Habilidades transferibles son habilidades de otras áreas de estudio o práctica que pueden aplicarse a diferentes carreras.

Habilidades técnicas también pueden aplicarse a varias profesiones; sin embargo, normalmente requieren el conocimiento de herramientas, procedimientos y políticas específicas.

**Habilidades Transferibles**

**Comunicación:** Como analista de ciberseguridad, necesitará comunicarse

**Resolución de problemas:** Una de sus principales tareas como analista de ciberseguridad será identificar y resolver problemas de forma proactiva.

**Gestionar el tiempo:** Tener un gran sentido de la urgencia y priorizar las tareas adecuadamente es esencial en el campo de la ciberseguridad

**Mentalidad de crecimiento:** Esta es una industria en evolución, por lo que una Habilidad transferible importante es la voluntad de aprender.

**Diversidad de perspectivas:** La única forma de llegar lejos es juntos.

**Habilidades Técnicas**

**Lenguajes de programación:** Al comprender cómo utilizar los lenguajes de programación, los analistas de ciberseguridad pueden automatizar tareas que, de otro modo, requerirían mucho tiempo.

**Herramientas de administración de información y eventos de seguridad (SIEM):** Las herramientas SIEM recopilan y analizan datos de registro, o registros de eventos.

**Sistemas de detección de intrusiones (IDS):** Los analistas de ciberseguridad utilizan los IDS para monitorizar la actividad del sistema

**Conocimientos sobre el panorama de las amenazas**: Estar al tanto de las tendencias actuales relacionadas con los agentes de amenazas

**Respuesta ante incidentes:** Los analistas de ciberseguridad deben ser capaces de seguir las políticas y procedimientos establecidos para responder adecuadamente a los incidentes.

* **analytical thinking**, which means to think carefully and thoroughly.
* **Collaboration** means working with stakeholders and other team members.
* When a specific threat or vulnerability is identified, an analyst might **install prevention software**,
* As an analyst prevents and encounters threats, risks, or vulnerabilities, they document and **report findings.**
* **set up appropriate processes. When involved with software development projects, it can be helpful for an analyst to understand programming languages.**
* **periodic security audit. This is a review of an organization’s records, Security Information and Event Management (SIEM)**

**Términos del glosario del Módulo 1**

Ciberseguridad (o seguridad): La práctica de garantizar la confidencialidad, integridad y disponibilidad de la información protegiendo las redes, los dispositivos, las personas y los datos del acceso no autorizado o de la explotación delictiva

Seguridad de la nube: El proceso de garantizar que los recursos almacenados en la Nube están configurados correctamente y que el acceso a dichos recursos está limitado a los usuarios autorizados

Amenaza interna: Un empleado actual o anterior, un proveedor externo o un socio de confianza que supone un riesgo para la Seguridad

Seguridad de red: La práctica de mantener la infraestructura de red de una organización a salvo de accesos no autorizados

Información de identificación personal (PII): Cualquier Información utilizada para inferir la identidad de un individuo

Postura de seguridad: La capacidad de una organización para gestionar su defensa de activos y datos críticos y reaccionar ante los cambios

Información de identificación personal sensible (SPII): Un tipo específico de PII que entra dentro de las directrices de manejo más estrictas

Habilidades técnicas: Habilidades que requieren el conocimiento de herramientas, Procedimientos y políticas específicas

Amenaza: Cualquier circunstancia o Evento que pueda impactar negativamente en los recursos

Agente de amenaza: Cualquier persona o grupo que presente un riesgo para la Seguridad

Habilidades transferibles: Habilidades de otras áreas que pueden aplicarse a diferentes carreras profesionales

Este módulo trata sobre ataques cibernéticos comunes, centrándose en tres tipos principales:

1. **Phishing**: Usa correos, llamadas o mensajes falsos para engañar a las personas y robarles datos o instalar malware. Tipos comunes:  
   * **BEC** (fraude por correo empresarial)
   * **Spear phishing** (ataques personalizados)
   * **Whaling** (dirigido a ejecutivos)
   * **Vishing** (llamadas falsas)
   * **Smishing** (mensajes de texto falsos)
2. **Software malicioso (malware)**: Como virus, gusanos y ransomware, que buscan dañar sistemas o extorsionar a los usuarios.
3. **Ingeniería social**: Manipula psicológicamente a las personas para que entreguen información o acceso. Estrategias típicas incluyen:  
   * Phishing en redes sociales
   * Ataques de “agujero de agua” (infectar sitios que la víctima frecuenta)
   * USB baiting (dejar USBs infectados)
   * Trucos físicos (como hacerse pasar por técnicos)

La ingeniería social funciona porque explota emociones humanas como la urgencia, la autoridad, la confianza y la escasez.

Esta lectura es una introducción y más adelante en el curso se enseñará cómo reconocer y defenderse de estos ataques.

**Malware: A software designed to harm devices or networks**

**Worm: Malware that self-replicates, spreading across the network and infecting computers**

**Ransomware: A malicious attack during which threat actors encrypt an organization's data and demand payment to restore access**

**Spyware: Malicious software installed on a user’s computer without their permission, which is used to spy on and steal user data**

**Phishing: The use of digital communications to trick people into revealing sensitive data or deploying malicious software**

**Spear phishing: A malicious email attack targeting a specific user or group of users that appears to originate from a trusted source**

**Whaling: A form of spear phishing during which threat actors target executives in order to gain access to sensitive data**

**Business email compromise (BEC): An attack in which a threat actor impersonates a known source to obtain a financial advantage**

**Vishing: The exploitation of electronic voice communication to obtain sensitive information or to impersonate a known source**

**Social engineering: A manipulation technique that exploits human error to gain unauthorized access to sensitive, private, and/or valuable data**

**Social media phishing: An attack in which a threat actor collects detailed information about their target on social media sites before initiating an attack**

**Watering hole attack: An attack in which a threat actor compromises a website frequently visited by a specific group of users**

**Physical social engineering: An attack in which a threat actor impersonates an employee, customer, or vendor to obtain unauthorized access to a physical location**

**USB baiting: An attack in which a threat actor strategically leaves a malware USB stick for an employee to find and unknowingly infect a network**

**Height Domains:**

1. **el primer dominio, la seguridad y la gestión de riesgos.**
2. **El segundo dominio es la Seguridad de los recursos.**
3. **El tercer dominio es la arquitectura e ingeniería de Seguridad.**
4. **El cuarto dominio de seguridad es la seguridad de la red y la comunicación.**
5. **Pasemos al quinto dominio: la gestión de identidades y accesos**
6. **El sexto dominio es la evaluación y las pruebas de Seguridad.**
7. **El séptimo dominio son las operaciones de Seguridad.**
8. **El octavo dominio final es la Seguridad del desarrollo de software.**

**Resumen sobre amenazas cibernéticas y tipos de hackers:**

1. **Amenaza Persistente Avanzada (APT):  
    Grupos altamente capacitados que acceden de forma no autorizada a redes de grandes empresas o entidades gubernamentales. Permanecen ocultos por mucho tiempo. Sus objetivos incluyen:**
   * **Dañar infraestructuras críticas.**
   * **Robar propiedad intelectual.**
2. **Amenazas internas:  
    Personas con acceso autorizado que lo usan para dañar la organización. Sus motivaciones pueden ser:**
   * **Sabotaje, corrupción, espionaje o filtración de datos.**
3. **Hacktivistas:  
    Utilizan tecnología con fines políticos o sociales. Sus acciones incluyen:**
   * **Manifestaciones, propaganda, campañas de cambio social o búsqueda de fama.**
4. **Tipos de hackers:**
   * **Autorizados (éticos): Usan sus habilidades para proteger sistemas, siguiendo la ley.**
   * **Semiautorizados (investigadores): Buscan vulnerabilidades sin explotarlas.**
   * **No autorizados (no éticos): Rompen la ley para obtener beneficios, como vender datos.**
   * **Otros tipos incluyen novatos, mercenarios, o vigilantes (que buscan proteger de hackers maliciosos).**

**Conclusión:  
 Los agentes de amenaza se definen por sus intenciones maliciosas, mientras que los hackers se clasifican según sus habilidades y motivaciones. Conocer sus perfiles ayuda a mejorar la ciberseguridad.**

## **Términos y definiciones del Curso 1, Módulo 2**

**Inteligencia artificial (IA) antagónica: Una técnica que manipula la inteligencia artificial (IA) y la tecnología de aprendizaje automático (ML) para llevar a cabo ataques de forma más eficiente.**

**Compromiso de correo electrónico empresarial (BEC): Un tipo de ataque de phishing en el que un agente de amenaza se hace pasar por una fuente conocida para obtener una ventaja financiera**

**CISSP: Certified Información Systems Security Professional (profesional certificado en seguridad de los sistemas de información) es una certificación en seguridad de la información reconocida en todo el mundo y muy solicitada, otorgada por el Consorcio Internacional de Certificación en Seguridad de los Sistemas de Información**

**Virus informático: Código malicioso escrito para interferir en las operaciones de la computadora y causar daños a los datos y al software**

**Ataque criptográfico: Ataque que afecta a las formas seguras de Comunicación entre un remitente y un destinatario**

**Hacker: Cualquier persona que utilice ordenadores para acceder a sistemas informáticos, redes o datos**

**Software malicioso: Software diseñado para dañar dispositivos o redes**

**Ataque de descifrado de contraseña: Intento de acceder a dispositivos, sistemas, redes o datos protegidos por contraseña**

**Phishing: El uso de las comunicaciones digitales para engañar a la gente para que revele Datos sensibles o despliegue software malicioso**

**Ataque físico: Incidente de Seguridad que afecta no sólo a los entornos digitales sino también a los físicos DONDE SE IMPLEMENTA**

**Ingeniería social física: Ataque en el que un agente de amenaza se hace pasar por un empleado, cliente o proveedor para obtener acceso no autorizado a un lugar físico**

**Ingeniería social: Una técnica de manipulación que explota el error humano para obtener información privada, acceso u objetos de valor**

**Phishing en redes sociales: Tipo de ataque en el que un agente de amenaza recopila información detallada sobre su objetivo en las redes sociales antes de iniciar el ataque**

**Spear phishing : ataque malicioso por correo electrónico dirigido a un usuario o grupo de usuarios específico, que parece proceder de una fuente de confianza**

**Ataque a la cadena de suministro: Ataque dirigido a sistemas, aplicaciones, hardware y/o software para localizar una vulnerabilidad en la que se pueda implementar software malicioso**

**USB baiting: Ataque en el que un agente de amenaza deja estratégicamente una memoria USB con software malicioso para que un empleado la encuentre y la instale con el fin de infectar una red sin saberlo**

**Virus : refiérase a "Virus informático"**

**Vishing : Explotación de las comunicaciones electrónicas de voz para obtener información confidencial o suplantar la identidad de una fuente conocida**

**Ataque de "agujero de agua": Un tipo de ataque en el que un agente de amenaza compromete un sitio web visitado con frecuencia por un grupo específico de usuarios.**

**Cómo se relacionan los controles, los marcos y el cumplimiento de la normativa**

**La tríada de confidencialidad, integridad y disponibilidad (C ID) es un Modelo** que ayuda a informar sobre cómo las organizaciones tienen en cuenta el riesgo a la hora de establecer sistemas y políticas de Seguridad.

**Los Marcos de seguridad son directrices que se utilizan para crear planes que ayuden a mitigar los riesgos y las amenazas a los datos y la privacidad.**

1. **Identificar y documentar los objetivos de Seguridad**
2. **Establecer directrices para alcanzar los objetivos de Seguridad**
3. **Implementar procesos de Seguridad sólidos**
4. **Monitorear y comunicar los resultados**

**Cumplimiento norma tivo es el proceso de adhesión a los Estándares internos y a las Regulaciones externas.**

**(NIST)** es una agencia con sede en EE.UU. que desarrolla múltiples marcos de cumplimiento voluntario que las organizaciones de todo el mundo pueden utilizar para ayudar a gestionar el riesgo. Marco de Ciberseguridad del NIST (CSF) y el Marco de Gestión de Riesgos del NIST (RMF).

**Otras empresas que se dedican a la normativa de la creación de marcos de seguridad:**

### **La Comisión Federal Reguladora de la Energía - Corporación Norteamericana de Confiabilidad Eléctrica (FERC-NERC) -** Medidas de seguridad para la Electricidad

### **El Programa Federal de Gestión de Riesgos y Autorizaciones (FedRAMP®) -** Servicios en la nube y ofertas de productos.

### **Centro para la Seguridad en Internet (CIS®) -** Seguridad en sistemas y las redes frente a los ataques.

### **Reglamento General de Protección de Datos (GDPR) - Ley de Protección de datos Europea.**

### **Estándar de seguridad de los datos para la industria de tarjetas de pago (PCI DSS) -** Garantizar que las organizaciones que almacenan, aceptan, procesan y transmiten información de tarjetas de crédito lo hacen en un entorno seguro.

### **La Ley de Transferencia y Responsabilidad de los Seguros Médicos (HIPAA) -** Para proteger la información sanitaria de los pacientes. Tiene tres normas:

1. Privacidad
2. Seguridad
3. Notificación de infracciones

Las organizaciones que almacenan datos de pacientes tienen la obligación legal de informar a los pacientes de una violación porque si la Información médica protegida (PHI) de los pacientes queda expuesta, puede conducir al robo de identidad y al fraude al seguro.

### **Organización Internacional de Normalización (ISO)**

La ISO se creó para establecer estándares internacionales relacionados con la tecnología, la fabricación y la gestión a través de las fronteras.

### **Controles de Sistemas y Organizaciones (SOC tipo 1, SOC tipo 2)**

Los SOC1 y SOC2 son una serie de informes que se centran en las políticas de acceso de los usuarios de una organización a diferentes niveles organizativos, como:

* Asociado
* Supervisor
* Gestor
* Ejecutivo
* Proveedores
* Otros

Cubren la confidencialidad, privacidad, integridad, disponibilidad, seguridad y la seguridad general de los datos. Los fallos de control en estas áreas pueden conducir al fraude.

**Orden ejecutiva presidencial 14028 de Estados Unidos**

Joe Biden publicó una orden ejecutiva relacionada con la mejora de la ciberseguridad de la nación para remediar el aumento de la actividad de los Agentes de amenaza.

**Conceptos éticos que guían las decisiones sobre ciberseguridad | Coursera**

**https://www.coursera.org/learn/foundations-of-cybersecurity/supplement/nCQJy/ethical-concepts-that-guide-cybersecurity-decisions**

**• La ética en ciberseguridad es crucial para tomar decisiones correctas al mitigar las amenazas y responder a ataques, protegiendo a organizaciones y personas.**

**• En Estados Unidos, los contraataques son generalmente ilegales según leyes como la Ley de Fraude y Abuso Informático de 1986 y otras, considerándose actos de vigilantismo.**

**• El punto de vista internacional sobre contraataques permite acciones defensivas directas, pero solo si no agravan la situación, el efecto es reversible y solo afecta al atacante inicial, según la Corte Internacional de Justicia (CIJ).**

**• Los principios éticos para profesionales de ciberseguridad se centran en la confidencialidad, la integridad y la disponibilidad (CID) de la información, la protección de la privacidad y cumplimiento de las leyes.**

**• Se destaca la importancia de la confidencialidad, la protección de la privacidad (incluyendo PII y SPII) y el cumplimiento legal, como la Ley HIPAA para proteger datos sensibles.**

**• Los profesionales de la seguridad deben actuar con imparcialidad, honestidad, transparencia y responsabilidad, basándose en las evidencias y actualizando sus conocimientos para una respuesta ética a los problemas de seguridad.**

**—-------------------------—-------------------------—-------------------------—-------------------------**

## **Términos y definiciones del Curso 1, Módulo 3**

**Recurso: Elemento que se percibe como poseedor de valor para una organización**

**Disponibilidad: La idea de que los datos son accesibles para aquellos que están autorizados a acceder a ellos**

**Cumplimiento normativo: El proceso de adhesión a los Estándares internos y a las Regulaciones externas**

**Confidencialidad: La idea de que sólo los usuarios autorizados pueden acceder a recursos o Datos específicos**

**Tríada de confidencialidad, integridad y disponibilidad (CID): Modelo que ayuda a informar sobre cómo las organizaciones tienen en cuenta el riesgo a la hora de establecer sistemas y políticas de Seguridad**

**Hacktivista: Persona que utiliza la piratería informática para lograr un objetivo político**

**Ley de Transferencia y Responsabilidad de los Seguros Médicos (HIPAA): Una ley federal estadounidense establecida para proteger la información sanitaria de los pacientes**

**Integridad: La idea de que los Datos son correctos, auténticos y fiables**

**Marco de Ciberseguridad (CSF) del Instituto Nacional de Estándares y Tecnología (NIST): Un framework voluntario que consiste en estándares, directrices y mejores prácticas para gestionar el riesgo de la ciberseguridad**

**Protección de la privacidad: El acto de salvaguardar la información personal del uso no autorizado**

**Información médica protegida (PHI) : Información relacionada con la salud o el estado físico o mental pasado, presente o futuro de una persona**

**Arquitectura de seguridad: Tipo de diseño de seguridad compuesto por múltiples componentes, como herramientas y procesos, que se utilizan para proteger a una organización de riesgos y amenazas externas**

**Controles de seguridad: Salvaguardas diseñadas para reducir riesgos de Seguridad específicos**

**Ética de la seguridad: Pautas para tomar decisiones adecuadas como profesional de la Seguridad**

**Marcos de seguridad: Directrices utilizadas para elaborar planes que ayuden a mitigar el riesgo y las amenazas a los Datos y a la privacidad**

**Gobernanza de seguridad: Prácticas que ayudan a apoyar, definir y dirigir los esfuerzos de seguridad de una organización**

**Información de identificación personal sensible (SPII): Un tipo específico de PII que entra dentro de las directrices de manejo más estrictas**

**COURSE 1 MODULE 4**

**Herramientas de administración de información y eventos de seguridad (SIEM)**

Una herramienta SIEM es una aplicación que recopila y analiza datos de registro para monitorizar las actividades críticas de una organización. Un registro A es un registro de los eventos que se producen en los sistemas de una organización.

### **Analizadores de protocolos de red (packet sniffers)**

Un analizador de protocolos de red, también conocido como rastreador de paquetes, es una herramienta diseñada para capturar y analizar el tráfico de datos en una red.

### **Manuales de estrategias**

Un libro de jugadas es un manual que proporciona detalles sobre cualquier acción operativa, como por ejemplo cómo responder a un incidente de seguridad. Las organizaciones suelen tener varios manuales de estrategias que documentan los procesos y procedimientos que deben seguir sus equipos.

Libro de jugadas de la cadena de **custodia**. La cadena de custodia es el proceso de documentación de la posesión y el control de las pruebas durante el ciclo de vida de un incidente.

El segundo manual de estrategias que puede utilizar su Equipo se denomina Manual de protección y preservación de evidencias . Proteger y preservar evidencias es el proceso de trabajar adecuadamente con evidencias digitales frágiles y volátiles.

Orden de volatilidad, que es una secuencia que describe el orden de los datos que deben conservarse del primero al último.

### **Programación**

Laprogramación es un proceso que puede utilizarse para crear un conjunto específico de instrucciones para que una computadora ejecute tareas.

**Automatización** es el uso de la tecnología para reducir el esfuerzo humano y manual en la realización de tareas comunes y repetitivas.

**Lenguaje de Consulta Estructurada (SQL)**

SQL se utiliza para crear, interactuar y solicitar información a una base de datos. Una base de datos es una colección organizada de información o datos.

Un punto de datos es una pieza específica de información.

**Sistemas Operativos**

Un sistema operativo es la interfaz entre el hardware de la computadora y el usuario.

