

TECNOLOGÍAS DE SEGURIDAD: CLOUD SECURITY

GRUPO 3 INTEGRANTES

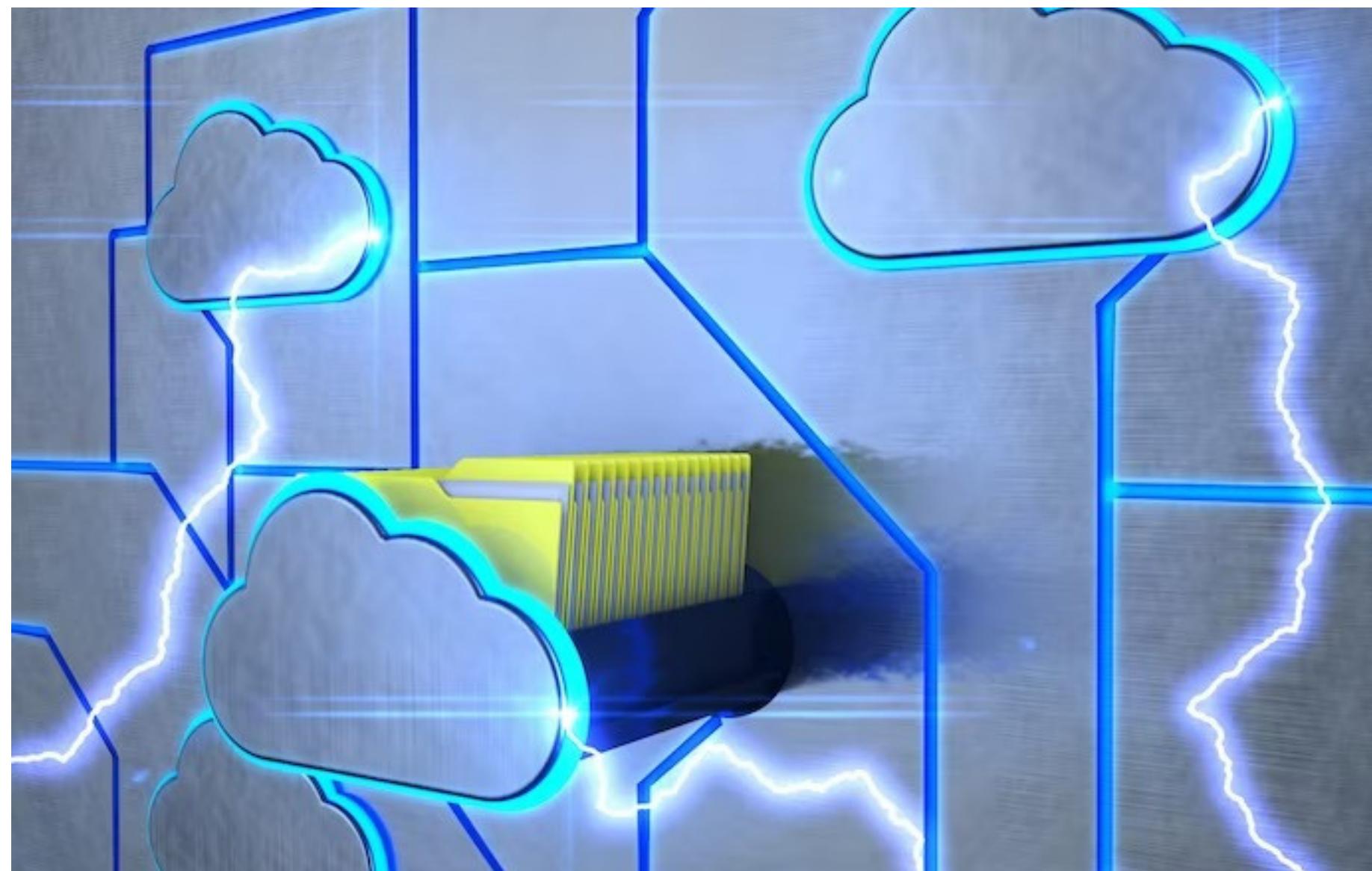
- NARDY CACHIPUENDO
- ARIEL GUAÑA
- CRISTOFER PAUCAR
- JUAN RENGIFO
- NATHALY SIMBA

PROFESOR: ING. JUAN HERRERA
FECHA: 14/11/2023



1. INTRODUCCIÓN

Definición



- Son las prácticas que ayudan a la protección de:
 - Datos
 - Aplicaciones
 - Sistemas almacenados
 - Sistemas procesados dentro de la nube
- La nube se encarga de salvaguardar la información que es accesible por medio de internet.

Beneficios y Desafíos

BENEFICIOS

- Escalabilidad: Facil adaptación a cambios.
- Accesibilidad: Facilita el acceso remoto a datos y aplicaciones
- Eficiencia: Reduce la necesidad de mantenimiento disminuyendo costos operativos.

DESAFÍOS

- Privacidad: Conocer quien tiene acceso al sistema es crucial.
- Cumplimiento Legal: El manejo de datos es diferente en cada región.
- Derechos de Acceso: Se debe garantizar una configuración correcta de roles y permisos.

Amenazas y Riesgos

AMENAZAS

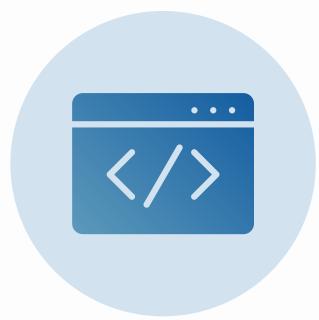
- Acceso no autorizado por comprometimiento de credenciales.
- Fugas de Datos: Pérdida de información sensible.
- Ataques DDoS (Denegación de Servicio Distribuido): Tráfico malicioso de datos que busca sobrecargar los servicios.

