Amenazas de Seguridad:

Las comunicaciones y la información que deseamos mantener privadas están protegidas (con políticas de acceso, firewalls, encriptación de datos, etc.) de quienes la utilizarían sin autorización (ladrones de identidad, delincuentes, estafadores, competidores, impostores).

Las **amenazas externas más comunes a las redes** incluyen las siguientes:

- Virus, gusanos y caballos de Troya.
- Spyware y adware.
- Ataques de día cero, también llamados “ataques de hora cero”.
- Ataques de piratas informáticos.
- Ataques por denegación de servicio.
- Interceptación y robo de datos.
- Robo de identidad.

Por lo general, los **componentes de seguridad de red** incluyen lo siguiente:

- Sistemas de firewall dedicados.
- Filtrado de firewall.
- Software antivirus y antispyware.
- Sistemas de prevención de intrusión (IPS).
- Redes privadas virtuales (VPN)
- Listas de control de acceso (ACL).

Conficker (2008, uno de los primeros virus): Aparición en Ucrania. Ataca W2000, XP, Vista, Server 2003 y 2008.

Desactiva servicios de Update, Windows Security Center, Defender, etc.

Bloquea cuentas de usuario, inunda ARP (Escaneo), vuelve los controladores de dominio lentos.

Hace inaccesibles actualizaciones de Antivirus y Parches de Windows.

Stuxnet (2010 – 2011): Gusano informático descubierto en Bielorrusia dedicado a espiar y programar sistemas industriales (SCADA).

Ataca los sistemas de control y monitoreo de infraestructura crítica (centrales nucleares).

Es capaz de reprogramar PLCs (Circuitos Lógicos Programables).

Rootkit: Programa de acceso de privilegios Root y comanda accesos para extraer datos.

Kapersky: Prototipo del Arma Cibernética producido para la Central nucleares Iraní Natantz.

En 2012 infectó a la Petrolera Chevron.

Seguridad informática:

- Integridad de la Información.
- Operatividad de la Información.
- Confidencialidad de la Información.

Seguridad en Internet:

Internet representa riesgos de seguridad importantes que las organizaciones ignoran o subestiman por su propia cuenta y riesgo.

Estar conectado a la red pública implica estar expuesto a permanentes ataques de diferente índole: virus, spoofing, sync flooding, DoS, entre otros.

Los ataques pueden producir **pérdidas**:

- Imagen corporativa (Ej: deface de páginas web).
- Económicas (Robo de información, transferencias de dinero).
- Infecciones de Malware.

Tendencias actuales de riesgos en Internet:

Año tras año son encontradas vulnerabilidades en cantidades exponenciales respecto de años anteriores. La cantidad de vulnerabilidades en los software existentes resulta enorme.

A raíz de la cantidad de vulnerabilidades surgen figuras como "Patch Manager" en las estructuras de TI.

Las actualizaciones, parches y service packs lanzados al mercado por los fabricantes de software provocaron que el trabajo de los administradores de sistemas se vuelva una pesadilla. La aplicación de estos, es un trabajo tiempo completo, requiere un intensivo trabajo de testeo, prueba e implementación, lo que dificulta esta tarea. Grandes problemas se presentan muchas veces, por ejemplo un parche arregla A pero "desarregla" B.

Hay un escaso tiempo desde que se descubre y se anuncia una vulnerabilidad hasta el momento en que los hackers saben cómo aprovecharla. Los ataques son cada vez más eficaces llegando a poder infectar 300.000 equipos en 14 minutos (virus MyDoom en enero de 2004). La rápida propagación de estas amenazas hace muy difícil responder con la suficiente rapidez para evitar los daños. La tendencia en referencia a daños económicos es cada vez más elevada.

Para una **defensa en profundidad** es necesario contar con prevención, detección y reacción.

Seguridad de la Información:

La seguridad de la información se caracteriza como la preservación de:

- **Confidencialidad:** Asegurándose de que la información sea accesible solamente a aquellas personas autorizadas para tener acceso.

- **Integridad:** Salvaguardar la exactitud de la totalidad de la información y de los métodos de proceso.
- **Disponibilidad:** Asegurando que los usuarios autorizados tengan acceso a la información cuando ésta sea requerida.
- **Oportunidad:** Asegurar que la información esté disponible en el momento en que esta sea solicitada.
- **Autenticidad:** Asegurar que la información recibida sea de quien dice ser.

Principios fundamentales:

- Principio del eslabón más débil.
- Defensa en profundidad.
- Punto de control centralizado.
- Seguridad en caso de fallo.
- Participación universal.
- Simplicidad.
- Principio de menor privilegio.
- La seguridad no se obtiene a través de la oscuridad.

Blancos de infraestructura:

- Web Servers / Web Services.
- DataBase Servers.
- E-mail servers.
- Routers.
- LDAP / Identity services.
- DNS.
- FTP Services.
- Clientes.
- Wireless.

La **secuencia de ataque** consiste en:

- Reconocimiento:
    - Ingeniería Social.
    - DNS Bases:
        - Intento de transferencia de zona.
        - Enumeración de zona.
        - Investigar lacnic.net.
- Huellas de S.O. y Aplicaciones:
    - Actividad inusual en servidores.
    - Escaneo (Ports, Robo, 802 y Bluetooth).
- Investigación y construcción de una herramienta.
- Explotar la vulnerabilidad.

¿Por qué triunfan los ataques?

La operación normal de la seguridad puede encargarse aproximadamente del 95% de la infraestructura de IT.

Existen 3 brechas importantes:

- La **ventana de vulnerabilidad** entre el surgimiento de un incidente y la aplicación de la solución (como un parche).
- **Sistemas no controlados:** Son aquellos que son ajenos pero inevitablemente interactúan con los propios. Pueden no poseer todas las actualizaciones y software de seguridad adecuados para la prevención de incidentes.
- **Ataques rápidos**: Se esparcen más rápido de lo que pueden reaccionar o responderlos. Pueden ser procesos, tecnologías o personas.

Políticas de Seguridad:

Es un conjunto de decisiones que, tomadas en conjunto, definen una postura respecto a la seguridad.

Define los alcances y límites de uso de los servicios de la red para un comportamiento aceptable y cual debería ser la respuesta en cada caso.

Debe ser aprobada al más alto nivel ejecutivo.

Planeamiento de seguridad:

Un plan de gerenciamiento de seguridad debe contar con:

- Definición funcional.
- Resumen de Intención/Alcance.
- Diseño de la documentación.
- Precondiciones de trabajo (Relevamiento).
- Resultados de análisis del relevamiento, conclusiones.
- Definición de políticas de seguridad, estándares y procedimientos.
    - Manejo de usuarios, contraseñas y accesos.
    - Rutinas de recupero de desastre.
- Recomendaciones y plan de seguridad física.
- Recomendaciones de segurización extendida.
- Apéndices:
    - Cumplir con las mejores prácticas de la industria.
    - Cumplir con los estándares de los S.O. que se utilizan.
    - Evaluación de riesgos perimetrales o circundantes (de las 3ras partes que interactúan con nuestra red o computador).

