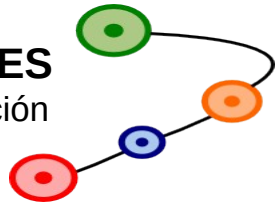
Administración y Gestión de Redes
Lic. en Sistemas de Información

Laboratorio de REDES
Recuperación de Información
y Estudios de la Web



Introducción a la Seguridad en Redes de Datos

Equipo docente:

Fernando Lorge (florge@unlu.edu.ar)
Santiago Ricci (sricci@unlu.edu.ar)
Alejandro Iglesias (aaiglesias@unlu.edu.ar)
Mauro Meloni (maurom@unlu.edu.ar)
Patricio Torres (ptorres@unlu.edu.ar)

- 2025 -

Presentación

- ¿Qué estudiamos?
- ¿por qué **Sistemas de Información**?
- ¿por qué **Información**?
- ¿Cómo sabemos si la información que gestionamos…
  - es la correcta?
  - sólo la poseemos nosotros?
- ¿Qué sucede si no tenemos acceso a esa información?

Activos de información

- La **información** debe considerarse un activo importante con el que cuentan las organizaciones para satisfacer sus objetivos, razón por la cual, tiene un **alto valor** para las mismas y **es crítica para su desempeño y subsistencia**.

- Es necesario **proteger los recursos de información** de una organización y la tecnología utilizada para su procesamiento frente a amenazas internas o externas, deliberadas o accidentales, **para garantizar la continuidad de las actividades**.

¿Qué debe protegerse?

Seguridad de la Información

La información que está:

- escrita o impresa.
- expuesta en una conversación.
- transmitida por correo tradicional.
- en el conocimiento de las personas.

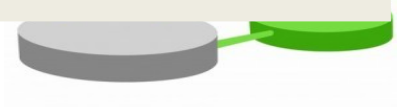
Seguridad Informática

- almacenada en un dispositivo electrónico.

Seguridad en redes de datos

- transmitida por medios electrónicos.
- almacenada en un nodo o nodos de una red de datos.
- … y todos los servicios y medios de procesamiento que permiten acceder a dicha esa información.

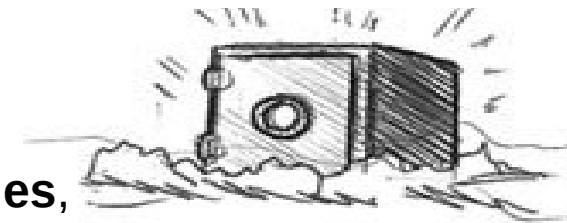
En la actualidad, la diferencia entre Seguridad Informática y Seguridad en Redes de Datos es cada vez más difusa.



Conceptos clave

Los activos (información, software, redes, hardware) se deben proteger contra **Amenazas**, que son todos aquellos elementos que atentan contra la seguridad de la información.

Una amenaza *no necesariamente* es maliciosa ni intencional: que falle un disco rígido, que se inunde un centro de datos.



Las amenazas aprovechan la existencia de **Vulnerabilidades**, es decir debilidades en los activos (la falta, inexistencia o debilidad en algún control), para producir un daño.

Conceptos clave

El **Riesgo** es la proximidad o posibilidad de daño sobre un activo.

El **Daño** es el resultado final de una amenaza.

El **Impacto** es cuán grave es ese daño de una amenaza.

Un **Control** o **Salvaguarda** es todo elemento, mecanismo, procedimiento, técnica, aplicación, etc. que ayuda a:

- disminuir o eliminar una vulnerabilidad, previniendo la acción de una amenaza, o
- detectar una amenaza que está en proceso, o
- recuperarse parcial o totalmente del daño producido por una amenaza.

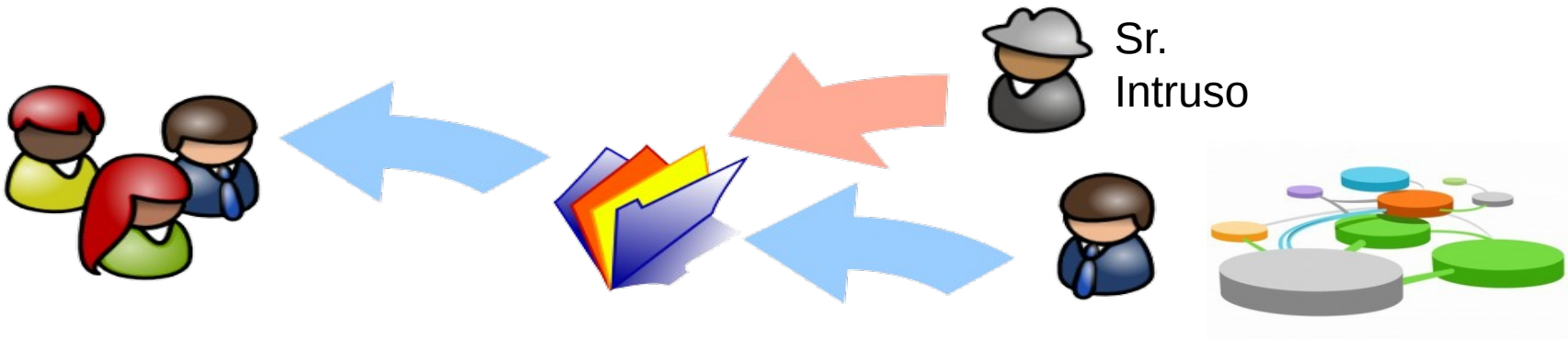
Seguridad de la Información

- Conjunto de metodologías, procedimientos y prácticas que buscan proteger la información, con el fin de minimizar los riesgos continuos a los que está expuesta, y a fin de **asegurar la continuidad de las operaciones** mediante la preservación de tres características principales:

  - **Integridad**
  - **Confidencialidad**
  - **Disponibilidad**

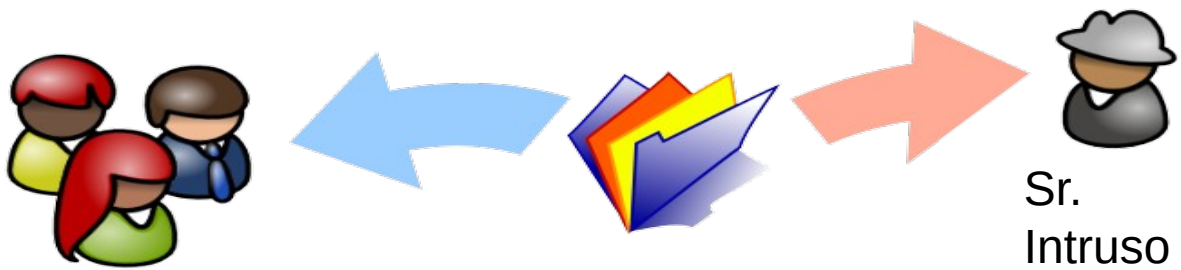
Integridad / Integrity

- Salvaguardar la **exactitud y totalidad** de la información almacenada o transmitida, cuyo contenido **debe permanecer inalterado a menos que sea modificado por personal autorizado**.
- Si se vulnera la integridad, la información puede aparecer manipulada, corrupta o incompleta.