RIESGOS

- Interrupciones del Servicio: Problemas técnicos, ataques cibernéticos o desastres naturales
- Fallas en la gestión de configuración resulta en vulnerabilidades.
- Interconexiones Inseguras: Conexiones entre servicios y sistemas pueden ser blanco de ataques

2. ARQUITECTURA

Componentes



Firewalls

Se utilizan para proteger las redes y los sistemas en la nube de posibles amenazas.

Ejemplos



Cifrado

Se utiliza para proteger las comunicaciones y los datos almacenados en la nube.

Ejemplos



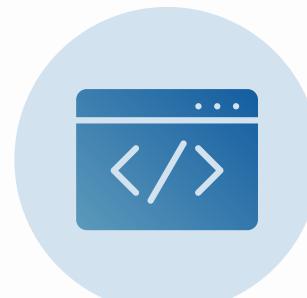
Autenticación

Se utiliza para garantizar que solo los usuarios autorizados tengan acceso a los recursos y servicios en la nube.

Ejemplos



Componentes



Gestión de identidad y accesos

Gestiona la administración de las identidades y los accesos de los usuarios a los recursos y servicios.

Ejemplos

okta



Protección contra amenazas

Incluye el uso de sistemas de detección y prevención de intrusiones, para identificar y bloquear actividades maliciosas.

Ejemplos

Malwarebytes



Monitoreo y auditoría

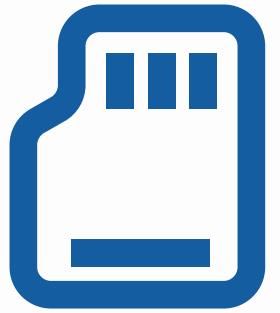
Registra y analiza eventos, para identificar actividades sospechosas.

Ejemplos

Nikto
a Practical Website Vulnerability Scanner



Estrategias



Cifrar datos confidenciales

Se utiliza para proteger los datos confidenciales almacenados en la nube.



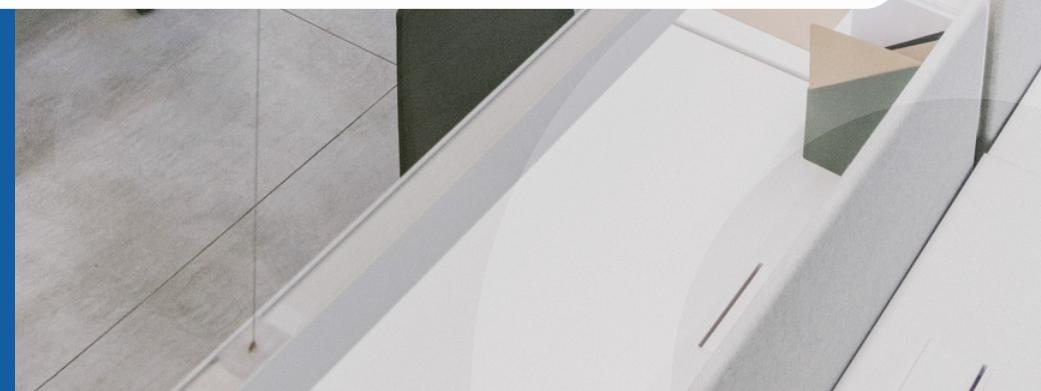
Segmentación

Divide la infraestructura de la nube en segmentos separados, cada uno con sus propios permisos y controles de acceso

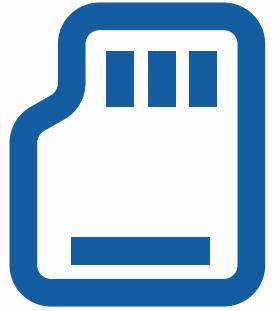


Restringir el tráfico

Evita que los datos confidenciales sean enviados a destinos no autorizados



Estrategias



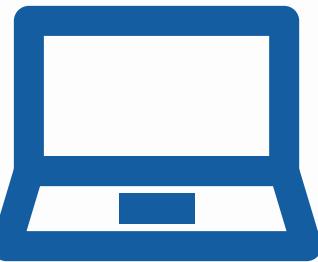
Implementar el escaneo de vulnerabilidad

Se pueden identificar las vulnerabilidades y tomar medidas para corregirlas antes de que sean explotadas por los atacantes.



Defensa en profundidad

Se implementan múltiples capas de seguridad para proteger los sistemas y datos en la nube.



Respaldo y recuperación de datos

Se crean copias de seguridad, para poder recuperarlos en caso de pérdida, corrupción o eliminación accidental.



3. AUTENTICACIÓN Y CONTROL DE ACCESO

¿Por qué la gestión de identidad es diferente en la nube?

Uno de los principales desafíos en la nube radica en la gestión de la identidad y el acceso a los recursos. Se utiliza:

LA FEDERACIÓN

Establece relaciones de confianza entre organizaciones y aplicándolas mediante tecnologías basadas en estándares.