Proactividad vs. Reactividad:

La utilización de software reactivo (como Antivirus, Anti-Spam, Parches de seguridad, Herramientas de remoción, etc.) no es suficiente. Es necesario utilizar software proactivos para detectar vulnerabilidades y posibles fallas en los sistemas de computadoras. Pero fundamentalmente, es necesario tener una actitud proactiva, es decir, no esperar la falla, sino tratar de evitarla lo antes posible.

Modelo de N-Tiers (N-Capas):

Es un concepto utilizado en Arquitectura Cliente-Servidor en redes de procesamiento de datos distribuidas.

Nace con la necesidad de compartir aplicaciones distribuidas en distintas computadoras y que las mismas otorguen servicios a través de Internet.

Normaliza las aplicaciones distribuyéndolas en capas para que el procesamiento sea seguro y confiable.

Ejemplos:

- **Tier One / Una Capa:** Aplicaciones corriendo en un único servidor.
- **Tier Two / Dos Capas:** Aplicaciones corriendo en dos computadoras: un servidor y un cliente.
- **Tier Three / Tres Capas:** Aplicaciones corriendo en dos computadoras y una base de datos: un servidor, un cliente y una base de datos que entrega datos a dicha aplicación.

Seguridad en el transporte:

Para mantener la integridad de la información/mensajes se hace necesario aplicar medidas especiales durante el transporte entre el remitente y en destinatario.

Los protocolos de red tradicionales no ofrecen garantías suficientes de seguridad para Internet.

Conceptos de seguridad:

- **Criptografía:** Es el arte de transformar mensajes de modo tal que sean ilegibles para todos aquellos a los que no se les confiere el modo de acceder a los mismos.
- **Criptoanálisis:** Es el estudio de las técnicas para quebrar mensajes criptografiados.
- **Criptología:** Es el estudio de la Criptografía y el Criptoanálisis.
- **Texto plano:** Es un mensaje original.
- **Texto cifrado:** Es el resultado de criptografiar un texto plano.

- **Encripción:** Es cualquier procedimiento para transformar un texto plano en un texto cifrado.
- **Desencripción:** Es el procedimiento de transformar un texto cifrado en el correspondiente texto plano.

X.509 - Estándar para Certificación Digital:

Es una pieza electrónica que prueba la identidad de su propietario, así como el derecho a acceder a la información. Prueba la identidad del destinatario previsto.

Los certificados digitales autentican usuarios y servidores. Guardan el formato de la Norma X.509.

X.509 es un formato estándar para certificados de clave pública, documentos digitales que asocian de forma segura pares de claves criptográficas con identidades como sitios web, individuos u organizaciones.

El certificado digital X.509 consiste en un formato estandarizado que se usa para los certificados de clave púbica (Public Key Infraestructure o PKI). Dicho de otra manera, un certificado X.509 v3 es un documento que ha sido codificado o firmado de manera digital.

Los **usos más comunes** del certificado electrónico x.509.v3 son los siguientes:

- Para la navegación web encriptada mediante protocolos SSL y certificado HTTPS.
- Correos electrónicos cifrados y firmados electrónicamente a través del protocolo S/MIME.
- Firma de documentos electrónicos.
- Autenticación de clientes.
- Identificación por vías electrónicas por parte de gobiernos o administraciones públicas.

Protocolos de transporte seguros:

SSL (Secure Sockets Layer):

Es un protocolo de transporte desarrollado por Netscape para transmisión de información privada vía Internet.

Utiliza métodos de encriptación basado en la RSA (Tecnología de Clave pública encriptada).

Se ubica entre TCP/IP y HTTP y realiza la autenticación con el servidor y el cliente (X.509). Se ejecuta en una capa entre los protocolos de aplicación (HTTP, SMTP) y sobre el protocolo de transporte TCP.

Capa de sockets seguros. Trabaja a nivel de sockets (puertos).

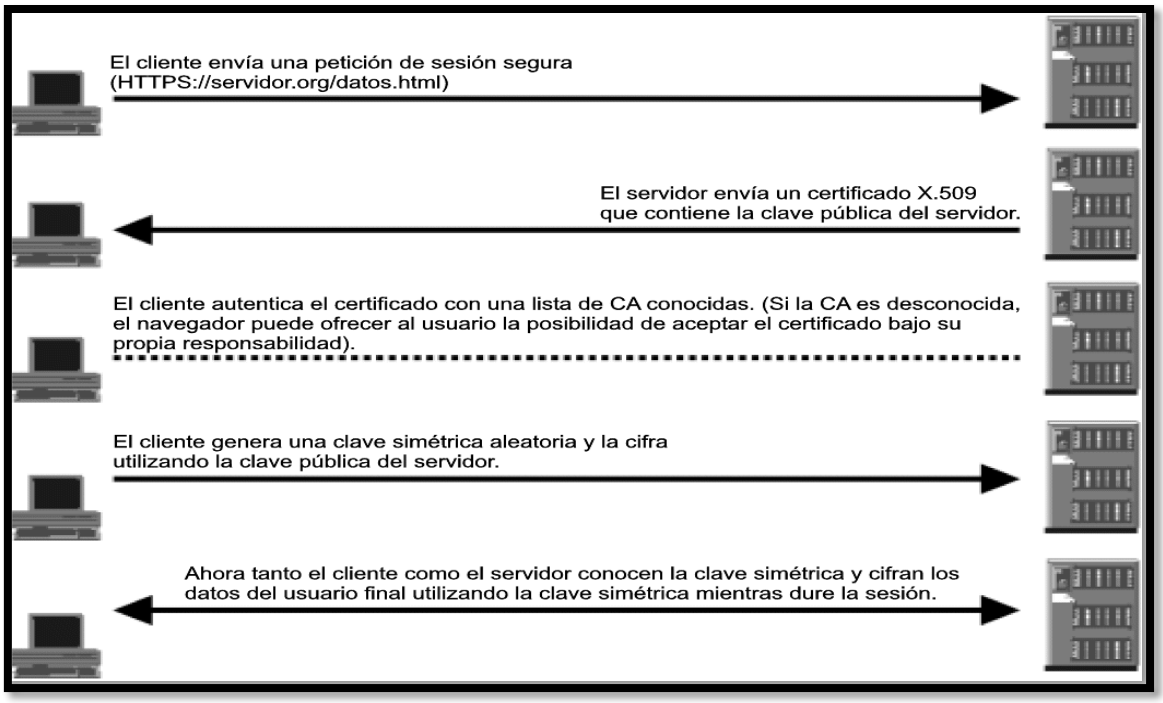
Identifica mutuamente cliente y servidor.

Encripta todos los datos para asegurar la privacidad.

Atiende exclusivamente a la confidencialidad de la información en el momento de la transacción entre el cliente y el servidor.

No opera sobre la información que se guarda en el servidor.

Es un estándar aprobado por IETF - RFC 2246.



TLS (Transport Layer Security):

Es la evolución del protocolo SSL (RFC 2246). TLS es una versión mejorada de SSL. Funciona de un modo muy parecido a SSL, utilizando cifrado que protege la transferencia de datos e información.

Circuito privado virtual entre dos puertos IP. Opcionalmente, asegura la autenticidad de una o ambas partes y la confidencialidad de los datos transmitidos.