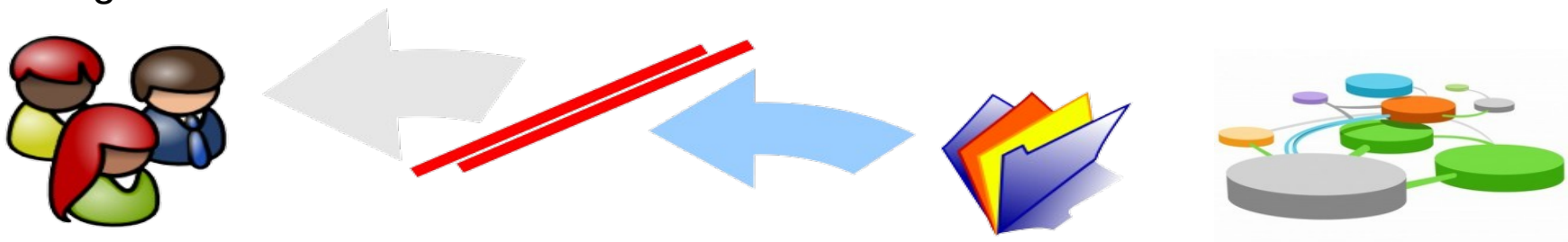
Confidencialidad / Confidentiality

- Asegurar que la información **llegue solamente a las personas autorizadas**, evitando a la vez que individuos no autorizados puedan acceder a dicha información.
- Si se vulnera la confidencialidad puede tener lugar la fuga de información, así como accesos no autorizados.
- La confidencialidad es una propiedad de difícil recuperación.



Disponibilidad / Availability

- La información, recursos y servicios relacionados **deben poder accederse** toda vez que el personal autorizado los requiera.
- La carencia de disponibilidad supone interrupción de un servicio o imposibilidad de acceso a cierta información en el momento y forma en que se la necesita.
- La disponibilidad afecta directamente a la productividad de una organización.



Un hacker se cambió las notas de la facultad

Le incautaron los servidores cuando intentaba borrar datos

2 de mayo de 2016

No una, sino varias veces, irrumpió en el sistema informático de la Universidad Argentina de la Empresa (UADE) para cambiar las notas de sus exámenes y de sus trabajos prácticos. Lo descubrieron. El operativo policial y judicial para desactivar al *hacker* incluyó el corte de la luz de la manzana en la que vive y el uso de drones, para filmar toda la escena y evitar que se escapara: cuando la policía entró en su casa, lo halló escondido en un cuarto, intentando borrar urgentemente información.

El joven, de 21 años, estudia Ingeniería de la Información en la UADE y ya tiene antecedentes en la materia. Antes del operativo del jueves pasado ya había sido investigado por la Policía Federal. Aunque en esta ocasión la Policía Metropolitana, por orden de la fiscal de ciberdelitos porteña, Daniela Dupuy, le secuestró nueve servidores (que estaban en plena tarea de ataque a la red de la universidad), varias notebooks, tabletas y *smartphones*, discos externos, dispositivos de red, cámaras y micrófonos ocultos.

La UADE había hecho la denuncia tras descubrir las alteraciones del registro de notas. Así comenzó la pesquisa del Área de Cibercrimen de la Metropolitana. Descubrieron los registros de conexiones donde figuraban las IP (protocolo de Internet) desde donde habían sido atacados los sistemas de la universidad. Se comprobó también que el mismo hacker también había atacado la red de la empresa de telefonía Claro, que

DIARIO LA NACION - http://www.lanacion.com.ar/1894585-un-hacker-se-cambio-las-notas-de-la-facultad
02-May-2016

Uber reveló que hackers accedieron a los datos de 57 millones de sus usuarios

La empresa ocultó durante un año la filtración y pagó 100.000 dólares para borrar la información de los perfiles expuestos

WASHINGTON.- Un grupo de hackers robó los datos personales de 57 millones de clientes y conductores de Uber , una filtración masiva que la empresa ocultó durante más de un año.

Entre esos 57 millones de usuarios figuran 600.000 choferes cuyos nombres y números de permisos de conducir fueron pirateados. Los nombres de los usuarios así como sus correos electrónicos y números de celulares fueron robados, informó Dara Khosrowshasi, el CEO de Uber, en un comunicado.

DIARIO LA NACION -
http://www.lanacion.com.ar/2084425-uber-revelo-que-hackers-accedieron-a-los-datos-de-57-millones-de-sus-usuarios

Un ciberataque bloquea el acceso a las computadoras de Telefónica en España

Un software malicioso infectó las PC corporativas de la sede central de la operadora española; exige dinero a cambio de su liberación; no afecta a su servicio de telefonía e Internet; otras empresas en Madrid parecen estar afectadas también

VIERNES 12 DE MAYO DE 2017 • 10:56 | Ramón Muñoz SEGUIR | EL PAÍS

Las computadoras de las oficinas de Telefónica en Madrid fueron infectadas por un ransomware. Foto: Reuters

DIARIO LA NACION -
http://www.lanacion.com.ar/2023172-un-ciberataque-bloquea-el-acceso-a-las-computadoras-de-telefonica-en-espana

Arquitectura de Seguridad OSI
Recomendación ITU-T X.800

- **Ataque a la seguridad (Security Attack):** Cualquier acción que comprometa la seguridad de la información perteneciente a una organización.
  - Ataque pasivo: por ej. lectura sin autorización, análisis de tráfico.
  - Ataque activo: alteración de mensajes/archivos, denegación de servicio.
- **Mecanismo de seguridad (Security Mechanism):** Un proceso (o un dispositivo que incorpora dicho proceso) que tiene por objetivo **detectar, prevenir o restaurar** de un ataque a la seguridad.
  - Cifrado, firma digital, control de acceso, control de ruteo, checksums, padding de tráfico, etc.

