

SEGURIDAD DE DATOS

01



¿QUÉ ES?

La seguridad de datos es esencial para proteger la información sensible de accesos no autorizados y posibles corrupciones. A continuación, se presenta un síntesis basada en la información proporcionada por PowerData



¿Qué es la seguridad de datos?

La seguridad de datos, también conocida como seguridad de la información o seguridad informática, implica la implementación de medidas que salvaguardan la privacidad digital y previenen accesos no autorizados a datos almacenados en diversos medios, como ordenadores, bases de datos y sitios web. Estas medidas incluyen la encriptación de datos, la tokenización y prácticas de gestión de claves, garantizando la protección de la información durante todo su ciclo de vida



01

COMPONENTES CLAVE DE LA SEGURIDAD DE DATOS

1. Personas: Es fundamental que los empleados comprenda y apliquen las políticas de seguridad establecidas por la organización

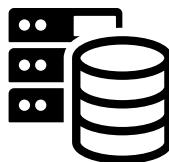
2. Procesos: Establecer procedimiento claros y efectivos para manejar y proteger los datos es esencial para mantener la integridad y confidencialidad de la información.

3. Tecnología: Utilizar herramientas y soluciones tecnologías adecuadas permite implementar controles de seguridad eficaces y adaptativos

Amenazas Actuales en la Seguridad de Datos



Con el auge del internet de las cosas (IoT), han surgido nuevas vulnerabilidades, ya que la interconexión de dispositivos crea más puntos de acceso para posibles ataques.



Además, los ataques de ransomware han incrementado en frecuencia y gravedad, afectando tanto a grandes organizaciones como usuarios individuales.



02

SEGURIDAD DE DATOS: LOCAL VS NUBE



Local y Nube

Aunque algunas empresas dudan en migrar a la nube por preocupaciones de seguridad, los proveedores de servicios en la nube suelen contar con equipos especializados y recursos dedicados para garantizar la protección de los datos. La clave está en evaluar las necesidades específicas de la organización y seleccionar la solución más adecuada.



Soluciones y
Habilidades
Importantes

Enmascaramiento de Datos: Protege la información sensible ocultándola, permitiendo su uso en entornos no seguros sin revelar datos reales.

Scure@Source: Ofrece inteligencia de seguridad de datos, ayudando a las organizaciones a comprender y mitigar riesgos asociados a datos confidenciales.

Implementar una estrategia robusta de seguridad de datos es esencial para proteger los activos críticos de una organización, mantener la confianza de los clientes y cumplir con las regulaciones vigentes.

04 CRIPTOGRAFÍA

“Es más fácil encontrar hombres voluntarios para morir, que encontrar aquellos que están dispuestos a soportar el dolor con paciencia” Julio César

Introducción

El objetivo original de la criptografía era mantener en secreto un mensaje, en la actualidad no se persigue únicamente la privacidad o confidencialidad de los datos, sino que se busca además garantizar la autenticidad de los mismos (el emisor del mensaje que leemos es el mismo que nos enviaron) y su no repudio (el emisor no puede negar el haber enviado el mensaje).

¿Qué es un cripto sistema?

Matemáticamente, podemos definir un criptosistema como una cuaterna de elementos.

- Un conjunto finito llamado alfabeto, , a partir del cual, y utilizando ciertas normas sintácticas y semánticas, podemos emitir un mensaje en claro (plain text) u obtener el texto en claro correspondiente a un mensaje cifrado (cipher text).
- Otro conjunto finito denominado espacio de claves, , formado por todos las posibles claves, tanto de cifrado como de descifrado, del criptosistema.



Criptosistemas de clave secreta

Denominados criptosistemas de clave secreta (de clave privada, de clave única o simétrico) o aquel criptosistema en el que la clave de cifrado, puede ser calculada a partir de la de descifrado, y viceversa. En la mayoría de estos sistemas, ambas claves coinciden, y por supuesto han de mantenerse como un secreto entre emisor y receptor: si un atacante descubre la clave utilizada en la comunicación, ha roto el criptosistema.

Cifradores de flujo

Son aquellos que pueden cifrar un solo bit de texto claro al mismo tiempo, y por tanto su cifrado se producto bit a bit.

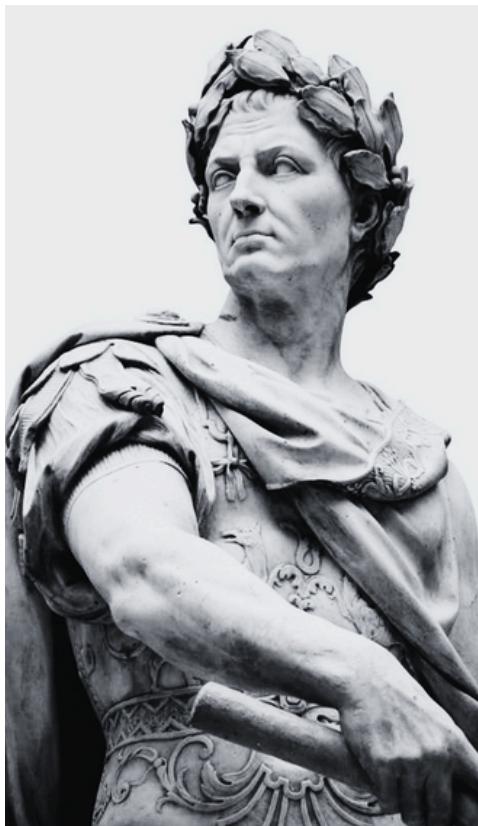
Cifradores de bloque

Cifran un bloque de bits (habitualmente, cada bloque es de 63 bits) como una única unidad.