**Vulnerabilidad Web**

Una vulnerabilidad web es un fallo único en una aplicación web que un agente de amenaza podría explotar mediante el uso de código.

**Software Antivirus**

Elsoftware antivirus es un programa de software utilizado para prevenir, detectar y eliminar software malicioso y virus.

### **Sistema de detección de intrusiones**

Un Sistema de detección de intrusiones (IDS) es una aplicación que monitoriza la actividad del sistema y alerta sobre posibles intrusiones.

**Encriptación**

La encriptación es el proceso de convertir datos de un formato legible a un formato codificado criptográficamente. La codificación criptográfica consiste en convertir el texto plano en texto cifrado seguro. El texto plano es la información no cifrada y el texto cifrado seguro es el resultado de la encriptación.

**Pentesting**

Las pruebas de penetración, también denominadas pen testing, son el acto de participar en un ataque simulado que ayuda a identificar vulnerabilidades en sistemas, redes, sitios web, aplicaciones y procesos.

**Crear un Portfolio para mi perfil en Ciberseguridad**

## **Opciones para crear su Portfolio**

Hay muchas maneras de presentar un Portfolio, incluyendo opciones de auto-presentación y en línea como:

* **Carpeta de documentación**
* **Google Drive o Dropbox™**
* **Sitios de Google**
* **Repositorio Git**

Podría crear subcarpetas con títulos como:

* **Currículum**
* **Educación**
* **Documentos de Portfolio**
* **Herramientas de ciberseguridad**
* **Programación**

**Google Sites -** Presentar artículos de portfolio.

**Repo Git -** Almacenar documentos, labs y capturas de pantalla sobre el programa de certificación.

## **Proyectos Portfolio**

ASÍ COMO se mencionó anteriormente, usted tendrá múltiples oportunidades a lo largo del programa de certificación para desarrollar elementos para incluir en su Portfolio. Estas oportunidades incluyen:

* Redacción de una declaración profesional
* Realización de una Auditoría de Seguridad
* Analizar la estructura y la seguridad de las redes
* Utilizar los comandos de Linux para gestionar los permisos de archivo
* Aplicación de filtros a las consultas SQL
* Identificar vulnerabilidades para un pequeño negocio (Business-to-Business)
* Documentación de incidentes con un Diario del gestor de incidentes
* Importación y análisis sintáctico de un archivo de texto en un escenario relacionado con la Seguridad
* Creación o revisión de un Currículum Vitae

**Module 1 Course 2**

**Dominios de la Seguridad.**

### **1. Seguridad y Gestión de Riesgos**

* **Objetivo: Definir y mantener la postura de seguridad de la organización.**
* **Incluye:**
  + **Metas y objetivos de seguridad claros.**
  + **Procesos para mitigar riesgos.**
  + **Cumplimiento legal y normativo.**
  + **Planes de continuidad del negocio.**
  + **Ética profesional.**
* **Procesos clave (InfoSec):**
  + **Respuesta ante incidentes.**
  + **Gestión de vulnerabilidades.**
  + **Seguridad de aplicaciones, nube e infraestructura.**

### **2. Seguridad de los Recursos**

* **Objetivo: Proteger activos físicos y digitales (datos).**
* **Incluye:**
  + **Almacenamiento, mantenimiento y destrucción segura de datos.**
  + **Registro y control de recursos.**
  + **Análisis de impacto y recuperación.**
  + **Uso de copias de seguridad para recuperación tras incidentes.**

### **3. Arquitectura de Seguridad e Ingeniería**

* **Objetivo: Diseñar sistemas seguros.**
* **Incluye principios de diseño como:**
  + **Modelo de amenazas.**
  + **Mínimo privilegio.**
  + **Defensa en profundidad.**
  + **Fallar seguro.**
  + **Confianza cero y verificación.**
* **Herramientas: SIEM para detectar comportamientos anómalos.**

### **4. Comunicación y Seguridad de Red**

* **Objetivo: Proteger las redes físicas, inalámbricas y en la nube.**
* **Incluye:**
  + **Seguridad de la red en oficinas, remoto o híbrido.**
  + **Controles como accesos restringidos.**
  + **Protección de comunicaciones externas e internas.**

### **5. Gestión de Identidad y Acceso (IAM)**

* **Objetivo: Controlar quién accede a qué.**
* **Incluye:**
  + **Verificación y autenticación de usuarios.**
  + **Aplicación del principio de mínimo privilegio.**
  + **Revocación de acceso cuando ya no se necesita.**

### **6. Evaluación y Pruebas de Seguridad**

* **Objetivo: Detectar y mitigar vulnerabilidades.**
* **Incluye:**
  + **Evaluaciones de seguridad.**
  + **Pruebas de penetración (pentesting).**
  + **Auditorías y análisis de permisos.**

### **7. Operaciones de Seguridad**

* **Objetivo: Responder y prevenir incidentes de seguridad.**
* **Incluye:**
  + **Monitorización, respuesta a incidentes y análisis forense.**
  + **Entrenamiento del personal.**
  + **Uso de herramientas como SIEM, gestión de registros y lecciones aprendidas tras incidentes.**

### **8. Seguridad en el Desarrollo de Software**

* **Objetivo: Crear aplicaciones seguras desde el inicio.**
* **Incluye:**
  + **Seguridad en cada fase del desarrollo (diseño, prueba, publicación).**
  + **Pruebas de seguridad del código.**
  + **Participación de QA y pentesters para verificar estándares.**

### **Objetivo principal**

* **Proteger los recursos (activos digitales y físicos) de una organización.**

### **Tipos de recursos**

* **Digitales: Información personal (SSN, fechas de nacimiento, cuentas bancarias, direcciones).**
* **Físicos: Quioscos de pago, servidores, PCs, oficinas.**

### **Estrategias comunes de gestión de riesgos**

1. **Aceptación: Se asume el riesgo sin acción para no interrumpir el negocio.**
2. **Evitación: Se elimina por completo el riesgo potencial.**
3. **Transferencia: Se delega el riesgo a un tercero (ej. aseguradoras).**
4. **Mitigación: Se reduce el impacto del riesgo.**

### **Marcos de gestión de riesgos**

* **NIST RMF: Framework del Instituto Nacional de Estándares y Tecnología.**
* **HITRUST: Framework para proteger información en el sector salud.**

### **Conceptos clave**

#### **Amenazas**

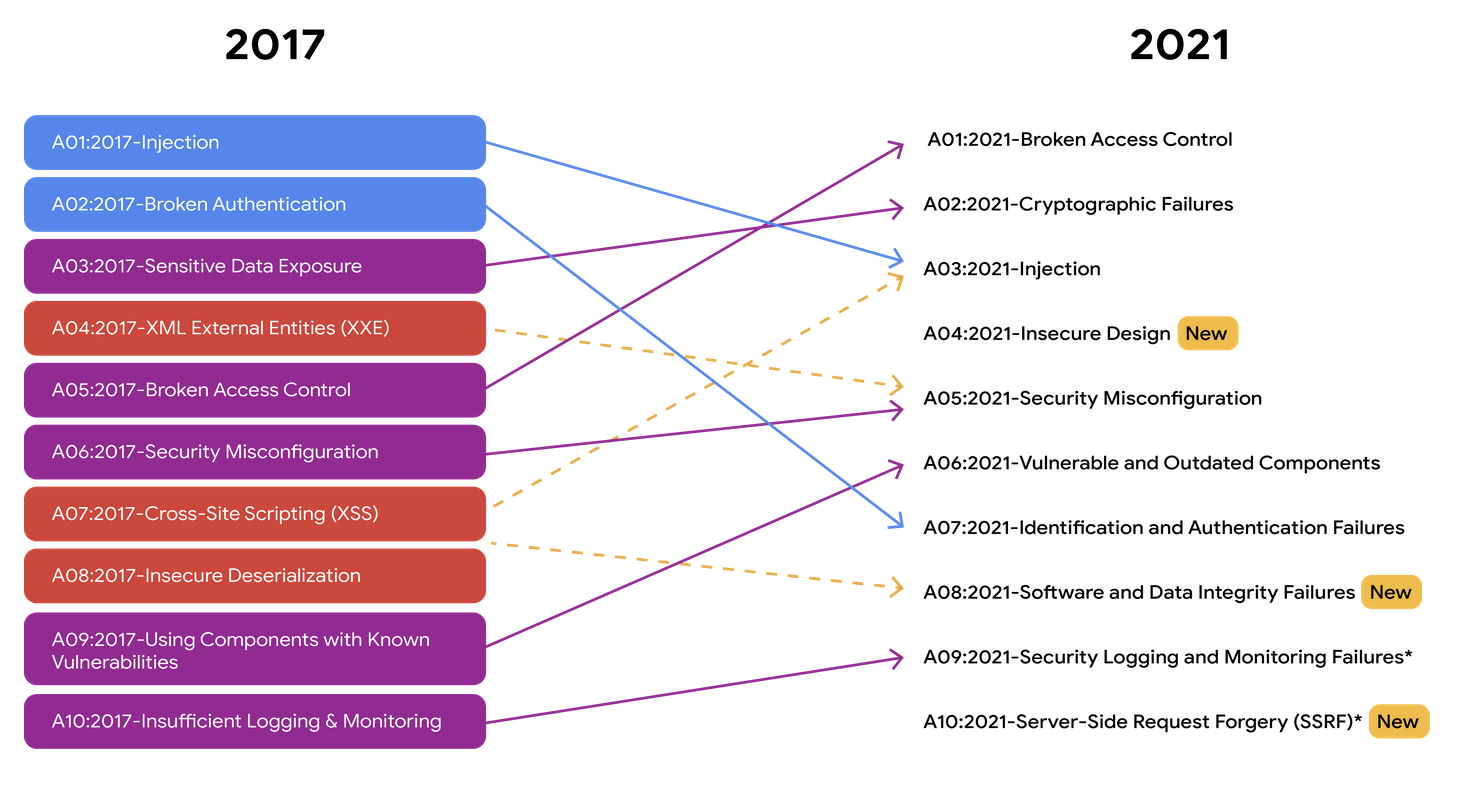
* **Eventos o circunstancias que pueden dañar los recursos.**
* **Tipos:**
  + **Internas: Personal o proveedores con acceso que lo usan de forma indebida.**
  + **APT (Amenazas Persistentes Avanzadas): Acceso no autorizado sostenido a largo plazo.**

#### **Riesgos**

* **Posibles impactos a la confidencialidad, integridad o disponibilidad de un recurso.**
* **Nivel de riesgo = Probabilidad de una amenaza.**
* **Ejemplo práctico: riesgo = llegar tarde; amenazas = tráfico, pinchazo, accidente.**

#### **Factores que aumentan los riesgos**

* **Externos: Actores fuera de la organización con intenciones maliciosas.**
* **Internos: Empleados, exempleados o socios con acceso indebido.**
* **Sistemas heredados: Infraestructura antigua aún activa pero vulnerable.**
* **Riesgo multiparte: Terceros con acceso a datos sensibles.**
* **Cumplimiento/licencias: Software no actualizado o mal gestionado.**

****

**Aquí tienes un resumen claro sobre las vulnerabilidades y sus ejemplos:**

### **¿Qué es una vulnerabilidad?**

* **Es una debilidad en un sistema que puede ser explotada por una amenaza.**
* **Las organizaciones deben realizar inspecciones regulares para detectarlas y corregirlas.**

### **Ejemplos de vulnerabilidades comunes:**

1. **ProxyLogon**
   * **Afecta a Microsoft Exchange.**
   * **Permite autenticación remota sin credenciales y ejecución de código malicioso.**
2. **ZeroLogon**
   * **Afecta al protocolo Netlogon (Microsoft).**
   * **Permite a un atacante autenticarse sin credenciales válidas y acceder a recursos.**
3. **Log4Shell**
   * **Afecta a la biblioteca Log4j (Java).**
   * **Permite ejecución remota de código y filtración de datos confidenciales.**
4. **PetitPotam**
   * **Afecta al protocolo NTLM en redes Windows.**
   * **Permite forzar autenticaciones y potencial robo de credenciales en LANs.**
5. **Fallos en el registro y monitoreo**
   * **Sistemas que no registran ni supervisan correctamente los eventos de seguridad.**
   * **Permiten que ataques pasen desapercibidos.**
6. **Falsificación de peticiones del lado del servidor (SSRF)**
   * **Manipula servidores para acceder a recursos internos o robar datos.**

**Module 2, Course 2**

### **¿Qué son los marcos de seguridad?**

* **Son directrices o planes que ayudan a mitigar riesgos y amenazas a los datos y la privacidad.**
* **Permiten a las organizaciones cumplir leyes y regulaciones, como HIPAA en el sector salud.**

### **¿Qué son los controles de seguridad?**

* **Son medidas concretas para reducir riesgos y amenazas.**
* **Se aplican junto a los marcos para reforzar la seguridad.**
* **Ejemplo: uso de MFA (autenticación multifactor) para proteger el acceso a datos médicos.**

### **Marcos específicos:**

1. **CTF (Cyber Threat Framework)**
   * **Desarrollado por el gobierno de EE.UU.**
   * **Proporciona un lenguaje común para describir y compartir información sobre ciberamenazas.**
   * **Mejora la capacidad de responder a amenazas de manera coordinada.**
2. **ISO/IEC 27001**
   * **Estándar internacionalmente reconocido para gestión de seguridad de la información.**
   * **Ayuda a proteger activos como: información financiera, propiedad intelectual, datos de empleados, etc.**
   * **Proporciona requisitos y controles recomendados, pero no obliga a usar controles específicos.**

### **Tipos de controles de seguridad:**

1. **Controles físicos**
   * **Ejemplos: puertas, cámaras, cerraduras, tarjetas de acceso, guardias.**
2. **Controles técnicos**
   * **Ejemplos: firewalls, MFA, antivirus.**
3. **Controles administrativos**
   * **Ejemplos: separación de funciones, procesos de autorización, clasificación de activos.**

**La tríada CID es un Modelo que ayuda a informar sobre cómo las organizaciones consideran el riesgo cuando establecen sistemas y políticas de Seguridad. Se compone de tres elementos que los analistas de ciberseguridad y las organizaciones trabajan para mantener: confidencialidad, integridad y disponibilidad.**

**Postura de seguridad satisfactoria, que se refiere a la capacidad de una organización para gestionar su defensa de los recursos y datos críticos y reaccionar ante los cambios.**

**La confidencialidad es la idea de que sólo los usuarios autorizados pueden acceder a recursos o datos específicos.**

**La integridad es la idea de que los datos son verificablemente correctos, auténticos y fiables. Es esencial disponer de protocolos para verificar la autenticidad de los Datos.**

**La Disponibilidad es la idea de que los Datos son accesibles para aquellos que están autorizados a utilizarlos.**

**La tríada CID es esencial para establecer la postura de Seguridad de una organización.**

**El Marco de Ciberseguridad del NIST** es un marco voluntario que consta de normas, directrices y mejores prácticas para gestionar los riesgos de ciberseguridad.

El CSF consta ahora de **seis** importantes funciones básicas: **Gobernar**, **Identificar**, **Proteger**, **Detectar**, **Responder** y **Recuperar.**

**Gobernar.** Esta función hace hincapié en la importancia de una sólida gobernanza de la ciberseguridad en todos los niveles de la organización. Se trata de establecer y mantener las estructuras y procesos necesarios para gestionar eficazmente los riesgos de ciberseguridad.

## **Principios de seguridad**

* **Minimizar la superficie de ataque:** La superficie de ataque se refiere a todas las vulnerabilidades potenciales que un Agente de amenaza podría explotar.
* **Principio de privilegio mínimo:** Los usuarios tienen la menor cantidad de acceso necesario para realizar sus tareas cotidianas.
* **Defensa en profundidad:** Las organizaciones deben disponer de diversos controles de seguridad que mitiguen los riesgos y amenazas.
* **Separación de funciones:** Las acciones críticas deben depender de varias personas**,**
* **Seguridad sencilla:** Evite las soluciones innecesariamente complicadas. La complejidad dificulta la seguridad.
* **Solucione correctamente los problemas de seguridad:** Cuando se produzcan incidentes de seguridad, identifique la causa raíz, contenga el impacto, identifique las vulnerabilidades y lleve a cabo pruebas para garantizar que la corrección se realiza correctamente.

**Principios de seguridad OWASP adicionales**

**Valores predeterminados seguros:** Las aplicaciones deben ser seguras por defecto, requiriendo esfuerzo adicional para que se vuelvan inseguras.

**Fallar con seguridad:** Ante fallos, los sistemas deben adoptar la opción más segura (por ejemplo, un firewall que falla debe bloquear todo el tráfico).

**No confiar en servicios externos:** No se debe asumir que los sistemas de terceros son seguros; hay que validar la información antes de usarla o compartirla.

**Evitar la seguridad por oscuridad:** No depender del secreto (como ocultar el código fuente) para proteger sistemas; la seguridad debe basarse en múltiples capas como políticas, controles y arquitectura robusta.

### 

# **Planificación de una Auditoría de Seguridad**

**Audit Scope and Goals**

**Summary:** The internal audit needs to align current business practices with industry standards and best practices. The audit is meant to provide mitigation recommendations for vulnerabilities found that are classified as “high risk,” and present an overall strategy to improve the security posture of the organization. The audit team needs to document their findings, provide remediation plans and efforts, and communicate with stakeholders.

**Scope:** The internal IT audit will assess the following:

* Assess user permissions
* Identify existing controls, procedures, and system protocols
* Account for technology currently in use

**Goals:** The goals for the internal IT audit are:

* Adhere to the NIST Cybersecurity Framework (CSF)
* Establish policies and procedures to ensure compliance with regulations
* Fortify system controls

**Risk Assessment**

## Current assets

Assets managed by the IT Department include:

* Employee equipment: end-user devices (desktops/laptops, smartphones), remote workstations, headsets, cables, keyboards, mice, docking stations, surveillance cameras, etc.
* Internal network: protected storage of customer, vendor, organizational data

## Risk description

Currently, there is inadequate management of assets. Additionally, proper controls are not in place and the organization may not be compliant with U.S. and international compliance regulations and standards.

## Control best practices

The organization will need to dedicate resources to managing assets. Additionally, they will need to determine the impact of the loss of existing assets, including systems, on business continuity.

## Risk score

On a scale of 1-10, the risk score is 8, which is fairly high. This is due to a lack of controls and adherence to necessary compliance regulations and standards.

## Additional comments

The likelihood of a lost asset or fines from governing bodies is high because the organization does not have all of the necessary controls in place and is not adhering to required regulations and standards related to keeping PII data private.

**Controls Assessment**

| **Administrative Controls** | | | |
| --- | --- | --- | --- |
| **Control name** | **Control type and explanation** | **Needs to be implemented**  **(X)** | **Priority** |
| Password policies | Preventative; establish password strength rules to improve security/reduce likelihood of account compromise through brute force or dictionary attack techniques | X | High |

| **Technical Controls** | | | |
| --- | --- | --- | --- |
| **Control Name** | **Control type and explanation** | **Needs to be implemented**  **(X)** | **Priority** |
| Intrusion Detection System (IDS) | Detective; allows IT team to identify possible intrusions (i.e., anomalous traffic) quickly | X | HIgh |
| Encryption | Deterrent; makes confidential information/data more secure (i.e., website payment transactions) | X | High/  Medium |

| **Physical Controls** | | | |
| --- | --- | --- | --- |
| **Control Name** | **Control type and explanation** | **Needs to be implemented**  **(X)** | **Priority** |
| Closed-circuit television (CCTV) surveillance | Preventative/detective; can reduce risk of certain events; can be used after event for investigation | X | High/  Medium |
| Locks | Preventative; physical and digital assets are more secure | X | High |

**Compliance Checklist**

* **General Data Protection Regulation (GDPR)**

GDPR is a European Union (EU) general data regulation that protects the processing of EU citizens’ data and their right to privacy in and out of EU territory. Additionally, if a breach occurs and a EU citizen’s data is compromised, they must be informed within 72 hours of the incident.