Establece una sesión:

- Acuerdo de algoritmos.
- Realiza autenticación.
- Compartir secretos.

Permite la transferencia de datos de aplicación asegurando privacidad e integridad.

El protocolo se debe emplear para establecer una conexión segura entre dos partes. Tiene 2 niveles:

- Protocolo de registro TLS (TLS Record Protocol).
- Protocolo de mutuo acuerdo TLS (TLS Handshake Protocol).

Utiliza cifrado simétrico y un certificado X.509 v3 por parte del interlocutor.

Los **objetivos** del protocolo son varios:

- **Seguridad criptográfica:** El protocolo se debe emplear para establecer una conexión segura entre dos partes.
- **Interoperabilidad:** Aplicaciones distintas deben poder intercambiar parámetros criptográficos sin necesidad de que ninguna de las dos conozca el código de la otra.
- **Extensibilidad:** El protocolo permite la incorporación de nuevos algoritmos criptográficos.
- **Eficiencia:** Los algoritmos criptográficos son costosos computacionalmente, por lo que el protocolo incluye un esquema de cache de sesiones para reducir el número de sesiones que deben inicializarse desde cero (usando criptografía de clave pública).

S-HTTP - Secure HTTP - HTTPS:

Es una extensión del protocolo HTTP. Es un protocolo de comunicaciones diseñado para el envío de mensajes individuales seguros solo con conexiones HTTP. Es un estándar aprobado por IETF (Internet Engineering Task Force).

Trabaja a nivel de aplicación, utiliza el método de encriptación PEM (Correo de privacidad mejorada). Trabaja junto con TLS (antes SSL).

No maneja ni voz ni datos corrientes.

Tiene un canal de cifrado apropiado para que el protocolo HTTP pueda traficar información sensible. El nivel de cifrado depende del navegador y del servidor remoto.

Es utilizado principalmente en entidades bancarias y otras operaciones que requieran contraseñas y/o envío de datos personales.

Al igual que SSL, permite tanto el cifrado como la autenticación digital.

S/MIME (Secure Multipurpose Internet Mail Extension):

Es un protocolo de mensajería segura. Trabaja a nivel de aplicación con certificados digitales de modo que el remitente/emisor queda autenticado. Utiliza tecnologías de encriptado.

Es un estándar aprobado por IETF y es utilizado por navegadores.

Usa formatos X.509 para los certificados digitales de autenticación.

SET (Transacciones Electrónicas Seguras):

Transacciones electrónicas seguras en redes abiertas como Internet. Está basado en la criptografía más segura, la criptografía de llaves públicas y privadas RSA.

Norma técnica anunciada por Visa y Mastercard en 1998 que incluye el uso de certificados digitales. Asegura y autentica la integridad de los participantes en una operación económica.

Su código aplica técnicas de criptografía manteniendo el carácter confidencial de la información.

IPSEC (IP Security):

Es un conjunto de protocolos para soportar seguridad de intercambio de paquetes en VPNs. Puede utilizar certificación digital. Fue desarrollado por el IETF con dos modos de encriptación:

- **Modo Transporte:** Encripta solo datos.
- **Modo Túnel:** Encripta cabecera y datos.

Tunneling PPTP (Point to Point Tunneling Protocol):

Protocolo de encapsulamiento utilizado en comunicaciones remotas. Se utiliza en redes LAN o redes con servidores de acceso remoto (RAS).

Utiliza un túnel para que paquetes de un protocolo se transporten a través de una red que utilice otro protocolo. El túnel establecido por medio de PPTP constituye un canal de VPN sobre infraestructura pública.

El paquete de protocolo origen puede ser encapsulado dentro de paquetes IP. El encapsulamiento incluye un método de encriptación.

SLIP (Serial Line Internet Protocol) - PPP (Point to Point Protocol):

Son estándares de Internet para la transmisión de paquetes de protocolo IP a través de línea serie en modo Full-Duplex (línea telefónica). Recibe y transmite los paquetes IP.

El más reciente y utilizado es PPP.

Para establecer la conexión punto a punto cada terminal dialoga con los paquetes del Protocolo LCP (Link Control Protocol), para luego ser autenticado.

Para realizar el intercambio de la conexión utiliza el Protocolo NCP (Network Control Protocol).

PAP (PPP Autentication Protocol) – CHAP (Challenge Handshake Autentication Protocol):

Son protocolos encargados de autenticar al usuario en lo que respecta a login y password para que se realice la conexión PPP. CHAP es el más seguro de los dos, ya que PAP transmite en texto claro (no encripta).

Seguridad Wireless

Esquemas de encriptación de datos para comunicaciones inalámbricas con **WEP (56bit y 128bit), WPA o WPA2.**

Existen varios métodos que van desde el uso casero al corporativo: PSK (Pre Shared Key), Radius, etc.

WEP - Wired Equivalency Privacy (totalmente inseguro):

"Privacidad equivalente a cableado". Es el primer estándar de encriptación inalámbrico con el objetivo de proveer confidencialidad, control de acceso e integridad.

WEP encripta los datos con el cifrado RC4 que es un cifrado simétrico que utiliza un conjunto de bits (keystream) que se combinan con el mensaje con un XOR para producir un mensaje cifrado.

Para reproducir el mensaje, el destinatario procesa el mensaje cifrado utilizando la misma clave (keystream).

Una de las inseguridades más conocidas y publicitadas en el ámbito de las redes inalámbricas es la que se provoca con la utilización del protocolo de autenticación WEP. El uso de este esquema de autenticación implica que la red es un paso más lejos de ser completamente abierta, pero que ese paso es bastante estrecho. WEP es bueno solo cuando es utilizado en transmisiones de datos entre redes compuestas por Access Points, las redes cableadas no pueden utilizar este protocolo de encriptación.

La utilización de WEP es problemática, pues ofrece una sensación de falsa seguridad debido a los VI demasiado pequeños utilizados y el hecho que las claves WEP son estáticas.

Los paquetes de clave, entonces, son similares, y un atacante solo debe recolectar la cantidad suficiente de paquetes de datos para descifrar la clave en cuestión.

Está basado en:

- Claves de 64, 128 o 256 bits.
- RC4, algoritmo de cifrado de datos.
- Vector de inicialización de 24bits.
- CRC, algoritmo de chequeo de integridad.

Ventajas:

- Soportado por todos los equipos, fácil de implementar.

Defectos:

- Vectores de inicialización pequeños, pueden encontrarse dos mensajes con el mismo.
- Aumentar los tamaños de las claves de cifrado sólo aumenta el tiempo necesario para romperlo.
- Clave de encriptación estática.

WPA (Wi-Fi Protected Access, no es recomendable utilizarlo):

WPA fue desarrollado con el objetivo de fortalecer el protocolo WEP solucionando todas las debilidades de su antecesor (fue un reemplazo temporario).

Es contundente la superioridad de este método de encriptación de datos frente a su predecesor o par en la actualidad. Es real que la dificultad para crackear o romper una encriptación realizada con método WPA es extremadamente difícil, pero no imposible.

La clave WPA varia a lo largo del tiempo, a diferencia de WEP que es estática.