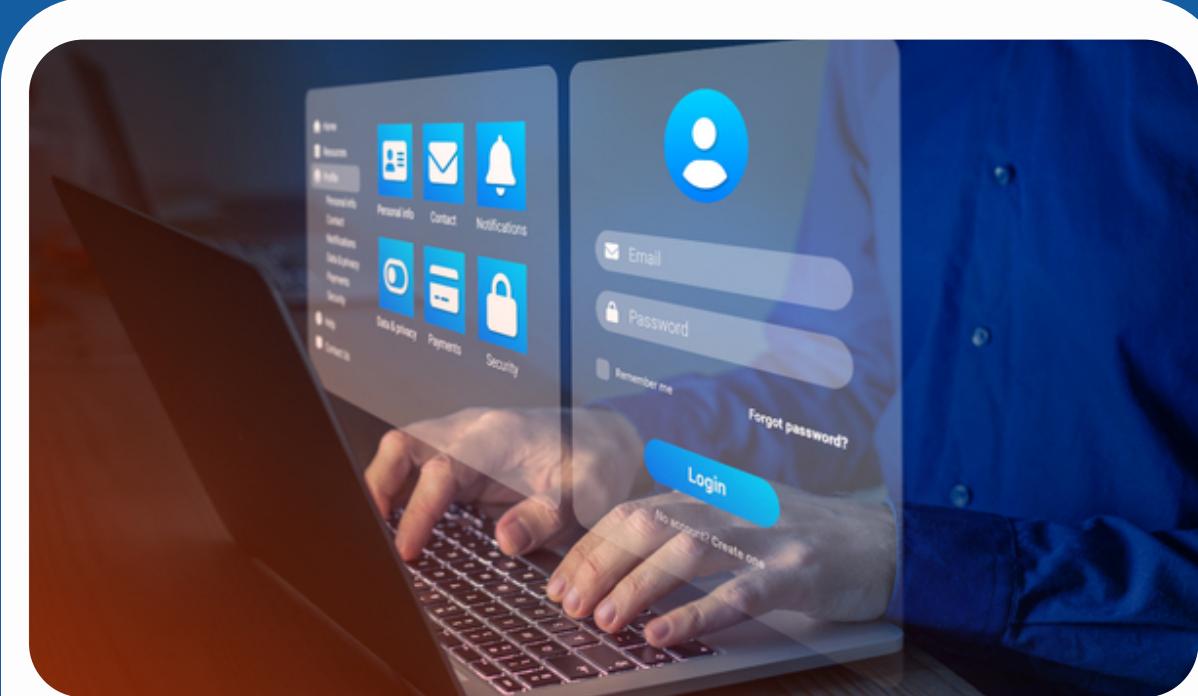
Autenticación y acceso sin la necesidad de administrar múltiples credenciales separadas



Autenticación

Métodos

- contraseñas
- factores de autenticación multifactor (MFA)
- autenticación biométrica.



Control de acceso

Métodos

- control de acceso basado en roles (RBAC)
- el control de acceso basado en políticas (ABAC)
- control de acceso basado en atributos (ABAC)

Autenticación multifactor o MFA

Método de confirmación de la identidad del usuario que utiliza al menos dos factores diferentes de autenticación

Lo que el usuario sabe

- contraseña

Algo que el usuario tiene

- token de seguridad
- una aplicación de autenticación móvil

Algo que el usuario es

- huella digital
- reconocimiento facial



¿CÓMO HACER QUE MFA SEA MÁS FÁCIL?

01. MFA ADAPTATIVO

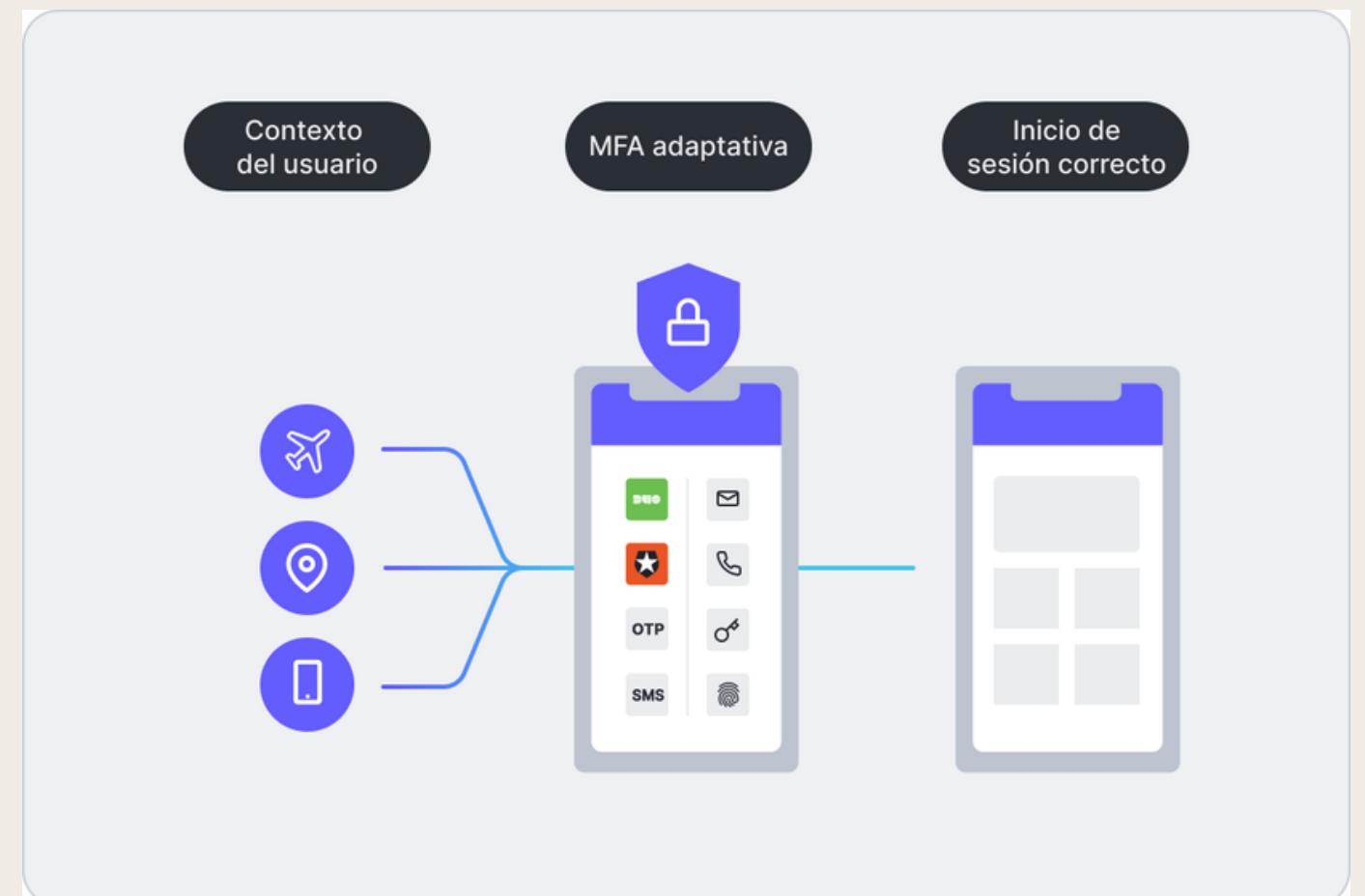
Utiliza la inteligencia artificial para asignar de forma inteligente un nivel de riesgo a cada acceso