**Explanation:** The organization needs to adhere to GDPR because we conduct business and collect personal information from people in the EU.

* **Payment Card Industry Data Security Standard (PCI DSS)**

PCI DSS is an international security standard meant to ensure that organizations storing, accepting, processing, and transmitting credit card information do so in a secure environment.

**Explanation:** The organization needs to adhere to PCI DSS because we store, accept, process, and transmit credit card information in person and online.

**Auditorías de seguridad**

**Auditoría de seguridad** es una revisión de los Controles de seguridad, políticas y Procedimientos de una organización contra un conjunto de expectativas.

**Controles de seguridad** son salvaguardas diseñadas para reducir riesgos de Seguridad específicos.

**Metas y objetivos de una auditoría**

El objetivo de una auditoría es garantizar que las prácticas de tecnología de la información (TI) de una organización cumplen las normas del sector y de la organización.

**Los factores que determinan los tipos de auditorías que implementa una organización incluyen:**

* Tipo de industria
* Tamaño de la organización
* Vínculos con las regulaciones gubernamentales aplicables
* La ubicación geográfica de un negocio (Business-to-Business)
* Una decisión empresarial de adherirse a un cumplimiento normativo específico

CONTROL CATEGORIES: <https://docs.google.com/document/d/1Ut_H5A9FHwuQEy6_qG6Lfy3zwF6GSJnj3DZTMaNRWEE/template/preview?resourcekey=0-i4dR5qZFqQyfzr8uk3OOmA>

Antes de realizar una auditoría, es fundamental elaborar una lista de comprobación que incluya:

1. **Alcance de la auditoría**: Definir los recursos a evaluar, la frecuencia de las auditorías, los beneficios para la organización y revisar políticas, protocolos y procedimientos.
2. **Evaluación de riesgos**: Analizar los riesgos en relación con el presupuesto, controles, procesos internos y regulaciones externas.
3. **Ejecución de la auditoría**: Evaluar la seguridad de los recursos definidos en el alcance.
4. **Plan de mitigación**: Diseñar estrategias para reducir riesgos, costes y sanciones que afecten la seguridad.
5. **Comunicación de resultados**: Presentar un informe con hallazgos, mejoras sugeridas y regulaciones aplicables.

# 

# **El futuro de las herramientas SIEM**

Las herramientas SIEM (Gestión de Información y Eventos de Seguridad) recopilan y analizan datos para monitorear la seguridad de una organización en tiempo real.

Actualmente requieren intervención humana para el análisis. Con la evolución de la ciberseguridad, las herramientas SIEM se están adaptando a entornos en la nube (alojados o nativos), lo que permite mayor flexibilidad y escalabilidad.

Además, se espera que sigan evolucionando para enfrentar nuevas amenazas, como el crecimiento del Internet de las cosas (IoT), y para manejar grandes volúmenes de datos. La integración de inteligencia artificial, aprendizaje automático y automatización (como SOAR) mejorará la detección de amenazas y permitirá respuestas más rápidas con menos intervención humana, liberando a los analistas para tareas más complejas.

**Resumen:**

Esta lectura profundiza en cómo los datos de los paneles SIEM ayudan a los profesionales de ciberseguridad a identificar amenazas, riesgos y vulnerabilidades. Se destacan dos herramientas SIEM: **Splunk** y **Chronicle**, ambas con diversos paneles diseñados para monitorear y analizar la seguridad de una organización.

### **Splunk**

Splunk ofrece versiones en la nube y local (Enterprise y Cloud), que permiten a los analistas visualizar datos operativos en tiempo real. Sus principales paneles son:

* **Postura de seguridad:** Muestra eventos recientes para monitorear amenazas en tiempo real.
* **Resumen ejecutivo:** Proporciona una visión general de la seguridad organizacional para partes interesadas.
* **Revisión de incidentes:** Permite identificar patrones sospechosos previos a un incidente.
* **Análisis de riesgos:** Evalúa el riesgo asociado a usuarios, equipos o IPs específicas.

### **Chronicle**

Chronicle es un SIEM en la nube de Google, enfocado en el análisis y búsqueda de datos de registro. Sus paneles incluyen:

* **Estadísticas empresariales:** Muestra alertas recientes con puntuaciones de confianza y gravedad.
* **Ingestión de datos y salud:** Supervisa la correcta recepción y procesamiento de registros.
* **Coincidencias de COI:** Identifica amenazas observando tendencias en dominios, IPs y dispositivos.
* **Panel principal:** Ofrece una visión general del estado de la seguridad y eventos relevantes.
* **Detecciones de reglas:** Muestra estadísticas de alertas generadas por reglas específicas.
* **Inicio de sesión de usuario:** Analiza comportamientos de acceso para detectar actividades sospechosas.

## Términos y definiciones del Curso 2, Módulo 3

Chronicle: Una herramienta nativa de la nube diseñada para retener, analizar y buscar datos

Respuesta ante incidentes: El rápido intento de una organización de identificar un ataque, contener los daños y corregir los efectos de una violación de la Seguridad

Registro: Registro A de los eventos que se producen en los sistemas de una organización

Métricas: Atributos técnicos clave como el tiempo de respuesta, la disponibilidad y la tasa de fallos, que se utilizan para evaluar el rendimiento de una aplicación de software

Sistema operativo (OS): La interfaz entre el hardware de la computadora y el usuario

Manual de estrategias: Un manual que proporciona detalles sobre cualquier acción operativa

Administración de información y eventos de seguridad (SIEM): Una aplicación que recopila y analiza los datos de registro para monitorizar las actividades críticas de una organización

Orquestación, automatización y respuesta de seguridad (SOAR): Una colección de aplicaciones, herramientas y flujos de trabajo que utilizan la automatización para responder a los eventos de Seguridad

Herramientas SIEM: Una plataforma de software que recopila, analiza y correlaciona datos de seguridad de diversas fuentes en toda su infraestructura de TI que ayuda a Identificar y Responder a las amenazas de seguridad en tiempo real, investigar los Incidentes de seguridad y cumplir con las Regulaciones de seguridad

Splunk Cloud: Una herramienta alojada en la nube que se utiliza para recopilar, buscar y monitorizar datos de registro

Splunk Enterprise: Una herramienta autoalojada utilizada para retener, analizar y buscar los datos de registro de una organización para proporcionar información de seguridad y alertas en tiempo real.

MODULE 4

Un libro **de estrategias** es un manual que proporciona detalles sobre cualquier acción operativa.

Los Manuales de estrategias a veces cubren incidentes y vulnerabilidades específicos. Entre ellos se incluyen el ransomware, el vishing, el compromiso del correo electrónico empresarial (BEC) y otros ataques ya comentados.

Los manuales de estrategias de respuesta ante incidentes y vulnerabilidades son utilizados habitualmente por los profesionales de la ciberseguridad de nivel básico.

Entre los pasos más comunes incluidos en los manuales de estrategias para incidentes y vulnerabilidades se incluyen:

* Preparación

Before incidents occur, mitigate potential impacts on the organization by documenting, establishing staffing plans, and educating users.

* Detección

Detect and analyze events by implementing defined processes and appropriate technology.

* Análisis

Mismo que la detección.

* Contención

Prevent further damage and reduce immediate impact of incidents.

* Erradicación

Completely remove artifacts of the incident so that an organization can return to normal operations.

* Recuperación de un incidente

Mismo que en la erradicación.

* Post-Accidente

Document the incident, inform organizational leadership, and apply lessons learned.

* Coordinación

Report incidents and share information throughout the response process, based on established standards.

SOAR es una pieza de software utilizada para automatizar tareas repetitivas generadas por herramientas como un SIEM o una detección y respuesta gestionadas (MDR).

COURSE 3 MODULE 1

**Los dispositivos de red** mantienen la información y los servicios para los usuarios de una red. Estos dispositivos se conectan a través de conexiones por cable e inalámbricas.

**La red es la infraestructura general que permite que los dispositivos se comuniquen entre sí.** Los dispositivos de red son vehículos especializados como routers y Switch que gestionan lo que se envía y recibe a través de la red.

* Un **router** se conecta a Internet a través de un **Módem**.
* **El firewall** es un dispositivo de seguridad que supervisa el tráfico entrante y saliente de su red.
* El router dirige el tráfico a los dispositivos de su red doméstica.
* **Switch**, que es un dispositivo opcional que puede utilizarse para conectar más dispositivos a su red proporcionando puertos y conexiones Ethernet adicionales.
* Todas los dispositivos de la red tienen una dirección física de red (MAC) y una dirección digital llamada (IP).
* **Los** servidores proporcionan información y servicios para dispositivos como computadoras, dispositivos domésticos inteligentes y teléfonos inteligentes en la red.
* Tanto los concentradores como los conmutadores dirigen el tráfico en una red local. Un **concentrador** es un dispositivo que proporciona un punto común de conexión para todos los dispositivos conectados directamente a él.
* Un **Switch** reenvía paquetes entre dispositivos conectados directamente a él. Analizan la dirección de destino de cada paquete de datos y lo envían al dispositivo previsto.

Diferencias entre un conmutador (Switch) y un concentrador (Hub).

| **Característica** | **Conmutador (Switch)** | **Concentrador (Hub)** |
| --- | --- | --- |
| **Funcionamiento** | Reenvía datos solo al puerto de destino específico | Reenvía datos a todos los puertos (difusión) |
| **Inteligencia** | Inteligente: aprende direcciones MAC de dispositivos | No inteligente: no distingue direcciones MAC |
| **Eficiencia de red** | Alta, reduce colisiones | Baja, muchas colisiones |
| **Seguridad** | Más seguro (solo destinatario recibe los datos) | Menos seguro (todos reciben los datos) |
| **Velocidad y rendimiento** | Mejor rendimiento, más rápido | Más lento, sobre todo en redes con mucho tráfico |
| **Uso actual** | Muy común en redes modernas | Prácticamente en desuso |
| **Costo** | Más caro | Más barato |

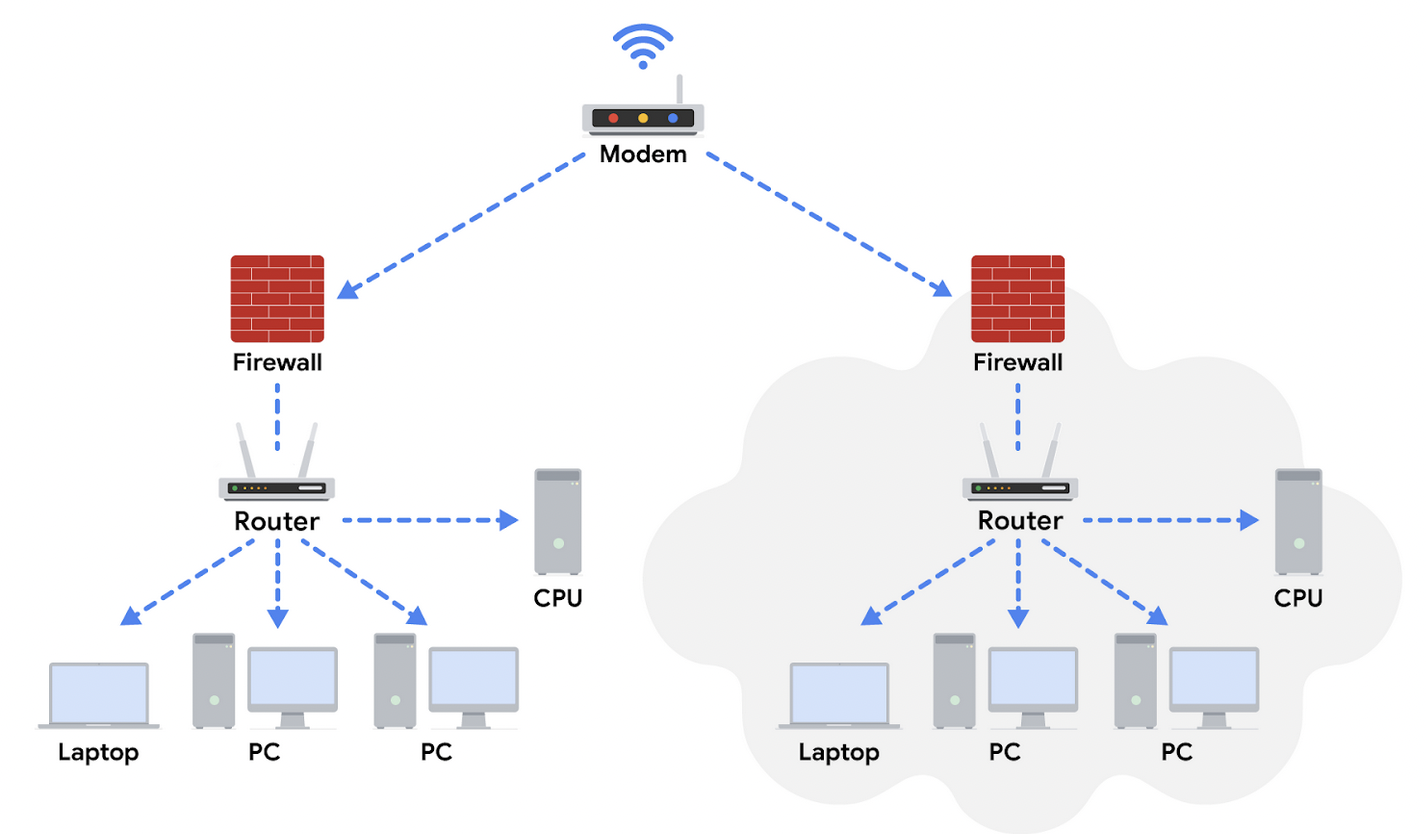
Los conmutadores forman parte de la capa de enlace de datos en el Modelo TCP/IP.

* **Los routers** conectan redes y dirigen el tráfico, basándose en la dirección IP de la red de destino. En el Modelo TCP/IP, los routers forman parte de la capa de red.
* **Los módems** suelen conectar su casa u oficina con un proveedor de servicios de Internet (ISP). Los ISP proporcionan conexión a Internet a través de líneas telefónicas o cables coaxiales.

**El módem** es el encargado de conectarte a tu ISP (es decir, a tu compañía de Internet).

**Un router**, básicamente, es el **periférico que se encarga de llevar la conexión a los dispositivos**.

* Un **punto de acceso inalámbrico** envía y recibe señales digitales a través de ondas de radio creando una red inalámbrica. Uso parecido al de un “Router”.
* **Los** **diagramas de** red son mapas que muestran los dispositivos de la red y cómo se conectan.



La **computación en** la nube, sin embargo, se refiere a la práctica de utilizar servidores, aplicaciones y servicios de red remotos que se alojan en Internet en lugar de en un lugar físico propiedad de la empresa.

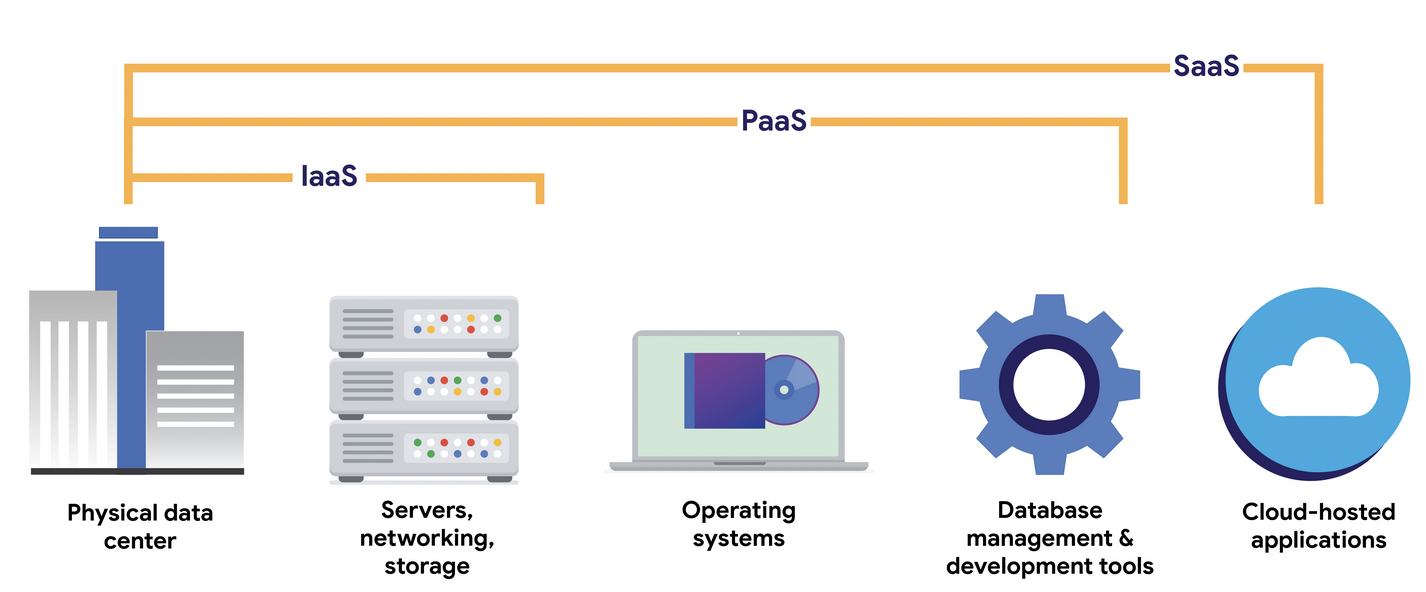
**On-premise**, lo que significa que todos los dispositivos utilizados para las operaciones de red se mantienen en una ubicación física propiedad de la empresa.

**Un proveedor de servicios en la nube (PSN)** es una empresa que ofrece servicios de computación en la nube.

Estos servicios pueden consumirlos a través de la interfaz de programación de aplicaciones (API) o la consola web del CSP.

**Software como servicio (SaaS** ) se refiere a conjuntos de software operados por el CSP que una empresa puede utilizar de forma remota sin alojar el software.

**La infraestructura como servicio (IaaS)** se refiere al uso de componentes informáticos virtuales ofrecidos por el CSP. Estos incluyen contenedores virtuales y almacenamiento que se configuran de forma remota a través de la API o la consola web del CSP.



Herramientas de Red



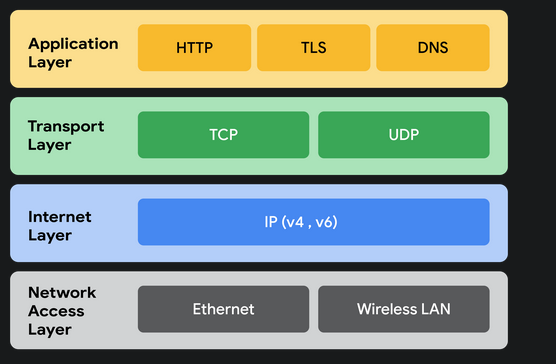
Tres de las principales razones por las que la computación en la nube resulta tan atractiva para las empresas son la Confiabilidad, la disminución de los costes y el aumento de la escalabilidad.

La fiabilidad en la computación en la nube se basa en el grado de disponibilidad de los servicios y Recursos de la nube, la seguridad de las conexiones y la frecuencia con la que los servicios funcionan eficazmente.

Los CSP disponen de centros de datos tan grandes, pueden ofrecer dispositivos y servicios virtuales a una fracción del coste que supone para las empresas instalar, parchear, actualizar y gestionar ellas mismas los componentes y el software.