Tiene protección contra ataques de "repetición" (replay attacks).

Tiene dos modos de operación:

- **Servidor de autenticación (Radius):** Distribuye claves diferentes a cada usuario.
- **Clave pre-compartida (Pre-Shared Key, PSK):** Menos seguro, de uso hogareño.

WPA con servidor de autenticación (Radius):

El servidor de autenticación luego de aceptar las credenciales del usuario, utiliza 802.1X para producir una clave única maestra para esa sesión.

TKIP distribuye esta clave al Access Point y al cliente, creando un sistema jerárquico de administración de claves, y utiliza este par de claves únicas para generar dinámicamente claves de inscripción de datos únicas, las cuales encriptan todos los paquetes que son transmitidos en forma wireless durante la sesión del usuario.

Cuando un usuario solicita el acceso a la red, el cliente envía las credenciales del usuario al servidor de autenticación a través del AP.

Si el servidor acepta las credenciales del usuario, la clave TKIP maestra es enviada tanto al cliente como al AP.

Se completa el proceso instalando las claves entre el AP y el cliente.

WPA sin servidor de autenticación (Radius) – Pre-Shared Key:

Usuarios hogareños y las pequeñas empresas que no tienen servidor Radius. Para estos casos, WPA provee la opción de utilizar Pre-Shared Key (PSK).

La diferencia básicamente radica en que la contraseña es manualmente ingresada en los clientes y en los Access Points y es utilizada para la autenticación.

WPA 2 (Wi-Fi Protected Access 2, usado actualmente):

Este protocolo de encriptación forma parte del estándar IEEE 802.11i. Reemplaza formalmente a WEP y otras funcionalidades originalmente creadas en el estándar original 802.11i.

Es un nuevo algoritmo basado en AES (Advanced Encryption Standard, sucesor de DES – Data Encryption Standard).

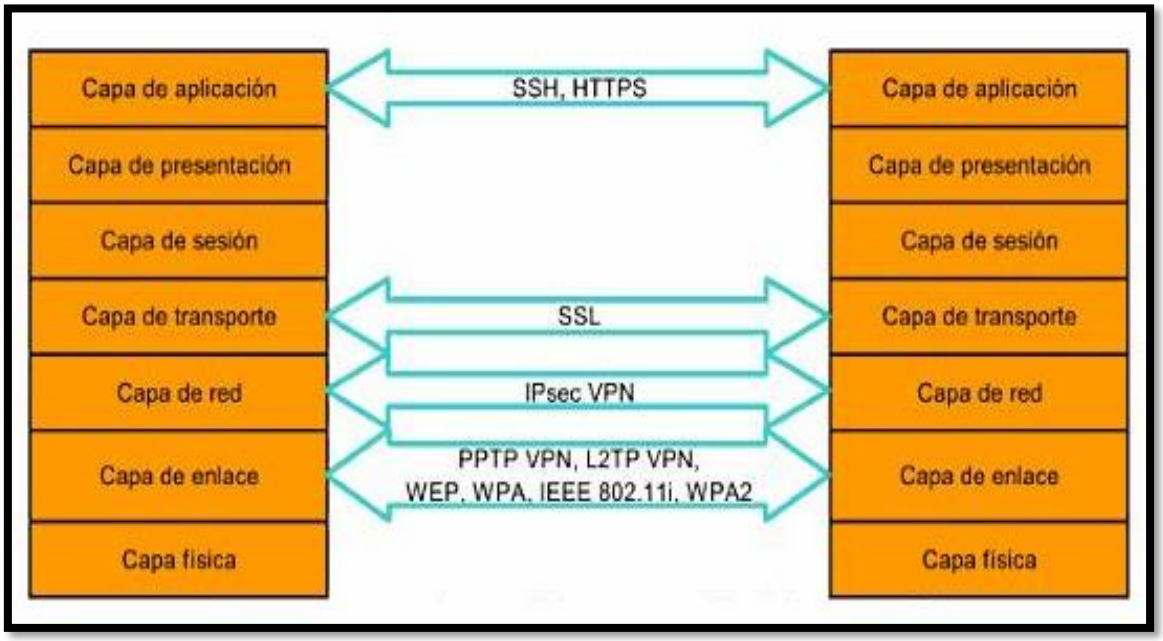
AES es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de EEUU el Instituto Nacional de Estándares y Tecnología (NIST).

Requerimientos de inscripción más fuertes.

Agrega dos mejoras para soportar el roaming de los clientes que se mueven entre los diferentes Access Points:

- El soporte caching de la clave PMK (Pair-wise Master key) utilizada en cada sesión entre el AP y el cliente permiten reconectar al cliente a un Access Point que ya haya utilizado sin la necesidad de re-autenticar.
- El soporte de pre-autenticación en WPA2 permite a un cliente pre-autenticar con el Access Point al que se dirige mientras mantiene la conexión con el Access Point que abandona.

Seguridad en el modelo OSI:



Configuración de Nodo de Internet

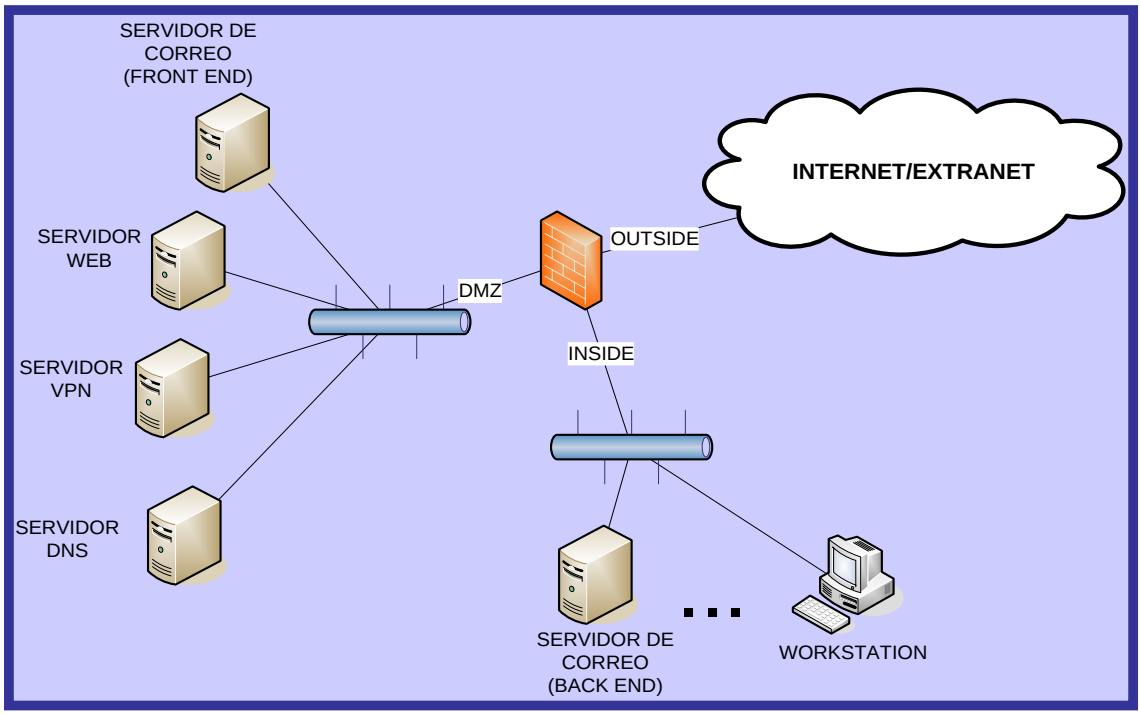
Topología y zonas:

Son secciones aisladas a través de un dispositivo Firewall. Habitualmente existen 3 zonas básicas: **Inside, DMZ, Outside**.

