PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR
FACULTAD DE INGENIERIA
CARRERA DE: SISTEMAS Y COMPUTACION



TRABAJO DE TITULACION

EVALUACION DE PROTOCOLOS Y HERRAMIENTAS PARA PROTEGER LA PRIVACIDAD DE LOS DATOS EN ENTORNOS VIRTUALES

AUTOR:
ATIK AMARU YUMBAY CHIMBO

QUITO DM, 2024

1. Capítulo I: introducción

1.1. Tema

Evaluación de Protocolos y Herramientas para Proteger la Privacidad de los Datos en Entornos Virtuales

1.2. Justificación

En la actualidad la migración hacia la nube se ha vuelto una actividad más frecuente, debido a los diversos beneficios que aportan como: la flexibilidad, escalabilidad y eficiencia. Aun así, esta migración tiene varios riesgos en el área de seguridad y privacidad de los datos, dado que existen diversos proveedores de servicios de la nube para almacenar, procesar y gestionar información crítica.

En este aspecto, La seguridad en la nube se ha vuelto un tema interesante para empresas y usuarios privados. Las amenazas cibernéticas y la perdida de información crítica pueden tener consecuencias graves, tales como perdida de dinero, daño a la reputación.

La necesidad de esta investigación se enfoca en tratar los problemas de seguridad asociados a la migración a la nube, especialmente a la protección de la privacidad de los datos. La evaluación de protocolos y herramientas de seguridad en la nube es decisiva para encontrar soluciones efectivas para mitigar los riesgos y garantizar la confidencialidad, integridad y disponibilidad de la información almacenada en entornos virtuales.

Como último recurso, este trabajo de integración curricular ayudara a fomentar un mayor nivel de conciencia y preparación en seguridad en la nube, el objetivo es promover un entorno digital seguro y confiable.

1.3. Planteamiento del Problema

En la actualidad el almacenamiento, procesamiento y transferencia de datos ha cambiado hacia un entorno de computación en la nube ofreciendo diversos beneficios como la escalabilidad y

eficiencia, pero a la vez obteniendo desafíos en la seguridad y privacidad de la información. Los proveedores de estos servicios manejan información sensible que pueden estar expuestos a amenazas de ataques cibernéticos, violación de seguridad y acceso no autorizado.

De lo antes planteado, nace la necesidad de evaluar y mejorar las medidas de seguridad de la nube para proteger la privacidad de los datos. A pesar de que existen avances en protocolos y herramientas de seguridad en la nube, continúan existiendo preguntas:

- Vulnerabilidad y amenazas Emergentes: vulnerabilidades y amenazas que enfrentan los entornos de la nube.
- Protocolos de seguridad: que protocolos de seguridad en la nube son apropiados para proteger la integridad y confidencialidad de los datos.
- Herramientas de seguridad: Comparar las diferentes herramientas de seguridad en la nube para la detección y reducción de amenazar.

Ante estas circunstancias, es necesario realizar una investigación de los protocolos y herramientas de seguridad en la nube disponibles, con el objetivo de mitigar los riesgos y garantizar la protección de datos en la nube.

1.4. Objetivos

1.4.1. Objetivo General

Evaluación de protocolos y herramientas para proteger la privacidad de los datos en entornos virtuales, con el fin de proporcionar recomendaciones para mejorar la seguridad en la nube

1.4.2. Objetivos Específicos

- Investigar las vulnerabilidades y amenazas más recientes que enfrentan los entornos de nube.

- Analizar las mejores prácticas y estrategias para la gestión de políticas de seguridad en entornos de nube, tomando en cuenta requisitos normativos y estándares de la industria.
- Analizar la eficiencia de los protocolos de seguridad en la nube para la protección de datos.

1.5. Alcance

El alcance de este proyecto se asegurará un enfoque claro y especifico en la evaluación de la seguridad en la nube y la protección de la privacidad de los datos en entornos virtuales al realizar un análisis de protocolos de seguridad en la nube: SSL/TLS, OAuth, SAML y la efectividad de cada protocolo en términos de autenticación, autorización y cifrado de datos en entornos de nube, evaluación de diferentes herramientas de seguridad en la nube como firewalls, sistemas de detección de intrusiones (IDS/IPS), herramientas de monitoreo para la detección y mitigación de amenazas e Investigación de las vulnerabilidades y amenazas más recientes que enfrentan los entornos de nube en la privacidad de los datos.

2. Capítulo II: Fundamentos de la Seguridad en la Nube

En el acelerado mundo digital en el que nos encontramos actualmente, donde la información es uno de los activos más valiosos de las empresas u organizaciones, la seguridad en la nube ha tomado importancia en la industria de la tecnología. La forma en que las empresas gestionan y almacenan datos ha cambiado de forma drástica adoptando rápidamente el uso de la computación en la nube, surgiendo desafíos en términos de seguridad, protección y privacidad de la información. Con este contexto, la investigación de los fundamentos de la seguridad en la Nube es el punto clave para comprender los conceptos esenciales que abarca. Se investigará los fundamentos esenciales de la seguridad en la Nube, como la definición de la nube y sus modelos

de servicios, los beneficios y desafíos que se puede encontrar, por último, pero no menos importante la seguridad en entornos de la nube.

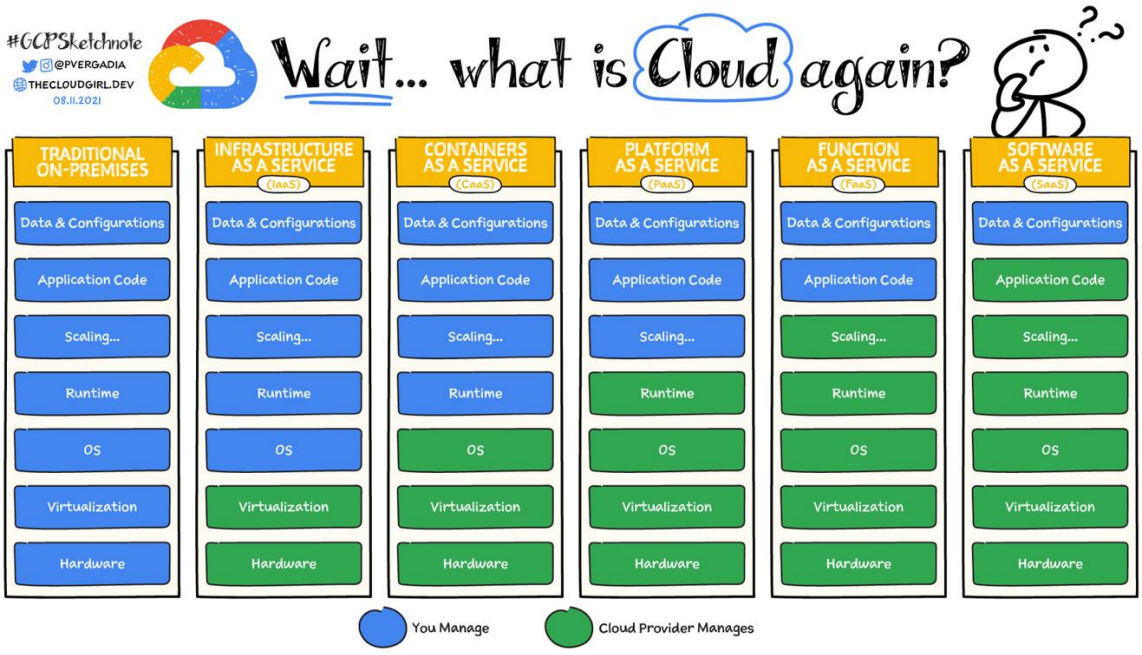
2.1. Definición de la nube y sus modelos de servicio

Podemos identificar diversos conceptos acerca de la computación en la nube, pero se nota que todos se refieren a la misma cosa, a la entrega de servicios y recursos de cómputo a través de internet, dejando de lado el almacenamiento y procesamiento de datos físicos o en servidores propios. Según (AWS, AWS, 2024) la computación en nube es el suministro a pedido de potencia de cómputo, bases de datos, almacenamiento, aplicación y otros recursos de TI a través de una plataforma de servicios en la nube a través de internet con pay-as-you-go (pago por uso). Una plataforma en la nube proporciona acceso rápido a recursos de TI flexible y de bajo coste. Con la computación en la nube, no necesita realizar grandes inversiones en hardware y dedicar mucho tiempo a la pesada tarea de administrar ese hardware. Otra definición de computación en la nube proporcionado por ATLASSIAN (Zettler, n.d.) la computación en la nube es la entrega de recursos informáticos, incluidos el almacenamiento, la potencia de procesamiento, las bases de datos, las redes, los análisis, la inteligencia artificial y las aplicaciones de software, a través de internet (la nube). Al externalizar estos recursos, las empresas pueden acceder a los activos informáticos que necesitan, en el momento en que los necesitan y sin tener que comprar ni mantener una infraestructura física local de TI. Esto proporciona recursos flexibles, innovación más rápida y economías de escalado.

Los modelos de servicios en la nube se dividen tres dependiendo las necesidades de usuarios y empresas, según Google Cloud, AWS, IBM los modelos de servicio de computación en la nube son:

- Software como Servicio (SaaS): El software como servicio le proporciona un producto completo que el proveedor del servicio ejecuta y administra. En la mayoría de los casos, quienes hablan de software como servicio en realidad se refieren a aplicaciones de usuario final. Con una oferta de SaaS, no tiene que pensar en cómo se mantiene el servicio ni en cómo se administra la infraestructura subyacente. Solo debe preocuparse por cómo utilizar ese sistema de software concreto. Un ejemplo común de una aplicación SaaS es un programa de correo electrónico basado en la web que le permite enviar y recibir mensajes sin tener que administrar la incorporación de características ni mantener los servidores y los sistemas operativos en los que se ejecuta el programa de correo electrónico, (AWS, AWS, 2024).
- Plataforma como Servicio (PaaS): La Plataforma como Servicio se distribuye a través de la web y permite que los desarrolladores puedan construir aplicaciones escalables y altamente disponibles, sin preocuparse del sistema operativo, el almacenamiento o las actualizaciones. Proporciona un espacio de trabajo que los desarrolladores pueden usar para desarrollar, gestionar, distribuir y testear sus aplicaciones de software**.** Este modelo de servicio iCloud hace que el proceso de desarrollo de aplicaciones sea mucho más simple, eficiente y competitivo**.** Varios usuarios pueden acceder a una plataforma PaaS a través de la misma aplicación de desarrollo. Esta plataforma integra servicios web, motores de bases de datos, para ayudar a los desarrolladores con el desarrollo, testeo y despliegue de apps, (Stackscale, 2023).

- Infraestructura como Servicio (IaaS): La infraestructura como servicio (IaaS) proporciona recursos de infraestructura bajo demanda a las empresas a través de la nube, como la computación, almacenamiento, redes y virtualización. Los clientes no tienen que gestionar, mantener ni actualizar su propia infraestructura de centro de datos, pero son los responsables del sistema operativo, middleware, máquinas virtuales y cualquier aplicación o dato, (Google cloud, 2024).



Ilustracion1: Nivel de control de los diferentes modelos de servicios, (Google cloud, 2024)

Estos modelos de servicio en la nube ofrecen diferentes niveles de control, flexibilidad y responsabilidad para los usuarios, pudiendo optar por el modelo que más se ajuste a las

necesidades del cliente.