Arquitectura de Seguridad OSI
Recomendación ITU-T X.800

- **Servicio de seguridad (Security Service):** Un proceso o servicio de comunicación que mejora la seguridad de los sistemas de procesamiento de datos y de las transferencias de información de una organización.
- Los conceptos de Confidencialidad, Integridad y Disponibilidad son servicios de seguridad, más otros que veremos en breve.
- Los servicios buscan contrarrestar los ataques a la seguridad, y pueden valerse de uno o más mecanismos de seguridad para proveerlo.

Servicios de Seguridad

- **Integridad:** La información debe llegar a destino sin modificaciones.
- **Confidencialidad:** La información que circula por la red sólo puede ser accedida (leída) por las partes autorizadas.
- **Disponibilidad:** Los servicios deben estar disponibles para las partes autorizadas.
- **Autenticación:** Asegurar la identidad del emisor, y que ésta no es falsa.
- **No repudio:** El transmisor y/o receptor de un mensaje no puedan negar haber emitido/recibido un mensaje.
- **Control de acceso:** Determinar qué actores tienen acceso a qué recursos y de qué manera (ro, rw).

¿Se les ocurren ejemplos? ?

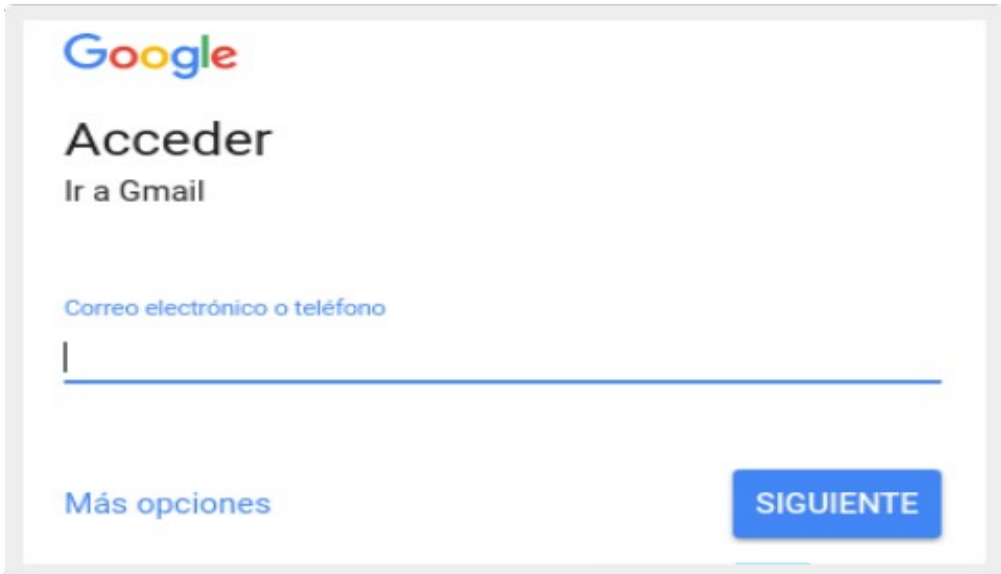
Id vs Autenticación vs Autorización

Para asegurar el acceso a un sistema informático, se deben ejecutar tres pasos **fundamentales y diferentes**:

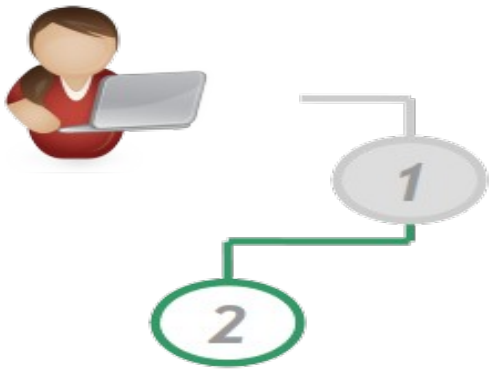
- **Identificación:** Indicarle al sistema cuál es la cuenta de usuario a utilizar.
- **Autenticación o Verificación:** Demostrarle al sistema, por ejemplo mediante la introducción de una clave, que el usuario es quien dice ser.
- **Autorización:** Probar que el usuario tiene permiso para acceder al recurso.

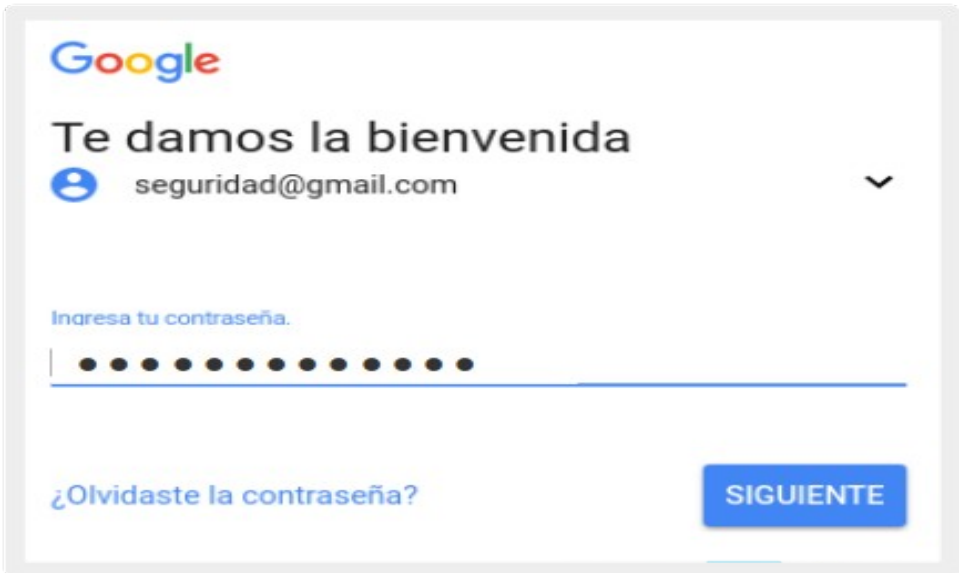
¿Se les ocurren ejemplos? ?