Cada una de estas zonas posee un nivel de seguridad distinto, yendo de mayor a menor nivel respectivamente.

Estas zonas deben ser definidas en función de los servicios que debe prestar cada equipo conectado a las mismas, considerando los accesos seguros y no seguros que deben soportar.

Estas zonas pueden ser asiladas de forma física (Diferentes NICs) o lógica (VLANS).



Zona Outside:

Es el área no segura.

Los dispositivos que se encuentran conectados a esta sección o zona se encuentran fuera del control de los administradores de seguridad o de la compañía.

Puede ser origen de conexiones con malas intenciones, por lo que deben proveerse los mecanismos de defensa y restricciones adecuados para evitar intrusiones o accesos indebidos.

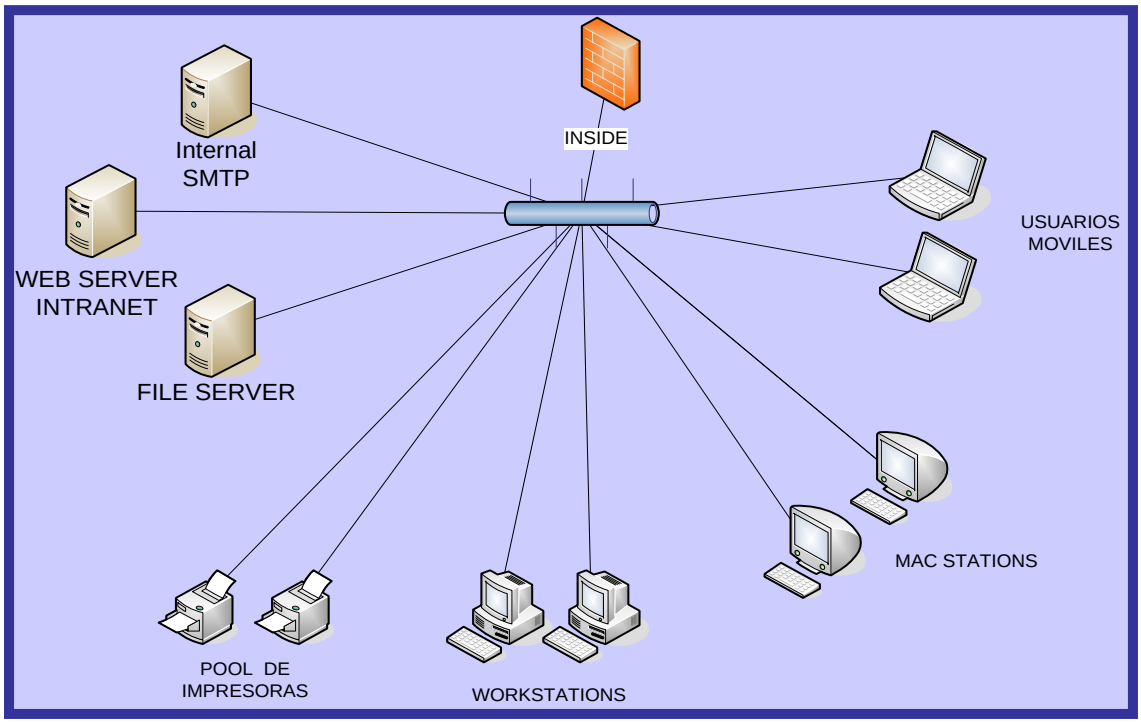
Zona Inside:

Es la zona más segura de la red.

Se distingue por la configuración restrictiva respecto de las otras zonas de seguridad.

Nunca debe poder ser accedida desde el exterior en forma directa.

En esta zona pueden residir los Servidores de Correo Electrónico Interno (SMTP), el servidor proxy, el servidor web interno, el servidor de nombre de dominio interno (DNS Interno), etc.



Zona DMZ:

Es donde se alojan los equipos que podrán ser accedidos desde el exterior y el interior de la red.

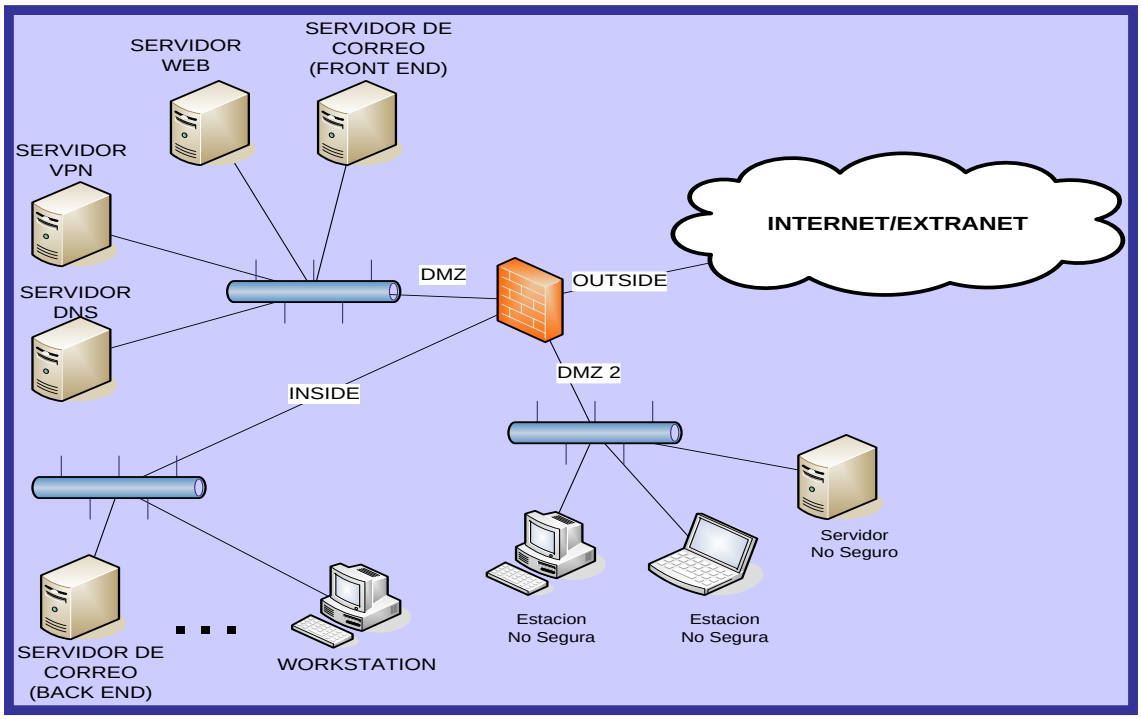
Se caracteriza por poseer cierta flexibilidad en las políticas de servicios en comparación a la zona Inside (Inflexible).