Esto aplica el conocimiento, las reglas comerciales o las políticas a factores basados en el usuario.

EJEMPLO

Inicio de sesión

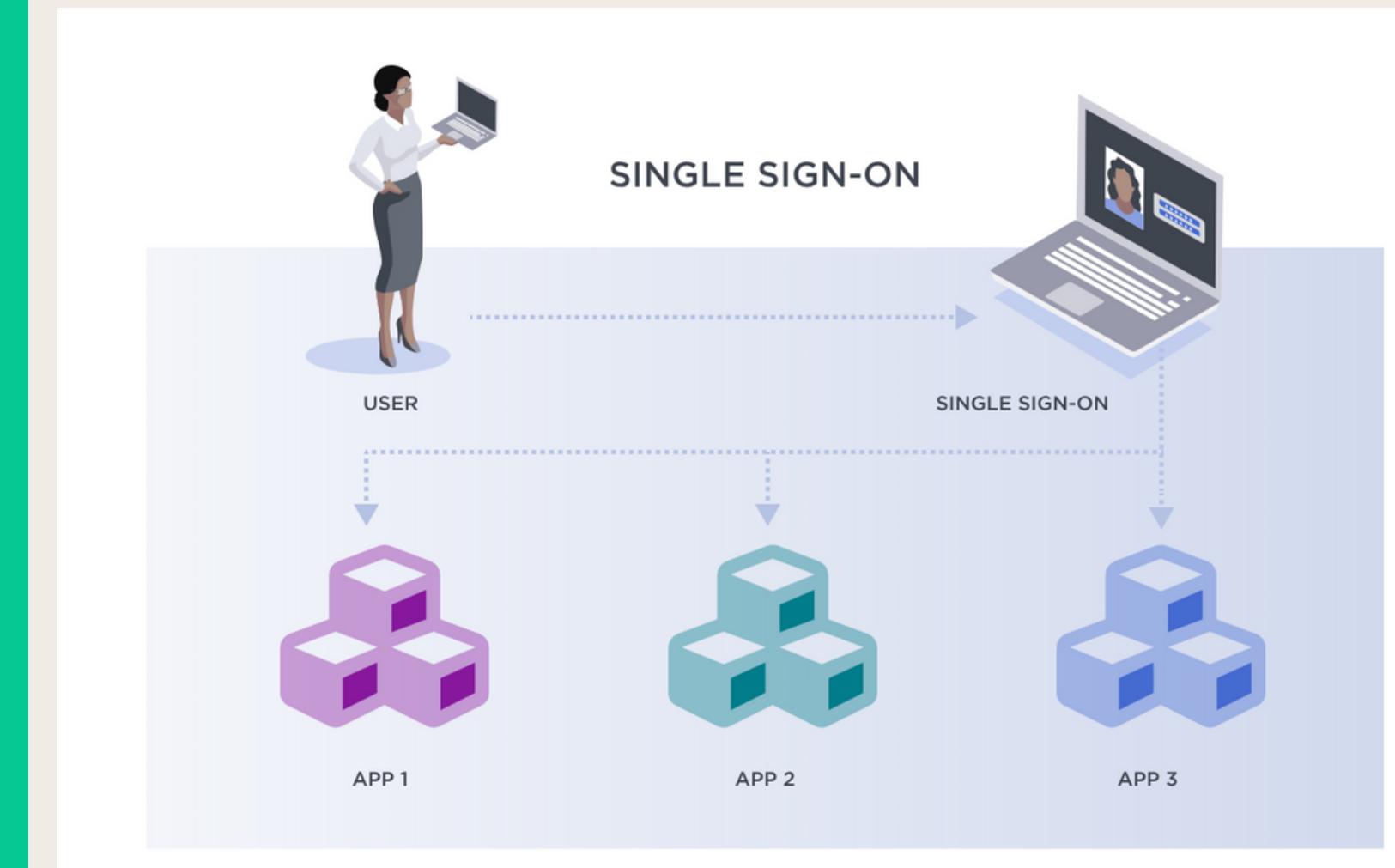
- desde casa
- desde un sitio desconocido



¿CÓMO HACER QUE MFA SEA MÁS FÁCIL?

02. INICIO DE SESIÓN ÚNICO (SSO)

Permite a los usuarios iniciar sesión en varias aplicaciones y sitios web con una única autenticación de usuario



¿CÓMO HACER QUE MFA SEA MÁS FÁCIL?