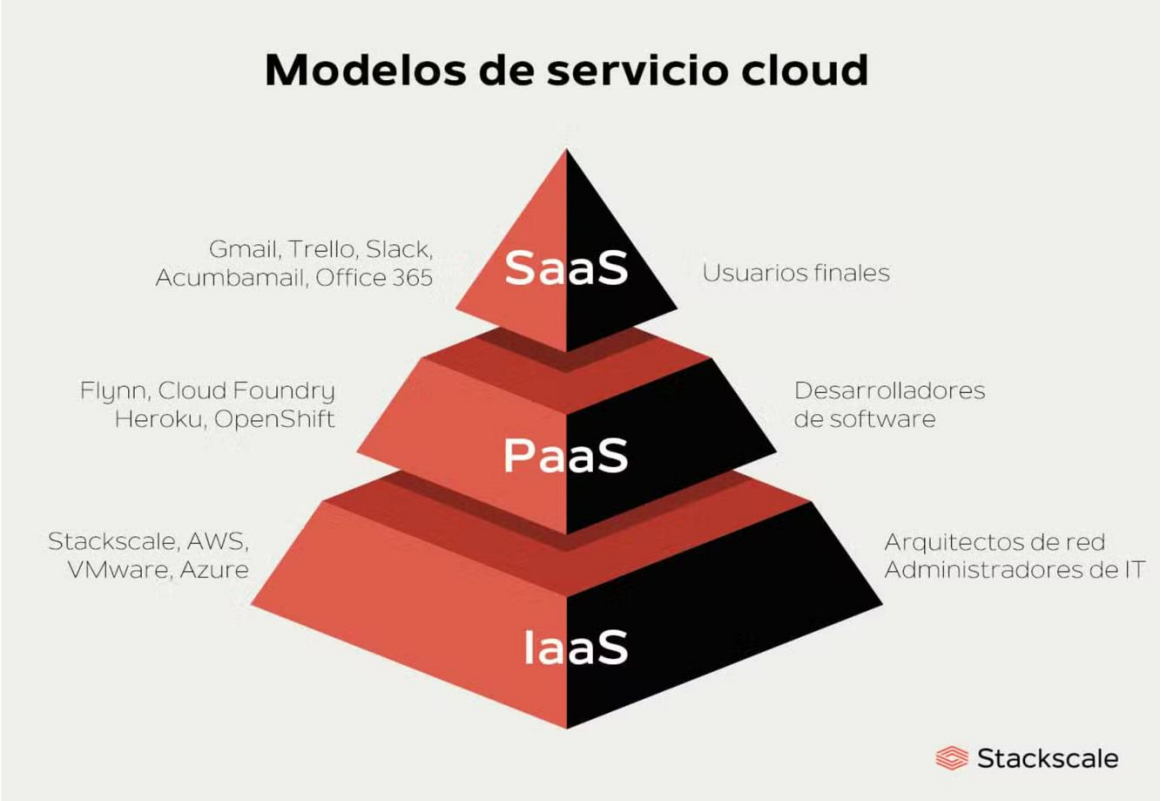


Ilustración2: Modelo de Servicio Cloud (Stackscale, 2023)

2.2. Principales beneficios y desafíos de la nube

La computación en la nube posee varios beneficios lo que ha llevado a diferentes organizaciones adoptarla, pero a la vez que tiene beneficios también abarca una serie de desafíos que deben ser afrontados para maximizar el uso de la computación en la nube. Según compañías como AWS, IBM, Google iCloud los beneficios que aporta la computación de la nube son: Estabilidad y flexibilidad, Costos Reducidos, Acceso global, Recuperación de datos y Actualizaciones automáticas.

- Escalabilidad y elasticidad: La computación en la nube le brinda a su empresa una mayor flexibilidad. Puedes escalar con rapidez los recursos y el almacenamiento para satisfacer las demandas empresariales sin tener que invertir en una

infraestructura física. Las empresas no necesitan pagar por la infraestructura que necesitan para mantener sus niveles de carga más altos. Asimismo, pueden reducir la escala rápidamente si no se usan los recursos, (Google Cloud, 2024)

- Costos Reducidos: Sin importar el modelo de servicio en la nube que elijas, solo pagas por los recursos que realmente usas. Esto te permite evitar la compilación y el aprovisionamiento en exceso de tu centro de datos, y permite que tus equipos de TI dediquen tiempo valioso a enfocarse en trabajos más estratégicos, (Google Cloud, 2024).
- Acceso Global: El almacenamiento en la nube permite que puedas acceder a los datos estén desde cualquier lugar y en cualquier momento. En lugar de estar vinculados a una ubicación o a un dispositivo específico, las personas pueden acceder a los datos desde cualquier lugar del mundo y con cualquier dispositivo, siempre y cuando tengan conexión a Internet, (Google Cloud, 2024)
- Recuperación de datos: Los proveedores de servicios en la nube ofrecen funciones de copia de seguridad y recuperación ante desastres. El almacenamiento de datos en la nube, en lugar de hacerlo a nivel local, puede ayudar a evitar la pérdida de datos en caso de una emergencia, como una falla de hardware, amenazas maliciosas o incluso un error simple que haya cometido el usuario, (Google Cloud, 2024).
- Actualizaciones automáticas: Con la tecnología basada en la nube evitas la preocupación de tener que hacer manualmente las actualizaciones de software, ya que son y utilizan lo que hay de más moderno en el mercado en términos de tecnología y mejores prácticas, (SYDLE, 2022).

También existen varios desafíos para la computación en la nube como: Seguridad y privacidad, Disponibilidad y Rendimiento, Visibilidad y Control Reducido, Cumplimiento normativo.

- Seguridad y privacidad: La mayor preocupación con la computación en la nube es la seguridad y privacidad de los datos. A medida que las organizaciones adoptan la nube a escala global, los riesgos se han vuelto más graves que nunca, con una gran cantidad de datos comerciales y de consumidores disponibles para que los piratas informáticos los vulneren, (Pathak, 2024).
- Disponibilidad y Rendimiento: Aunque parezca que la computación promete una alta disponibilidad y rendimiento esto no es 100% verdad, la desventaja más común en la conexión a internet. Con la computación en la nube, una mala conexión podría impedirte acceder a la información o aplicaciones que necesitas. Incluso los principales proveedores de servicios en la nube pueden experimentar tiempo de inactividad debido a un desastre natural, o un rendimiento más lento debido a un problema técnico imprevisto que podría afectar la conectividad, (Pathak, 2024).
- Visibilidad y Control Reducido: La computación en la nube ofrece el beneficio de no tener que administrar la infraestructura y los recursos como servidores para mantener los sistemas en funcionamiento. Aunque ahorra tiempo, gastos. los usuarios terminan teniendo un control y una visibilidad reducidos de su software, sistemas, aplicaciones y activos informáticos. Como resultado, a las organizaciones les resulta difícil verificar qué tan eficientes son los sistemas de seguridad debido a la falta de acceso a los datos y a las herramientas de seguridad en la nube, (Pathak, 2024).

- Cumplimiento Normativo: Las normas de cumplimiento son cada vez más estrictas debido al aumento de los ciberataques y los problemas de privacidad de datos. Los organismos reguladores como HIPAA, GDPR que garantizan que las organizaciones cumplan con las normas aplicables, reglas y regulaciones federales para mantener seguridad de datos y privacidad para sus negocios y clientes. Sin embargo, el cumplimiento es otro gran desafío para las organizaciones que adoptan la nube, (Pathak, 2024).

Para resumir lo expuesto la computación en la nube ofrece tanto beneficios como desafíos que se tienen que abordar para mitigarlos, minimizarlos garantizando una migración segura y exitosa.

2.3. Importancia de la seguridad en entornos de nube

Nosotros hablamos de seguridad en la nube a la protección de los entornos de la nube, aplicaciones, datos e información de los servicios de la nube. La migración a la nube como ya se ha mencionado anteriormente tienes sus ventajas y desventajas, por lo cual, las organizaciones tienen que ser conscientes de los peligros y amenazas a la seguridad que pueden surgir.

- La protección de los datos: Uno de los pilares fundamentales de la seguridad en la nube es la protección de datos. Los proveedores de servicios en la nube implementan diversas medidas de seguridad para garantizar la integridad, confidencialidad y disponibilidad de los datos almacenados. Esto incluye el uso de técnicas de cifrado robustas para proteger la información, tanto en reposo como en tránsito, lo que dificulta considerablemente su acceso no autorizado. Asimismo, se establecen mecanismos de autenticación y autorización para asegurar que solo las personas autorizadas tengan acceso a los recursos en la nube, (Access Quality, 2023).

- Confianza del cliente y usuarios: La seguridad en la nube no sólo protege los activos digitales de una organización, sino que también fomenta la confianza de los clientes y usuarios. En un entorno donde la privacidad y la protección de datos son aspectos cruciales, una robusta estrategia de seguridad en la nube puede marcar la diferencia entre ganar nuevos clientes y perderlos frente a la competencia, (Access Quality, 2023).
- Cumplimiento Normativo: Gira en torno a la protección de la privacidad del usuario, tal como lo establecen los órganos legislativos, como GDPR en Europa o HIPAA en Estados Unidos. Los gobiernos asumieron la importancia de proteger la información de los usuarios privados para que no sea explotada con fines de lucro. Así, las organizaciones deben seguir los reglamentos para cumplir con estas políticas, (Kaspersky, 2024)
- Protección contra amenazas: Otro aspecto relevante en la seguridad en la nube es la capacidad de recuperación ante desastres. A pesar de todas las medidas preventivas, los incidentes de seguridad pueden ocurrir. Desde ataques cibernéticos, errores humanos o fallas técnicas. Por esta razón, es esencial contar con estrategias de copia de seguridad y recuperación de datos que permitan restaurar la información en caso de pérdida. Los proveedores del servicio suelen ofrecer soluciones de respaldo y redundancia para garantizar la continuidad del negocio, (Access Quality, 2023).

Se puede asumir, que la importancia de la seguridad en la computación de la nube consiste en la protección de los datos sensibles, cumplimiento de las normas, protección frente a las amenazas

y la confianza cliente-usuario. Una estrategia es el pilar fundamental para garantizar una migración a la nube segura.

3. Capitulo III: Vulnerabilidades y Amenazas en la Nube

Las amenazas y las vulnerabilidades en la nube representan desafíos significativos para la seguridad de los datos. Estas amenazas abarcan un gran número de ataques (cibernéticos), mientras que la vulnerabilidad se relaciona a una debilidad propia del sistema. Por lo tanto, es importante que las organizaciones comprendan que las amenazas y las vulnerabilidades son peligrosas, por lo cual, deben implementar medidas de seguridad sólidas como la implementación de controles de acceso, educación a los empleados sobre buenas prácticas de seguridad y otras estrategias para evitar que vulneren la seguridad. (Check Point , 2024).

3.1. Tipos de amenazas

La investigación sobre las amenazas en la nube nos mostró un resultado, que siendo sinceros es de esperarse, donde existen diversas manera y modos de como transgredir la seguridad en la nube y los más conocidos son:

- Ataques de Phishing
    - Consiste en el engañar a la víctima para que revele información personal, como contraseñas, números de tarjetas de crédito o información de cuentas bancarias. Esto se logra mediante correos electrónicos o mensajes que proceder de fuentes supuestamente confiables, como entidades bancarias, servíos en línea o incluso de un compañero de trabajo.

    - Los ataques de phishing pueden ocasionar la obtención de credenciales y datos sensibles.
    - Verizon Data Breach Investigations Report (DBIR) 2023, Informa que el 36% de las violaciones de datos incluyen phishing.
- Ransomware
    - Es un ataque utilizando software malicioso para bloquear acceso a datos o sistemas de la víctima, exigiendo un pago para restaurar el sistema o acceso.
    - Según informe de Sophos, el 37% de organizaciones globales han sido o son víctimas de ataques ransomware.
- Ataques de DDoS (Denegación de Servicio)
    - Es un ataque cibernético enfocado en sobrecargar el sitio web o servicio para que se vuelva lento o deje de funcionar, debido a la enorme cantidad de tráfico en el sitio web.
    - Nestcout señala un aumento en un 20% en los ataques DDoS dirigidos a servicio en la nube. (NETSCOUT, 2023)
- Malware en la Nube
    - El malware puede infiltrarse en sistemas en la nube a través de archivos infectados o vulnerabilidades en el software.
    - MCAfee informo que un 48% de las organizaciones han detectado malware en sus entornos.
- Creds

- El Credential Stuffing es un ataque automatizado usando bots para acceder a un sitio web con credenciales compradas en la Dark web.