1. Identificación / Identification

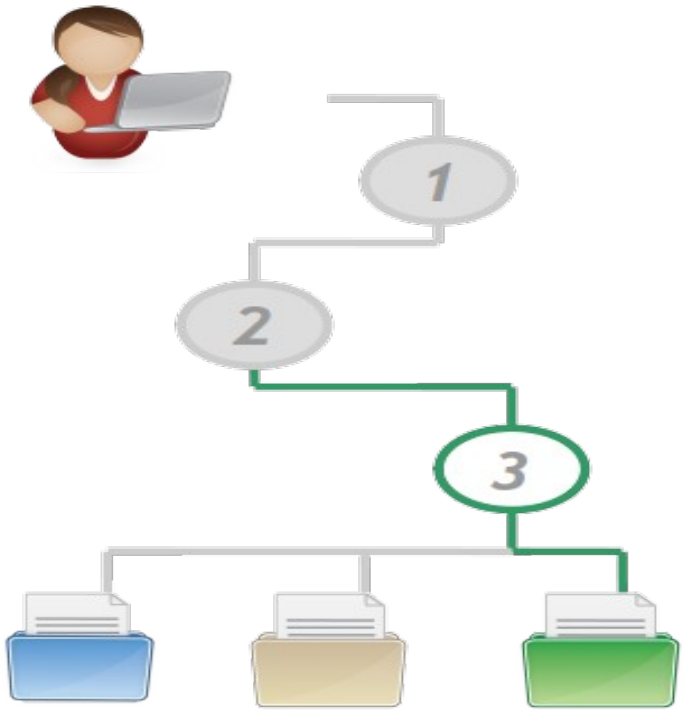


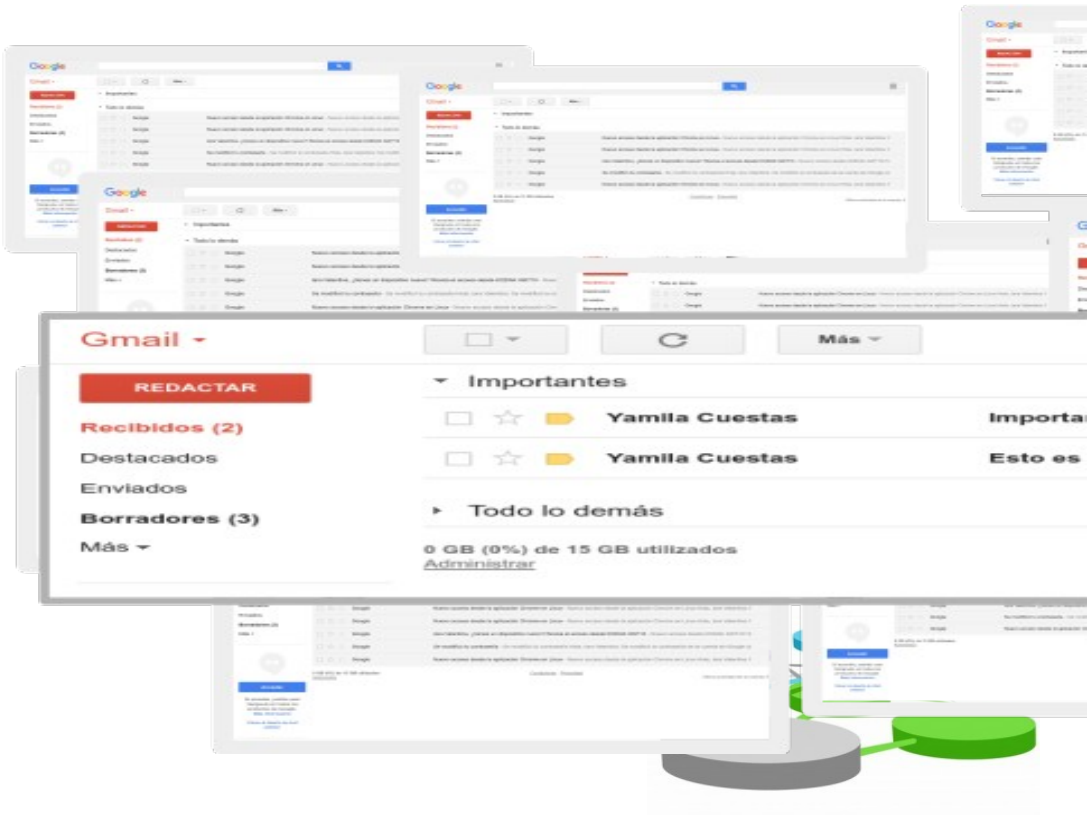
2. Autenticación / Authentication





3. Autorización / Authorization





Impacto potencial

Según el estándar FIPS PUB 199 (EE.UU.):

- **Bajo:** ante la pérdida de confidencialidad, integridad o disponibilidad puede esperarse que tenga un efecto adverso limitado en las operaciones de la organización, sus recursos o individuos
- **Moderado:** ante la pérdida de confidencialidad, integridad o disponibilidad puede esperarse que tenga un efecto adverso serio en las operaciones de la organización, sus recursos o individuos
- **Alto:** ante la pérdida de confidencialidad, integridad o disponibilidad puede esperarse que tenga un efecto adverso severo o catastrófico en las operaciones de la organización, sus recursos o individuos.

Ataques

- **Intercepción:** El destino recibe la información enviada por el origen, pero ésa ha sido interceptada por un tercero.
- **Modificación:** La información enviada por el origen es interceptada por el atacante, modificada y reenviada al destino.
- **Interrupción:** La información nunca llegará a su destino.
- **Generación:** El intruso genera y envía la información al destino haciéndose pasar por el origen real.

¿Qué servicio de seguridad afecta cada uno? ⃝?

Intruso pasivo vs Intruso activo

- **Intruso pasivo:** Es aquél que accede a recursos e información que se suponen privados sin realizar ninguna acción sobre ellos, es decir, visualiza datos de archivos, bases de datos, o monitorea el tráfico de una red determinada.
- **Intruso activo:** Es el que modifica archivos, bases de datos, reenvía deliberadamente la información que es capaz de
capturar, o genera nuevos datos/mensajes
- Misma clasificación que para ataques.

¿Qué servicio de seguridad afecta cada uno? ?

Estrategias para brindar Seguridad

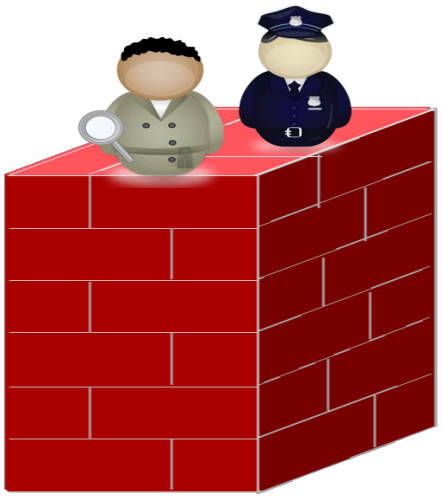
- **Menor privilegio** / least privilege:
  - cada actor (usuario, admin, programa, sistema, etc) debe tener los privilegios mínimos para su accionar, y no más que esos.
- **Defensa en profundidad** / defense in depth:
  - implementar mecanismos de seguridad a distintos niveles, uno sobre el otro: hardware, software, políticas, procedimientos.
- **Seguridad desde el diseño** / security by design:
  - debe tenerse en cuenta desde la concepción de un sistema.
- **Cuello de botella** / choke point:
  - forzar a que el flujo de información pase siempre por un punto de control.