## **El Modelo TCP/IP**

El **Modelo TCP/IP** es un framework utilizado para visualizar cómo se organizan y transmiten los datos a través de una red.



#### **Capa de transporte**

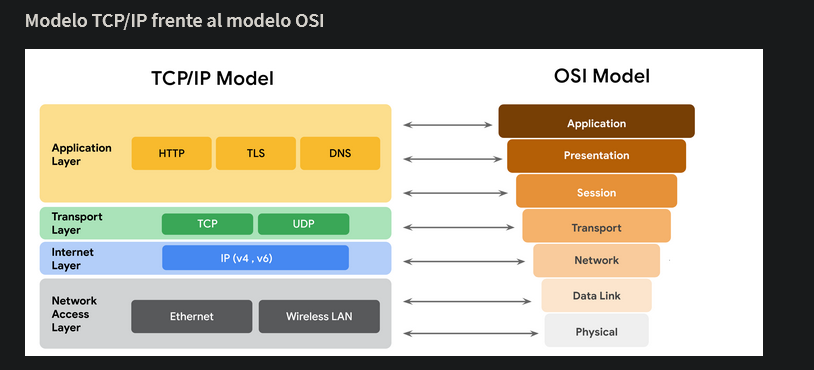
Se encarga de la entrega de datos entre dos sistemas. Sus principales protocolos son:

* **TCP (Protocolo de Control de Transmisión):** Establece conexión entre dispositivos, garantiza una transmisión confiable e incluye el número de puerto de destino.
* **UDP (Protocolo de Datagramas de Usuario):** No establece conexión, es menos confiable pero más rápido, ideal para aplicaciones en tiempo real como video en streaming.

#### **Capa de aplicación**

Gestiona las solicitudes y respuestas de red, y permite el acceso a servicios de Internet. Protocolos comunes incluyen:

* **HTTP**, **SMTP**, **SSH**, **FTP**, **DNS** Esta capa depende de las capas inferiores para el envío de datos.



El **OSI** organiza visualmente los protocolos de redes en diferentes capas. Los profesionales de las redes suelen utilizar este modelo para comunicarse entre sí sobre posibles fuentes de problemas o amenazas a la seguridad cuando se producen.

**Capa 7 – Aplicación** Interactúa directamente con el usuario a través de programas como navegadores o correos. Usa protocolos como **HTTP, HTTPS, SMTP, DNS**.

**Capa 6 – Presentación** Traduce, comprime y encripta los datos para que puedan ser entendidos por el otro sistema. Ejemplo: **SSL** para cifrado en sitios web seguros.

**Capa 5 – Sesión** Establece, mantiene y finaliza la comunicación entre dispositivos. Gestiona **autenticación, reconexión** y puntos de control si la sesión se interrumpe.

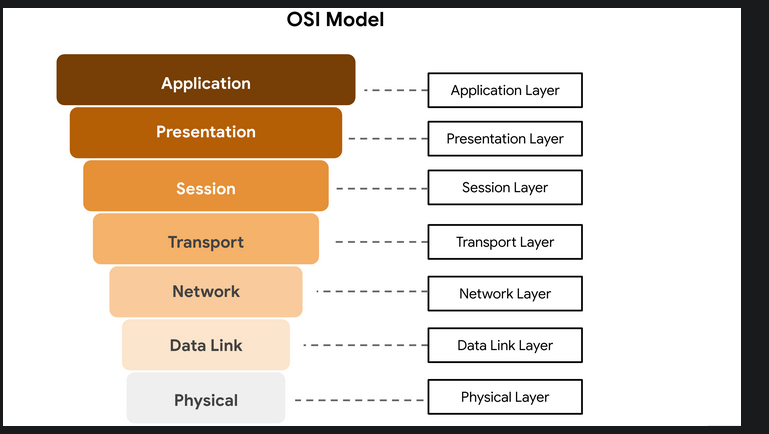
**Capa 4 – Transporte** Asegura que los datos lleguen correctamente, dividiéndolos en segmentos. Usa **TCP (confiable)** y **UDP (rápido pero no confiable)**.

**Capa 3 – Red** Determina la mejor ruta para enviar datos entre redes diferentes. Usa **direcciones IP** y **routers**.

**Capa 2 – Enlace de datos** Se encarga de enviar datos dentro de la misma red local. Usa **conmutadores, tarjetas de red** y protocolos como **HDLC** o **NCP**.

**Capa 1 – Física** Transmite los bits (0 y 1) a través de cables, conectores y hardware como **módems y hubs**.

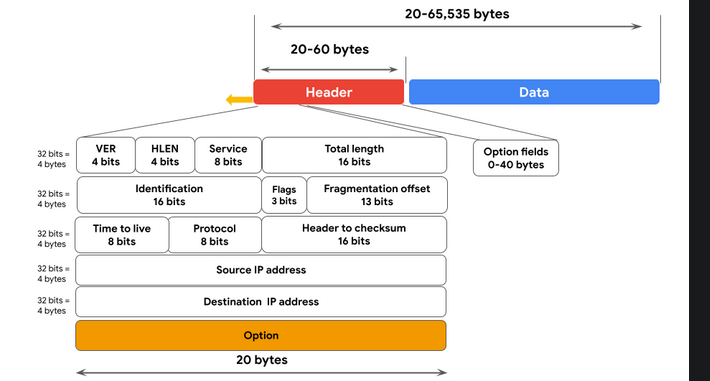
El Modelo TCP/IP contiene cuatro capas y el modelo OSI, siete.



**¿De qué manera está formada un IP?**

El formato del Encabezado IPv4 viene determinado por el protocolo IPv4 e incluye la información de enrutamiento IP que los dispositivos utilizan para dirigir el Paquete. El tamaño del encabezado IPv4 oscila entre 20 y 60 bytes. Los primeros 20 bytes son un conjunto fijo de información que contiene datos como la dirección IP de origen y destino, la longitud de la cabecera y la longitud total del paquete. El último conjunto de bytes puede oscilar entre 0 y 40 y está formado por el campo de opciones.

La longitud de la sección de Datos de un paquete IPv4 puede variar mucho en tamaño. Sin embargo, el tamaño máximo posible de un paquete IPv4 es de 65.535 bytes. Contiene el mensaje que se transfiere por Internet, como la información de un sitio web o el texto de un correo electrónico.



Hay 13 campos dentro del Encabezado de un paquete IPv4:

* **Versión (VER):** Este componente de 4 bits indica a los dispositivos receptores qué protocolo está utilizando el paquete. El paquete utilizado en la ilustración anterior es un paquete IPv4.
* **Longitud del Encabezado IP (HLEN o IHL):** HLEN es la longitud del encabezado del paquete. Este valor indica dónde termina el encabezado del paquete y dónde comienza el segmento de datos.
* **Tipo de servicio (ToS):** Los routers priorizan la entrega de paquetes para mantener la calidad del servicio en la red. El Campo ToS proporciona al router esta Información.
* **Longitud total:** Este campo comunica la longitud total de todo el paquete IP, incluyendo la cabecera y los datos. El tamaño máximo de un paquete IPv4 es de 65.535 bytes.

Cuando los paquetes se dividen pasará lo siguiente:

* **Identificación:** Los paquetes IPv4 pueden tener hasta 65, 535 bytes, pero la mayoría de las redes tienen un límite menor. En estos casos, los paquetes se dividen, o fragmentan, en paquetes IP más pequeños. El campo de identificación proporciona un identificador Único para todos los fragmentos del paquete IP original, de forma que puedan ser reensamblados una vez que lleguen a su destino.
* **Banderas:** Este Campo proporciona al dispositivo de enrutamiento más información sobre si el paquete original ha sido fragmentado y si hay más fragmentos en tránsito.
* **Desplazamiento de fragmentación:** El campo de offset de fragmentación indica a los dispositivos de encaminamiento a qué parte del paquete original pertenece el fragmento.

* **Tiempo de vida (TTL** ): El TTL impide que los paquetes de datos sean reenviados por los routers indefinidamente. Contiene un contador que establece la fuente. El contador se decrementa en uno a medida que pasa por cada router a lo largo de su ruta de acceso. Cuando el contador TTL llega a cero, el router que tiene el paquete en ese momento lo descarta y devuelve al remitente un mensaje de error ICMP Time Exceeded.
* **Protocolo:** El campo de protocolo indica al dispositivo receptor qué protocolo se utilizará para la parte de datos del paquete.
* **Suma de comprobación del encabezado:** El campo de suma de comprobación de encabezado contiene una suma de comprobación que puede utilizarse para detectar la corrupción del encabezado IP en tránsito. Los paquetes corruptos se descartan.
* **Dirección IP de origen:** La dirección IP de origen es la dirección IPv4 del dispositivo emisor.
* **Dirección IP de destino:** La dirección IP de destino es la dirección IPv4 del dispositivo de destino.
* **Opciones:** El campo de opciones permite aplicar opciones de Seguridad al Paquete si el valor HLEN es superior a cinco. El Campo comunica estas opciones a los dispositivos de enrutamiento.

**Diferencias IPV4 e IPV6**

Las direcciones IPv4 se componen de cuatro números decimales separados por puntos, cada número va de 0 a 255.

Permiten hasta 4.300 millones de direcciones posibles.

Las direcciones IPv6 están formadas por ocho números hexadecimales separados por dos puntos, cada número consta de hasta cuatro dígitos hexadecimales. Juntos, todos los números abarcan 16 bytes y permiten hasta 340 undecilillones de direcciones (340 seguidos de 36 ceros). Un ejemplo de dirección IPv6 sería: 2002:0db8:0000:0000:0000:ff21:0023:1234.

Existen algunas diferencias de Seguridad importantes entre IPv4 e IPv6. IPv6 ofrece un enrutamiento más eficaz y elimina las colisiones de direcciones privadas que pueden producirse en IPv4 cuando dos dispositivos de la misma red intentan utilizar la misma dirección.

**Module 2 Course 3**

Un **protocolo** de red es un conjunto de reglas utilizadas por dos o más dispositivos de una red para describir el orden de entrega y la estructura de los datos.

Los protocolos de red sirven como instrucciones que acompañan a la información del paquete de datos.

Algunos protocolos tienen vulnerabilidades que los actores maliciosos explotan.

Los protocolos de red pueden dividirse en tres categorías principales: protocolos de comunicación, protocolos de gestión y protocolos de seguridad.

**Protocolos de comunicación**

Los protocolos de comunicación rigen el intercambio de información en la transmisión por red.

El **Protocolo de control de transmisión (TCP** ) es un protocolo de comunicación de Internet que permite que dos dispositivos formen una conexión y transmitan datos.

**Funcionamiento de los paquetes mediante el protocolo TCP**

En primer lugar, el dispositivo envía una solicitud de sincronización (SYN) a un servidor. A continuación, el servidor responde con un paquete SYN/ACK para acusar recibo de la solicitud del dispositivo. Una vez que el servidor recibe el último paquete ACK del dispositivo, se establece una conexión TCP.

El **Protocolo de Datagramas de Usuario (UDP)** es un protocolo no orientado a la conexión que no establece una conexión entre dispositivos antes de una transmisión.

Por ejemplo, un uso de UDP es para enviar solicitudes DNS a servidores DNS locales.

El Protocolo **de transferencia de hipertexto (HTTP)** es un protocolo de capa de aplicación que proporciona un método de comunicación entre clientes y servidores de sitios web. HTTP utiliza el puerto 80. HTTP se considera inseguro, por lo que está siendo sustituido en la mayoría de los sitios web por una versión segura, denominada HTTPS que utiliza la encriptación de SSL/TLS para la comunicación.

El **sistema de nombres de dominio (DNS)** es un protocolo que traduce los nombres de dominio de Internet en direcciones IP. Cuando una computadora de cliente desea acceder al dominio de un sitio web utilizando su navegador de Internet, se envía una consulta a un servidor DNS dedicado. El servidor DNS busca entonces la dirección IP que corresponde al dominio del sitio web. DNS utiliza normalmente UDP en el puerto 53.

**Protocolos de gestión**

Los protocolos de gestión se utilizan para supervisar y gestionar la actividad en una red.

El **Protocolo simple de administración de red (SNMP)** es un protocolo de red utilizado para supervisar y gestionar los dispositivos de una red. SNMP puede restablecer una contraseña en un dispositivo de red o cambiar su configuración base.

El **Protocolo de mensajes de control de Internet (ICMP)** es un protocolo de Internet utilizado por los dispositivos para informarse mutuamente de los errores de transmisión de datos a través de la red. El ICMP es utilizado por un dispositivo receptor para enviar un informe al dispositivo emisor sobre la transmisión de datos.

La emisión del comando "ping" en un sistema operativo Linux.

### **Protocolos de Seguridad**

Los protocolos de Seguridad son protocolos de red que garantizan que los datos se envían y reciben de forma segura a través de una red.

Los protocolos de Seguridad utilizan algoritmos de encriptación para proteger los datos en tránsito.

**Protocolo seguro de transferencia de hipertexto (HTTPS** ) es un protocolo de red que proporciona un método seguro de comunicación entre clientes y servidores de sitios web.

HTTPS utiliza la encriptación secure sockets layer/transport layer security (SSL/TLS) en todas las transmisiones para que los actores maliciosos no puedan leer la información contenida. HTTPS utiliza el puerto 443.

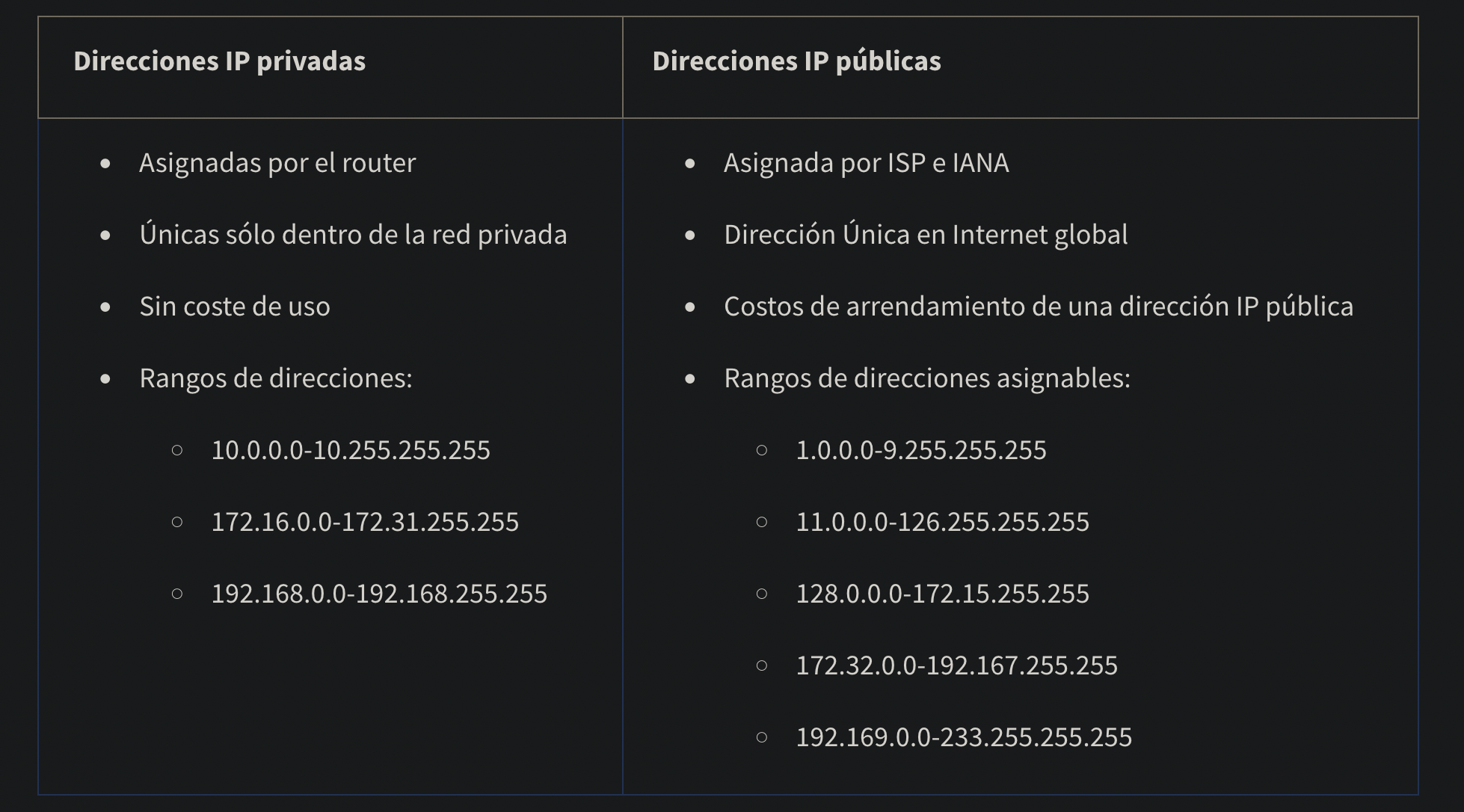
SFTP se utiliza a menudo con el almacenamiento en la nube.

La Autoridad de Números Asignados en Internet (IANA) asigna números de puerto a algunos protocolos.

Para que los dispositivos con direcciones IP privadas puedan comunicarse con la Internet pública, necesitan tener una única dirección IP pública que represente a todos los dispositivos de la LAN ante el público.

Para los mensajes salientes, el router puede sustituir una dirección IP de origen privada por su dirección IP pública y realizar la operación inversa para las respuestas.

Este proceso se conoce como traducción de direcciones de red (NAT) se necesita tener el router configurado para que pueda hacer eso.



El Protocolo de configuración dinámica de host (DHCP) pertenece a la familia de protocolos de red de gestión. DHCP es un protocolo de capa de aplicación que se utiliza en una red para configurar dispositivos.

Funciona con el router para asignar una dirección IP Única a cada dispositivo y proporcionar las direcciones del servidor DNS y de la puerta de enlace predeterminada adecuados para cada dispositivo.

Los servidores DHCP operan en el puerto UDP 67 mientras que los clientes DHCP lo hacen en el puerto UDP 68.

## **Protocolo de resolución de direcciones**

Por eso es necesario el protocolo de resolución de direcciones (ARP). ARP es principalmente un protocolo de la capa de acceso a la red en el Modelo TCP/IP que se utiliza para traducir las direcciones IP que se encuentran en los paquetes de datos a la dirección MAC del dispositivo de hardware.

Cada dispositivo de la red ejecuta ARP y mantiene un registro de las direcciones IP y MAC coincidentes en un caché ARP.

## **Telnet**

Telnet es un protocolo de capa de aplicación que se utiliza para conectar con un sistema remoto.

Telnet puede utilizarse para conectarse a dispositivos locales o remotos y utiliza el puerto TCP 23.

**SSH**

El protocolo Secure Shell (SSH) se utiliza para crear una conexión segura con un sistema remoto.

Proporciona una alternativa para la autenticación segura y la encriptación de la comunicación.

SSH funciona a través del puerto TCP 22 y es un sustituto de protocolos menos seguros, como Telnet.

## **Protocolo de oficina de correos**

El protocolo de oficina de correos (POP) es un protocolo de capa de aplicación (capa 4 del Modelo TCP/IP) utilizado para gestionar y recuperar correo electrónico de un servidor de correo.

Los dispositivos de los usuarios enviarán solicitudes al servidor de correo remoto y descargarán los mensajes de correo electrónico localmente.

La autenticación en texto plano sin cifrar utiliza el puerto TCP/UDP 110 y los correos electrónicos cifrados utilizan la Capa de sockets seguros/Seguridad de la capa de transporte (SSL/TLS) a través del puerto TCP/UDP 995.