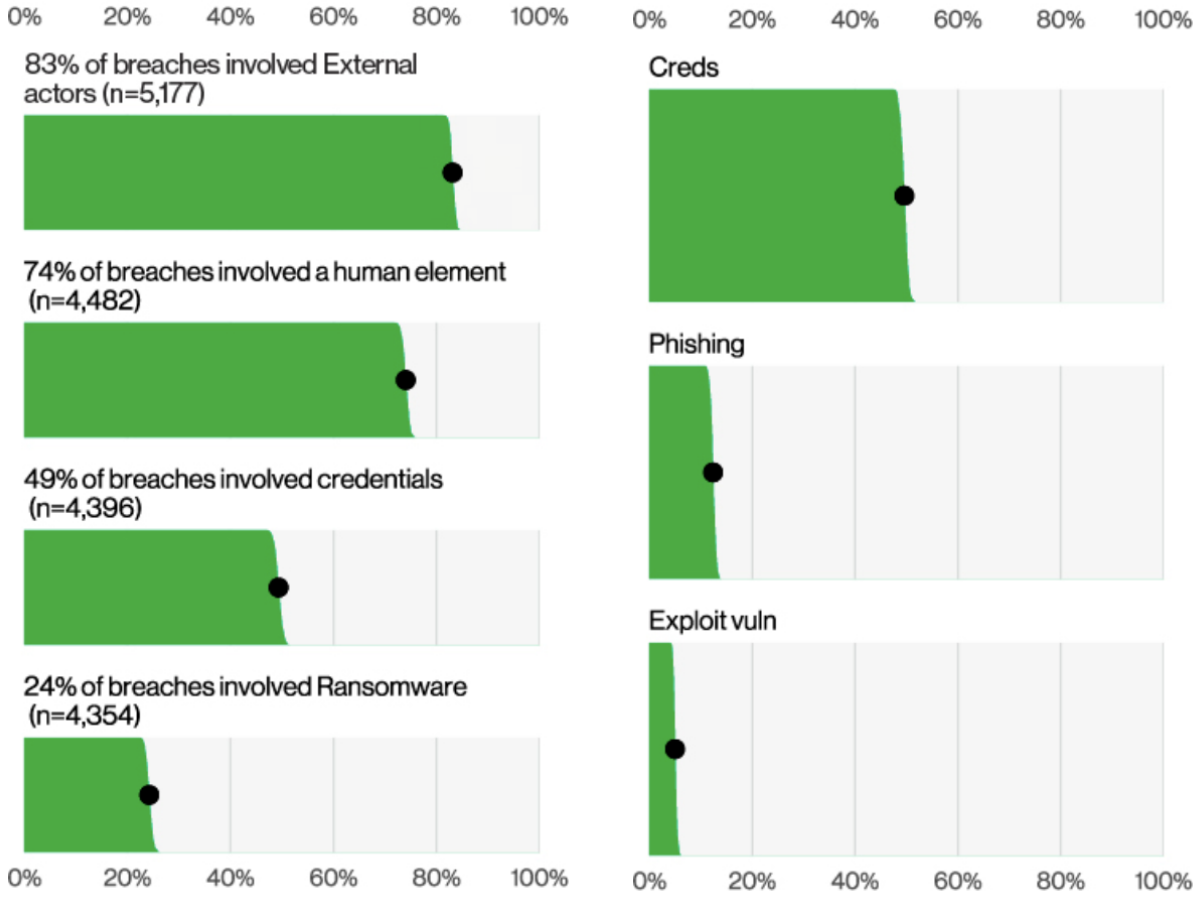


Ilustración 5: Brechas de seguridad y 3 principales formas de ataques. (Verizon, 2023)

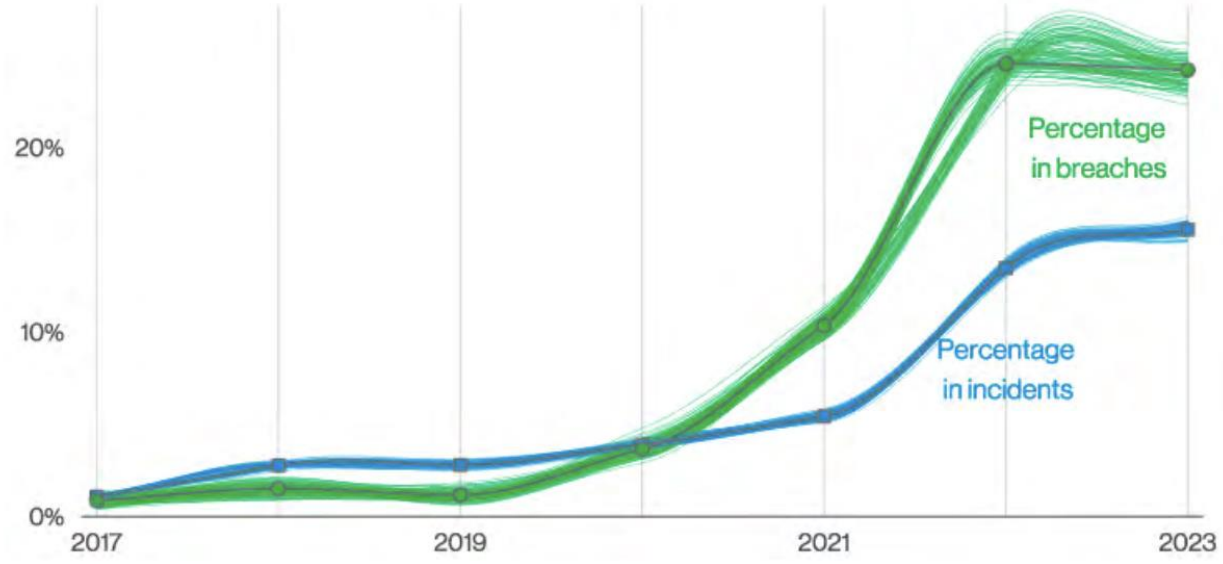


Ilustración 6: Ransomware uno de los principales ataques. (Verizon, 2023)

Las Amenazas de seguridad pueden proceder de manera externa, interna, múltiples y socios. Las amenazas externas provienen de fuentes fuera de las organizaciones, por ejemplos grupos criminales, empleados antiguos, hackers. Las amenazas internas se producen dentro de la organización, incluyendo a empleados, empleados temporales, pasantes y trabajadores de otras áreas. Las amenazas de socios son terceros con una relación comercial con la organización, como vendedores, proveedores de servicios, etc. Donde existe cierto nivel de confianza y privilegios entre socios comerciales. Este ataque se centra en utilizar a este socio para puente de ataque.

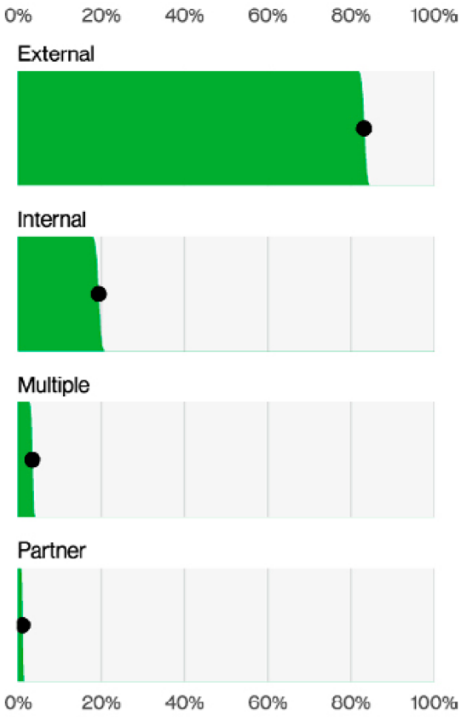


Ilustración 7: Actores en las amenazas de seguridad. (Verizon, 2023)

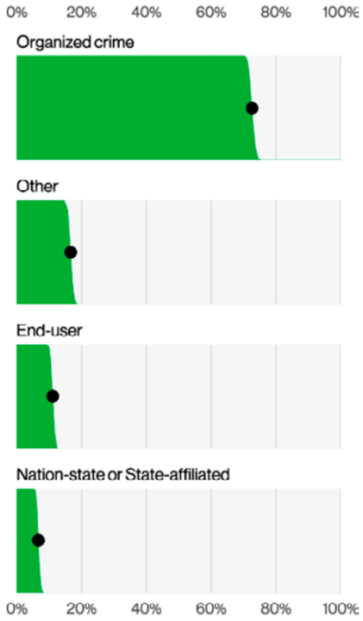


Ilustración 8: Atacantes. (Verizon, 2023)

Region	Frequency	Top patterns	Threat actors	Actor motives
APAC	699 incidents, 164 with confirmed data disclosure	Social Engineering, System Intrusion and Basic Web Application Attacks represent 93% of breaches	External (92%), Internal (9%), Partner (2%), Multiple (2%) (breaches)	Financial (61%), Espionage (39%), Convenience (2%), Grudge (2%), Secondary (1%) (breaches)
EMEA	2,557 incidents, 637 with confirmed data disclosure	System Intrusion, Social Engineering and Basic Web Application Attacks represent 97% of breaches	External (98%), Internal (2%), Multiple (1%) (breaches)	Financial (91%), Espionage (8%), Ideology (1%), Fun (1%) (breaches)
LAC	535 incidents, 65 with confirmed data disclosure	System Intrusion, Social Engineering and Basic Web Application Attacks represent 94% of breaches	External (95%), Internal (5%), Partner (2%), Multiple (2%) (breaches)	Financial (93%), Espionage (11%), Ideology (2%) (breaches)
NA	9,036 incidents, 1,924 with confirmed data disclosure	System Intrusion, Basic Web Application Attacks and Social Engineering represent 85% of breaches	External (94%), Internal (12%), Multiple (9%), Partner (2%) (breaches)	Financial (99%), Espionage (1%), Grudge (1%) (breaches)

Ilustración 9: Incidentes a nivel global. (Verizon, 2023)

3.2. Vulnerabilidades en la nube

Las vulnerabilidades en la nube pueden aparecer por distintos factores como:

- Configuraciones incorrectas
    - La configuración incorrecta de los servicios en la nube puede llevar a la exposición no intencionada de datos y sistemas.
    - Según un informe de Gartner, para el 2025, el 99% de las fallas de seguridad en la nube serán aplicados a errores del cliente. (Gartner, 2019)
- Vulnerabilidades en la API
    - Interfaces de Programación de Aplicaciones o más conocido como API; las API mal protegidas pueden ser explotadas para obtener acceso no autorizado a servicios y datos.
    - La CSA (Cloud Security Alliance) identifico las vulnerabilidades de las API como una de las principales amenazas. (González, 2022)
- Acceso no autorizado

- El acceso no autorizado puede ocurrir debido a insuficientes controles de acceso o a credenciales comprometidas.
- IBM Security informo que encontró que un 19% de las violaciones de datos en la nube se debieron a credenciales comprometidas. (IBM, 2024)

- Inadecuada protección de datos.
  - La inadecuada protección de datos puede ocasionar la perdida de datos que suelen ocurrir por errores humanos, ataques maliciosos o fallos técnicos.
  - Según el estudio de Veeam menciona que el 36% de las organizaciones han experimentado perdida de datos en la nube. (veeam, 2022)

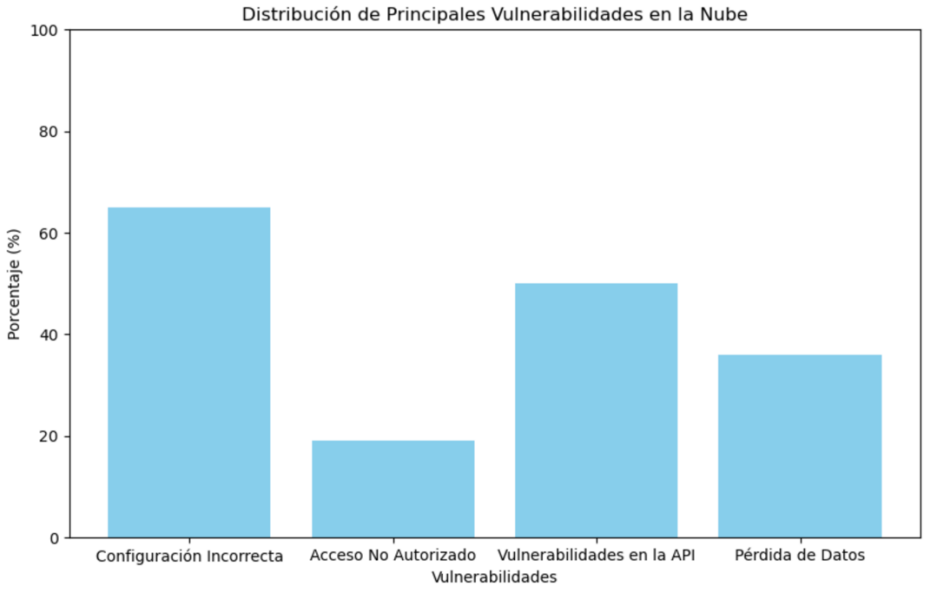


Ilustración 10: Distribución de principales vulnerabilidades en la nube

3.3. Comparación con Sistemas Tradicionales

- Seguridad Física vs. Virtual
  - La seguridad tradicional o física, se trata de tener una gran seguridad física, debido a que los datos se almacenas en servidores locales.