En esta zona pueden residir los servidores de correo electrónico externo (SMTP), el servidor web externo, webmail, etc.

Otras Zonas:

Son aquellas que contienen equipos que, aun cuando pertenecen a la institución, no se consideran suficientemente seguros como para ser integrados dentro de la red institucional.

En esta zona pueden residir los servidores de acceso remoto para usuarios externos conectados por módem, máquinas para capacitación, etc.



Zona de Sistemas Legacy:

Corresponde a la parte de la topología del nodo que contiene a la red con servidores de sistemas que perduran en el tiempo y son los sistemas administrativos y de gestión más sensibles de la organización.

Es la zona de mayor seguridad dentro de la topología de la red.

Puede estar protegido por un Firewall, Proxy o Servidor de transacciones seguras.

Servidor Web de Transacciones Seguras:

Posee un sistema operativo asegurado que permite resguardar dentro de esta zona servidores legacy con sistemas críticos (financieros, administrativos, logísticos).

Prohíbe todos los servicios de Internet que accedan a esta zona y pongan en peligro la operatividad de los mismos.

Ejemplos: FTP, Telnet.

Es un servidor de seguridad para nodos de Internet diseñado para proteger los sistemas legacy y las bases de datos puestas a disposición para consultas de usuarios de Internet.

Consiste en un computador con una interfaz de red de doble boca, que hace de pasarela (Gateway) entre la zona de Intranet / Internet y la zona de seguridad en la red definida a tal efecto.

Servidor Web de Transacciones Intermedias:

En caso que el usuario de Internet necesite acceder a servicios de esta zona se debe establecer un servidor intermedio web que atienda las consultas de usuarios y solicite los datos a los sistemas legacy cumpliendo así con la teoría del modelo de N-capas.

Ningún usuario habilitado a realizar consultas podrá acceder directamente a los servidores legacy, teniendo que comunicarse obligatoriamente a través de este servidor de Web Intermedio.

Este servidor intercambia los set de datos necesarios para cumplir con las consultas solicitadas y las entrega a los usuarios como una página web.

Por lo tanto es mandatorio definir con autorización de los usuarios que sistemas se podrán acceder y que usuarios están autorizados a realizar dichas consultas.

Políticas de Restricción de Servicios:

- FTP → Seguridad
- TELNET → Prohibido
- SSH → Restringido
- IRC – ICQ → Ancho de banda
- REAL AUDIO → Ancho de banda
- File Mgmt. → Restricción de lugares y cuotas
- Mail Mgmt. → Restricción de atacheados
- Mail Mgmt. → Filtro Spam activado
- Bw Mgmt. → Restricción de ancho de banda
- Antivirus → HTTP, MAIL, FTP y aplicaciones

Sistemas de detección de intrusos:

Los sistemas de detección de intrusos (IDS/IPS – Intrusion Detection/Prevention Systems) permiten detectar ataques, registrarlos y dar aviso en la medida que se produzcan.

Identifican el tráfico que viola las políticas de seguridad a través de análisis de protocolo y búsquedas de contenido pudiendo finalizar de manera automática cualquier sesión transgresora.

Es también un programa encargado de vigilar y auditar los puertos disponibles en un nodo de Internet.

Sobre los accesos indebidos o servicios prohibidos de intentos de usuarios no autorizados, genera las alertas necesarias registrando la información respectiva de la solicitud o incursión.

A través de una consola de gestión centralizada permiten monitorear y controlar toda la red así como definir reglas y políticas.

Manejan en forma automática la gestión e instalación de parches.

Políticas de Restricción de Servicios:

El **Protocolo Sencillo de Administración de Redes (SNMP)** puede utilizarse para examinar la tabla de ruteo en un dispositivo, esto sirve para aprender los detalles más íntimos acerca del objetivo de la topología de red perteneciente a una organización. Es un servicio prohibido para usuarios externos con respecto a los servidores de los nodos y topologías de Intranet.

TraceRoute puede utilizarse para relevar el número de redes intermedias y los ruteadores en torno al servidor especifico. Por medio de dicho programa se puede verificar la ruta que realiza un conjunto de paquetes o bloques de información a través de una red de Internet. Los nodos de Internet prohíben el uso de dicho programa a través de sus servidores o su Intranet.

Whois es un servicio de información que provee datos acerca de todos los dominios DNS y el administrador del sistema responsable para cada dominio. No obstante que esta información normalmente es anticuada.

Ping es un software que puede ser empleado para localizar un servidor particular y determinar si se puede alcanzar. Esta simple herramienta puede ser usada como un programa de escaneo que por medio de solitudes a la dirección de un servidor haga posible construir una lista de los servidores que actualmente son residentes en la red.

Rutinas Anti-Spoofing: Los Firewall están dotados de una regla que evita el procedimiento que cambia la fuente de origen de un conjunto de datos en una red, por ejemplo adoptando otra identidad de remitente para engañar al mismo. Esta regla se la denomina Zero Spoofing y es activada para identificar correctamente a corresponsales y remitentes para que no oculten su identidad o procedencia dentro de la red.

Ataques y amenazas

Denegación de Servicio (DoS):

Un ataque DoS es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

Intenta corromper/saturar los recursos de un sistema por medio de peticiones para lograr la desactivación o impedir el acceso a otros usuarios.

Busca la imposibilidad de la víctima de acceder y/o permitir el acceso a un recurso determinado.

Provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema.

Un ataque DoS puede generar:

- Un consumo de recursos computacionales, tales como ancho de banda, espacio de disco, o tiempo de procesador.
- Una alteración de información de configuración, tales como información de rutas de encaminamiento.
- Una alteración de información de estado, tales como interrupción de sesiones TCP.

- Una interrupción de componentes físicos de red.
- Una obstrucción de medios de comunicación entre usuarios de un servicio y la víctima, de manera que no puedan comunicarse adecuadamente.

Algunos ataques DoS son:

- Inundación SYN (SYN Flood).
- Inundación ICMP (ICMP Flood).
- SMURF (ICMP Flood).
- Inundación UDP (UDP Flood).
- Peer-to-peer.
- Utilización de recursos.
- A nivel de aplicación.
- Degradación de servicio.
- Slowloris (HTTP requests parciales. low-rate).
- BotNet.

Jamming o Flooding (DDoS):

La técnica de Flooding o inundación busca generar solicitudes maliciosas a un servicio con la finalidad de hacer que el mismo se sature o entre en un modo de espera, de esta forma anula o limita su funcionamiento.

Son ataques que saturan los recursos del sistema, como memoria, disco o red.

Se producen mediante peticiones de conexión utilizando una IP falsa.

Los más conocidos de este tipo son el “ping de la muerte” (bloqueando el equipo) o el envío de cientos de mails al mismo tiempo.