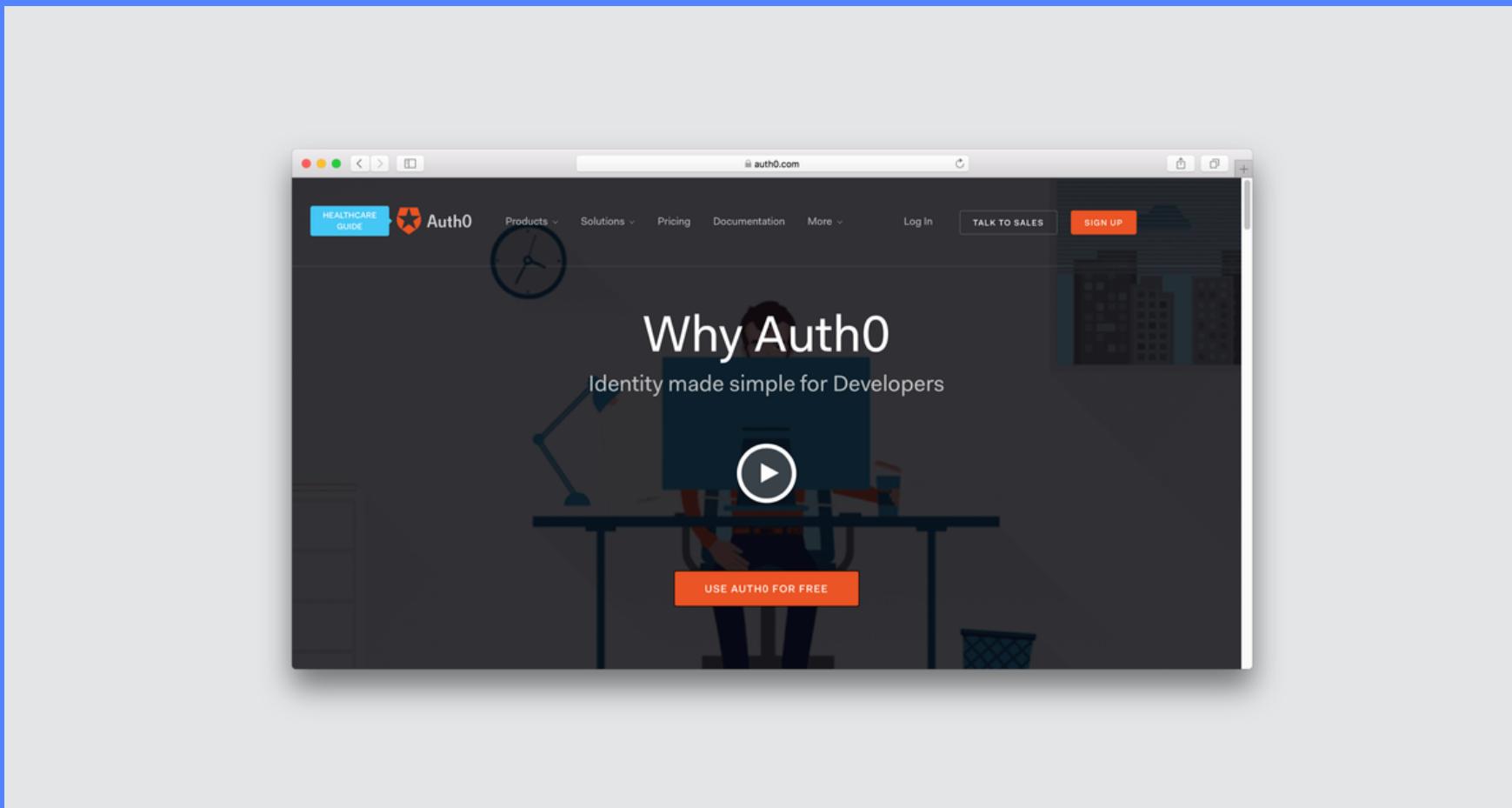
03. AUTENTICACIÓN PUSH

El sistema de seguridad emite automáticamente un tercer código de identificación de un solo uso para el dispositivo móvil del usuario.