    - La seguridad en la nube se centra en la protección virtual y la implementación de políticas de acceso y cifrado para el protección y privacidad de los datos.
- Escalabilidad
    - Tradicional: La escalabilidad puede ser limitada por el hardware.
    - Nube: Es una de las mayores ventajas, permitiendo a las organizaciones aumentar o disminuir recursos según les convenga.
- Costos
    - Tradicional: El costo corresponde a la infraestructura física, Personal de TI y actualizaciones de hardware.
    - Nube: Los costos pueden variar dependiendo de los modelos de pago, además invertir en configuraciones adecuadas y soluciones de seguridad.

La seguridad en la nube siempre va a presentar desafíos que requieren un enfoque proactivo e integral. Las organizaciones deben implementar medidas robustas y mantenerse informado sobre las tendencias emergentes en seguridad cibernética.

En última instancia, es esencial poseer diferentes estrategias y respuestas para prevenir los incidentes de seguridad para la protección de los datos. (Kolesnikov, 2024)

- Estas estrategias pueden ser:
- Implementar Autenticación Multifactorial (MFA)
- Revisar configuraciones Regularmente
- Utilizar Cifrado de Datos en Transito y en Reposo
- Capacitar a los Empleados en Ciberseguridad

4. Capitulo IV: Protocolos de seguridad en la nube

Los protocolos de seguridad en la nube son conjuntos de reglas y estándares diseñados para proteger la seguridad y privacidad de los datos. Estableciendo medidas y procedimientos que ayudan a detectar y responder de manera correcta a amenazas y vulnerabilidades.

La importancia de los protocolos de seguridad en la nube se compone de diferentes puntos como:

- Protección de datos sensibles
    - Es garantizar que los datos personales estén encriptados y solo sean accesibles para usuarios autorizados. Asegurando que los datos no sean alterados o manipulados durante la transmisión o almacenamiento de los datos.
- Prevención de Accesos no autorizados
    - Mediante la autenticación y autorización según los protocolos como OAuth y SAML que aportan a verificar la identidad de los usuarios y determinar permisos de acceso, evitando accesos no autorizados.
- Mitigación de Amenazas Cibernéticas
    - Protección frente ataques proporcionando medidas defensivas contras ataques cibernéticos comunes, los anteriormente estudiados.
- Cumplimiento Normativo
    - Regulaciones y Estándares que ayudan a las organizaciones a cumplir con diversas regulaciones y estándares industriales que requieren estrictas medidas de seguridad para la protección de datos.
- Confianza

- Es mantener la confianza del cliente mediante la implementación de protocolos de seguridad robustos.

La seguridad en la nube abarca un gran número de protocolos que se utilizan para proteger datos en tránsito, en reposo. A continuación, enumerare los protocolos más comunes utilizados en la nube:

- SSL/TLS
- Ipsec
- OAuth
- SAML
- Kerberos
- LDAP
- VPN
- HTTPS
- MFA

Todos los protocolos mencionados y los no mencionados trabajan en conjunto para desarrollar un entorno seguro y confiable, protegiendo los datos y servicios frente a amenazas cibernéticas.

4.1 SSL/TLS: El protocolo SSL/TLS es un estándar de seguridad utilizada para establecer conexiones cifradas entre un cliente y un servidor en internet. Garantizando la confidencialidad y la integridad de la información transmitida (WhatsApp). En la actualidad podemos decir que el protocolo SSL fue reemplazado por TLS, que es su versión más segura y actualizada. (redalia, 2024)

Resumen de las diferencias: SSL en comparación con TLS

	SSL	TLS
Qué significa	*SSL* son las siglas de Secure Sockets Layer (capa de sockets seguros).	*TLS* son las siglas de Transport Layer Security (seguridad de la capa de transporte).
Historial de versiones	TLS sustituyó SSL. SSL pasó por las versiones 1.0, 2.0 y 3.0.	TLS es la versión mejorada de SSL. TLS ha pasado por las versiones 1.0, 1.1, 1.2 y 1.3.
Actividad	Todas las versiones de SSL están obsoletas.	Las versiones 1.2 y 1.3 de TLS se utilizan activamente.
Mensajes de alerta	SSL solo tiene dos tipos de mensajes de alerta. Los mensajes de alerta no están cifrados.	Los mensajes de alerta de TLS están cifrados y son más diversos.
Autentificación de mensajes	SSL usa MAC.	TLS usa HMAC.
Conjuntos de cifrado	SSL admite algoritmos más antiguos con vulnerabilidades de seguridad conocidas.	TLS utiliza algoritmos de cifrado avanzados.
Protocolo de enlace	Un protocolo de enlace SSL es complejo y lento.	Un protocolo de enlace TLS tiene menos pasos y una conexión más rápida.

Ilustración 11: SSL/TLS. (AWS, 2024)

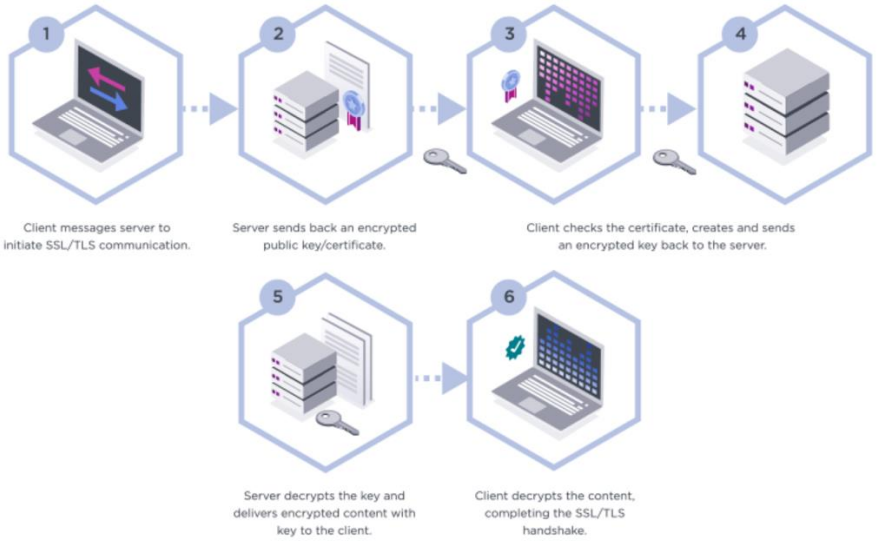


Ilustración 12: Funcionamiento SSL. (ENTRUST, 2024)

4.2 OAuth: Conocido como Open Authorization es un protocolo de autorización que permite a las aplicaciones obtengan acceso a los usuarios sin necesidad de compartir credenciales de inicio de sesión del usuario. EL flujo con el que trabaja este protocolo se divide en 5 pasos:

- Solicitud de autorización: La aplicación solicita permiso al usuario para acceder a sus recursos en el proveedor de servicios.
- Concesión de autorización: El usuario acepta o niega la solicitud de autorización.
- Generación de código de autorización: Al tener permiso del usuario el proveedor genera un código de autorización.
- Intercambio de código de autorización por token de acceso: la aplicación utiliza el código de autorización para solicitar un token de acceso.
- Acceso: Con el token de acceso valido, puede acceder a todos los recursos.

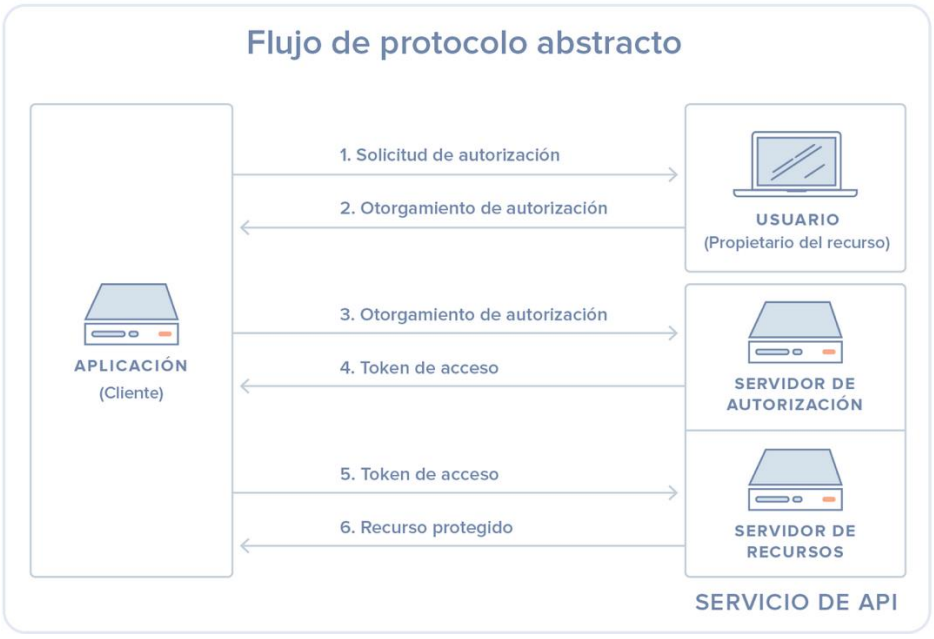


Ilustración 13: Flujo de protocolo. (Mitchell Anicas, 2018)

El protocolo OAuth permite que las aplicaciones accedan a los datos del usuario de forma segura sin comprometer la seguridad de sus cuentas. Esta es una forma segura de delegar acceso sin mostrar las credenciales del usuario al iniciar sesión. (IBM, 2024)

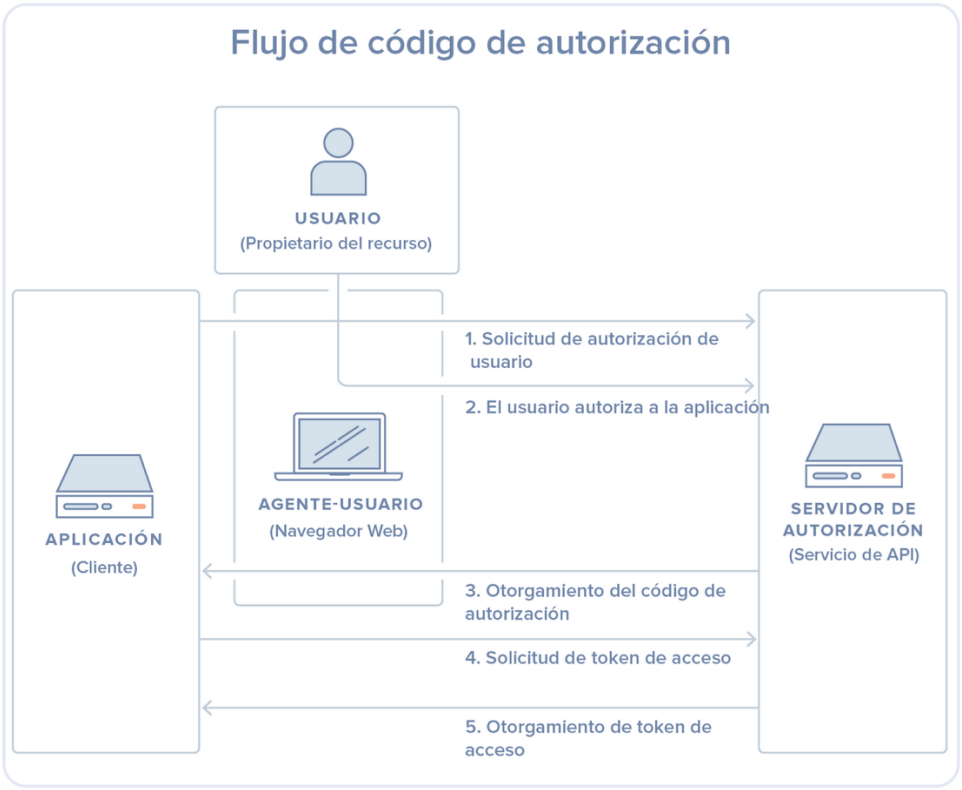


Ilustración 14: Flujo de código de autorización. (Mitchell Anicas, 2018)

4.3 SAML: Es un estándar de intercambio de datos de autenticación y autorización entre dominios de seguridad. El objetivo de SAML es permitir que los usuarios autenticados accedan a múltiples aplicaciones utilizando un único inicio de sesión. El funcionamiento de SAML contiene 2 cosas:

- IdP (Identity Provider): Es el sistema responsable de autenticar a los usuarios y proporcionar tokens de seguridad basados en el SAML.
- SP (Service Provider): Es el sistema que proporciona servicios a los usuarios para autenticar a los usuarios. Este servicio se encarga de consumir los tokens creados por IdP para permitir el acceso de los usuarios.