Syn Flood (DoS):

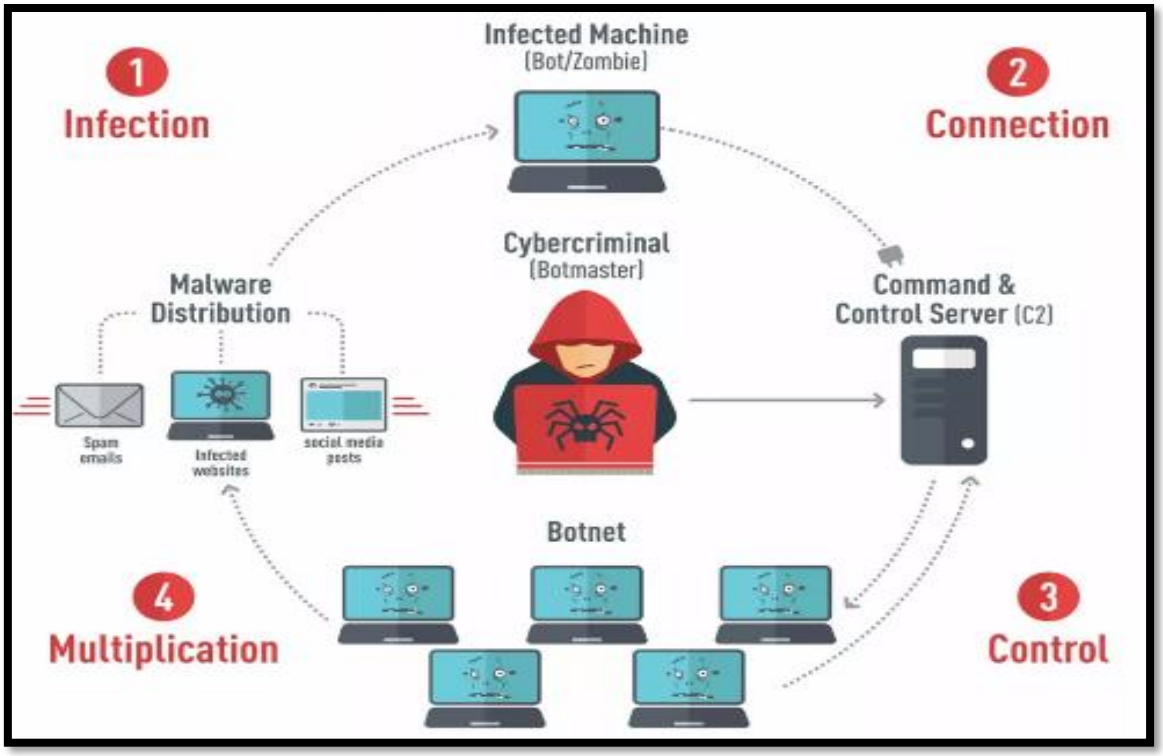
El ataque se basa con el comienzo de cientos de conexiones a un servidor, e interrumpiéndola inmediatamente.

BotNet (DoS):

Es un conjunto o red de robots informáticos, terminales o bots, que se ejecutan de manera autónoma y automática. Ejecutan software que permite su control total o parcial desde ubicaciones remotas.

Las terminales se denominan bots o zombies.

El atacante de la botnet puede controlar todos los terminales/servidores infectados de forma remota.



Connection Flood:

Se basa en la característica de los ISP de tener un tope máximo de conexiones por falta de balanceo de carga.

Mail Bombing:

Envío masivo de mails a un mismo destinatario saturando la casilla de mail.

Mail Spamming:

Es enviar publicidad sin la previa autorización del usuario. El concepto de spamming se aplica a blogs, redes sociales y telefonía móvil.

Port Scanning (Escaneo de Puertos):

Se busca encontrar puertos abiertos mediante un escaneo de IP, realizado por rangos o a una IP en particular.

Los Firewalls actuales identifican el escaneo de puertos consecutivos y detienen el ataque, aunque hay escaneos no consecutivos y alternativos entre IP para despistar a los dispositivos de seguridad.

Tipos de escaneo:

- **Conexión TCPconnect():** Búsqueda de un puerto abierto.
- **FTP Bounce Attack:** Conexión mediante FTP desde un servidor Proxy para dificultar conocer origen del ataque.
- **TCP SYN:** Envío de un paquete de comienzo de comunicación determinando puertos abiertos.
- **TCP FIN Stealth Port Scanning:** Envío de un paquete de fin de comunicación para conocer puertos abiertos o cerrados.
- **Escaneo de Fragmentación:** Transmisión de pequeños paquetes para monitorear la red.
- **Eavesdropping-Packet Sniffing:** se "olfatea" los paquetes para detectar IP's.
- **Snooping-Downloading:** ídem al anterior y además se hacen copias locales de los paquetes.

Autenticación:

Estos ataques se caracterizan por la disponibilidad de credenciales reales por parte de un atacante malintencionado. Se toman sesiones ya establecidas por la victima o se obtiene su nombre de usuario y password.

Ataques de autenticación:

- **Hoping:** El atacante ingresa en un sistema ajeno, luego a otro, a otro, para hacer imposible la verdadera localización.
- **IP Session Hijacking:** Una vez que el usuario verdadero ingresa al sistema, se toma esa conexión sin restricciones de seguridad.
- **Obtención de passwords:** Se obtiene la password mediante técnicas de espionaje y aprovechando la poca frecuencia de cambios de password.
- **BackDoors:** Se utiliza un código puesto en sistemas finales para ingresar sin restricciones de seguridad. Permite saltearse métodos de autenticación para realizar determinadas tareas.
- **Exploits:** Son programas que aprovechan la debilidad, fallo o error de un sistema para ingresar al mismo.

Phishing:

Tienen por objetivo el robo de datos personales, de identidad, e información de credenciales financieras.

Se simula un sitio web para capturar datos de login con una pantalla de ingreso al sistema.

Utilizan en combinación ingeniería social y tecnología para alcanzar sus objetivos.

El phishing no se presenta exclusivamente para los robos de identidad directa, también se manifiesta en la instalación de software malicioso.

Algunos ejemplos utilizados son:

- Emails falsificados y forjados.
- Llamadas telefónicas para "corroborar" información.
- Robo de identidad autoritativa para la obtención de información por niveles menores.

Pharming:

Consiste en el robo de identidad, pero no de un usuario, sino de un sitio web.

Utilizan técnicas de "DNS Hijacking" y "DNS Poisoning" que consisten en la publicación ilegitima de resolución de un dominio mediante la modificación de los registros de un servidor DNS.

Otra técnica es registrar un dominio parecido y "pescar" a los desprevenidos.

Por ejemplo, si un atacante ganara acceso a mi DNS podría cambiar el apuntamiento de un dominio como www.mibanco.com con un IP A, hacia un IP X. Cuando yo intente entrar a www.mibanco.com en realidad estaré viendo la página que el atacante me quiera mostrar, pues para mi DNS, el nombre de dominio mibanco.com resolverá al IP X en lugar de la IP original que es el A.

Spoofing:

Consiste en sustituir la fuente origen por datos adulterados, adoptando una identidad falsa.

La **suplantación de identidad o spoofing** hace referencia al uso de técnicas a través de las cuales un atacante se hace pasar por una entidad distinta a través de la falsificación de los datos en una comunicación.

Consiste en usurpar una identidad electrónica para ocultar la propia identidad y así cometer delitos en Internet.