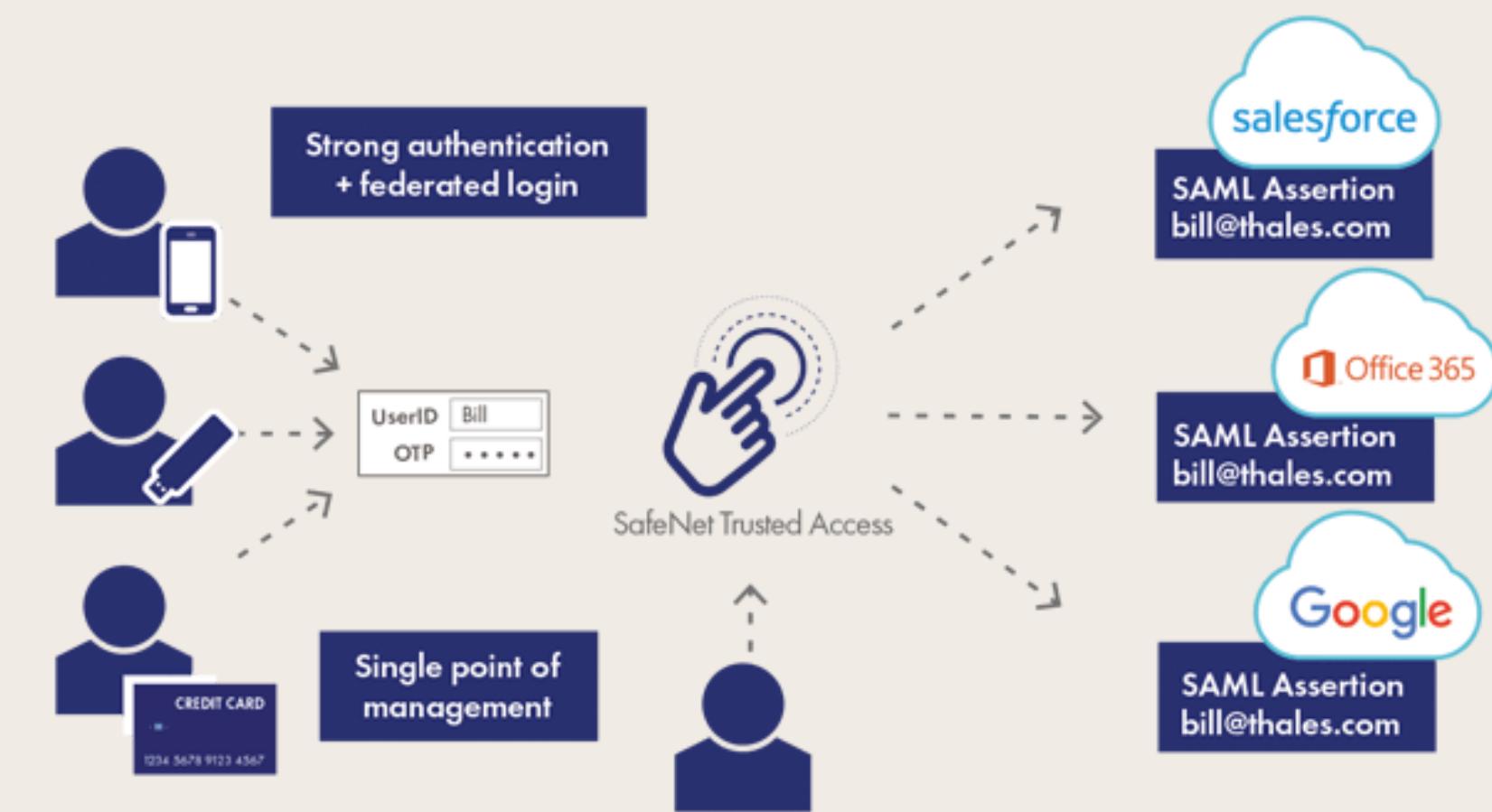
HERRAMIENTAS - SOLUCIONES

Auth0 ofrece soluciones de Gestión de Identidades y Accesos (IAM) en la nube.



Se utiliza con mayor frecuencia para delegar el control de acceso y las autorizaciones entre servicios.

SafeNet Trusted Access de Thales ofrece federación de identidades, controles de acceso y autenticación sólida para aplicaciones locales y SaaS.



4. ENCRIPCIÓN Y PROTECCIÓN DE DATOS EN LA NUBE

ENCRYPTACIÓN Y PROTECCIÓN DE DATOS EN LA NUBE

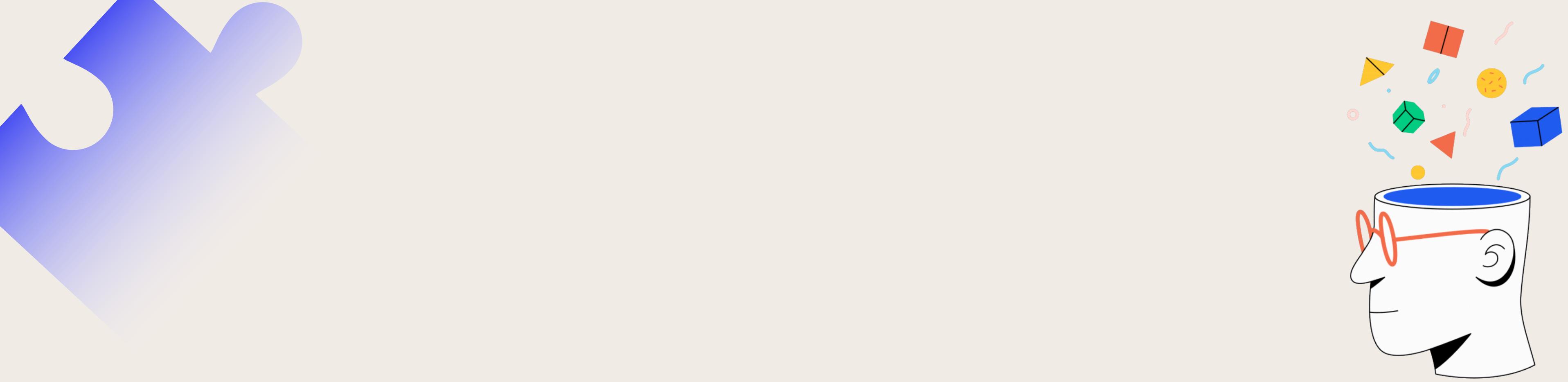
La protección de datos en la nube se refiere a un conjunto de medidas de seguridad y almacenamiento diseñadas para resguardar los datos almacenados en entornos de nube, así como la información que entra y sale de ellos.