El flujo de este protocolo es similar al protocolo de OAuth, pero con la diferencia que solo con un usuario se podrá acceder a diferentes servicios. SAML es utilizados en entornos empresariales para proporcionar SSO, facilitando la integración segura de sistemas y aplicaciones en diferentes

dominios de seguridad. (Universidad de sevilla , 2024)

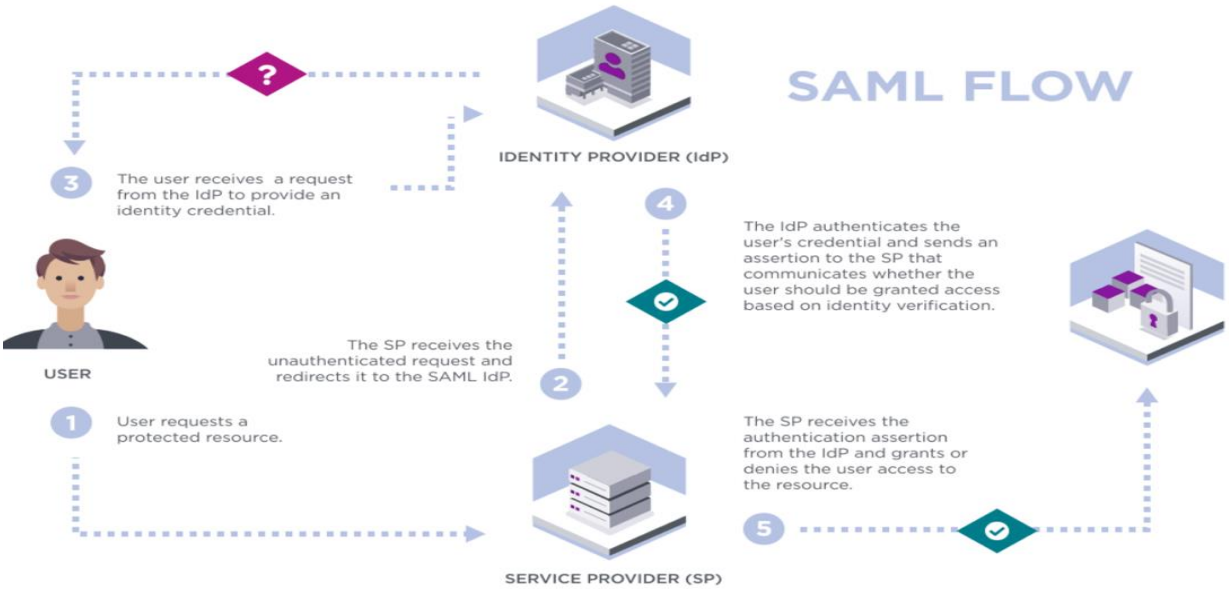


Ilustración 15: SSL/TLS. (ENTRUST, 2024)

4.4 IPsec: Conocido por sus siglas IPsec (Internet Protocol Security) son protocolos que aseguran las comunicaciones a nivel de red IP mediante la autenticación y el cifrado de cada paquete IP en una sesión de comunicación. Se utiliza para la creación de conexiones de red seguras, como las VPNs (Redes Privadas Virtuales), proporcionando seguridad a nivel de red para la transferencia de datos. (AWS, 2024) Operando en dos modos:

- Modo transporte: cifra el contenido en paquete de datos
- Modo Túnel: El paquete IP es cifrado y se encapsula en un nuevo paquete IP.

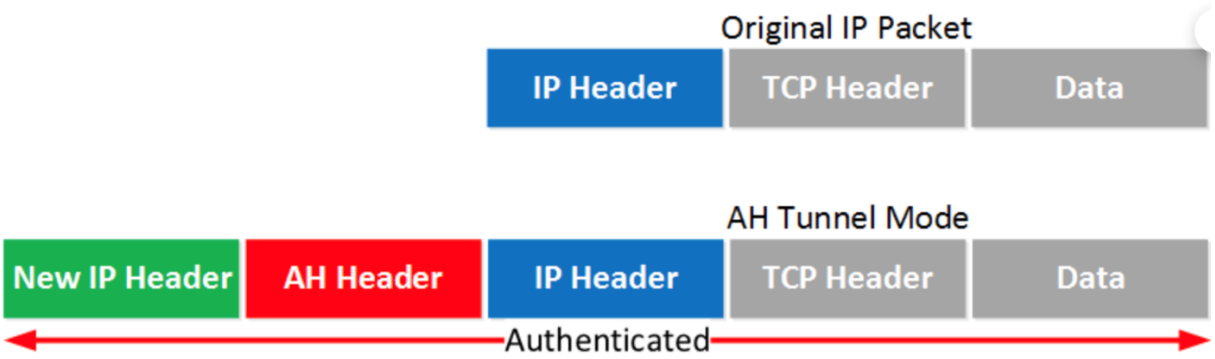


Ilustración 16: Modo Túnel. (Networking Lessons, 2024)

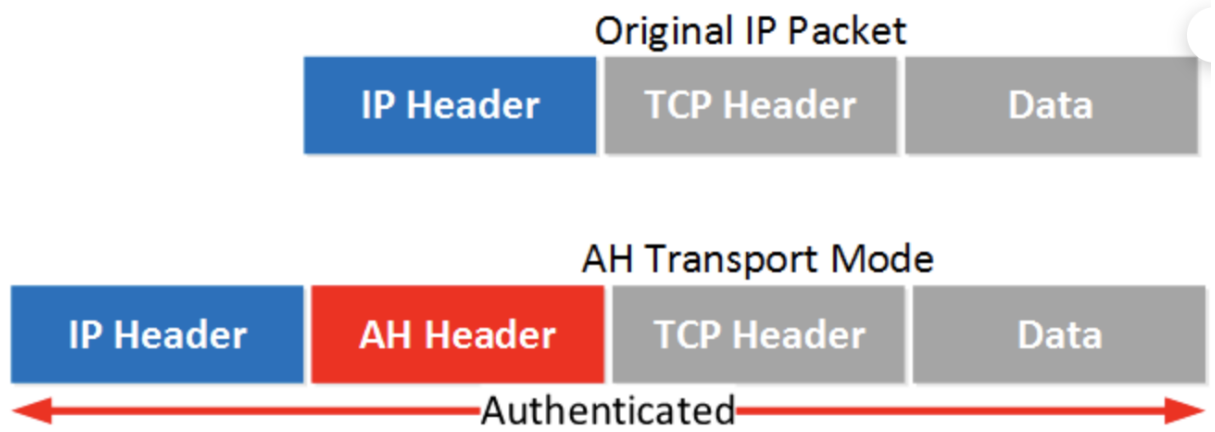


Ilustración 17: Modo Transporte. (Networking Lessons, 2024)

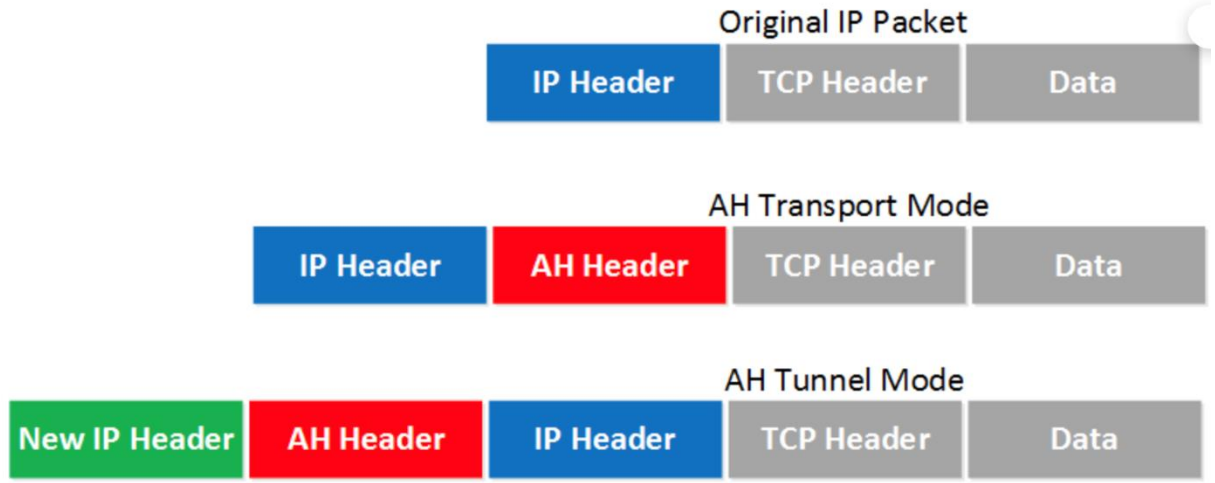


Ilustración 17: IP original, Modo transporte y Modo Túnel. (Networking Lessons, 2024)

4.5 Kerberos: Es un protocolo de autenticación de red que utiliza tickets para que los nodos se puedan comunicar de manera segura por una red insegura. Estos protocolos están presentes en redes corporativas y educativas para autenticar a los usuarios en servicios de red. (Microsoft , 2023)

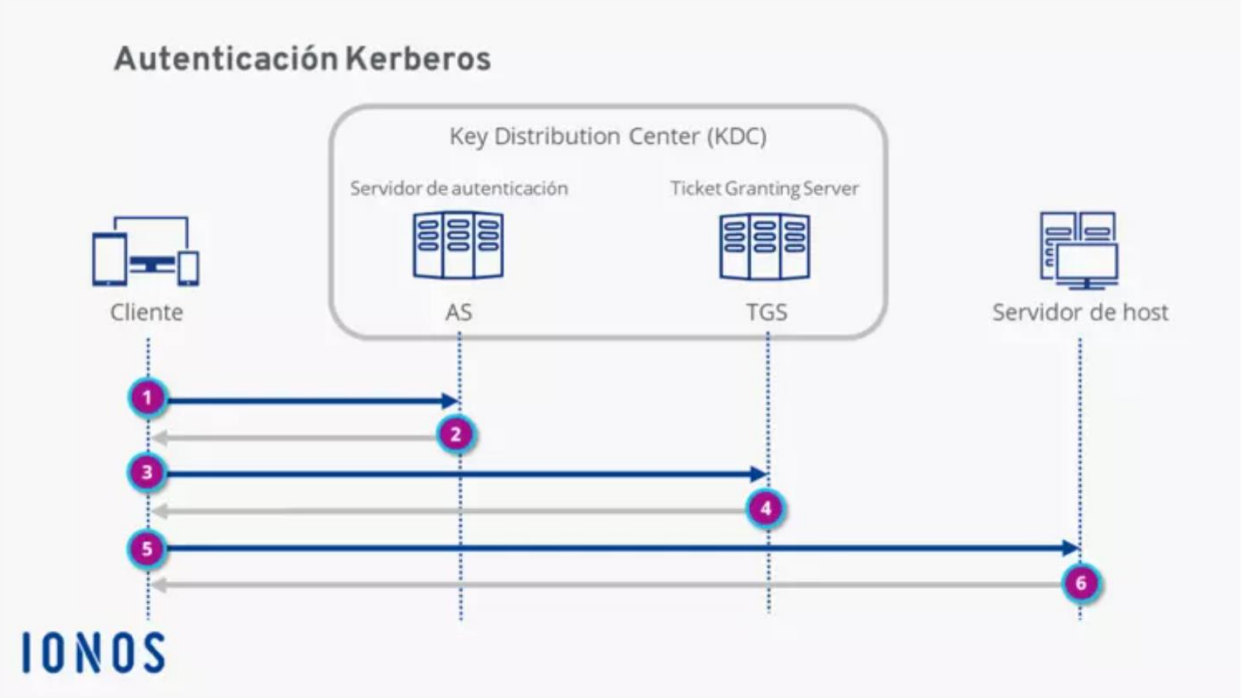


Ilustración 18: Proceso de autenticación. (IONOS, 2021)