Cuando se utiliza POP, el correo tiene que terminar de descargarse en un dispositivo local antes de poder ser leído. Después de descargarse, el correo puede o no borrarse del servidor de correo, por lo que no garantiza que un usuario pueda sincronizar el mismo correo electrónico en varios dispositivos.

## **Protocolo de acceso a mensajes de Internet (IMAP)**

IMAP se utiliza para el correo electrónico entrante. Descarga las cabeceras de los correos electrónicos y el contenido del mensaje.

El contenido también permanece en el servidor de correo electrónico, lo que permite a los usuarios acceder a su correo electrónico desde múltiples dispositivos.

IMAP utiliza el puerto TCP 143 para el correo electrónico no cifrado y el puerto TCP 993 a través del protocolo TLS. El uso de IMAP permite a los usuarios leer parcialmente el correo electrónico antes de que termine de descargarse.

## **Protocolo simple de transmisión de correo**

El Protocolo simple de transmisión de correo (SMTP) se utiliza para transmitir y encaminar el correo electrónico del remitente a la dirección del destinatario.

SMTP funciona con el software del Agente de Transferencia de Mensajes (MTA), que busca en los servidores DNS para resolver las direcciones de correo electrónico en direcciones IP, con el fin de garantizar que los correos electrónicos lleguen a su destino previsto.

SMTP utiliza el puerto TCP/UDP 25 para los correos electrónicos no cifrados y el puerto TCP/UDP 587 que utiliza TLS para los correos electrónicos cifrados.

Los firewalls pueden filtrar el Tráfico no deseado basándose en los números de puerto.



**Wi-Fi** hace referencia a un conjunto de Estándares que definen la comunicación para las LAN inalámbricas.

Los Estándares y protocolos Wi-Fi se basan en la familia 802.11 de estándares de comunicación de Internet determinados por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE).

### **Privacidad equivalente por cable**

La privacidad equivalente por cable (WEP) es un protocolo de seguridad inalámbrica diseñado para proporcionar a los usuarios el mismo nivel de privacidad en las conexiones de red inalámbricas que el que tienen en las conexiones de red por cable.

### **Acceso Wi-Fi protegido**

WPA siempre pretendió ser una medida transitoria para poder establecer la retrocompatibilidad con el hardware más antiguo.

Los fallos de WEP estaban en el propio protocolo y en cómo se utilizaba la encriptación.

Los atacantes pueden introducirse en el proceso de protocolo de enlace de autenticación WPA e insertar una nueva clave de encriptación en lugar de la dinámica asignada por WPA. Si establecen la nueva clave en todos ceros, es como si la transmisión no estuviera encriptada en absoluto.

**WPA2 (Wi-Fi Protected Access 2)**

Lanzado en 2004, WPA2 mejoró la seguridad Wi-Fi respecto a su predecesor (WPA) al incorporar el **Estándar de Encriptación Avanzada (AES)** y el protocolo **CCMP** para la autenticación e integridad de los mensajes. A pesar de ser considerado un estándar de seguridad robusto durante mucho tiempo, WPA2 es vulnerable a los ataques **KRACK (Key Reinstallation Attacks)**.

Existen dos modos principales de WPA2:

1. **WPA2 Personal:**
   * **Uso ideal:** Redes domésticas.
   * **Implementación:** Fácil y rápida configuración.
   * **Seguridad:** Utiliza una frase de contraseña global que se aplica a todos los dispositivos de la red.
   * **Limitación:** No es práctico para organizaciones grandes debido a la contraseña compartida.
2. **WPA2 Enterprise:**
   * **Uso ideal:** Aplicaciones empresariales.
   * **Seguridad:** Ofrece la seguridad necesaria para redes inalámbricas en entornos corporativos.
   * **Implementación:** Configuración inicial más compleja.
   * **Gestión:** Permite un control individualizado y centralizado del acceso Wi-Fi. Los administradores pueden conceder o revocar el acceso a usuarios específicos.
   * **Protección de claves:** Los usuarios nunca acceden directamente a las claves de encriptación, lo que impide su recuperación desde dispositivos individuales.

**WPA3 (Wi-Fi Protected Access 3)**

Desarrollado en 2018 como respuesta a las vulnerabilidades de WPA2 (especialmente KRACK), WPA3 está ganando adopción a medida que más dispositivos compatibles llegan al mercado. Sus diferencias y mejoras clave son:

* **Resistencia a KRACK:** Aborda la vulnerabilidad del protocolo de enlace de autenticación presente en WPA2.
* **Autenticación Simultánea de Iguales (SAE):** Utiliza SAE, un protocolo de acuerdo de autenticación de contraseñas y compartición de claves. Esto impide que los atacantes capturen datos de la red para intentar descifrarlos offline.
* **Encriptación más robusta:**
  + Ofrece encriptación de **128 bits** como estándar para contraseñas más seguras.
  + El modo **WPA3-Enterprise** ofrece una encriptación opcional de **192 bits**, proporcionando una capa adicional de seguridad para entornos empresariales.

**División en subredes y CID**

La **división en subredes** es la subdivisión de una red en grupos lógicos denominados subredes.

CIDR permite a los profesionales de la ciberseguridad segmentar las redes classful en trozos más pequeños.

El direccionamiento entre dominios sin clase (CIDR) es un método de asignación de máscaras de subred a direcciones IP para crear una subred. El direccionamiento sin clase sustituye al direccionamiento con clase.

Las direcciones IP CIDR tienen el mismo formato que las direcciones IPv4, pero incluyen una barra oblicua ("/'") seguida de un número al final de la dirección.

Ejemplo 192.168.100.0/24, engloba todas las IP entre 192.168.100.0 y 192.168.100.255.

La división en subredes permite a los profesionales y analistas de redes crear una red dentro de su propia red sin solicitar otra dirección IP de red a su proveedor de servicios de Internet. Este proceso utiliza el ancho de banda de la red de forma más eficiente y mejora el rendimiento de la red. La división en subredes es uno de los componentes de la creación de subredes aisladas mediante el aislamiento físico, la configuración del enrutamiento y los firewalls.

PROXIES/ VPN/ FIREWALL

Un servidor proxy es otra forma de añadir Seguridad a su red privada. Los servidores proxy utilizan la traducción de direcciones de red (NAT) para servir de barrera entre los clientes de la red y las amenazas externas.

Los proxies directos gestionan las consultas de los clientes internos cuando acceden a Recursos externos a la red.

Los proxies inversos funcionan de forma opuesta a los proxies directos; gestionan las peticiones de sistemas externos a servicios de la red interna.

Por ejemplo, puede crear filtros para bloquear los sitios web identificados por contener software malicioso.

**VPN**

Una VPN es un servicio que encripta Datos en tránsito y disfraza su dirección IP. Las VPN utilizan un proceso llamado Encapsulación. La encapsulación envuelve sus datos no cifrados en un paquete de datos cifrados.

Permite que sus datos se envíen a través de la red pública permaneciendo en el anonimato.

**Firewall**

Los cortafuegos son dispositivos de seguridad de red, ya sean virtuales (NVA) o físicos, que examinan el tráfico de red y lo filtran antes de permitir su acceso a una red privada.

Existen dos categorías principales de firewalls.

* **Sin estado:** Una clase de firewall que funciona basándose en reglas predefinidas y no realiza un seguimiento de la información de los paquetes de datos
* **Con estado:** Una clase de firewall que hace un seguimiento de la información que pasa a través de él y filtra proactivamente las amenazas.

Los **Cortafuegos de Nueva Generación (NGFW)** representan la tecnología de protección más avanzada. Superan a los cortafuegos con estado al incluir características como la **inspección profunda de paquetes** (DPI), que examina los datos dentro de los paquetes para identificar amenazas, y sistemas de **prevención de intrusiones**. Los NGFW pueden inspeccionar el tráfico en la capa de aplicación y suelen ser conscientes de las aplicaciones específicas. A diferencia de los cortafuegos tradicionales que bloquean por IP y puerto, los NGFW pueden configurar reglas para permitir o bloquear tráfico basándose en la aplicación. Además, algunos NGFW ofrecen funcionalidades adicionales como sandboxing de malware, antivirus de red y filtrado de URL y DNS.

Las empresas utilizan las VPN de sitio a sitio en gran medida para extender su red a otras redes y ubicaciones. Esto es especialmente útil para las organizaciones que tienen muchas oficinas en todo el mundo.

IPSec se utiliza habitualmente en las VPN de sitio a sitio para crear un túnel cifrado entre la red principal y la red remota. Una desventaja de las VPN de sitio a sitio es lo complejas que pueden ser de configurar y gestionar en comparación con las VPN remotas.

## **VPN WireGuard frente a VPN IPSec**

WireGuard es un protocolo VPN de alta velocidad, con una encriptación avanzada, para proteger a los usuarios cuando acceden a Internet.

Está diseñado para ser sencillo de configurar y mantener.

WireGuard también es de código abierto, lo que facilita a los usuarios su implementación y depuración. Este protocolo es útil para procesos que requieren velocidades de descarga más rápidas, como la transmisión de contenidos de vídeo o la descarga de archivos de gran tamaño.

### **VPN IPSec**

IPSec es otro protocolo VPN que puede utilizarse para configurar VPN. La mayoría de los proveedores de VPN utilizan IPSec para encriptar y autenticar los paquetes de datos con el fin de establecer conexiones seguras y encriptadas. Muy compatible con sistemas del mercado.

Un protocolo VPN es similar a un protocolo de redes: Es un conjunto de reglas o instrucciones que determinarán cómo se mueven los datos entre los puntos finales. Existen dos tipos de VPN: de acceso remoto y de sitio a sitio. Las VPN de acceso remoto establecen una conexión entre un dispositivo personal y un servidor VPN y encriptan o desencriptan los datos intercambiados con un dispositivo personal. Las empresas utilizan las VPN de sitio a sitio en gran medida para extender su red a diferentes ubicaciones y redes. IPSec puede utilizarse para crear conexiones de sitio a sitio y WireGuard puede utilizarse tanto para conexiones de sitio a sitio como para conexiones de acceso remoto.

**Module 3 Course 3**

**Ataques de Interceptación de Red**: Funcionan capturando el tráfico de red para robar información o interferir en la transmisión. Los atacantes usan herramientas para "olfatear" (sniffing) los datos en tránsito, pudiendo ver información confidencial o incluso alterar el tráfico insertando código malicioso o modificando mensajes, como cambiar la cuenta de un destinatario en una transferencia bancaria. El curso profundizará en el sniffing malicioso, los ataques en ruta y los ataques de repetición.

**Ataques de Puerta Trasera**: Son puntos débiles intencionales dejados en sistemas por programadores o administradores para facilitar tareas, pero que también pueden ser explotados por atacantes para obtener acceso no autorizado. Los atacantes también pueden instalar sus propias puertas traseras tras una intrusión para asegurar un acceso persistente. Una vez dentro, pueden causar daños significativos como instalar malware, realizar ataques DoS (inundando la red con tráfico), robar información o modificar configuraciones de seguridad.

Posibles Impactos en una Organización: Los ataques de red pueden tener graves consecuencias:

* **Financieras**: Interrupciones operativas que impiden generar ingresos, costes de reparación de infraestructura, pagos de ransomware y gastos legales por filtración de datos de clientes.
* **Reputación**: Pérdida de confianza del público y de clientes si se hace público un ciberataque, llevando a la elección de competidores.
* **Seguridad Pública**: Ataques a redes gubernamentales o de infraestructuras críticas (eléctrica, agua, defensa) pueden poner en riesgo la seguridad y el bienestar de los ciudadanos. Los gobiernos están invirtiendo en ciberseguridad para contrarrestar estas amenazas.

**¿Qué es un analizador de protocolos de red?**

* Es una herramienta para capturar y analizar el tráfico de datos en una red.
* También se le llama sniffer de paquetes o analizador de paquetes.
* Se utiliza principalmente para investigar redes y detectar actividades sospechosas.

**Ejemplos de analizadores de protocolos de red comunes:**

* SolarWinds NetFlow Traffic Analyzer
* ManageEngine OpManager
* Azure Network Watcher
* Wireshark
* tcpdump

**Enfoque de esta lectura:**

* Se centrará exclusivamente en tcpdump.
* Lo aprendido sobre tcpdump se puede aplicar a otros analizadores.
* El objetivo es preparar a los analistas de ciberseguridad para defenderse de intrusiones en la red.
* En el futuro, se practicará la identificación de un ataque DoS en un registro de tcpdump.

**¿Qué es tcpdump?**

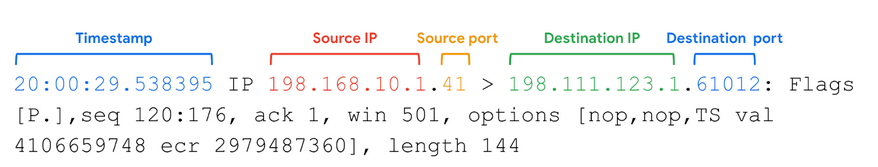
* Es un analizador de protocolos de red de línea de comandos.
* Es popular y ligero (bajo uso de memoria y CPU).
* Utiliza la biblioteca de código abierto libpcap.
* Es basado en texto (todos los comandos se ejecutan en la terminal).
* Se puede instalar en otros sistemas Unix como macOS.
* Está preinstalado en muchas distribuciones de Linux.

**¿Qué información proporciona tcpdump?**

* Ofrece un análisis breve de los paquetes.
* Convierte información clave del tráfico en formatos legibles.
* Imprime información sobre cada paquete directamente en la terminal.
* Muestra la dirección IP de origen.
* Muestra la dirección IP de destino.
* Muestra los números de puerto utilizados en las comunicaciones.

**Interpretación de la salida de tcpdump:**

* La salida se muestra como los paquetes capturados en la línea de comandos.
* Opcionalmente, se puede guardar en un archivo de registro.
* La captura de paquetes contiene información importante sobre el tráfico de la red.



Alguna de la información que recibe de una captura de paquetes incluye:

* **Marca** de tiempo: La salida comienza con la marca de tiempo, formateada como horas, minutos, segundos y fracciones de segundo.
* **IP** de origen: El origen del paquete lo proporciona su dirección IP de origen.
* **Puerto** de origen: Este número de puerto es donde se originó el paquete.
* **IP** de destino: La dirección IP de destino es hacia dónde se está transmitiendo el paquete.
* **Puerto de** destino: Este número de puerto es hacia donde se está transmitiendo el paquete.
* Establecer una línea de base para los patrones de tráfico de red y las métricas de utilización de la red.
* Detectar e identificar el tráfico malicioso
* Crear alertas personalizadas para enviar las notificaciones adecuadas cuando surjan problemas en la red o amenazas a la seguridad.
* Localizar la mensajería instantánea (MI), el tráfico o los puntos de acceso inalámbricos no autorizados.

Una **botnet** es una colección de computadoras infectadas por software malicioso que están bajo el control de un único agente de amenaza, conocido como "bot-herder" Cada computadora de la botnet puede ser controlada a distancia para enviar un paquete de datos a un sistema objetivo.

# **Visión general de las tácticas de interceptación**

Este texto explica cómo los ataques de interceptación, que involucran el sniffing de paquetes (captura e inspección de datos en la red) y la suplantación de IP (falsificación de direcciones IP y MAC), son utilizados por hackers.

Sniffing de paquetes: Se detalla cómo las tarjetas de interfaz de red (NIC) pueden configurarse en modo promiscuo para capturar todo el tráfico, permitiendo a los atacantes obtener información sensible o direcciones para la suplantación.

Suplantación de IP: Tras el sniffing, los atacantes pueden hacerse pasar por dispositivos autorizados. Los firewalls pueden mitigar esto rechazando tráfico no autorizado.

Se describen tres ataques específicos:

Ataque en ruta (Man-in-the-Middle): El atacante intercepta la comunicación entre dos entidades de confianza para robar información (como credenciales) o manipular búsquedas DNS, redirigiendo a sitios maliciosos. La encriptación (TLS) es la principal defensa.

Ataque Smurf: Se combina la suplantación de IP con una técnica DoS. El atacante suplanta la IP de una víctima y envía paquetes (a menudo pings ICMP) a la dirección de broadcast de la red, inundando a todos los dispositivos y causando una denegación de servicio. Los firewalls avanzados con detección de anomalías son clave para la protección.

Ataque DoS (Denegación de Servicio): A diferencia de la suplantación de IP, el atacante envía paquetes legítimos (con su dirección IP real) para sobrecargar el sistema objetivo e impedir su funcionamiento normal. La encriptación estándar es una defensa importante en múltiples niveles.

**Denial of service attack (DoS)**

Definition

A network attack that targets a network or server and floods it with network traffic

**Distributed denial of service attack (DDoS)**

Definition

A type of denial or service attack that uses multiple devices or servers in different locations to flood the target network with unwanted traffic

**SYN flood attack**

Definition

A type of DoS attack that simulates a TCP/IP connection and floods a server with SYN packets.

**Packet sniffing**

Definition

The practice of capturing and inspecting data packets across a network

**IP spoofing**

Definition

A network attack performed when an attacker changes the source IP of a data packet to impersonate an authorized system and gain access to a network

**On-path attack**

Definition

An attack where a malicious actor places themselves in the middle of an authorized connection and intercepts or alters the data in transit.

**Module 4 Course 3**

Este contenido aborda el tema de los ataques de fuerza bruta y las técnicas de endurecimiento del sistema operativo (OS) para prevenir dichos ataques. Se discuten los tipos de ataques, la evaluación de vulnerabilidades, y las medidas de prevención que las organizaciones pueden implementar.

- Los ataques de fuerza bruta son intentos sistemáticos para adivinar contraseñas y credenciales de acceso, utilizando métodos como ataques simples y ataques de diccionario.

- Las máquinas virtuales (VM) permiten ejecutar software en un entorno aislado, ofreciendo seguridad adicional y facilitando la evaluación de vulnerabilidades antes de un ataque real.

- Los espacios aislados, o "sandboxing", son entornos de prueba para evaluar software sospechoso sin riesgo para la red principal.

- Las medidas preventivas incluyen el uso de técnicas de hashing y salting para proteger contraseñas, la implementación de autenticación de múltiples factores (MFA) y de dos factores (2FA), y el uso de sistemas CAPTCHA para prevenir intentos automatizados de acceso.

- Las políticas de contraseñas establecen directrices para la creación y manejo de contraseñas seguras en una organización.

Conclusiones clave: Los ataques de fuerza bruta son amenazantes, pero mediante una combinación de técnicas de seguridad y buenas prácticas, las organizaciones pueden protegerse eficazmente. La evaluación constante de vulnerabilidades y la implementación de medidas de autenticación robustas son esenciales para salvaguardar la información sensible.

El curso "Aplicaciones de Seguridad de red" en Coursera aborda estrategias para endurecer la seguridad de las redes, presentando diversas herramientas y tecnologías utilizadas por analistas de seguridad.

- El endurecimiento de la red implica implementar dispositivos y estrategias que protejan y fortalezcan la seguridad de la misma.

- La defensa en profundidad consiste en añadir capas de seguridad para alcanzar un nivel de protección deseado.

- Se introducen cuatro dispositivos clave en la protección de redes: cortafuegos, sistemas de detección de intrusiones (IDS), sistemas de prevención de intrusiones (IPS) y sistemas de administración de información y eventos de seguridad (SIEM).

- Los cortafuegos regulan el tráfico de datos según reglas específicas y son fundamentales para cualquier sistema.

- El IDS supervisa el tráfico en busca de intrusiones basadas en firmas conocidas, aunque no puede detener ataques.