Criptosistemas de clave publica

Cuando un receptor desea recibir una información cifrada, ha de hacer llegar a todos los potenciales emisores su clave pública, para que esos cifren los mensajes con dicha clave. De este modo, el único que podrá descifrar el mensaje será el legítimo receptor, mediante su clave privada.

CRYPTOGRAPHY CLASSICAL



El cifrado César es uno de los más antiguos que se conocen.

Deben su nombre al emperador Julio César, que presuntamente lo utilizó para establecer comunicaciones seguras con sus generales durante las Guerras Galicas.

Origen histórico del cifrado César

El cifrado César es uno de los métodos de encriptación más antiguos conocidos, y su origen se remonta al Imperio Romano, hace más de 2,000 años.

Fue utilizado por Julio César, un importante general, político y dictador romano, para proteger mensajes militares que enviaban a sus tropas o aliados.

05 CRIPTOSISTEMA DE VIGENÈRE

¿Qué es el cifrado de Vigenère?

Es un método de encriptación poli alfabética, lo que significa que usa varía letras clave para cifrar el mensaje, no solo una letra como en el cifrado Cesar

- Fue descrito por el diplomático Blaise de Vigenère en el siglo XVI, aunque en realidad ya había sido inventado por otros autores.

- El resultado es el mensaje cifrado



¿Cómo funciona?

- Se elige una palabra clave (por ejemplo: "CLAVE").
- Esa palabra clave se repite tantas veces como haga falta para igualar la longitud del mensaje
- Luego se suma cada letra del mensaje original con la letra correspondiente de la clave, como si cada letra fuera una posición en el alfabeto

06 PROTOCOLOS

Importante para la protección de los datos en la base de datos

Cada fotografía cuenta una historia. Puede ser un retrato que revele la profundidad de una mirada, una calle vacía que sugiera soledad o un paisaje que despierte asombro. La magia de la fotografía radica en su capacidad para evocar sentimientos sin necesidad de palabras, en su poder para transportarnos a otros lugares y momentos con solo una imagen.

La fotografía no tiene barreras; es un lenguaje universal. Puede ser documental, conceptual, abstracta o incluso surrealista, pero en todas sus formas nos invita a mirar el mundo desde ángulos inesperados.

- **Autenticación de los usuarios:** uno de los elementos más importantes incluye la gestión de identidades del usuario, para identificar que se la persona indicada que solicita el acceso a una información y así evitar fraudes como la suplantación de identidad
- **Cifrado de datos:** a través del cifrado de datos es como los sistemas mantienen encriptada la información que se transmiten entre usuarios para evitar que sea interceptada en el camino
- **Organización de los datos:** Este elemento tiene que ver con la forma en que se almacena la información del usuario para que pueda ser utilizada cuando la situación lo amerite.

PROTOCOLO TCP/IP

El protocolo de control de trasmisión/Protocolo de internet o transmission Control Protocol/Internet Protocol (TCP/IP) corresponde a un conjunto de reglas que permiten la comunicación de dos equipos entre si a través de internet

Para evitar la información entre dos equipos y garantizar su comunicación, el protocolo TC/IP divide los datos en paquetes individuales y una vez que llegan a su destino, son ensamblados nuevamente para armar la información completa. Esto asegura que la información enviada sea más exacta

Para garantizar que cada comunicación llegue intacta al destino deseado, el modelado TCP/IP divide los datos en paquetes individuales y una vez que llegan a su destino envían los datos en paquetes pequeños hace que sea más fácil mantener la exactitud que enviando todos los datos a la vez.

PROTOCOLO HTTP

El protocolo de transferencia de hipertexto (HTTP) se encarga de proteger la información que es transferida a través de la World Wide Web (www). Cuando el usuario ingresa una dirección URL en el navegador, la información es enviada al sitio web a través del protocolo HTTP.





Posteriormente, la página web solicitada por el usuario emite una respuesta y muestra los resultados que cumplan con los criterios de la búsqueda realizada por el usuario en el navegador

En este caso, para garantizar la seguridad de la información y disminuir vulnerabilidades es necesarios contar con certificados SSL, o HTTPS, los cuales sirven para cifrar la información transmitida al sitio web

PROTOCOLO SSH

El protocolo Secure Socket Shell (en español es llamado intérprete de órdenes seguro) tiene como objetivo ofrecer una opción confiable para tener acceso remoto a un ordenador de forma segura, a través de un canal.

PROTOCOLO FTP

El protocolo de transferencia de archivo o File Transfer Protocol (FTP) es utilidad para transferir archivos a través de redes que están conectadas al protocolo TCP. Gracias al FTP, el usuario se puede conectar a un servidor para obtener los archivos o información que necesite.

Para ello, dicho protocolo se encarga de cifrar los datos de los dispositivos conectados a internet, de manera que las personas ajenas no puedan acceder a dicha información.



"Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum."



**DIEGO FLORES
GONZÁLEZ**