4.6 LDAP: Conocido como Lightweight Directory Access Protocol un protocolo para acceder y mantener servicios de directorio distribuidos. Este protocolo permite administrar información sobre usuarios, grupos y recursos en una red, utilizada generalmente para identificar a los usuarios en sistemas operativos y aplicaciones. Funcionan al conectarse a un servidor LDAP y enviar solicitudes para buscar, agregar, modifica o eliminar entradas en el directorio. (onelogin, 2024)

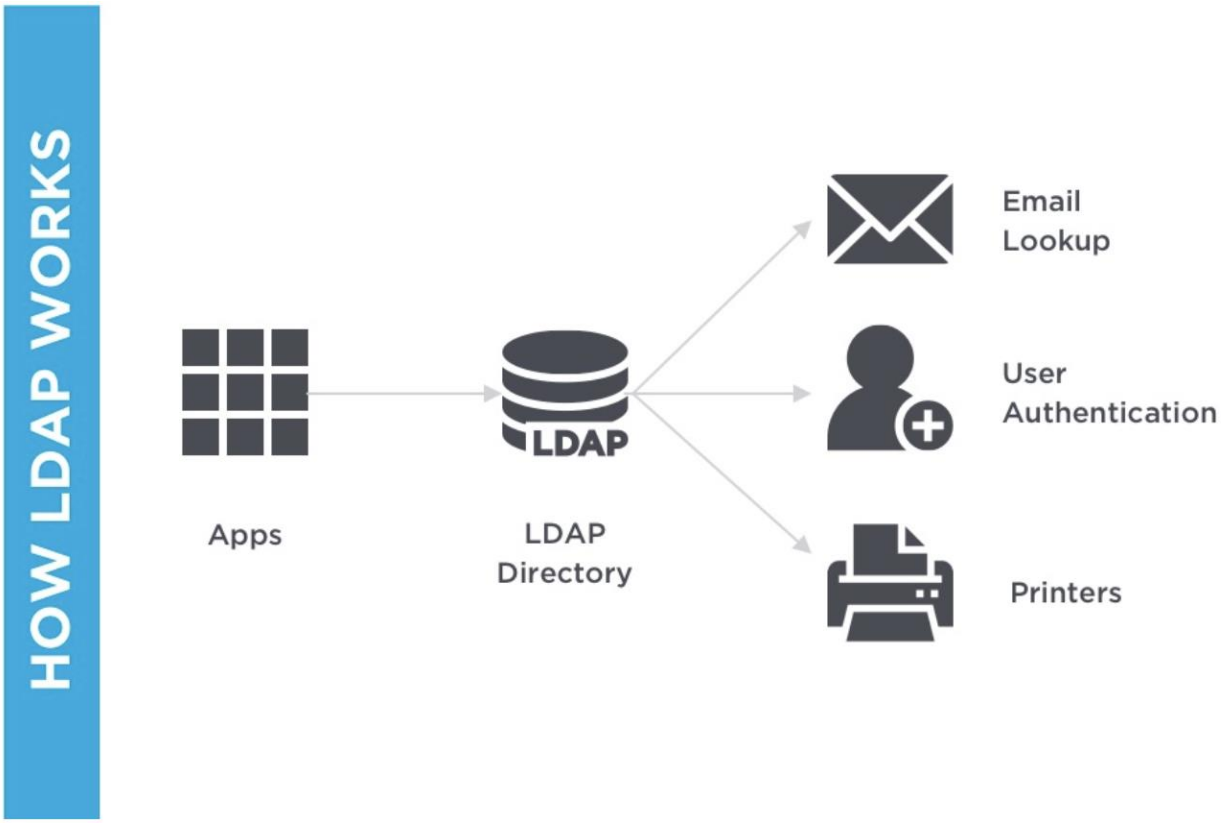


Ilustración 18: Como trabaja. (onelogin, 2024)

4.7 VPN: Una VPN es la extensión de una red privada a través de una red pública, permitiendo a los usuarios enviar y recibir datos como si estuvieran conectados directamente a la red privada. Se utiliza para permitir el acceso remoto seguro a redes corporativas, también se usa para mejorar la privacidad y seguridad al navegar por internet. (AWS, 2024)

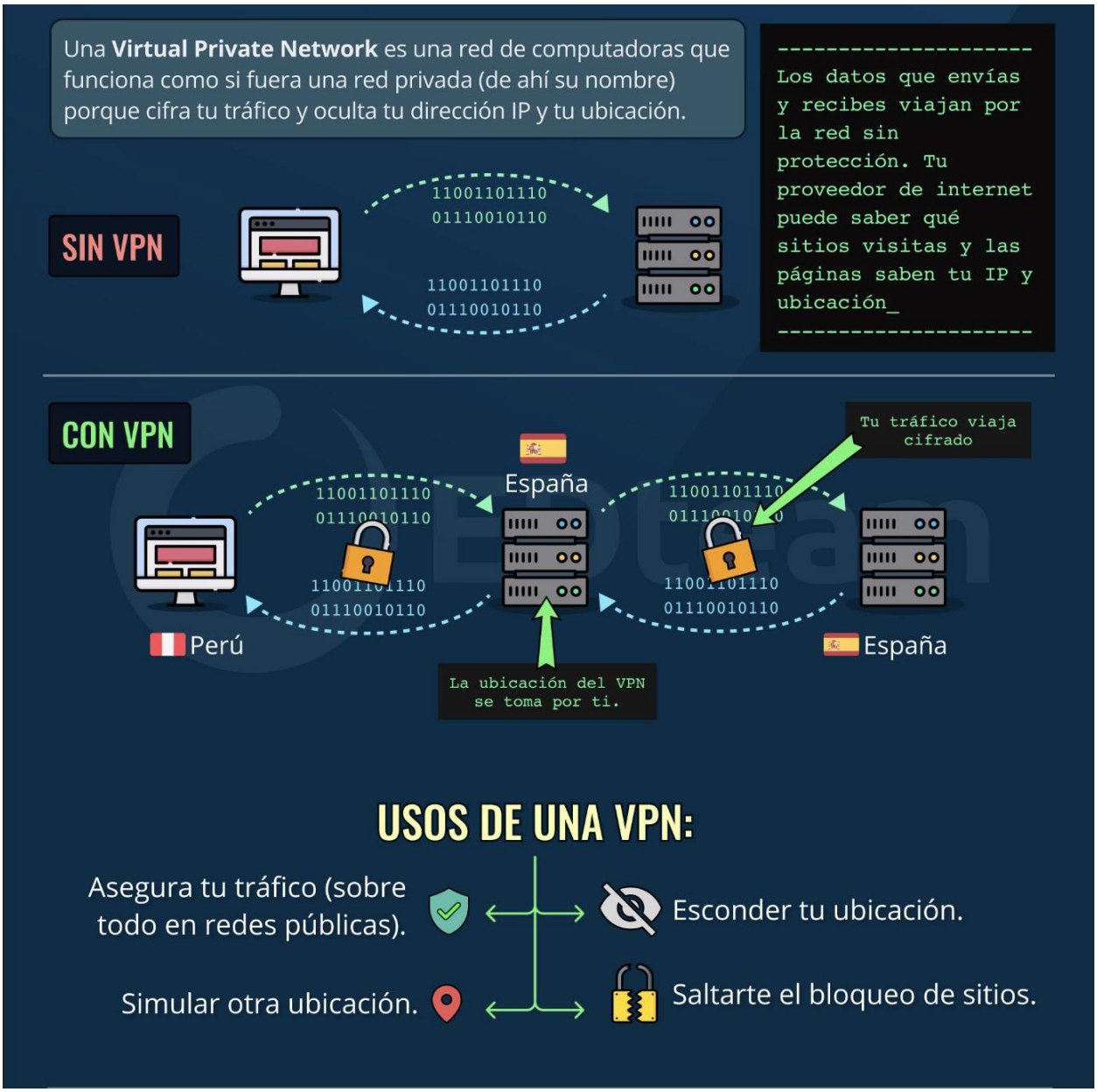


Ilustración 19: VPN. (EDteam, 2021)

4.8 HTTPS: es una versión segura de HTTP que utiliza SSL/TLS para cifrar la comunicación entre un navegador web y un servidor. Se utiliza para proteger la

transmisión de datos sensibles en sitios web. (cloudflare, 2024)

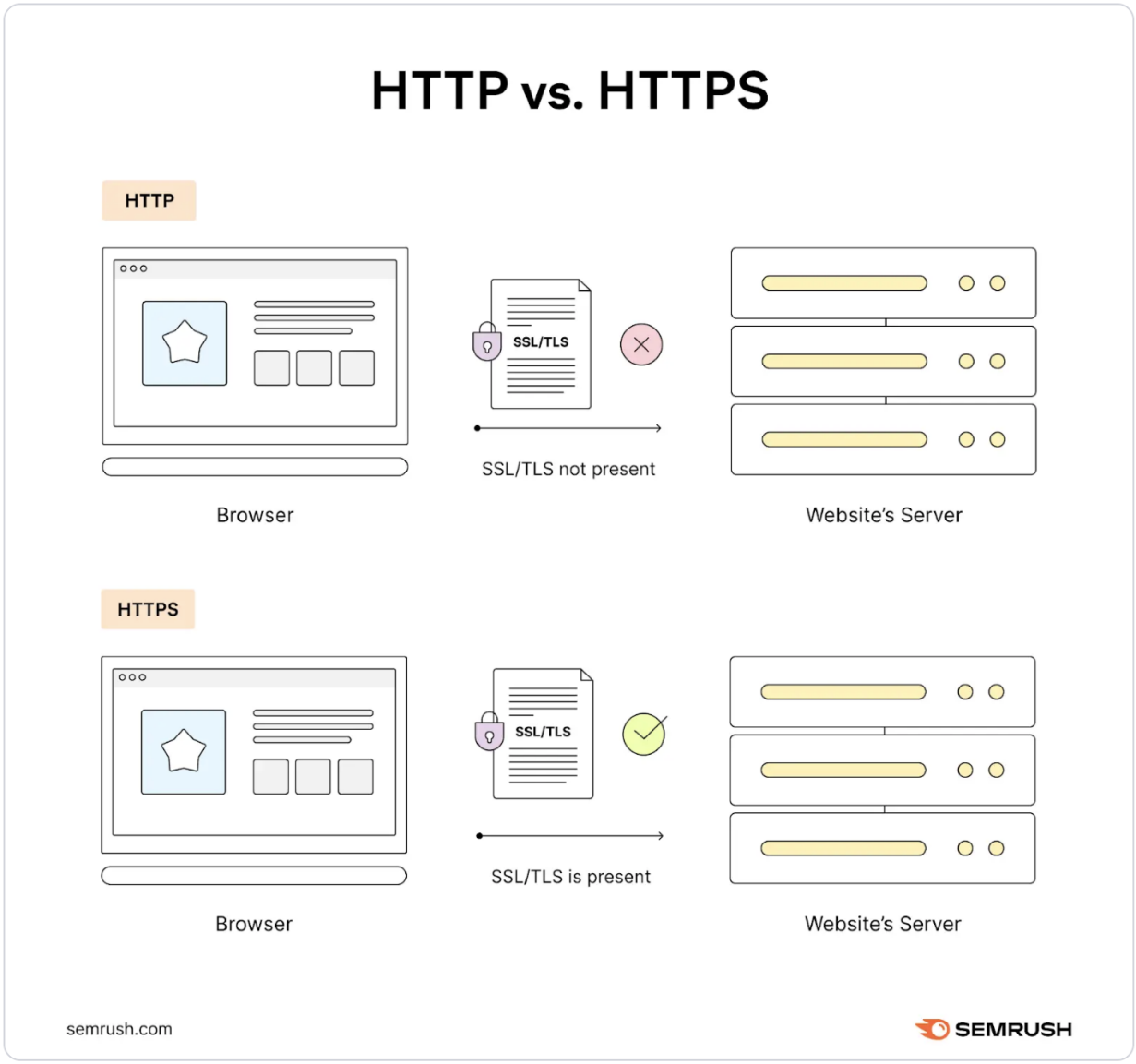


Ilustración 20: HTTP vs HTTPS con SSL/TLS. (Semrush Blog, 2024)

4.9 MFA: Es un método de autenticación que requiere más de una forma de verificación para acceder a un sistema o aplicación. Aumenta la seguridad en la autenticación de usuarios en sistemas sensibles y aplicaciones. (onelogin, 2024)



Ilustración 20: Funcionamiento MFA. (akamai, 2024)

Tabla 1

Ventajas y desventajas sobre los protocolos de seguridad en la nube.