Fuente: ZWICKY, E. et al.. 2000. Building Internet Firewalls (2nd ed), capítulo 3

Estrategias para brindar Seguridad

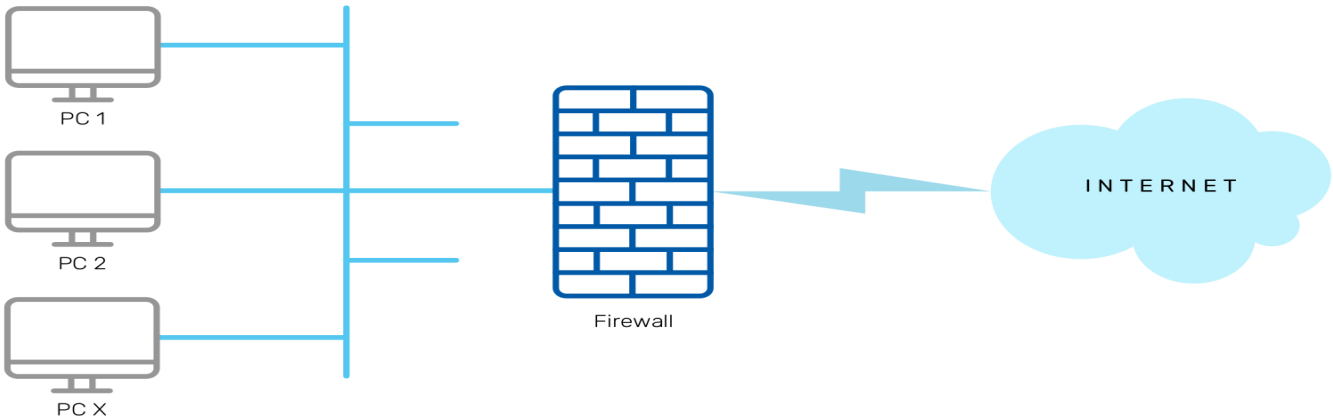
- **Punto más débil** / weakest link:
  - la defensa es tan fuerte como lo es su punto más débil.
- **Fallar en forma segura** / fail-safe stance / default deny:
  - si algo falla, toda solicitud debe ser denegada.
- **Diversidad de defensa** / diversity
  - utilizar mecanismos de seguridad de distinto tipo y proveedor.
- **Simplicidad** / simplicity:
  - a mayor complejidad, más difícil es aportar seguridad.
- **Transparencia** / transparency:
  - evitar basarse en algoritmos secretos (security by obscurity).

Fuente: ZWICKY, E. et al.. 2000. Building Internet Firewalls (2nd ed), capítulo 3

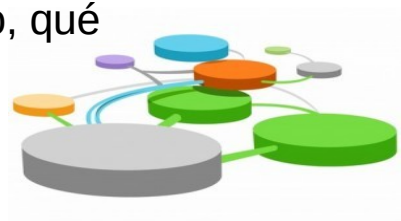


Mecanismos - Firewalls

Cortafuegos / Firewall

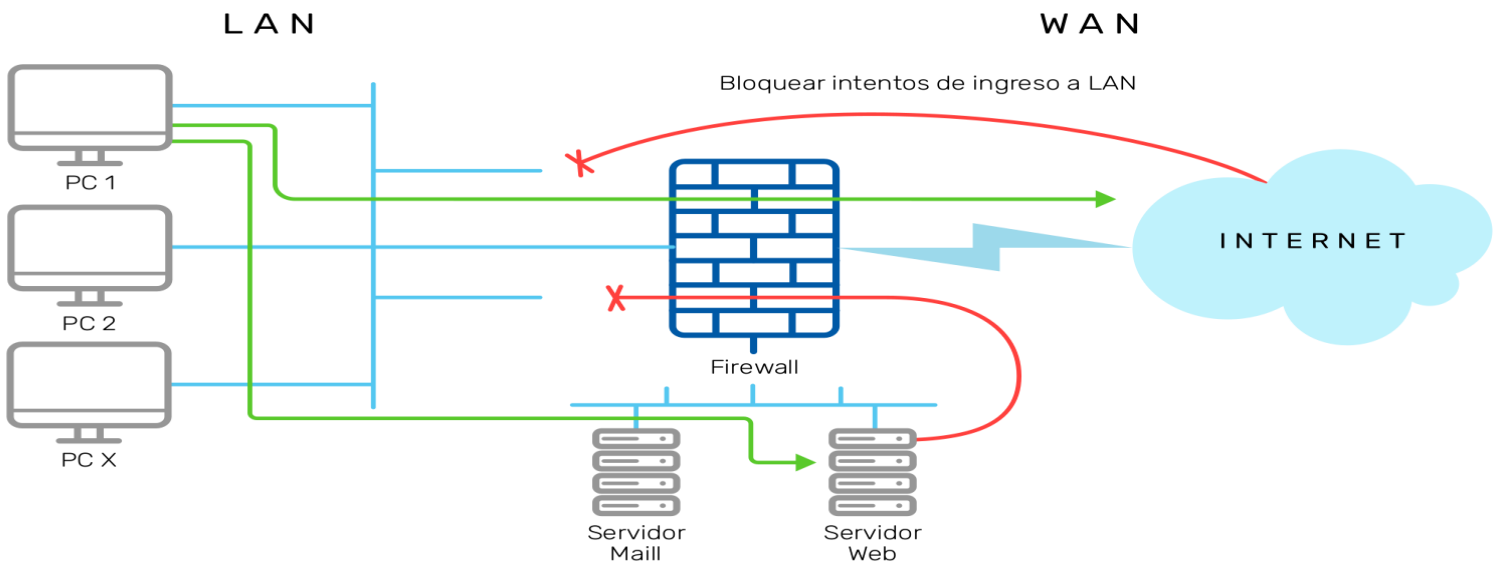


- Un **cortafuegos o firewall** es una barrera a través de la cual debe pasar el tráfico que va en direcciones opuestas.
- La **política de seguridad** de firewall determina, en un sentido y otro, qué tráfico pasa y qué tráfico no, según las reglas definidas (**ACL**) y los encabezados o el contenido de cada paquete entrante y saliente.