- El IPS proporciona una protección superior al detectar y bloquear intrusiones activamente, aunque su operación en línea puede presentar riesgos.

- Los dispositivos de captura de paquetes registran datos transmitidos en la red, útiles para la investigación de alertas.

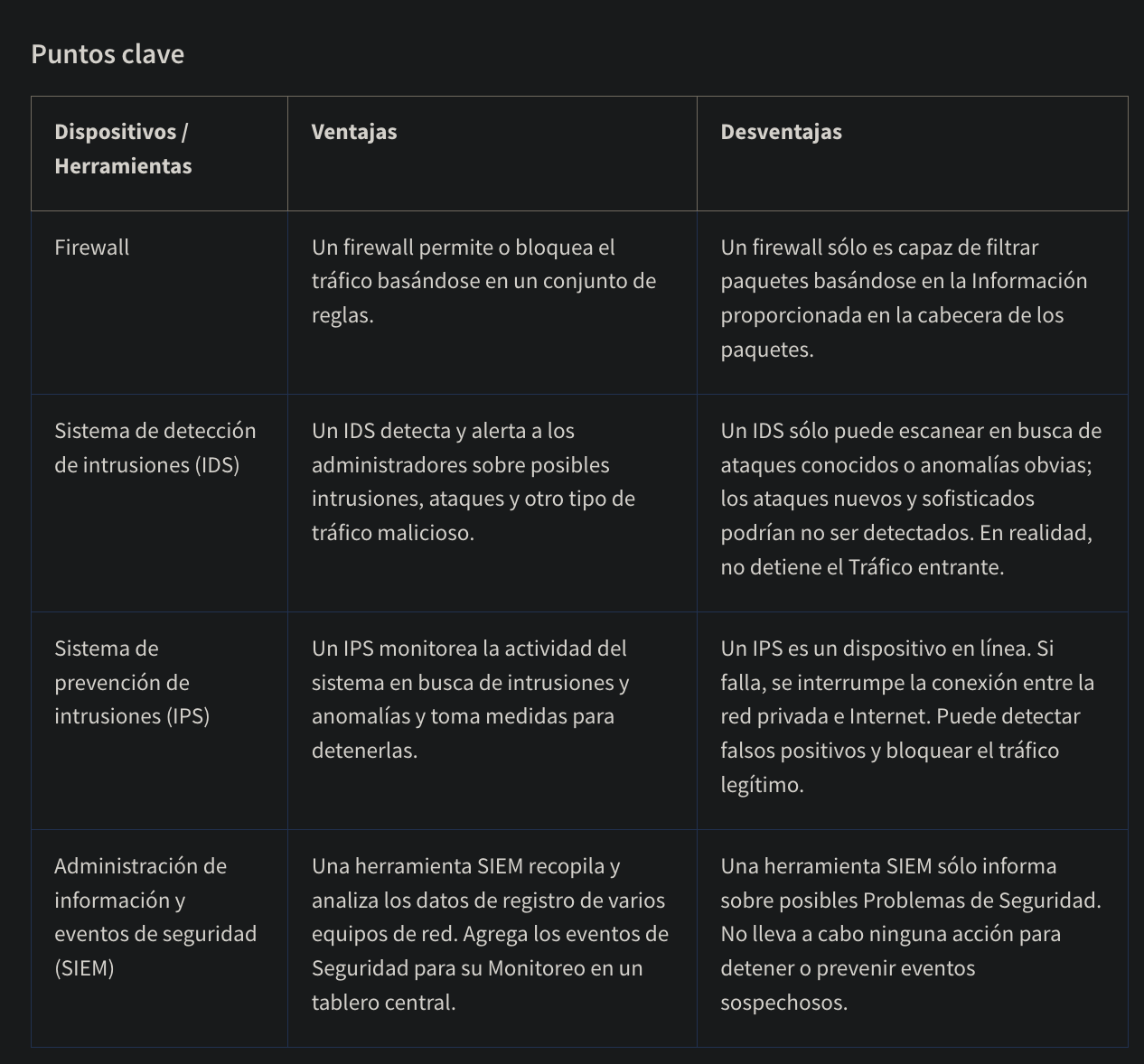
- Las herramientas SIEM agregan y analizan eventos de seguridad en tiempo real, permitiendo un monitoreo efectivo, aunque no sustituyen la experiencia de analistas de seguridad.

Puntos clave:

- Cada dispositivo ofrece ventajas específicas, pero también tiene limitaciones.

- La implementación de herramientas y la necesidad de personal adicional representan costos considerables.

- La selección del nivel de seguridad adecuado debe equilibrar costos y riesgos organizacionales.

****

Aquí tienes un **resumen claro y estructurado** sobre el tema **"Seguridad de la Nube"**:

### **Resumen: Seguridad de la Nube**

La adopción de servicios en la nube aporta ventajas como la escalabilidad, el ahorro de costes y la rápida implementación, pero también introduce desafíos únicos de seguridad que deben ser gestionados cuidadosamente.

#### **1. Gestión de identidad y acceso (IAM)**

IAM permite controlar quién accede a qué recursos y con qué permisos. Una configuración incorrecta de roles puede otorgar privilegios innecesarios, aumentando el riesgo de accesos no autorizados.

#### **2. Configuración**

La configuración precisa es clave para mantener la seguridad y el cumplimiento. Los errores durante migraciones o la configuración incorrecta de servicios en la nube son causas frecuentes de brechas de seguridad.

#### **3. Superficie de ataque**

Cada nuevo servicio o aplicación en la nube amplía la superficie de ataque. Aunque los CSP suelen implementar buenas prácticas de seguridad, es vital que las organizaciones diseñen sus redes minimizando los puntos de entrada vulnerables.

#### **4. Ataques de día cero**

Son exploits desconocidos previamente. Los CSP están mejor posicionados para detectarlos y aplicar parches rápidamente, migrando cargas de trabajo y protegiendo a sus clientes sin interrupciones significativas.

#### **5. Visibilidad y seguimiento**

Los CSP ofrecen herramientas como registros de flujo y duplicación de paquetes para supervisar la red. Sin embargo, las organizaciones pierden cierto nivel de control directo sobre la infraestructura, lo cual puede generar inquietudes de visibilidad.

#### **6. Evolución constante de la nube**

Las actualizaciones frecuentes por parte de los CSP requieren que las organizaciones adapten sus procesos y configuraciones. Aunque los CSP mejoran sus servicios constantemente, esto añade complejidad al mantenimiento de la seguridad.

#### **7. Modelo de Responsabilidad Compartida**

El CSP es responsable de proteger la infraestructura subyacente (centros de datos, hardware, hipervisores). La organización usuaria es responsable de proteger sus propios datos, aplicaciones y configuraciones. Confusiones en este modelo pueden generar brechas de seguridad evitables.

En resumen, **la seguridad en la nube exige una gestión activa, una configuración precisa y una comprensión clara del modelo de responsabilidad compartida** entre el proveedor y la organización usuaria.

### **Resumen: Endurecimiento de Seguridad de la Nube**

El endurecimiento de la seguridad de la nube implica aplicar técnicas y herramientas para proteger los recursos e infraestructuras en entornos de nube. Las principales prácticas incluyen:

* **Gestión de acceso e identidad (IAM):** Controla quién accede a qué recursos y cómo. Es fundamental para proteger identidades digitales y garantizar un acceso autorizado a los servicios en la nube.
* **Hipervisores:** Son plataformas que permiten ejecutar máquinas virtuales. Los hipervisores tipo uno, como VMware ESXi, son usados por proveedores de servicios en la nube (CSP). Las vulnerabilidades pueden provocar escapes de máquina virtual (VM escape), por lo que su seguridad es crítica.
* **Líneas de base:** Definen configuraciones estándar para el entorno de nube, permitiendo detectar cambios no autorizados. Incluyen restricciones de acceso, gestión de contraseñas, encriptación de archivos y servicios de detección de amenazas.
* **Criptografía en la nube:** Protege la confidencialidad e integridad de los datos mediante cifrado. Se basa en claves criptográficas seguras para proteger datos en tránsito y en reposo.
* **Borrado criptográfico:** Técnica para destruir claves de cifrado, volviendo los datos ininteligibles e irrecuperables sin la clave, útil al eliminar datos en la nube.
* **Gestión de claves:** Requiere asegurar las claves criptográficas mediante tecnologías como TPM y CloudHSM. Los clientes pueden usar sus propias claves, siendo responsables de su protección, mientras que el proveedor se encarga de la infraestructura subyacente (modelo de responsabilidad compartida).

Estas prácticas son esenciales para reforzar la postura de seguridad de las organizaciones en entornos de nube pública y proteger eficazmente los datos sensibles.

**Module 1 Course 4**

Este contenido ofrece una comparación de varios sistemas operativos comúnmente utilizados, destacando sus características, vulnerabilidades y la importancia de mantenerse actualizado.

- Los sistemas operativos populares incluyen Windows, macOS, Linux, ChromeOS, Android e iOS, cada uno con diferentes niveles de acceso al código y aplicaciones.

- Windows y macOS son sistemas operativos para computadoras personales y son en su mayoría de código cerrado, mientras que Linux es completamente de código abierto y permite colaboraciones comunitarias.

- ChromeOS, derivado de Chromium OS, se utiliza principalmente en educación y combina elementos de código abierto y cerrado.

- Android e iOS son para dispositivos móviles, donde Android es de código abierto y iOS tiene componentes de código abierto parcial.

- Todos los sistemas operativos enfrentan vulnerabilidades de seguridad, especialmente los sistemas heredados que no reciben actualizaciones y pueden quedar expuestos a nuevas amenazas.

- Es esencial que los analistas de seguridad comprendan las implicaciones de los sistemas operativos heredados y los riesgos asociados a su uso.

**Puntos clave:**

**-** Familiaridad con los sistemas operativos es crucial para los analistas de seguridad.

- La actualización constante de sistemas operativos es vital para mantener su seguridad.

Esta lectura del curso de Coursera aborda cómo los sistemas operativos (OS) gestionan las solicitudes de los usuarios mediante un proceso estructurado. Se examinan las funciones del BIOS y UEFI, el ciclo de tareas del usuario a la aplicación, del OS al hardware, y la analogía entre el funcionamiento de una computadora y un restaurante.

- Los sistemas operativos son fundamentales para conectar aplicaciones y hardware, permitiendo a los usuarios realizar tareas efectivas.

- Al iniciar una computadora, el BIOS o UEFI proporcionan instrucciones de carga, siendo UEFI el estándar más moderno con características de seguridad mejoradas.

- La finalización de una tarea en una computadora sigue un proceso secuencial: el usuario inicia la solicitud, la aplicación procesa la solicitud, el sistema operativo interpreta y comunica la solicitud al hardware, que completa la tarea.

- Se utiliza una analogía entre el uso de aplicaciones y hacer un pedido en un restaurante, donde el OS actúa como la cocina que procesa las solicitudes.

- Un ejemplo de cómo funciona el OS es el proceso para descargar un archivo desde un navegador, mostrando la comunicación entre el usuario, la aplicación y el hardware.

**Puntos clave:**

**-** El sistema operativo opera en segundo plano, pero es esencial para el uso eficiente de las computadoras.

- Se destaca la importancia de comprender el funcionamiento de los sistemas operativos para mejorar la seguridad, dado que todos enfrentan vulnerabilidades.

****

La lectura sobre tecnología de virtualización en Coursera se centra en el concepto de máquinas virtuales (VM) y su importancia en la gestión de sistemas operativos. A continuación se presentan los principales puntos tratados en el contenido.

- \*\*Definición de máquina virtual\*\*Una máquina virtual es una representación virtual de una computadora física que simula el hardware a través de software, permitiendo que múltiples VMs se ejecuten en una sola computadora.

- \*\*Funcionamiento y recursos\*\*Las máquinas virtuales comparten los recursos físicos de la computadora anfitriona, como la memoria RAM, permitiendo operar varios sistemas operativos simultáneamente en un entorno controlado.

- \*\*Beneficios de la virtualización\*\*: La virtualización mejora la seguridad mediante el aislamiento de tareas en entornos separados, así como la eficiencia en el manejo de recursos, facilitando la ejecución de múltiples aplicaciones y pruebas.

- \*\*Importancia en seguridad\*\*La virtualización es clave en el campo de la seguridad informática, al proporcionar entornos aislados donde se pueden analizar amenazas sin riesgo para la computadora anfitriona.

- \*\*Gestión de máquinas virtuales\*\*Las máquinas virtuales se administran con hipervisores, software que permite gestionar las VMs y asignar los recursos entre ellas, destacando el hipervisor KVM, integrado en Linux.

- \*\*Otras formas de virtualización\*\*Existen tecnologías de virtualización que no requieren sistemas operativos, como la creación de servidores y redes virtuales a partir de hardware físico existente.

\*\*Conclusiones clave\*\*La tecnología de virtualización es esencial para optimizar el uso de hardware y mejorar la seguridad, permitiendo un manejo eficiente de diferentes entornos informáticos. Sin embargo, se deben considerar los riesgos asociados, como la posibilidad de que el software malicioso escape de las VMs.  
La línea de comandos en uso es un segmento del curso que compara las interfaces gráficas de usuario (GUI) y las interfaces de línea de comandos (CLI) en el contexto de la ciberseguridad. En este texto, se analizan las diferencias y ventajas de cada interfaz.

- Las GUI utilizan iconos y gráficos en la pantalla, mientras que las CLI se basan únicamente en texto, mostrando líneas de código.

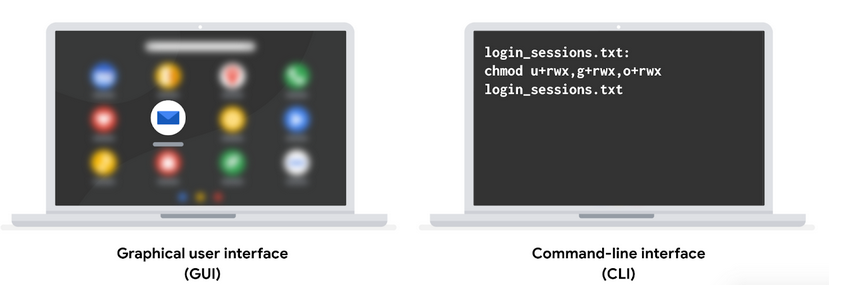
- Una GUI permite realizar una sola petición a la vez, en contraste con las CLI que pueden manejar múltiples peticiones simultáneamente.

- Para los analistas de seguridad, la CLI es ventajosa por su rapidez y eficiencia en la realización de tareas complejas.

- El historial de comandos en una CLI permite un seguimiento efectivo de las acciones, lo cual es fundamental durante incidentes de seguridad y para verificar acciones realizadas.

- Familiarizarse con ambas interfaces es crucial para los profesionales de ciberseguridad, dado que cada una tiene sus propias aplicaciones y beneficios.

Conclusiones clave: Las GUI y las CLI son interfaces importantes en ciberseguridad, con la CLI preferida para tareas complejas por su capacidad de manejar múltiples acciones y por sus registros de historial útiles para auditorías y análisis.



La explicación de la arquitectura de Linux proporciona una visión detallada de los componentes esenciales que conforman este sistema operativo. Entender la organización de Linux es crucial para los analistas de seguridad, ya que facilita la comprensión de su funcionamiento.

- Usuario: El usuario interactúa con la computadora, iniciando y gestionando tareas. Linux es un sistema multiusuario, permitiendo que varios usuarios utilicen los recursos simultáneamente.

- Aplicaciones: Programas que realizan tareas específicas, algunas preinstaladas y otras instaladas mediante un administrador de paquetes.

- Shell: Intérprete de línea de comandos que traduce las órdenes del usuario al kernel y viceversa.

- Estándar de jerarquía del sistema de archivos (FHS): Organiza los datos en Linux, definiendo dónde se almacenan los archivos y directorios.

- Kernel: Componente que gestiona procesos y memoria, controlando el hardware y comunicándose con las aplicaciones.

- Hardware: Componentes físicos de la computadora, clasificados como periféricos (no esenciales) e internos (esenciales para el funcionamiento).

**Distribuciones Linux**

La comprensión de la arquitectura de Linux, que incluye el usuario, las aplicaciones, el shell, el FHS, el kernel y el hardware, es fundamental para el correcto funcionamiento del sistema y la labor de los analistas de seguridad.

Kali Linux, Ubuntu, Parrot, Red Hat Enterprise Linux y AlmaLinux son distribuciones de Linux relevantes en ciberseguridad. Kali Linux, basada en Debian, destaca por sus numerosas herramientas preinstaladas para pruebas de penetración y análisis forense digital, actividades cruciales en seguridad. Ubuntu, también basado en Debian y de fácil uso con CLI y GUI, es popular en seguridad y computación en la nube, contando con gran soporte comunitario y acceso a herramientas de seguridad. Parrot, similar a Kali Linux y también basado en Debian, ofrece herramientas preinstaladas para seguridad y una GUI amigable. Red Hat Enterprise Linux, a diferencia de las anteriores, es una distribución de suscripción empresarial con soporte dedicado. Finalmente, AlmaLinux es una distribución comunitaria creada como reemplazo estable de CentOS, asegurando compatibilidad con aplicaciones y configuraciones de este último.

Un paquete de software es un componente que contiene los archivos necesarios para instalar una aplicación, incluyendo sus dependencias. Los administradores de paquetes son herramientas esenciales en Linux que facilitan la instalación, gestión y eliminación de estos paquetes, además de resolver problemas de dependencias. Es crucial utilizar las versiones más recientes de los paquetes por sus correcciones de errores y parches de seguridad.

Diferentes distribuciones de Linux utilizan administradores de paquetes específicos basados en su distribución madre. Por ejemplo, las distribuciones derivadas de Debian (como Ubuntu) utilizan administradores como dpkg y archivos .deb, mientras que las derivadas de Red Hat (como CentOS) usan RPM y archivos .rpm. Conocer esta relación es importante para la correcta instalación de aplicaciones.

El **shell** es el intérprete de la línea de comandos.