- Protección de datos
- Seguridad de datos

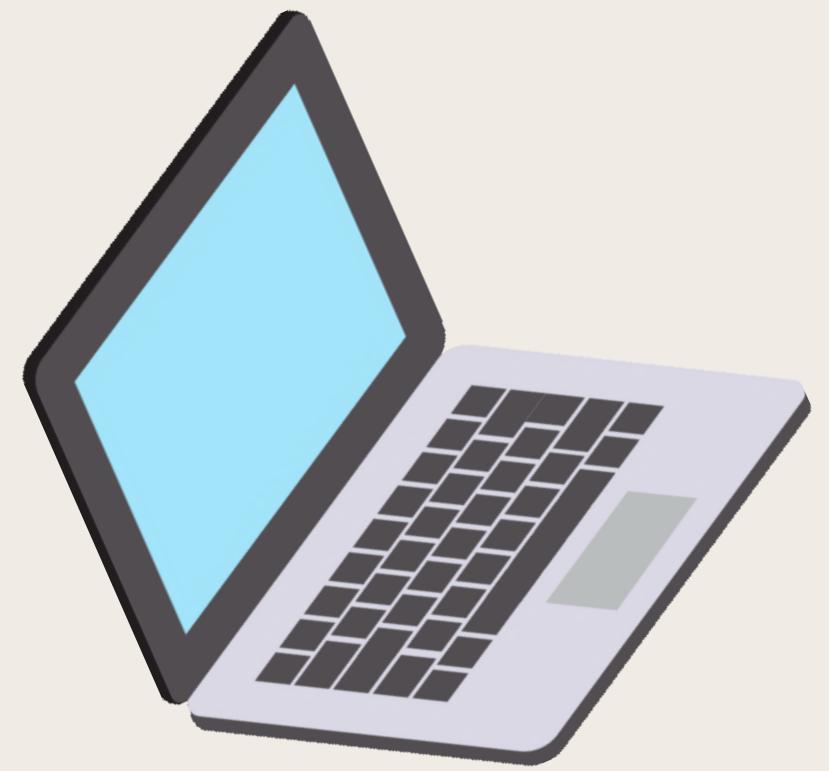




- La seguridad de los datos en la nube se aplica a las empresas administradas internamente como a las gestionadas por un proveedor de servicios externo.
- Está diseñado para proteger los datos y las aplicaciones de los usuarios, administrar las amenazas y proporcionar controles de acceso seguros a las empresas
- Esto es especialmente cierto para las empresas internacionales que deben cumplir con el RGPD



ENcriptación

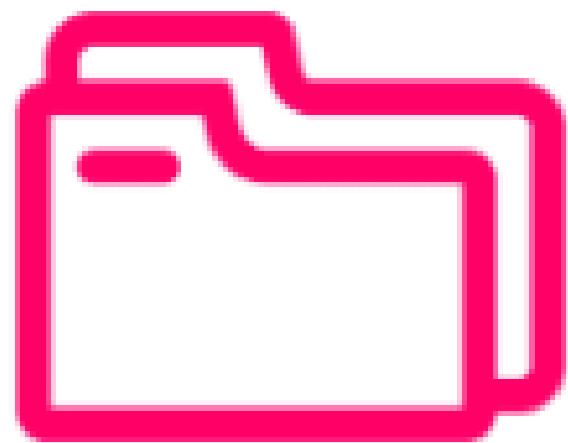


- El proceso de codificar texto legible en un código seguro
- La encriptación utiliza una fórmula llamada «cifrado» o algoritmo de encriptación.
- En ciberseguridad la encriptación es un pilar de muchos protocolos y procedimientos de ciberseguridad en especial en IPP.



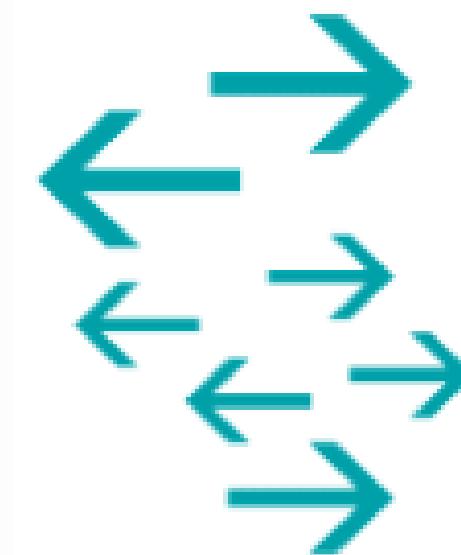
ENCRYPTION

Encriptación



En reposo

La encriptación en reposo se refiere a la protección de datos almacenados en servidores o dispositivos de almacenamiento en la nube.



En tránsito

La encriptación en tránsito se utiliza para proteger los datos mientras se transfieren entre un usuario y un servidor en la nube.

Encriptación en la nube y beneficios.

- El cifrado de datos en la nube es el proceso de proteger la información contenida en los servidores virtuales y la forma de acceder a dicha información.

01

Mantiene la confidencialidad de los datos.

02

Ayuda a las organizaciones a cumplir con las regulaciones.

03

Protege los datos en todos los dispositivos.

04

Protege los datos en ambientes laborales híbridos.

05

Preserva la propiedad intelectual.

Herramientas de Encriptación



OpenSSL

Es una biblioteca de código abierto que proporciona una amplia gama de herramientas y utilidades para la criptografía, incluyendo la creación y gestión de certificados digitales y la encriptación de datos.



GNU PGP

GnuPG nos permite usar criptografía simétrica y asimétrica para cifrar y firmar nuestros datos.

Herramientas de Encriptación



VeraCrypt

VeraCrypt

Una herramienta de código abierto que permite crear unidades virtuales encriptadas y cifrar archivos y particiones



BitLocker

Disponible en sistemas Windows, BitLocker permite cifrar unidades de disco completo para proteger los datos en un dispositivo



LUKS
Linux Unified Key Setup

LUKS (Linux Unified Key Setup)

Una herramienta de encriptación utilizada comúnmente en sistemas Linux para proteger volúmenes de disco.

Herramientas de Encriptación : Servicios



Amazon Web Services

AWS ofrece una amplia gama de servicios y características de seguridad, incluyendo AWS Key Management Service (KMS) para la gestión de claves y AWS Identity and Access Management (IAM) para la gestión de accesos.



Microsoft Azure

Azure proporciona herramientas como Azure Key Vault y Azure Security Center



Google Cloud Platform

GCP cuenta con Google Cloud Key Management Service (KMS) y herramientas de seguridad como Identity and Access Management (IAM)

5. CUMPLIMIENTO Y NORMATIVAS EN LA SEGURIDAD DE LA NUBE



CUMPLIMIENTO Y NORMATIVAS EN LA SEGURIDAD DE LA NUBE

En el mundo digital actual, donde la información es un activo vital, la seguridad de la nube juega un papel fundamental. En esta presentación, exploraremos a fondo los estándares de seguridad y cumplimiento en la nube, entendiendo su importancia en la protección de datos y la construcción de la confianza del cliente.