Cortafuegos / Firewall

Son un medio eficaz para proteger un sistema local, o una red de sistemas, de las amenazas de seguridad que existen en las redes externas filtrando, por ejemplo, el tráfico entrante y saliente entre la red de computadoras de una organización e Internet.



Objetivos de diseño de un FW

1. Todo el tráfico de adentro hacia afuera de una red, y viceversa, debe pasar a través del firewall. Esto se logra bloqueando físicamente todo el acceso a la red local, excepto a través del firewall.
2. Solo se permitirá el paso del tráfico autorizado, según lo definido por la política de seguridad local. Dependiendo del tipo de firewall son las políticas que se pueden definir (los veremos en breve).
3. El firewall en sí mismo debe ser inmune a intrusiones. Esto requiere el uso de un sistema reforzado con un sistema operativo seguro.

Servicios que puede brindar

- **Control de acceso:** Este servicio lo consigue obteniendo tanta información como sea posible de los paquetes que pasan por él.
  Con esta información y con una política de seguridad determina si autoriza o no el paso de un paquete hacia/desde la red destino.
- **Registro de actividades:** Un cortafuegos puede registrar todas las actividades, autorizadas y denegadas, que lo atraviesan.
  Este registro es una herramienta muy valiosa para supervisar la actividad de un intruso para averiguar las áreas susceptibles de haber sido dañadas, e incluso para identificarlo (y posiblemente atraparlo).
- **Extremo de NAT o de VPN:** Al estar en el borde, suele ser un buen lugar para realizar NAT o (des)encapsular VPNs.

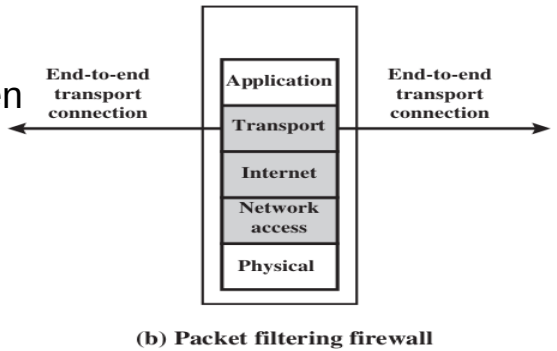
Políticas de seguridad (“las 4 P”)

- **Paranoica:** todo está prohibido, aún aquello que debería estar permitido; como si no hubiera interconexión.
- **Prudente:** todo está prohibido, excepto aquello que se permita de manera explícita.
- **Permisiva:** todo está permitido, excepto aquello que se prohíba de manera explícita.
- **Promiscua:** se permite todo, aun aquello que debería prohibirse.

Tipos de Firewall

Filtro de paquetes simple / Stateless Packet Filtering (1ra gen)

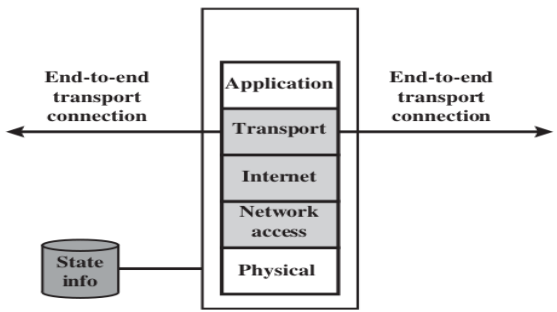
- Revisa los paquetes que le llegan y los deja pasar, o no, basándose en una lista de reglas y en las características de ese paquete.
- Interfaz, IP Origen/Destino, Protocolo, Puerto Origen/Destino, etc.



(b) Packet filtering firewall

Filtro de paquetes con estado / Stateful Inspection Firewall (2da generación)

- Extiende el filtro de paquetes simple con la adición de una base de datos local que brinda contexto (estados de conexión, dirección del flujo, conexiones relacionadas, etc) para determinar la decisión a tomar. La base de información se actualiza constantemente.
  Ver [IFW] en la bibliografía.

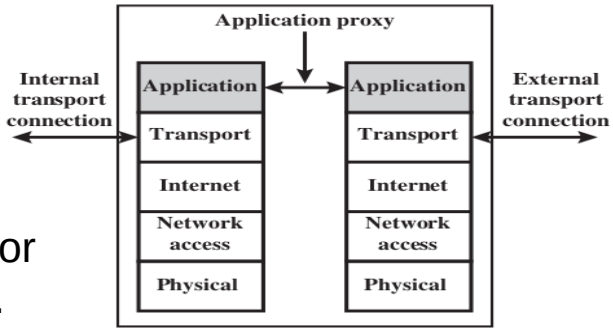


(c) Stateful inspection firewall

Tipos de Firewall

Filtro a nivel de aplicación /
Application-Level Gateway o Proxy (3ra generación)

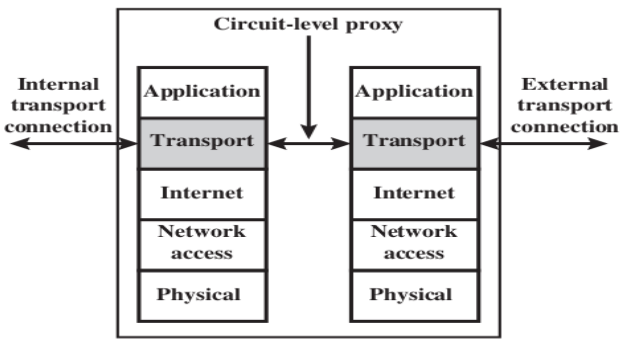
- Opera como intermediario entre el cliente y el servidor de cierta aplicación. Comprende el protocolo y puede filtrar por mensajes o PDUs del mismo, por usuario, por acción, etc.
- ¿Ejemplo clásico?



(d) Application proxy firewall

Gateway a nivel de “circuito” / Circuit-Level Gateway

- Autentica a un cliente y una vez establecida la autenticación, opera como intermediario entre conexiones TCP o flujos UDP hacia múltiples destinos.
- Ejemplo: Proxy SOCKS.