## **Tipos de shell**

Entre los diferentes tipos de shell de Linux se incluyen los siguientes:

* Bourne-Again Shell (bash)
* C Shell (csh)
* Shell Korn (ksh)
* Shell C mejorada (tcsh)
* Shell Z (zsh)

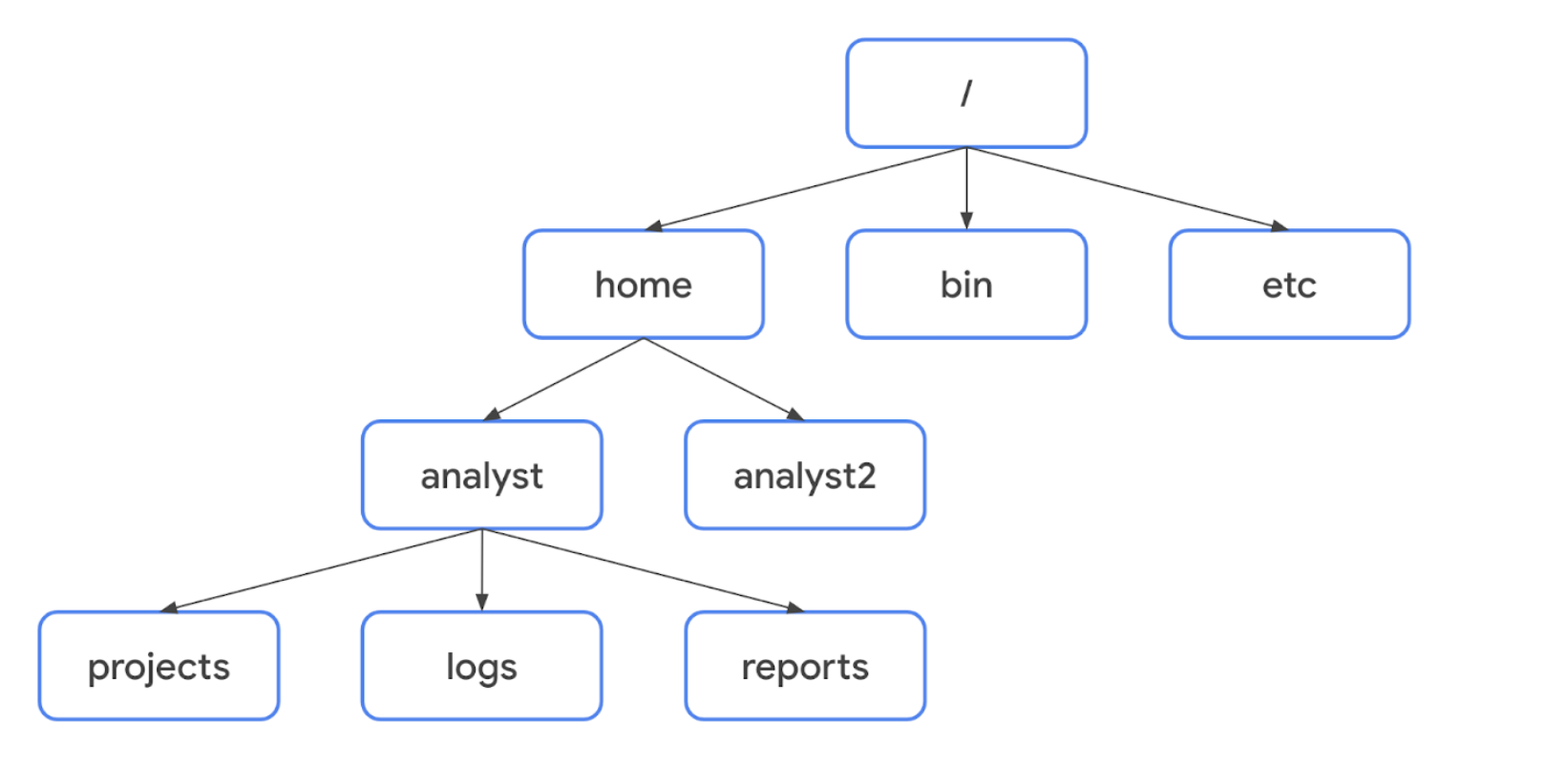
Todas las shell de Linux utilizan los comandos comunes de Linux, pero pueden diferir en otras características. Por ejemplo, ksh y Bash utilizan el signo del dólar (*$*) para indicar dónde teclea el usuario sus comandos. Otros shells, como zsh, utilizan el signo de porcentaje (*%*) para este propósito.

**Bash** es el shell por defecto en la mayoría de las distribuciones de Linux. Se considera un shell fácil de usar.

## **Estándar de jerarquía del sistema de archivos (FHS)**

Anteriormente, usted aprendió que el **Estándar de jerarquía del sistema de archivos** (FHS **)** es el componente de Linux que organiza los datos. El FHS es importante porque define cómo se organizan los directorios, el contenido de los directorios y otros tipos de almacenamiento en el sistema operativo.

Este diagrama ilustra la jerarquía de relaciones bajo el FHS:



Una **ruta de** archivo es la ubicación de un archivo o directorio.

El **directorio raíz** es el directorio de más alto nivel en Linux, y siempre se representa con una barra oblicua (*/*).

*/home*: Cada usuario del sistema tiene su propio directorio personal.

*/bin*: Este directorio significa "binario" y contiene archivos binarios y otros ejecutables.

*/etc*: Directorio que almacena los archivos de configuración del sistema.

*/tmp*: Este Directorio almacena muchos archivos temporales. El directorio */tmp* es utilizado habitualmente por los atacantes porque cualquier persona del sistema puede modificar los datos de estos archivos.

*/mnt*: Este Directorio significa "montar" y almacena soportes, como unidades USB y discos duros.

*man hier* para obtener más información sobre el FHS y sus directorios estándar.

La **ruta de archivo absoluta** es la ruta de archivo completa, que parte de la raíz. Por ejemplo, */home/analyst/projects* es una ruta de archivo absoluta. La **ruta de** archivo relativa es la ruta de archivo que parte del directorio actual de un usuario.

El comando *pwd* imprime en pantalla el directorio de trabajo.

Para saber cuál es su nombre de usuario, utilice el comando *whoami*.

El comando *cd* navega entre directorios.

El comando *cat* muestra el contenido de un archivo.

El comando *head* muestra sólo el principio de un archivo, por defecto 10 líneas.

El comando *tail* hace lo contrario que *head*. Este comando puede utilizarse para mostrar sólo el final de un archivo, por defecto 10 líneas.

El comando *less* devuelve el contenido de un archivo página a página.

El comando **grep** busca en un archivo especificado y devuelve todas las líneas del archivo que contengan una cadena o texto especificado.

Por ejemplo, si se introduce **grep** **OS** **updates.txt**, se obtendrán todas las líneas que contengan **OS** en el archivo **updates.txt**.

El comando **pipe** envía la salida estándar de un comando como entrada estándar a otro comando para su posterior procesamiento.

Por ejemplo, *ls /home/analyst/reports | grep users* devuelve los nombres de archivos y directorios del directorio *reports* que contienen *users*. Antes de la tubería, *ls* indica que se listen los nombres de los archivos y directorios en *reports*. Luego, envía esta salida al comando después de la tubería. En este caso, *grep users* devuelve todos los nombres de archivos o directorios que contienen *users* de la entrada que recibió.

El comando *find* busca directorios y archivos que cumplan los criterios especificados.

Cuando se utiliza *find*, el primer argumento después de *find* indica dónde empezar a buscar. Por ejemplo, si se introduce *find /home/analyst/projects*, se buscará todo a partir del directorio *projects*.

La diferencia entre estas dos opciones es que *-name* distingue entre mayúsculas y minúsculas, y *-iname* no. Para ello, escriba *find /home/analyst/projects -name "\*log\*"*. También podría introducir *find /home/analyst/projects -iname "\*log\*"*.

Cuando *-name* es la opción, los archivos con nombres que incluyan *Log* o *LOG*, por ejemplo, no se devolverán porque esta opción distingue entre mayúsculas y minúsculas. Sin embargo, sí se devolverán si la opción es *-iname*.

Para buscar archivos o directorios modificados por última vez en un periodo de tiempo determinado. Para esta búsqueda se puede utilizar la opción *-mtime.*

Al introducir *find /home/analyst/projects -mtime -3* se obtienen todos los archivos y directorios del directorio *projects* que se han modificado en los últimos tres días.

*-mtime* se basa en días, por lo que al introducir *-mtime +1* se indican todos los archivos o directorios modificados por última vez hace más de un día, y al introducir *-mtime -1* se indican todos los archivos o directorios modificados por última vez hace menos de un día.

*-mmin* en lugar de *-mtime* si se desea basar la búsqueda en minutos en lugar de días.

El comando *mkdir* crea un nuevo directorio. mkdir directory\_name

El comando *rmdir* elimina, o borra, un directorio. rmdir file\_name

El comando *touch y nano* crea un nuevo archivo. touch file\_name

nano file\_name

Comando *mv y cp.* Se utilizan para mover o copiar directorios.

mv route\_directory\_name route\_directory\_name\_destination

cp route\_directory\_name route\_directory\_name\_destination

Para escribir un archivo podemos usar echo “escribir” > file\_name y para sobreescribir en un archivo podemos usar el comando echo “escribir” >> file\_name

**Permisos Linux**

**-r:** Read

**-w:** Write

**-x:** Execute

**Donde se pueden aplicar los permisos:**

**-u:** User

**-g:** Group

**-o:** Other

**ls -la:** Mostrar archivos ocultos y permisos

**ls -l:** Mostrar archivos y permisos

**ls -l:** Mostrar archivos ocultos

Cambiar permisos:

chmod u+r, g+w, o-x file\_name (Aquí le ponemos permisos de lectura a un usuario, añadimos permisos de escritura al grupo y quitamos el permiso de ejecutar a otros.)

**Tabla permisos lectura, ejecución y escritura para usuarios, grupos y otros:**

| Carácter | Ejemplo | Significado |
| --- | --- | --- |
| 1º | **d**rwxrwxrwx | Tipo de archivo: |
|  |  | d para un directorio |
|  |  | - para un archivo regular |
| 2º | d**r**wxrwxrwx | Permisos de lectura para el usuario: |
|  |  | r si el usuario tiene permisos de lectura |
|  |  | - si el usuario carece de permisos de lectura |
| 3º | dr**w**xrwxrwx | Permisos de escritura para el usuario: |
|  |  | w si el usuario tiene permisos de escritura |
|  |  | - si el usuario carece de permisos de escritura |
| 4º | drw**x**rwxrwx | Permisos de ejecución para el usuario: |
|  |  | x si el usuario tiene permisos de ejecución |
|  |  | - si el usuario carece de permisos de ejecución |
| 5º | drwx**r**wxrwx | Permisos de lectura para el grupo: |
|  |  | r si el grupo tiene permisos de lectura |
|  |  | - si el grupo carece de permisos de lectura |
| 6º | drwxr**w**xrwx | Permisos de escritura para el grupo: |
|  |  | w si el grupo tiene permisos de escritura |
|  |  | - si el grupo carece de permisos de escritura |
| 7º | drwxrw**x**rwx | Permisos de ejecución para el grupo: |
|  |  | x si el grupo tiene permisos de ejecución |
|  |  | - si el grupo carece de permisos de ejecución |
| 8º | drwxrwx**r**wx | Permisos de lectura para otros: |
|  |  | r si el otro tipo de propietario tiene permisos de lectura |
|  |  | - si el otro tipo de propietario carece de permisos de lectura |
| 9º | drwxrwxr**w**x | Permisos de escritura para otro: |
|  |  | w si el otro tipo de propietario tiene permisos de escritura |
|  |  | - si el otro tipo de propietario carece de permisos de escritura |
| 10º | drwxrwxrw**x** | Permisos de ejecución para otro: |
|  |  | x si el otro tipo de propietario tiene permisos de ejecución |
|  |  | - si el otro tipo de propietario carece de permisos de ejecución |

| **Carácter** | **Descripción** |
| --- | --- |
| *u* | Indica que se realizarán cambios en los permisos de usuario |
| *g* | Indica que se realizarán cambios en los permisos de grupo |
| *o* | Indica que se realizarán cambios en otros permisos |
| *+* | Añade permisos al usuario, grupo u otro |
| *-* | Elimina permisos del usuario, grupo u otro |
| *=* | Asigna permisos al usuario, grupo u otro |

**Principio de privilegio mínimo:** Establece que un usuario, programa o proceso debe tener únicamente los derechos de acceso necesarios para realizar sus tareas específicas, y nada más.

Se recomienda utilizar ***sudo*** en Linux cuando necesite privilegios elevados.

**useradd**

El comando *useradd* añade un usuario al sistema. Para añadir un usuario con el nombre de usuario de *fgarcia* con *sudo*, introduzca *sudo useradd fgarcia*. Existen opciones adicionales que puede utilizar con *useradd*:

* *-g*: Establece el grupo por defecto del usuario, también llamado su grupo primario.
* *-G*: Añade al usuario a grupos adicionales, también llamados grupos suplementarios o secundarios.

Para utilizar la opción *-g*, el grupo primario debe especificarse después de *-g*. Por ejemplo, al introducir *sudo useradd -g security fgarcia* se añade *fgarcia* como nuevo usuario y se asigna que su grupo primario sea *security*.

Para utilizar la opción *-G*, el grupo suplementario debe pasarse al comando después de *-G*. Puede añadir más de un grupo suplementario a la vez con la opción *-G*. Al introducir *sudo useradd -G finance,admin fgarcia* se añade *fgarcia* como nuevo usuario y se añade a los grupos existentes *finance* y *admin*.

**usermod**

El comando *usermod* modifica las cuentas de usuario existentes. Las mismas opciones *-g* y *-G* del comando *useradd* pueden utilizarse con *usermod* si ya existe un usuario.

Por ejemplo, si introduce *sudo usermod -g executive fgarcia* cambiará el grupo primario de *fgarcia*por el grupo *executive*.

También necesita la opción *-a*, que añade el usuario a un grupo existente y sólo se utiliza con la opción *-G*. Por ejemplo, introduciendo *sudo usermod -a -G marketing fgarcia* añadiría el usuario existente *fgarcia* al grupo suplementario *marketing*.

El uso de *-a* con *-G* garantiza que se añadan los nuevos grupos pero que no se sustituyan los grupos existentes.

Existen otras opciones que puede utilizar con *usermod* para especificar cómo desea modificar el usuario, entre las que se incluyen:

* *-d*: Cambia el Directorio personal del usuario.
* *-l*: Cambia el nombre de usuario.
* *-L*: Bloquea la cuenta para que el usuario no pueda registrarse.

La opción siempre va después del comando *usermod*. Por ejemplo, para cambiar el directorio principal de *fgarcia*a */home/garcia\_f*, introduzca *sudo usermod -d /home/garcia\_f fgarcia*.

**userdel**

El comando *userdel* borra un usuario del sistema.

Introducir *sudo userdel -r fgarcia* eliminaría *fgarcia* como usuario y borraría todos los archivos de su directorio personal.

**usermod**

En lugar de borrar al usuario, podría considerar desactivar su cuenta con *usermod -L*.

### **chown**

El comando *chown* cambia la propiedad de un archivo o directorio. Puede utilizar *chown* para cambiar la propiedad del usuario o del grupo. Para cambiar el usuario propietario del archivo *access.txt* a *fgarcia*, introduzca *sudo chown fgarcia access.txt*. Para cambiar el propietario de grupo de *access.txt* a *security*, introduzca *sudo chown :security access.txt*. Debe introducir dos puntos (*:*) antes de *security* para designar como nombre de grupo.

### **man**

El comando *man* muestra información sobre otros comandos y su funcionamiento.

**apropos**

El comando *apropos* busca en las descripciones de las páginas de manual una cadena especificada.

También puede incluir la opción *-a* para buscar varias palabras. Por ejemplo, si introduce *apropos -a graph editor* obtendrá las páginas de manual que contengan las palabras "gráfico" y "editor" en sus descripciones.

### **qué es**

El comando *whatis* muestra la descripción de un comando en una sola línea.

**Module 4 Course 4**

**SQL Querys**

*SELECT*indica qué columnas devolver.

*FROM* indica qué tabla consultar.

*\** Indica todos los campos y columnas de la tabla

*ORDER BY*, escríbala al final de la consulta y especifique una columna en la que basar la ordenación.

SELECT customerid, city, country

FROM customers

ORDER BY country;

ORDER BY con la palabra clave DESC para ordenar en orden descendente.

SELECT customerid, city, country

FROM customers

ORDER BY customerid DESC;

También puede elegir varias columnas para ordenar. Por ejemplo, puede elegir primero la columna *country* y después la columna *city*.

SELECT customerid, city, country

FROM customers

ORDER BY country, city;

*SELECT* y *FROM* son palabras clave importantes en las consultas SQL. Se utiliza *SELECT* para indicar qué columnas devolver y *FROM* para indicar qué tabla consultar. También puede incluir *ORDER BY* en su consulta para organizar la salida.

*WHERE* indica la condición para un filtro.

SELECT firstname, lastname, title, email

FROM employees

WHERE title = 'IT Staff';

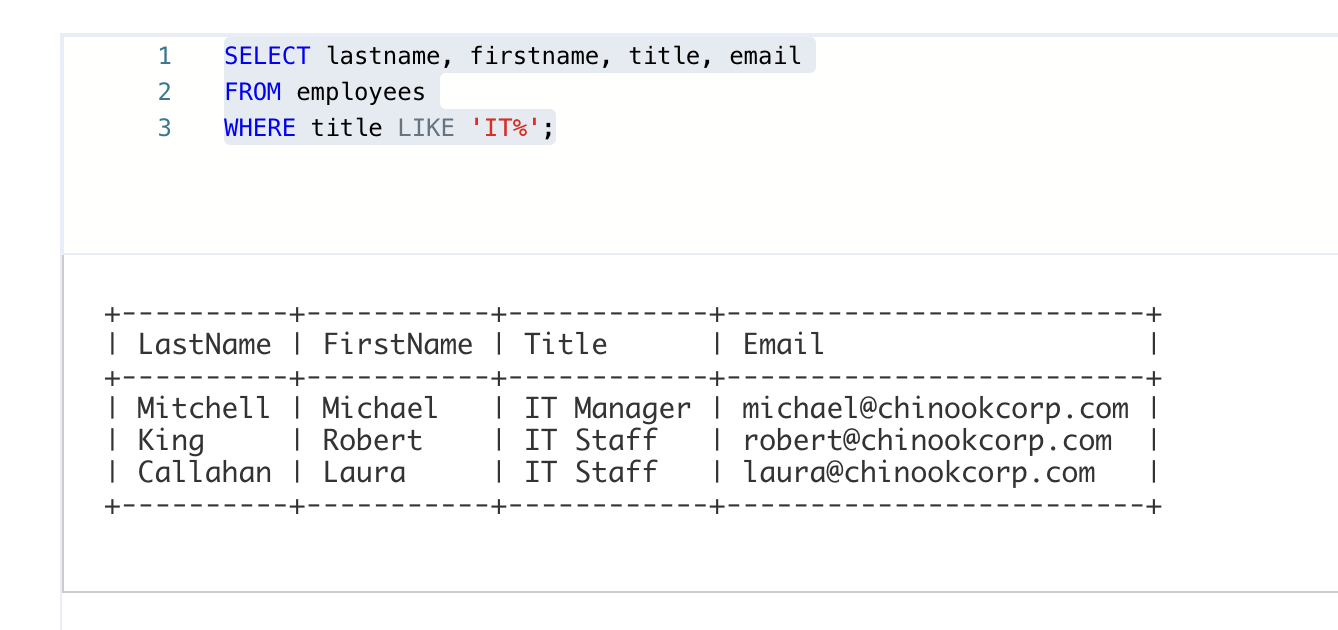
Filtrado por patrones:

Un **comodín** es un carácter especial que puede ser sustituido por cualquier otro carácter. Dos de los comodines más útiles son el signo de porcentaje (*%*) y el guión bajo (*\_*):

* El signo de porcentaje sustituye a cualquier otro carácter.
* El símbolo de subrayado sólo sustituye a otro carácter.

| *'a%'* | apple123, art |
| --- | --- |

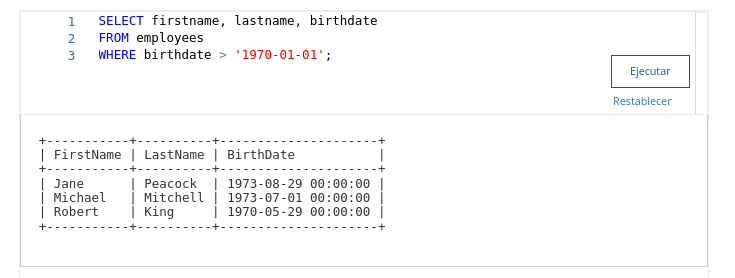
*LIKE* en lugar del signo igual (=). LIKE se utiliza con WHERE para buscar un patrón en una columna.