IMPORTANCIA DE LA SEGURIDAD EN LA NUBE

La seguridad en la nube es crucial para proteger los datos y garantizar el cumplimiento de las normativas. Las organizaciones deben cumplir con estándares como ISO 27001 y GDPR para mantener la confidencialidad e integridad de la información.



ESTÁNDARES DE CUMPLIMIENTO

Los estándares de cumplimiento, como HIPAA y PCI DSS, son fundamentales para proteger la información sensible en la nube. Estos aseguran que las organizaciones cumplan con requisitos específicos para garantizar la seguridad y la privacidad.



NORMATIVAS DE PROTECCIÓN DE DATOS

Las normativas como el RGPD imponen requisitos estrictos sobre la protección de datos personales en la nube. Es crucial para las organizaciones asegurarse de cumplir con estas normativas para evitar sanciones y proteger la privacidad de los usuarios.



ISO 27001 (SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - ISMS)

¿Para qué sirve?

- Propósito Principal: Establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información.
- Enfoque en la Gestión de Riesgos: Identificación y evaluación de riesgos para la información y aplicación de controles para reducir o eliminar esos riesgos.

¿Cómo funciona?

- Ciclo PDCA: Basado en el ciclo Plan-Do-Check-Act.
 - Planificación: Establecer políticas, objetivos y procesos relevantes para la gestión de riesgos y la seguridad de la información.
 - Implementación (Hacer): Implementar y operar los controles y procesos definidos.
 - Monitoreo y Revisión (Verificar): Evaluar y realizar auditorías internas para garantizar la conformidad con la norma.
 - Mejora Continua (Actuar): Realizar acciones para mejorar continuamente el sistema de gestión de seguridad de la información.



SOC 2 (INFORME DE CONTROL DE ORGANIZACIONES Y SERVICIOS)

¿Para qué sirve?

- Propósito Principal: Evaluar y garantizar la seguridad, disponibilidad, integridad del sistema, confidencialidad y privacidad de los datos almacenados en la nube.
- Centrado en Empresas que Manejan Datos Sensibles: Es particularmente relevante para las organizaciones que almacenan y procesan datos confidenciales de clientes.

¿Cómo funciona?

- Criterios de Evaluación: Evalúa la efectividad de los controles de seguridad de una organización en cinco áreas clave.
 - Seguridad: Protección contra el acceso no autorizado.
 - Disponibilidad: Asegura la disponibilidad del sistema.
 - Integridad del Sistema: Mantiene la integridad de la información.
 - Confidencialidad: Garantiza la confidencialidad de la información.
 - Privacidad de la Información: Manejo ético y adecuado de la información personal.



GDPR (REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS)

¿Para qué sirve?

- Propósito Principal: Proteger la privacidad y los derechos de los ciudadanos de la Unión Europea en relación con el procesamiento de sus datos personales.
- Enfoque en Derechos Individuales: Proporciona a los individuos un mayor control sobre sus datos personales.

¿Cómo funciona?

- Principios Clave:
 - Consentimiento Informado: Se requiere el consentimiento claro y explícito para procesar datos personales.
 - Derechos del Individuo: Incluye el derecho al acceso, rectificación y eliminación de datos.
 - Obligación de Notificación de Brechas: Las organizaciones deben informar sobre violaciones de datos en un plazo de 72 horas.



HIPAA (LEY DE PORTABILIDAD Y RESPONSABILIDAD DEL SEGURO MÉDICO)

¿Para qué sirve?

- Propósito Principal: Proteger la privacidad y seguridad de la información de salud protegida (PHI) en el ámbito de la atención médica.
- Enfoque en la Salud: Aplicable a entidades que manejan información de salud, como proveedores de servicios de salud y compañías de seguros.

¿Cómo funciona?

- Requisitos Específicos:
 - Protección de la PHI: Establece estándares para el manejo seguro de información médica.
 - Control de Acceso: Define quién puede acceder a la información de salud y bajo qué condiciones.



Health Insurance Portability and Accountability Act

CONCLUSIONES

La seguridad en la nube es fundamental para proteger los datos y garantizar el funcionamiento seguro de las aplicaciones y servicios en entornos cloud.

La implementación de autenticación multifactor (MFA) y el control de acceso basado en roles son pilares esenciales para prevenir accesos no autorizados y fortalecer la seguridad.

La encriptación de datos en reposo y en tránsito, junto con una sólida gestión de claves, es crucial para garantizar la confidencialidad e integridad de la información almacenada en la nube.

La adhesión a normativas y estándares en la nube es esencial para garantizar la seguridad, privacidad y cumplimiento normativo de los datos almacenados y procesados en entornos cloud.

FUENTES DE CONSULTA

- <https://cloud.google.com/solutions/security/?hl=en>
- <https://www.redeszone.net/tutoriales/seguridad/control-de-acceso-que-es/>
- <https://canvia.com/control-acceso-usuarios-nube/>
- <https://www.deltaprotect.com/blog/seguridad-en-la-nube>
- [https://www.trendmicro.com/es_mx/what-is/cloud-security.html#:~:text=La%20seguridad%20en%20la%20nube%20inicia%20con%20la%20arquitectura%20de,detección%20de%20intrusiones%20\(IDS\)](https://www.trendmicro.com/es_mx/what-is/cloud-security.html#:~:text=La%20seguridad%20en%20la%20nube%20inicia%20con%20la%20arquitectura%20de,detección%20de%20intrusiones%20(IDS))
- <https://ayscom.com/es/estrategias-para-aumentar-la-seguridad-en-la-nube/>
- <https://es-la.tenable.com/blog/five-core-principles-for-hybrid-cloud-security>

**GRACIAS
POR SU
ATENCIÓN**