Protocolo	**Descripción**	**Ventajas**	**Desventajas**	**Estadísticas**
SSL/TLS	Protocolo de encriptación de datos en tránsito.	Encriptación, autenticación, integridad.	Configuración compleja, susceptible a ciertos ataques.	95% de los sitios web usan TLS.
IPsec	Seguridad a nivel de red IP mediante autenticación y cifrado.	Seguridad de red, autenticación, cifrado.	Complejo de configurar, puede afectar el rendimiento.	Mercado crecerá 14% anualmente.
OAuth	Protocolo para compartir recursos entre sitios sin	Mejora la seguridad, facilita integración.	Complejidad de implementación, posibles problemas de configuración.	Uso creció 30% anualmente.

	compartir credenciales.			
SAML	Estándar para intercambio de autenticación y autorización entre dominios.	SSO, mejora experiencia del usuario.	Complejo de implementar, requiere infraestructura adicional.	Usado por 70% de las empresas.
Kerberos	Protocolo de autenticación de red basado en tickets.	Seguridad robusta, previene ataques de reproducción.	Complejo de configurar, dependencia de servidor de tiempo.	85% de adopción en entornos empresariales
LDAP	Protocolo para acceso y mantenimiento de servicios de directorio.	Escalable, eficiente en manejo de datos.	Complejo de implementar, requiere mantenimiento.	Usado por 80% de las organizaciones
VPN	Extiende una red privada sobre una red pública.	Mejora privacidad, acceso remoto seguro.	Puede reducir velocidad, servicios pueden bloquear VPN.	27% de usuarios de Internet usan VPN.
HTTPS	Extensión de HTTP con encriptación SSL/TLS.	Encriptación de datos, mejora confianza.	Requiere administración de	80% de sitios web usan HTTPS.

			certificados, puede aumentar latencia.	
MFA	Método de autenticación con más de una verificación.	Mejora seguridad, reduce riesgo de acceso no autorizado.	Inconveniente para usuarios, requiere gestión adicional.	Bloquea 99.9% de ataques automatizados

Nota: (onelogin, 2024) (cloudflare, 2024) (AWS, 2024) (onelogin, 2024) (Microsoft , 2023) (AWS, 2024) (IBM, 2024) (redalia, 2024)

Para implementar protocolos de seguridad en la nube de una manera efectiva requiere de buenas prácticas, políticas bien definidas. El proceso para implementar de manera correcta protocolos de seguridad en la nube seria realizar:

- Una evaluación y planificación de la seguridad
- Tener control de acceso y autenticación
- Una encriptación de datos
- Monitoreo
- DevOPs
- Cumplimiento Normativo y Políticas
- Recuperación frente desastres
- Seguridad de la red
- Actualizaciones y mantenimiento

Adoptando estas buenas prácticas ayudan a fortalecer la seguridad en la nube, disminuyendo el riesgo de ataques cibernéticos y garantizando la protección de datos. Es necesario un enfoque proactivo y continuo, adaptándonos a las nuevas amenazas y tecnologías emergentes.

4.10 Brechas de seguridad en la Nube

Las brechas de seguridad en la nube son una preocupación que van en aumento por el incremento de organizaciones que deciden migrar a un servicio en la nube. Donde los datos son expuestos, robados o accedidos debido a brechas en la infraestructura, aplicaciones o servicios en la nube. Las causas más comunes de brechas de seguridad se deben a:

- Configuraciones Incorrectas
    - Son errores en la configuración de recursos en la nube, servidores, bases de datos y servicios de almacenamiento, donde se pueden dejar datos expuestos.
- Accesos no autorizados
    - Usuarios no autorizados pueden acceder a datos sensibles debido a credenciales comprometidos o controles de acceso insuficientes.
- Inseguridad en APIs
    - Apis inseguras que son atacadas para poder acceder a datos sensible a través de ellas.
- Insider threats
    - Empleados malintencionados o negligentes pueden comprometer la seguridad al acceder o exponer datos sensibles.
- Malware y Ransomware

    - Softwares maliciosos que infecta sistemas, comprometiendo, bloqueando acceso a datos importantes.
- Phishing
    - Ataques de ingeniería social para engañar a los usuarios para que revelen información.

Tipos de Brechas:

- Data Breach (Filtración de Datos)
    - No es más que el acceso no autorizado a datos sensibles, como información personal, financiero.
- Account Hijacking (Secuestro de Cuentas)
    - Es obtener la cuenta de un usuario para acceder a su información y recursos.
- Denial of services (Denegación de servicios)
    - Son ataques que saturan los recursos de un sistema para impedir el acceso a usuarios legítimos.

Para tener un mayor entendimiento se presentará algunas estadísticas

- Frecuencia de Brechas de Seguridad
    - 45% de las brechas ocurren en entornos de la nube (PingSafe, 2023).
    - 82% de las organizaciones han experimentado al menos una brecha de seguridad en la nube (PingSafe, 2023).
    - 83% de las empresas reportaron haber sufrido una brecha de seguridad en la nube (PingSafe, 2023).
- Causas de las Brechas

- 82% de las brechas de seguridad en la nube se atribuyen a errores humanos, además de una incorrecta configuración de recursos en la nube (PingSafe, 2023).
- Las configuraciones incorrectas poseen el 23% de los incidentes de seguridad en la nube (PingSafe, 2023).

Ejemplos de ataques (Navarro, 2024):

- Dropbox, LinkedIn y Twitter (2024)
  - Investigadores de seguridad descubrieron una base de datos de 26 mil millones de registros de datos filtrados, incluyendo nombres de usuario y contraseñas.
- Bank of America (febrero 2024)
  - Un fallo de seguridad en Infosys McCamish, un proveedor de software financiero, llevo a la exposición de datos personales y de cuentas de 57,028 clientes de back of America.
- Microsoft
  - Violación de datos en su plataforma Azure, que comprometió a cuentas de ejecutivos de alto nivel, incluida tomas de control de cuentas y tentativas de phishing.
- Volkswagen
  - Víctima de un ataque cibernético que resulto en el robo de 19,000 documentos del servidor de la compañía.
- Tesla

    - Dos ex empleados de Tesla fueron responsables de filtrar los datos personales de 74,745 empleados y exempleados a un periódico alemán.

Las brechas de seguridad representan una gran amenaza a las organizaciones de todos los tamaños. Resultando en pérdidas financieras, danos a la reputación de las organizaciones, pérdida de confianza del cliente. Por lo tanto, es recomendable una estrategia de seguridad robusta y bien planificada para proteger los datos y mantener la confianza del cliente y socios.

- Configuración Segura
    - Utilizar herramientas automatizadas para detectar y corregir configuraciones incorrectas
    - Asegurarse que las configuraciones en la nube o servicio sean revisadas y validadas regularmente.
- Control de Acceso
    - Implementar la autenticación multifacto para toda la organización.
    - Control de permisos y accesos a los datos o recursos.
- Cifrar datos
    - Cifrar los datos en tránsito como en reposo para la protección de información sensible.
- Monitoreo
    - Sistema de monitorio continuo para detectar actividades sospechosas ante incidentes de seguridad
- Capacitar al personal
    - Proporcionar capacitaciones en seguridad de la información a los empleados.
    - Realizar simulacros de seguridad para evaluar la preparación de los empleados.

- Proteger APIs
    - Asegurarse que las APIs sean seguras e identificar vulnerabilidades.
- Establecer un Plan de respuesta ante incidentes
    - Desarrollar un plan de respuesta donde incluya el procedimiento para identificar, como proceder y eliminación.
- Normativas y Estándares
    - Cumplir con las normativas y estándares de seguridad.
    - Búsqueda de certificaciones para demostrar el compromiso con la seguridad de la información del cliente.

5. Capitulo V: Herramientas de Seguridad en la Nube

Las herramientas de seguridad en la nube son soluciones de software diseñadas para proteger datos, servicios en la computación en la nube. Estas herramientas asumen diversos aspectos de seguridad, con su pilar en la protección de datos, gestión de identidades y accesos, respuesta frente amenazas, encriptación y cumplimiento normativo.

Las herramientas más comunes en la seguridad de la nube son:

- Firewalls de aplicaciones Web (WAF)
    - Es la protección de aplicaciones web contra ataques de inyección SQL, XSS entre otros.
    - Ejemplo: AWS WAF permite a los usuarios crear reglas que bloquean tráfico web malicioso.
- Gestión de Identidades y Accesos (IAM)

    - Simplemente es un control de quienes tienen acceso a ciertos recursos y con ciertos permisos, asegurando que solo los usuarios autorizados puedan ingresar a los datos sensibles.
    - Ejemplo: AWS IAM permite definir políticas detalladas de permisos y gestionar las identidades de usuarios y roles.
- Herramientas de encriptación
    - Se aseguran de que los datos estén encriptados
    - Ejemplo: Azure Disk Encryption para encriptar discos y volúmenes en máquinas virtuales, protegiendo datos almacenados en Azure.
- Sistemas de detección y respuesta amenazas
    - Monitorea la red y las actividades de los usuarios para detectar y responder frente a comportamientos anómalos y amenazas.
    - Ejemplo: Google Cloud Security Command Center visibilidad en tiempo real de la seguridad de los recursos de Google Cloud, permitiendo detectar y responder a incidentes inmediatamente.
- Plataformas de Gestión de seguridad en la nube
    - Organizaciones que ayudan a evaluar y asegurar la infraestructura en la nube, garantizando el cumplimiento de las mejores prácticas y normas de seguridad.
    - Ejemplo: Prisma Cloud de Palo Alto Networks evalúa continuamente la configuración de seguridad y detecta riesgos en entornos multicloud.
- Herramientas de seguridad de la carga de trabajo en la nube
    - Protegen las cargas de trabajo en la nube, contenedores, máquinas virtuales, vulnerabilidades y amenazas.

6. Conclusiones

Para empezar tras la evaluación de protocolos y herramientas para proteger la privacidad de los datos se ha llegado a la conclusión de que las estadísticas muestran que las amenazas y vulnerabilidades en entornos virtuales han ido incrementando de forma notoria, por ejemplo, un 36% en ataques de phishing, 37% ransomware, 20% DDoS asimismo un 48% en Malware, es por eso que se ha visto afectada la seguridad de los datos de diferentes organizaciones que han optado por migrar a un entorno virtual.

Para minimizar el riesgo de las amenazas y vulnerabilidad, se sabe que existen diferentes protocolos de seguridad como: SSL/TLS, Ipsec, OAuth, SAML, Kerberos, LDAP, VPN, HTTPS, MFA los cuales se deben implementar para autenticación, transmisión de datos, cifrado, proporcionar acceso seguro de forma remota y mejorar la privacidad, lo cual también nos garantiza la confidencialidad e integridad de los datos.

Por otra parte, es preciso tener presente que los errores más comunes a la hora de llevar a cabo medidas de seguridad frente a amenazas en entornos virtuales es la falta de capacitación continua en empleados, ya que los errores humanos son responsables en gran medida de las brechas de seguridad.