Por ejemplo, si desea enviar un correo electrónico a los empleados cuyo título sea *'IT Staff'* o *'IT Manager'*, puede utilizar el operador *LIKE* combinado con el comodín *%*:

Como otro ejemplo, si desea buscar en la tabla de facturas para encontrar todos los clientes ubicados en estados con una abreviatura de *'NY'*, *'NV'*, *'NS'* o *'NT'*, puede utilizar el patrón *'N\_'* en la columna *state*:

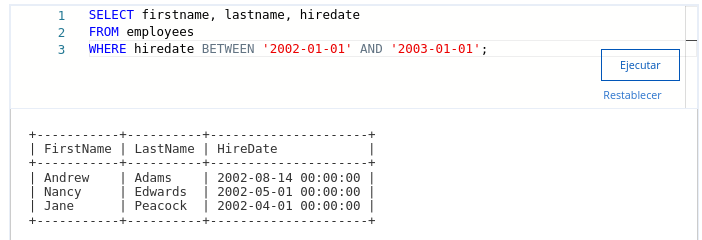
**Operadores de comparación**

| Operador | Utilice |
| --- | --- |
| *<* | menor que |
| *>* | mayor que |
| *=* | igual a |
| *<=* | menor o igual que |
| *>=* | mayor que o igual a |
| *<>* | no igual a |



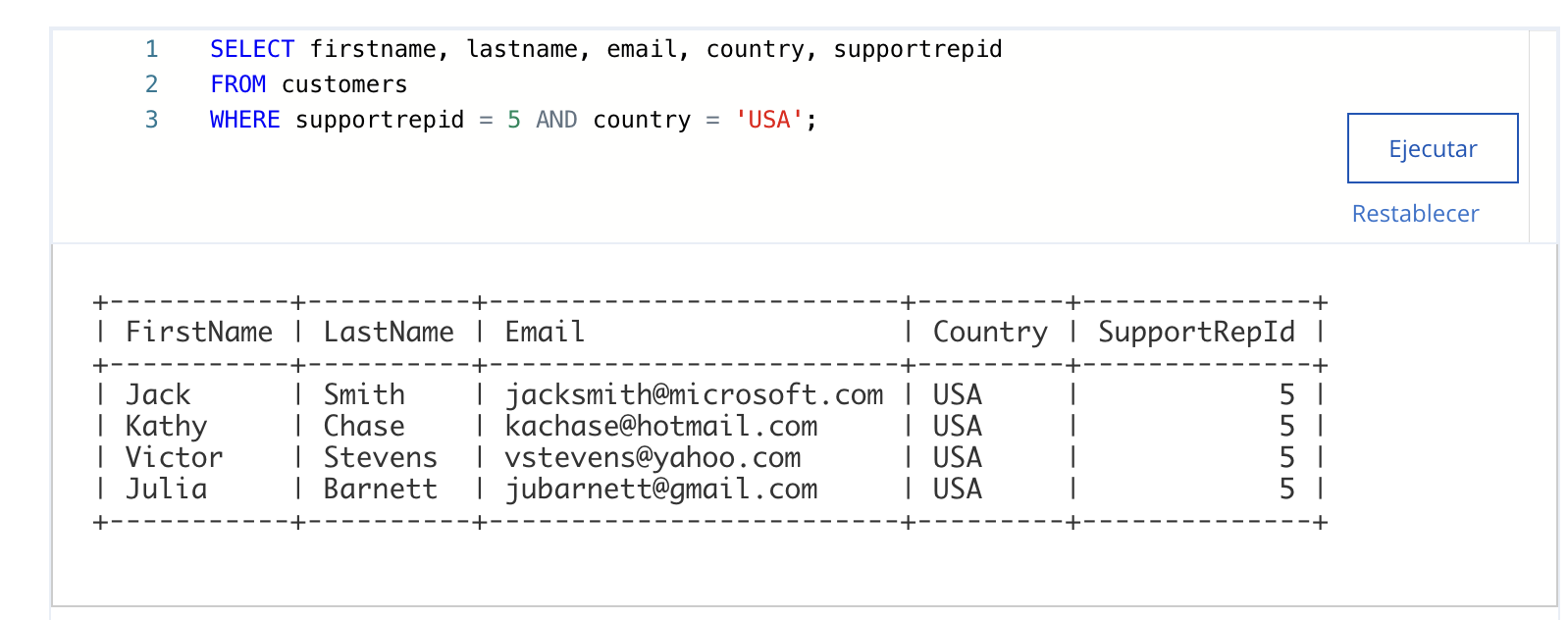
### **ENTRE**

*BETWEEN* filtra por números o fechas dentro de un rango.

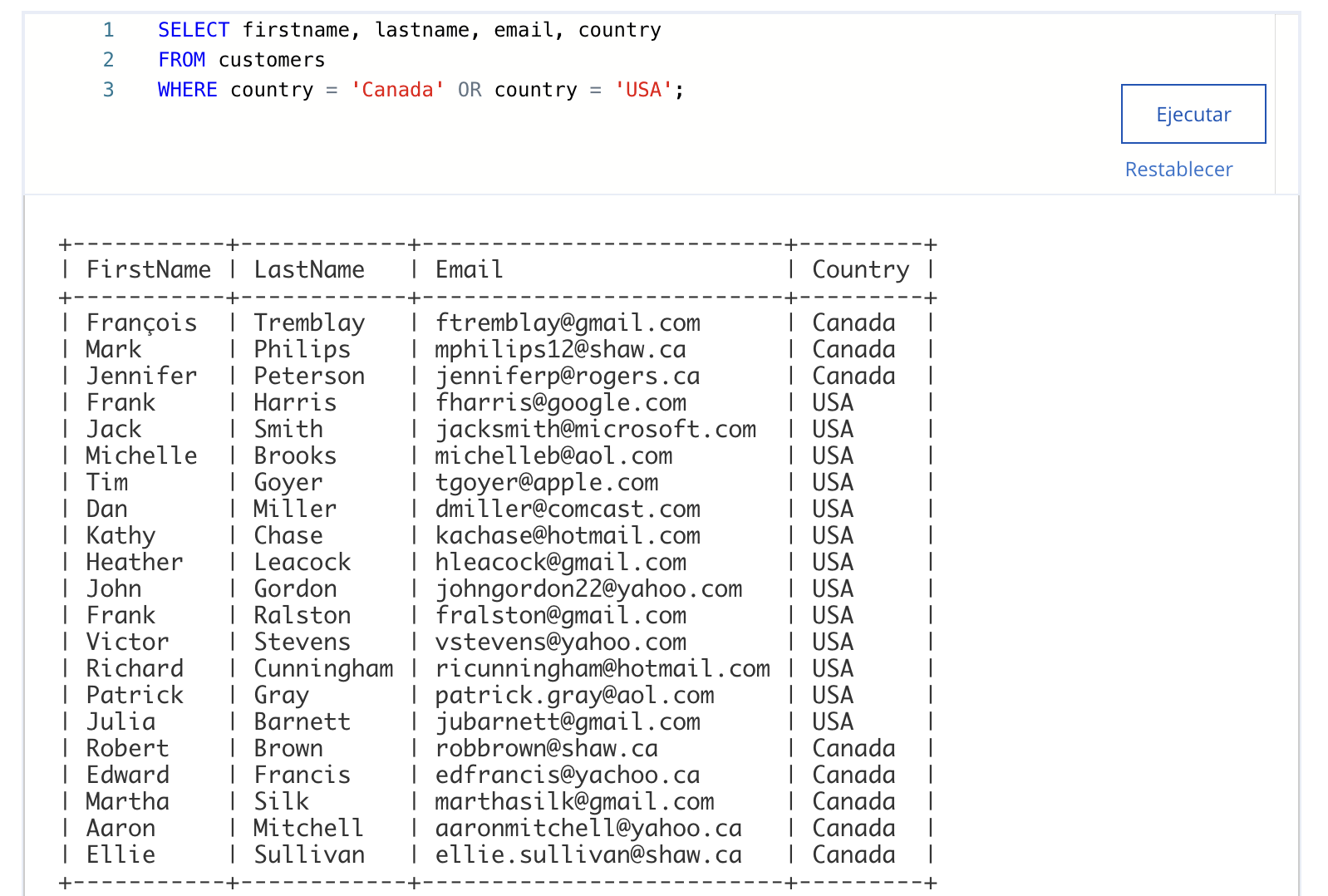


## **Operadores Lógicos**

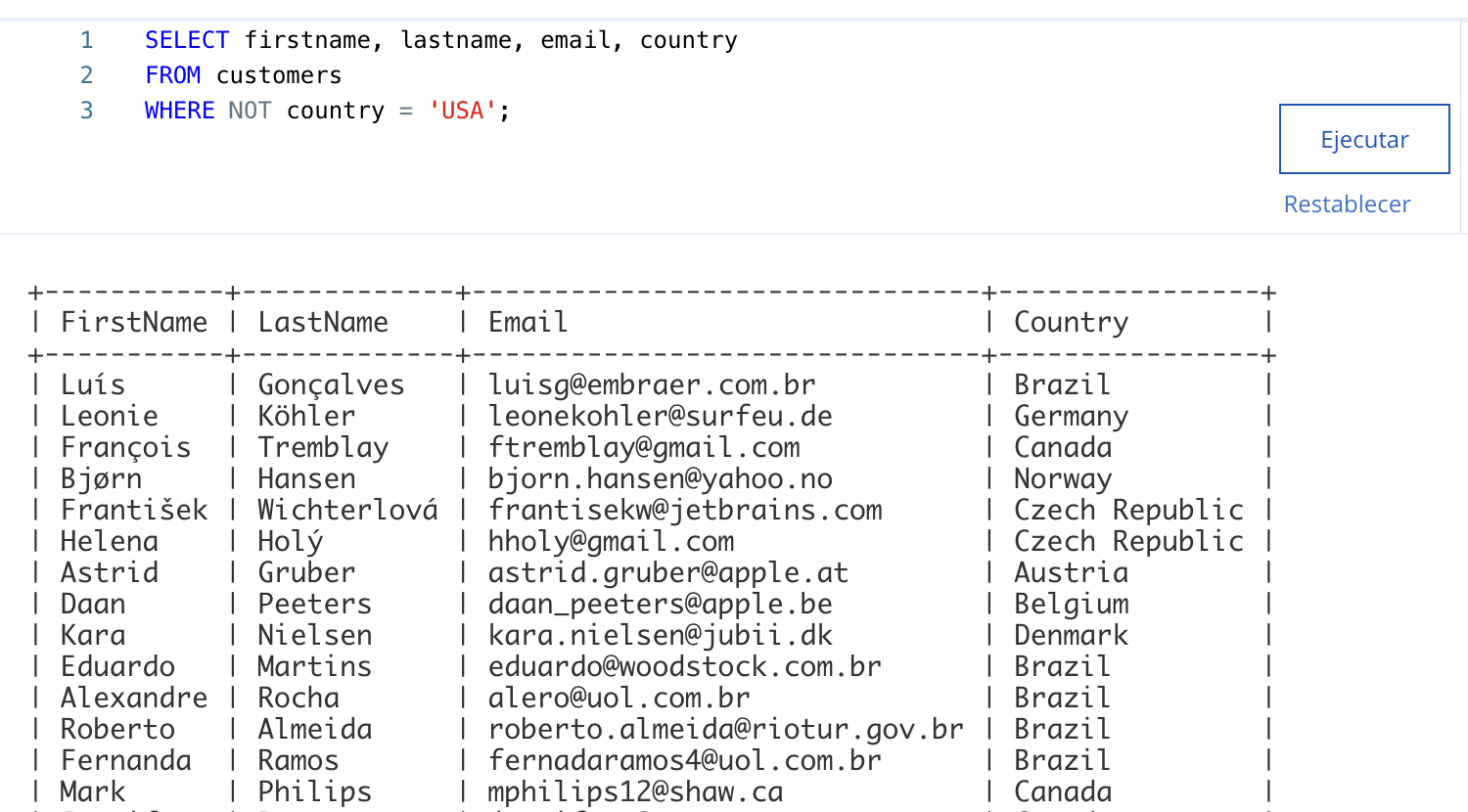
*AND* especifica que ambas condiciones deben cumplirse simultáneamente.



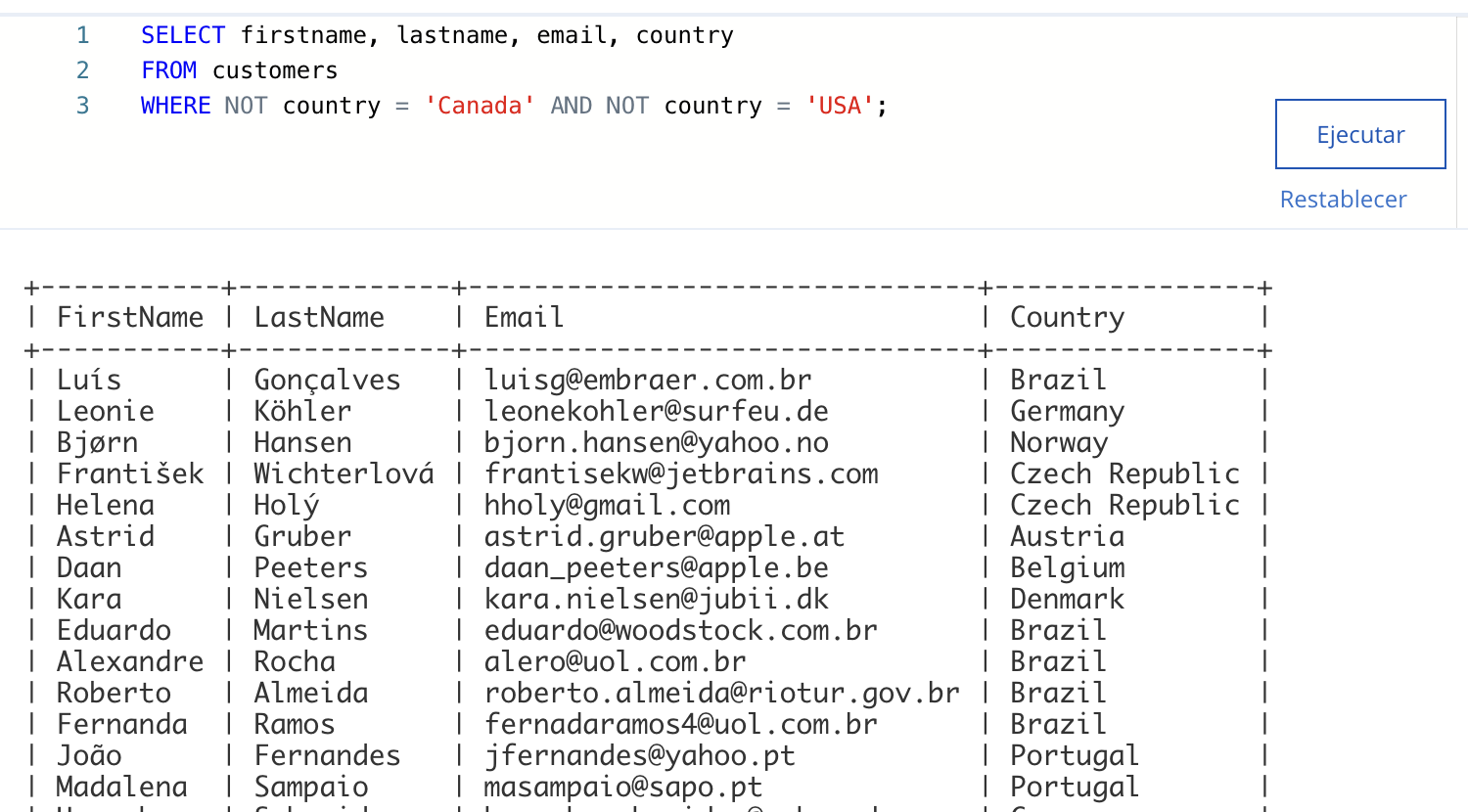
El operador *OR* también conecta dos condiciones, pero *OR* especifica que puede cumplirse cualquiera de ellas.



El operador *NOT* niega una condición. Esto significa que SQL devuelve todos los registros que no coinciden con la condición especificada en la consulta.



En la siguiente consulta, *NOT* se coloca antes de la primera condición, se une a una segunda condición con *AND*, y luego *NOT* también se coloca antes de esa segunda condición. Puede ejecutarla para explorar lo que devuelve:



El operador *AND* requiere que dos condiciones sean verdaderas simultáneamente, el operador *OR* requiere que una o ambas condiciones sean verdaderas, y el operador *NOT* niega una condición. Los operadores lógicos pueden combinarse entre sí para crear consultas aún más específicas.

Uniones de tablas externas e internas

**INNER JOIN**

*INNER JOIN* devuelve las filas que coinciden en una columna especificada que existe en más de una tabla.

Sólo devuelve las filas en las que hay una coincidencia, pero al igual que otros tipos de uniones, devuelve todas las columnas especificadas de todas las tablas unidas.

Por ejemplo, si la consulta une dos tablas con *SELECT \**, se devuelven todas las columnas de ambas tablas.

Si existe en dos tablas se devuelve dos veces.

### **La sintaxis de un inner join**

*SELECT \**

*FROM employees*

*INNER JOIN machines ON employees.device\_id = machines.device\_id;*

Debe especificar las dos tablas a unir incluyendo la primera o tabla izquierda después de *FROM* y la segunda o tabla derecha después de *INNER JOIN*.

Después del nombre de la tabla derecha, utilice la palabra clave *ON* y el operador *=* para indicar la columna sobre la que está uniendo las tablas. Es importante que especifique tanto el nombre de la tabla como el de la columna en esta parte de la unión colocando un punto (*.*) entre la tabla y la columna.

## **Uniones externas**

Las uniones externas amplían lo que se devuelve de una unión. Cada tipo de unión externa devuelve todas las filas de una tabla o de ambas.

### **LEFT JOIN izquierdas**

Al unir dos tablas, *LEFT JOIN*devuelve todos los registros de la primera tabla, pero sólo devuelve las filas de la segunda tabla que coincidan en una columna especificada.

*SELECT \**

*FROM employees*

*LEFT JOIN machines ON employees.device\_id = machines.device\_id;*

### **RIGHT JOIN**

Al unir dos tablas, RIGHT JOIN devuelve todos los registros de la segunda tabla, pero sólo devuelve las filas de la primera tabla que coinciden en una columna especificada.

La siguiente consulta demuestra la sintaxis de *RIGHT JOIN*:

*SELECT \**

*FROM employees*

*RIGHT JOIN machines ON employees.device\_id = machines.device\_id;*

**Nota:** Puede utilizar *LEFT JOIN* y *RIGHT JOIN* y obtener exactamente los mismos resultados si utiliza las tablas en orden inverso.

### **Uniones externas completas**

*FULL OUTER JOIN* devuelve todos los registros de ambas tablas. Puede considerarse como una forma de unir completamente dos tablas.

*SELECT \**

*FROM employees*

*FULL OUTER JOIN machines ON employees.device\_id = machines.device\_id;*

En resumen:

INNER JOIN, devuelve los registros buscados de las tablas pero si unos de los campos no tienen datos en común estos son omitidos y no se muestran.

LEFT JOIN, se muestran a la izquierda los contenidos que tienen datos en común y a la derecha también junto con los que no coinciden.

RIGHT JOIN, lo mismo que LEFT JOIN pero a la inversa, datos sin cosas en común a la izquierda.

FULL OUTTER JOIN, muestra todos los contenidos de las tablas solicitadas aunque no tengan datos en común.

**Ejemplos prácticos.**

SELECT customerid, trackid

FROM invoices

INNER JOIN invoice\_items ON invoice\_items.invoiceid = invoices.invoiceid;

**Funciones de agregación**

* ***COUNT* devuelve un único número que representa el número de filas devueltas por la consulta.**
* ***AVG* devuelve un único número que representa la media de los datos numéricos de una columna.**
* ***SUM* devuelve un único número que representa la suma de los datos numéricos de una columna.**