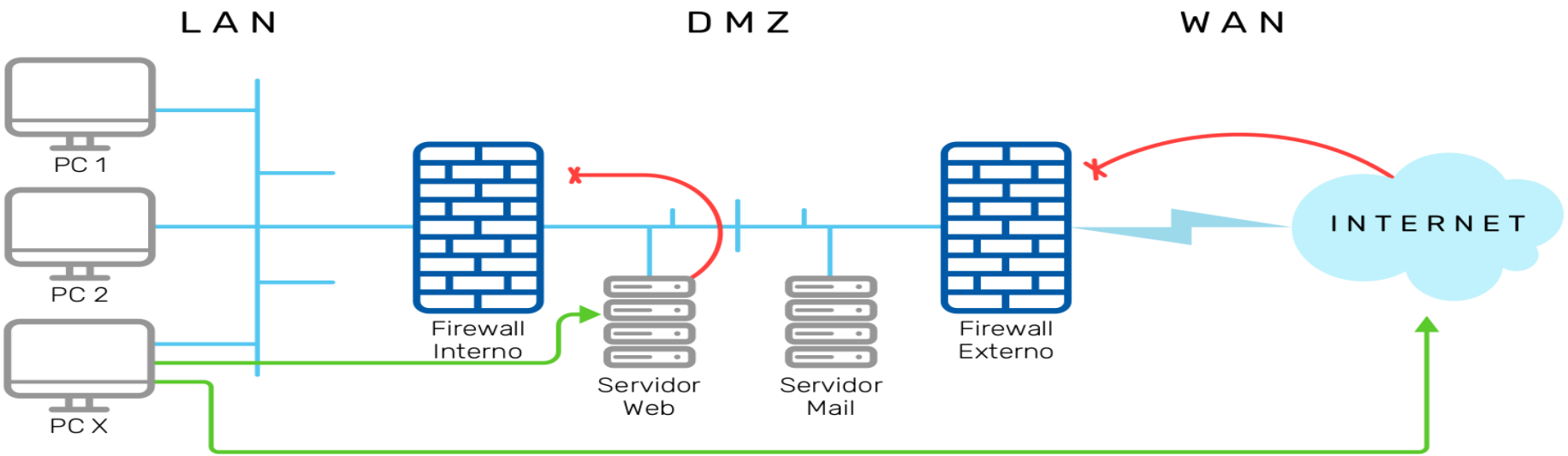
(e) Circuit-level proxy firewall

Fuente: STALLINGS. W. Cryptography and Network Security, Capítulo 22, pág. 6.

¿Dónde se emplazan?

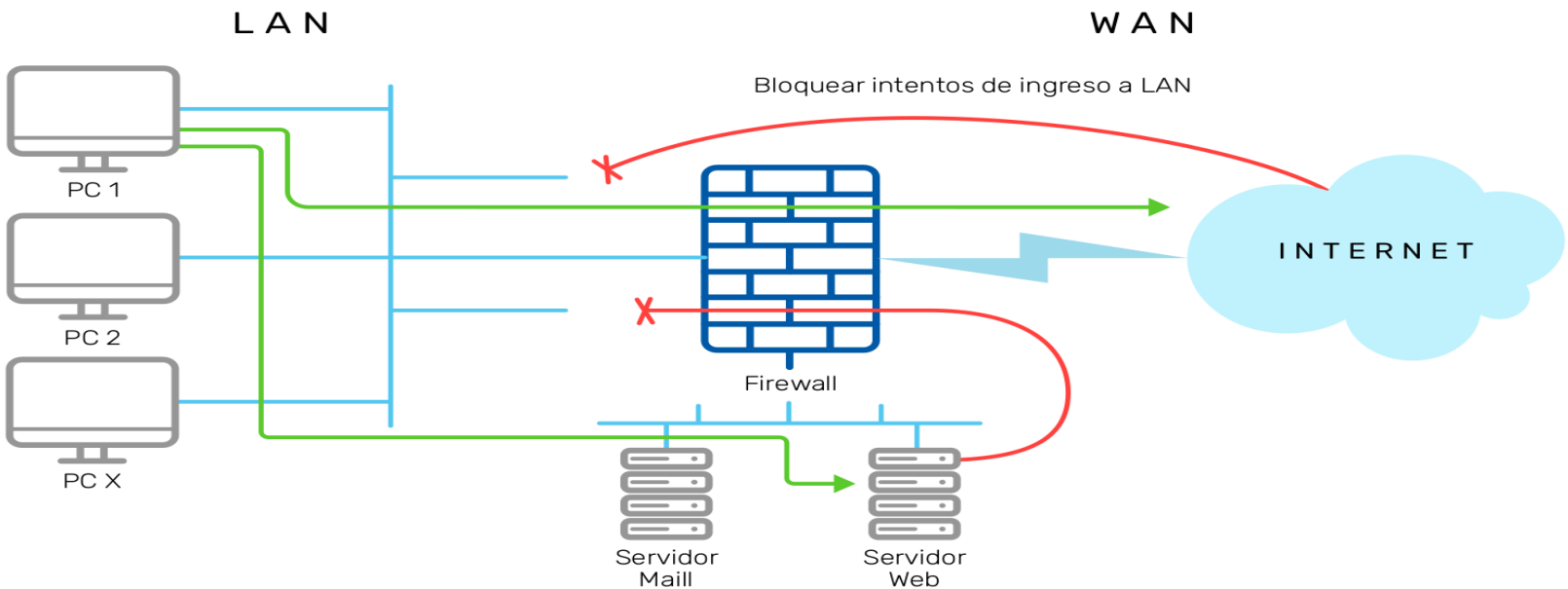
- **Borde de la red:** lo más habitual, un router o bridge bien asegurado, con pocos o nulos servicios hacia el exterior, autenticación fuerte y una política prudente.
- **Host-Based Firewall:** protege sólo a ese host/servidor y sólo admite acceso a las aplicaciones (puertos) provistas por ese host/servidor.
- **Personal Firewalls:** en cada estación de trabajo personal, para impedir accesos remotos a recursos o servicios que sólo deben compartirse localmente.
  Clásico ejemplo: el firewall de los S.O. modernos.
- **Web Application Firewalls:** a nivel de aplicación, se implementan antes (o en) un servidor web que posee cierta aplicación para filtrar los mensajes de dicho protocolo.
  Son un caso particular de *Application-Level Gateway*.
- **Process Firewall:** a nivel de sistema operativo, monitorea las llamadas a sistema que realizan ciertos procesos, bloqueando aquellas que están fuera del patrón común de uso de éste, o fuera de la política definida para éste. Equiv. a *Sandboxing*.