Por último, pero no menos importante, se puede concluir que las herramientas de seguridad tales como firewalls, sistemas de detección de intrusiones y herramientas de monitoreo son esenciales para proteger los datos y servicios en la nube, si se los administra de forma adecuada estos pueden proporcionar defensas contra amenazas, gestionar accesos, ayudar al cumplimiento de las normas y apoyar la estabilidad dando una visibilidad continua.

7. Recomendaciones

- Implementar MFA reduce el riesgo de accesos no autorizados añadiendo capas adicionales de seguridad.
- Realizar auditorías de las configuraciones de seguridad para detectar y corregir posibles errores que puedan comprometer la seguridad.
- Utilizar técnicas de cifrado para proteger data sensible tanto en tránsito como en reposo. Algunos ejemplos de estos sistemas de seguridad los podemos encontrar en empresas como: Cisco, BAE, Sophos y otros tantos.
- Capacitar a los empleados ofreciendo programas de capacitación regulares sobre las mejores prácticas de seguridad y como identificar amenazas, además se puede realizar simulacros de seguridad y entrenamientos en respuesta a incidentes para evaluar la preparación de los empleados y mejorar continuamente las estrategias de defensa.
- Cumplir con todas las normativas y estándares de seguridad para proteger los datos, evitar sanciones y pérdida de confianza de los clientes, y también buscar certificaciones de seguridad que ayuden a demostrar el compromiso con la protección de la información.
- Lo más importante es implementar un Plan de Respuesta frente incidentes estableciendo contramedidas que incluya procedimientos para su contención, identificación, eliminación de la amenaza y recuperación de datos si se llegaron a perder.

Bibliografía

- Access Quality. (27 de julio de 2023). Obtenido de La Importancia de la Seguridad en la Nube: Protección de Nuestros Activos Digitales: https://www.accessq.com.mx/importancia-seguridad-nube/
- akamai. (2024). Obtenido de https://www.akamai.com/glossary/what-is-cloud-mfa
- Arazi, E. (15 de Noviembre de 2021). *radware Blog*. Obtenido de Cuatro vulnerabilidades comunes en la nube que conducen a una violación de datos: https://www.radware.com/blog/cloud-security-8/2021/11/cuatro-vulnerabilidades-comunes-en-la-nube-que-conducen-a-una-violacion-de-datos/?lang=es
- AWS. (2024). *AWS*. Obtenido de ¿Qué es la computación en nube?: Amazon Web Services
- AWS. (2024). *AWS*. Obtenido de Tipos de computación en la nube: https://aws.amazon.com/es/types-of-cloud-computing/
- AWS. (2024). Obtenido de https://aws.amazon.com/es/what-is/ipsec/#:~:text=IPSec%20is%20a%20set%20of,make%20the%20protocol%20more%20secure.
- AWS. (2024). Obtenido de https://aws.amazon.com/es/what-is/vpn/
- AWS. (2024). Obtenido de SSL y TLS: https://aws.amazon.com/es/compare/the-difference-between-ssl-and-tls/
- CCPA. (Marzo de 13 de 2024). Obtenido de https://oag.ca.gov/privacy/ccpa
- CEPAL. (05 de Enero de 2024). Obtenido de https://biblioguias.cepal.org/c.php?g=495473&p=4398118

- Check Point . (2024). Obtenido de Los 15 problemas, amenazas y preocupaciones principales de la seguridad en la nube: https://www.checkpoint.com/es/cyber-hub/cloud-security/what-is-cloud-security/top-cloud-security-issues-threats-and-concerns/
- Check Point . (2024). Obtenido de Top 7 Cloud Vulnerabilities In 2024: https://www.checkpoint.com/es/cyber-hub/cloud-security/what-is-cloud-security/top-7-cloud-vulnerabilities-in-2024/
- Check Point. (2024). Obtenido de https://www.checkpoint.com/es/cyber-hub/network-security/what-is-an-intrusion-detection-system-ids/
- CHECK POINT. (2024). Obtenido de https://www.checkpoint.com/es/cyber-hub/network-security/what-is-ips/
- Check Point. (2024). Obtenido de https://www.checkpoint.com/es/cyber-hub/cloud-security/what-is-cloud-security/top-cloud-security-issues-threats-and-concerns/
- Check point. (24 de Enero de 2024). Obtenido de https://www.cybertalk.org/2024/01/24/the-future-of-cloud-security-20-statistics-trends-to-track/
- cloudflare. (2024). Obtenido de https://www.cloudflare.com/learning/ssl/what-is-https/
- Cyber, T. (18 de Abril de 2023). *linkedin*. Obtenido de Vulnerabilidades peligrosas de la computación en la nube en 2023: https://www.linkedin.com/pulse/vulnerabilidades-peligrosas-de-la-computaci%C3%B3n-en-nube-tag-cyber/
- DATADOG. (2024). Obtenido de https://www.datadoghq.com/
- EDteam. (2021). Obtenido de https://ed.team/blog/que-es-una-vpn
- Elad, B. (03 de Enero de 2024). *enterpriseappstoday*. Obtenido de https://www.enterpriseappstoday.com/stats/cloud-security-statistics.html

- Elastic Security . (2024). Obtenido de https://www.elastic.co/security
- ENTRUST. (2024). Obtenido de que es SAML: https://www.entrust.com/es/resources/learn/what-is-saml
- ENTRUST. (2024). Obtenido de Que es SSL: https://www.entrust.com/es/resources/learn/what-is-ssl
- Faster Capital. (19 de abril de 2024). Obtenido de https://fastercapital.com/es/contenido/Estandares-de-la-industria--impulsando-la-eficiencia-y-la-coherencia.html
- Fitzgerald, A. (14 de Febrero de 2024). *secureframe*. Obtenido de https://secureframe.com/blog/cloud-security-statistics
- Gartner. (10 de octubre de 2019). *Gartner*. Obtenido de Gartner: https://www.gartner.es/es/articulos/es-segura-la-nube
- González, E. (12 de julio de 2022). *Bit life*. Obtenido de https://bitlifemedia.com/2022/07/seguridad-en-la-nube-amenazas/
- Google cloud. (2024). *Google cloud*. Obtenido de PaaS, IaaS, SaaS y CaaS: ¿en qué se diferencian?: https://cloud.google.com/learn/paas-vs-iaas-vs-saas?hl=es
- Google Cloud. (2024). *Google Cloud*. Obtenido de Ventajas y desventajas de la computación en la nube: https://cloud.google.com/learn/advantages-of-cloud-computing?hl=es-419
- HIPAA. (2024). Obtenido de https://www.hipaajournal.com/
- IBM. (2024). *IBM*. Obtenido de https://www.ibm.com/es-es/topics/data-breach
- IBM. (2024). Obtenido de https://www.ibm.com/es-es/products/qradar-siem

- IBM. (26 de Marzo de 2024). Obtenido de OAuth: https://www.ibm.com/docs/es/was/9.0.5?topic=resources-oauth
- Interfacing. (2024). Obtenido de https://www.interfacing.com/es/que-es-el-soc-2
- Intersoft Consulting. (2024). Obtenido de https://gdpr-info.eu/
- IONOS. (4 de noviembre de 2021). Obtenido de https://www.ionos.es/digitalguide/servidores/seguridad/kerberos/
- ISO. (22 de septiembre de 2023). Obtenido de https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27001-y-para-que-sirve/
- Jones, W. b. (23 de abril de 2024). *Expert insights*. Obtenido de https://expertinsights.com/insights/50-cloud-security-stats-you-should-know/
- Kaspersky. (2024). *Kaspersky*. Obtenido de ¿Qué es la seguridad en la nube?: https://latam.kaspersky.com/resource-center/definitions/what-is-cloud-security
- Kolesnikov, N. (31 de Enero de 2024). *Techopedia*. Obtenido de 50 Estadísticas Clave de Ciberseguridad para Abril de 2024: https://www.techopedia.com/es/estadisticas-ciberseguridad
- Marcos Flores Miranda. (11 de Marzo de 2024). *Delete Technology*. Obtenido de https://www.deletetechnology.com/blog/todo-sobre-nist-sp-800-53-gu%C3%ADa-esencial-de-ciberseguridad
- Microsoft . (3 de agosto de 2023). Obtenido de https://learn.microsoft.com/es-es/windows-server/security/kerberos/kerberos-authentication-overview
- MICROSOFT SENTINEL. (2024). Obtenido de https://azure.microsoft.com/en-us/products/microsoft-sentinel/

- Mitchell Anicas. (30 de Marzo de 2018). Obtenido de Una introducción a OAuth 2: https://www.digitalocean.com/community/tutorials/una-introduccion-a-oauth-2-es
- Navarro, L. (2024). *hackmetrix*. Obtenido de Cybersecurity Experts : https://blog.hackmetrix.com/ejemplos-de-ciberataques/
- NETSCOUT. (12 de Octubre de 2023). *TMCNET*. Obtenido de https://www.tmcnet.com/usubmit/-netscout-identifico-casi-79-millones-de-ataques-ddos-/2023/10/12/9898087.htm
- Networking Lessons. (2024). Obtenido de https://networklessons.com/cisco/ccie-routing-switching/ipsec-internet-protocol-security
- onelogin. (2024). Obtenido de https://www.onelogin.com/learn/what-is-ldap#:~:text=The%20Lightweight%20Directory%20Access%20Protocol,printers%2C%20LDAP%20is%20the%20answer.
- onelogin. (2024). Obtenido de https://www.onelogin.com/learn/what-is-mfa
- Paloalto Networks. (2024). Obtenido de https://www.paloaltonetworks.lat/cyberpedia/what-is-an-intrusion-detection-system-ids
- Pathak, A. (2024). *Geekflare*. Obtenido de 9 desafíos y riesgos en la computación en la nube y Strategies a Preventrélos: https://geekflare.com/es/challenges-and-risks-in-cloud-computing/
- PingSafe. (28 de septiembre de 2023). *PingSafe*. Obtenido de https://www.pingsafe.com/blog/cloud-security-statistics/
- PIRANI. (14 de 2022OCTUBRE). Obtenido de https://www.piranirisk.com/es/blog/cumplimiento-normativo-que-es-como-evita-riesgos

- PYM. (2024). Obtenido de Explicación del protocolo OAuth 2: https://programacionymas.com/blog/protocolo-oauth-2
- redalia. (2024). Obtenido de Protocolo SSL/TLS: https://www.redalia.es/ssl/protocolo-ssl/
- Semrush Blog. (enero de 22 de 2024). Obtenido de https://www.semrush.com/blog/what-is-https/
- SOPHOS. (2023). Informe de Sophos sobre amenazas 2023: Los mercados delictivos maduros presentan nuevos retos para los responsables de la seguridad. En Sophos. Sophos X-Ops.
- Souza, R. M. (17 de Enero de 2024). *DLA PIPER*. Obtenido de https://www.dlapiper.com/en-gb/insights/publications/2024/01/dla-piper-gdpr-fines-and-data-breach-survey-january-2024
- splunk. (2024). Obtenido de https://www.splunk.com/
- Stackscale. (1 de Febrero de 2023). *Stackscale grupo aire*. Obtenido de Principales modelos de servicio cloud: IaaS, PaaS y SaaS: https://www.stackscale.com/es/blog/modelos-de-servicio-cloud/
- SYDLE. (23 de febrero de 2022). *SYDLE*. Obtenido de 13 ventajas del cloud computing: https://www.sydle.com/es/blog/ventajas-cloud-computing-6154ae3d0e94dd1b0fa01fd6
- T Systems. (34 de Abril de 2019). Obtenido de Un repaso a las principales vulnerabilidades en la nube: https://www.t-systemsblog.es/principales-vulnerabilidades-en-la-nube/
- Thales. (5 de julio de 2023). Obtenido de https://cpl.thalesgroup.com/about-us/newsroom/2023-cloud-security-cyberattacks-data-breaches-press-release

- Universidad de sevilla . (2024). El estandar SAML. En *El estandar SAML* (págs. 32-62). Sevilla.
- veeam. (22 de febrero de 2022). Obtenido de https://www.veeam.com/es/news/89-percent-of-organizations-falling-short-on-data-protection.html
- Verizon. (2023). 2023 Data Breach Investigations Report. En Verizon. DBIR.
- Zettler, K. (s.f.). *Desarrollo de software*. Obtenido de ¿Qué es la computación en la nube?: https://www.atlassian.com/es/microservices/cloud-computing