácil instalación y gestión.
- **Rendimiento Optimizado:** Ubuntu Server está optimizado para operar en diversos entornos, desde pequeños servidores hasta grandes centros de datos.



Seguridad y Ética en Almacenamiento de Datos

Herramientas y Utilidades Específicas de Ubuntu para la Gestión de Bases de Datos

- Ubuntu ofrece varias herramientas que facilitan la gestión y el mantenimiento de bases de datos:
- **Snap y APT:** Permiten una instalación fácil y rápida de servicios de bases de datos mediante gestores de paquetes que manejan dependencias automáticamente.
- **Landscape:** Una herramienta de gestión de sistemas para Ubuntu que permite a los administradores supervisar, gestionar y actualizar sus servidores de forma eficiente.
- **Soporte de la Comunidad y Comercial:** Ubuntu tiene una gran comunidad de usuarios y desarrolladores, así como soporte profesional disponible a través de Canonical, ofreciendo asistencia y recursos valiosos.



Seguridad y Ética en Almacenamiento de Datos

Ubuntu server

Las distribuciones de Linux como Ubuntu Server crean un entorno robusto y seguro para las bases de datos, optimizando el rendimiento y asegurando la integridad y la seguridad de los datos en todo momento. En la próxima sección, se abordarán los aspectos éticos relacionados con el almacenamiento y la gestión de datos, enfatizando la importancia de consideraciones éticas en el uso de tecnologías de la información.



Seguridad y Ética en Almacenamiento de Datos

11) Ética y los Datos

Responsabilidades Éticas al Manejar Datos

- En la era digital, los datos son un recurso extremadamente valioso pero también pueden ser un campo minado ético. Las responsabilidades éticas al manejar datos incluyen:
- **Transparencia:** Las organizaciones deben ser claras sobre cómo y por qué recopilan datos, y qué hacen con ellos.
- **Consentimiento:** Es crucial obtener el consentimiento informado de los usuarios antes de recopilar, almacenar o procesar sus datos.



Seguridad y Ética en Almacenamiento de Datos

Responsabilidades Éticas al Manejar Datos

- **Privacidad:** Proteger la privacidad de los individuos implementando medidas de seguridad adecuadas y asegurando que los datos sean accesibles solo para quienes tienen derecho a verlos.
- **Integridad:** Asegurarse de que los datos no sean alterados de manera maliciosa o negligente.
- **Inclusión:** Evitar sesgos en la recopilación y análisis de datos que puedan llevar a discriminación.



Seguridad y Ética en Almacenamiento de Datos

Impacto de la Legislación sobre la Privacidad de Datos (ej. GDPR)

- El Reglamento General de Protección de Datos (GDPR) es una legislación de la Unión Europea que establece guías y requisitos para el manejo de datos personales de los ciudadanos de la UE. Esta legislación ha repercutido globalmente, obligando a las organizaciones a:
 1. Implementar medidas de seguridad adecuadas para proteger los datos personales.
 2. Asegurar la transparencia en el uso de los datos.
 3. Facilitar a los individuos el acceso a sus propios datos y el derecho a ser olvidados.
 4. Reportar brechas de datos de manera oportuna.

El cumplimiento de estas y otras legislaciones similares no solo es una obligación legal, sino también una práctica ética que protege a los usuarios y refuerza la confianza en las tecnologías digitales.



Seguridad y Ética en Almacenamiento de Datos

Ética y Normativas en Argentina

- En Argentina, la regulación sobre la protección de datos personales se basa en la Ley de Protección de Datos Personales N° 25.326, que es similar en espíritu al GDPR europeo. Esta ley asegura que los ciudadanos tengan control sobre sus datos personales y establece requisitos claros para su tratamiento:
- **Consentimiento explícito:** Los datos no pueden ser recopilados sin el consentimiento explícito del individuo, excepto en circunstancias específicas definidas por la ley.



Seguridad y Ética en Almacenamiento de Datos

Ética y Normativas en Argentina

- **Derecho de acceso, rectificación y supresión:** Los individuos tienen derecho a acceder a sus datos personales, solicitar correcciones y, en algunos casos, pedir que se eliminen.
- **Seguridad de los datos:** Las entidades que manejan datos deben tomar medidas técnicas y organizativas adecuadas para protegerlos de accesos no autorizados o procesamientos ilícitos.

Además, Argentina es miembro activo de la Red Iberoamericana de Protección de Datos, lo que facilita la cooperación regional en materia de protección de datos y el intercambio de buenas prácticas.



Seguridad y Ética en Almacenamiento de Datos

Impacto de la Inteligencia Artificial en el Manejo de Datos

- La Inteligencia Artificial (IA) juega un papel cada vez más importante en el análisis y manejo de grandes volúmenes de datos. Sin embargo, el uso de IA en bases de datos y en el manejo de información pública plantea varias cuestiones éticas:
- **Transparencia:** Debe ser clara la manera en que los sistemas de IA toman decisiones, especialmente cuando esas decisiones afectan a las personas directamente.



Seguridad y Ética en Almacenamiento de Datos

Impacto de la Inteligencia Artificial en el Manejo de Datos

- **Sesgo y Justicia:** Los algoritmos de IA pueden perpetuar o incluso exacerbar sesgos existentes en los datos. Es crucial implementar prácticas que identifiquen y corrijan sesgos en los modelos de IA.
- **Privacidad:** La IA puede identificar patrones que podrían exponer información sensible de maneras no intencionadas. Las técnicas como el aprendizaje federado o el cifrado homomórfico pueden ayudar a mitigar estos riesgos.



Seguridad y Ética en Almacenamiento de Datos

Manejo de Información Pública

- El manejo de información pública con tecnologías de bases de datos e IA debe ser guiado por principios de apertura y responsabilidad:
- **Acceso público:** Asegurar que la información pública sea accesible de manera que fomente la transparencia y la participación ciudadana.
- **Protección de datos sensibles:** Al mismo tiempo, es vital proteger los datos personales y sensibles para prevenir el mal uso o la exposición que puedan afectar la privacidad individual.
-



¡Muchas gracias!