Emplazamiento clásico (I)

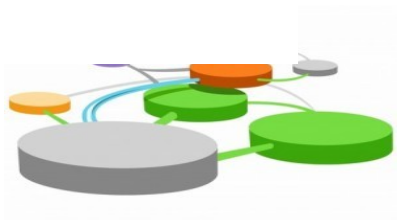


Se suele llamar **DMZ** o *zona desmilitarizada* a un segmento de red que aloja los hosts que proveen servicios accedidos tanto interna como externamente (web servers, email, proxy, dns, etc).
Por su exposición a los riesgos de Internet se separan de la LAN.

Emplazamiento clásico (II)



Aquí sencillamente se consolidan ambos FW en uno solo.



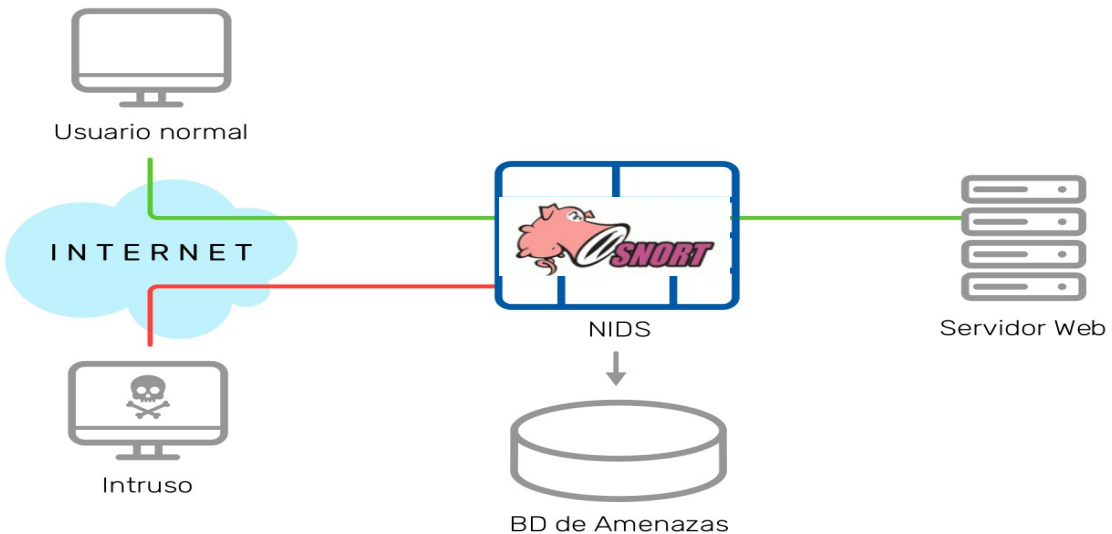
Sistema de Detección de Intrusiones

- Un **Sistema de Detección de Intrusiones (IDS)** monitorea y busca identificar patrones que puedan indicar un ataque o la violación de una política, ya sea a la red o a sistemas en particular.
- Puede basarse en firmas, patrones y/o heurísticas del tráfico monitoreado.
- Identifica ataques una vez que éstos están en proceso, o que ya ocurrieron, pero no los previene.
- Puede implementarse de tal manera que es posible analizar también el tráfico generado dentro del perímetro que se busca asegurar (detección de ataques internos).
- Puede generar alertas e interactuar con firewalls para contener un ataque en proceso.

IDS - Forma de operación

Analizando la información que recolecta y comparándola con una base de datos que contiene firmas (signaturas) de ataques conocidos.

Buscando "anormalidades" en el patrón de tráfico que analiza, tomando como referencia parámetros definidos por el administrador tal como volumen de tráfico normal, picos, tamaño de paquetes, protocolos, etc.



Sistema de Prevención de Intrusiones

- Un **Sistema de Prevención de Intrusiones (IPS)**, al igual que un IDS, monitorea el tráfico tratando de identificar posibles ataques, pero toma un rol activo, pues actuando “en el medio” intenta prevenir o bloquear dichos ataques.
- Operan utilizando signaturas y/o análisis estadístico.
- Posibles acciones: generar alarmas, descartar paquetes maliciosos, bloquear todo el tráfico desde determinada dirección IP, restablecer la conexión TCP.
- Es básicamente un IDS + Firewall.
- Ejemplo: *fail2ban, suricata, denyhosts*

Si perdieron acceso por errar varias veces la clave en el servidor de correo o en voip, los bloqueó un IPS.

Security Information and Event Management (SIEM)

- Recolecta registros (logs) de diversos dispositivos/aplicaciones para su análisis.
- Busca correlacionar eventos e identificar anormalidades o comportamientos que sean indicio de un incidente de seguridad.
- También se utilizan para la recolección de registros para cumplir con “Conformidad a normativas”.
- SEM (Security Event Management) → análisis de eventos en tiempo real
- SIM (Security Information Management) → almacenamiento de registros a largo plazo para su posterior análisis, generación de reportes, cumplimiento de regulaciones, análisis forense...

Unified Threat Management (UTM)

Gestión Unificada de Amenazas - Solución de seguridad “Todo en Uno”:

- Firewall
- IDS/IPS
- Anti.. virus, spam, phishing, spyware
- Filtro de contenidos
- Balanceo de carga
- Data leak prevention
- Deep Packet Inspection
- VPN
- SIEM

? ¿Desventaja?

Puede proveer “Conformidad a normativas”

Managed Security Service Provider

Proveedor de Servicio de Administración de Seguridad

Básicamente, delegar el monitoreo y la respuesta a incidentes de seguridad en una empresa que se dedica a ello.

- Administración y monitoreo remoto de firewalls, IDS, IPS, Gateways... (típicamente vía VPN, con mecanismos de contingencia como conexiones por celular o POTS)
- Análisis de vulnerabilidades (escaneo de red, aplicaciones, ...)
- Análisis y reportes de eventos registrados por dispositivos (posiblemente en sistemas SIEM)
- Diferentes soluciones para aplicaciones "in-house", en la nube, SaaS, ...
- Alternativa para aquellas empresas que necesitan “Conformidad a normativas” pero no tienen el staff necesario.

Bibliografía

- STALLINGS, W. 2011. *Cryptography and Network Security: Principles and Practice* (5th ed). Prentice Hall.
  - Capítulo 1: Overview
  - Capítulo 22: Firewalls
- HERTZOG, R. & MAS, R. 2015. *El manual del Administrador de Debian*. Freexian.
  - Capítulo 14. Sección 2: "Firewall o el filtrado de paquetes"
- ZWICKY, E.; COOPER S. & CHAPMAN D. B.. 2000. *Building Internet Firewalls* (2nd ed). O'Reilly Media.
  - Capítulo 3: Security Strategies
- EVANS, Julia - iptables. https://twitter.com/b0rk/status/1054056111626686465