El objetivo es engañar a la seguridad para conseguir acceso a recursos de un tercer sistema que ha establecido algún tipo de confianza basada en el nombre o la dirección IP del host suplantado (Firewall/Filtro de Red).

Tipos de Spoofing:

- IP spoofing.
- ARP spoofing.
- DNS spoofing.
- Web spoofing.
- E-mail spoofing.
- Fake-mail: otra forma de spoofing, que consta con el envío de mail con un remitente falso.

Identificadores a suplantar:

- Servicio → Nombres de dominio, direcciones correo electrónico, nombres de recursos compartidos.
- Red → Dirección IP.
- Enlace → Dirección MAC.

Ransomware:

"Secuestro de Datos". Son programas que restringen el acceso a determinadas partes o archivo del sistema operativo infectado:

- Retienen el control del equipo.
- Encriptan la información almacenada en el mismo para que no pueda ser accedida.
- Solicitan un rescate financiero en criptomonedas para que sean desactivados.

Algunos ejemplos son: Peyta, Reveton, Cryptolocker, TorrentLocker, Cryptowall, TeslaCrypt, Mamba, WannaCry, etc.

Ataques Wireless:

Man in the Middle: Consiste en una técnica de sniffing de paquetes circulante e inyección de datos malignos para producir determinados resultados.

ARP Poisoning: Envenenamiento de las tablas de ARP existentes mediante el reclamo de direcciones IP asignadas a otras direcciones físicas.

WEP/WPA header sniffing: Un atacante puede generar a propósito la reconexión de los clientes ya conectados mediante diferentes técnicas, logrando así que se regenere el "handshake" de conexión inicial (el cual no es encriptado).

DDoS: Son utilizados para inhabilitar dispositivos momentáneamente y obligar a los clientes auténticos a solicitar una reconexión a la red. Ocurre cuando se bombardea un AP con pedidos y mensajes falsos y este no tiene capacidad para dar servicios a los usuarios legítimos.

Robo de identidad (MAC Spoofing): "Escuchar" el tráfico de red e identificar la dirección MAC de una computadora para clonarla.

Inyección de red: Inyectar comandos de reconfiguración que afecten a routers, switches. Ocurre en un AP expuesto a tráfico no filtrado.

Virus y Malware

Virus:

Es un programa de terminal que puede infectar otros programas modificándolos para incluir una copia de sí mismo. Tienen la función de propagarse, replicándose, y algunos contienen además una carga dañina.

Se adjuntan a programas o archivos e insertan su propio código "genético" dentro de ellos para propagarse.

Puede provocar desde una simple broma hasta daños importantes en los sistemas o bloquear las redes informáticas generando tráfico inútil.

Los virus inician su dispersión debido a una ejecución intencional (inocente) que provoca la infección y propagación de este software malintencionado. Se pueden prevenir.

Prevención de virus:

Educación a usuarios – Software Antivirus – Aplicación de políticas de seguridad.

El 50% de los casos de infecciones de virus se debe a una ejecución autorizada por el usuario. Las aplicaciones de seguridad, no presentan ninguna ventaja si el usuario no es educado respecto de los virus informáticos.

Las políticas de seguridad resultan fundamentales.

Gusano (worms):

Es un malware que tiene la propiedad de residir en memoria y duplicarse a sí mismo, consumiendo recursos. La velocidad de propagación y transmisión de estos puede provocar saturaciones de sistema y de la red.

No requieren intervención del usuario y se transmiten generalmente por fallas o "agujeros" de seguridad existentes, los cuales aprovechan para vulnerar los sistemas.

La infección de una sola estación puede significar el contagio de toda una red.

Trojans (Troyanos – Caballos de Troya):

Un troyano es un malware escondido dentro de una aplicación que aparenta ser legítima. En la mayoría de los casos los usuarios no se percatan que tienen uno instalado en su máquina, y el nivel de daños que pueden provocar varia ampliamente.

Abren puertas traseras (backdoors) que son utilizadas para acceder a las computadoras víctima de forma remota y usarlas como zombies.

Pueden expandirse masivamente por ordenadores no protegidos (sin Firewall).

Las terminales/computadoras infectadas son utilizados por el spammer como zombies, que envían spam a sus órdenes, pudiendo incluso rastrear los discos duros o correos nuevos (sobre todo cadenas) en busca de más direcciones.

El usuario ignora haber sido infectado y al ser identificado como spammer por los servidores a los que envía spam sin saberlo, lo que puede conducir a que no se le deje acceder a determinadas páginas o servicios.

Actualmente, el 40% de los mensajes de spam se envían de esta forma.

Antivirus:

Su función primordial es la prevención de ejecución de código malicioso y su replicación en memoria. Analizan desde archivos hasta comunicaciones (E-mail, trafico web, etc.)

Son una necesidad básica de cualquier computadora, desde hogareñas hasta servidores corporativos.

La defensa de estos ante un virus informático depende de la brecha de tiempo entre el reporte del incidente de seguridad y la respuesta y solución por parte del fabricante.

Las diferentes empresas de seguridad se atribuyen la mejor detección, pero la realidad es que el disponer de un antivirus instalado no asegura la protección total de una computadora o servidor.

No protegen la computadora de vulnerabilidades particulares de algunas aplicaciones de servicio, sin embargo generalmente si lo hacen con los servicios estándar del S.O.

Appliances Antivirus:

Son dispositivos de hardware avocados al análisis de protocolos y aplicaciones en particular. Proveen una independencia en cuanto a capacidad de procesamiento de las computadoras que protegen.

Están colocados de forma perimetral, ya que no pueden actuar directamente sobre las estaciones de trabajo sino sobre las comunicaciones que se llevan a cabo en la red.

Son independientes del sistema operativo usado en la estación de trabajo.

Política Antivirus:

- Ejecutar siempre el antivirus corporativo y mantener actualizados tanto el engine como los patrones de virus.
- Nunca abrir archivos o macros de remitente desconocido, no confiable sospechoso. Borrarlos y vaciarlos de la papelera.
- Eliminar el spam, cadenas de correo y correo basura similar, sin reenviar.
- Nunca descargar archivos de fuentes sospechosas. En la media de lo posible, ejecutar solamente los programas descargados de la URL original o de la intranet corporativa.
- Evitar las carpetas compartidas salvo que sea requisito indispensable.

- Pasar siempre el antivirus a los dispositivos USB.
- Hacer copia de seguridad regular de los datos críticos y de las configuraciones, y almacenarlos en lugar seguro.
- En caso de conflicto de pruebas de aplicaciones con el antivirus, pasarlo primero antes de deshabilitarlo. Pasar posteriormente la prueba e inmediatamente volver a activar el antivirus.
- Comprobar la política frecuentemente, debido a que prácticamente a diario se descubren nuevas formas de infección que podrían requerir un cambio en el procedimiento.

Spyware:

Se llama **"pest" (peste o alimaña)** a toda aplicación instalada en el PC de un usuario, sin su consentimiento o como parte de un consentimiento genérico, que habitualmente se ejecuta en background y es resistente a su desinstalación. El objetivo suele ser ilícito o por lo menos no acordado con el usuario.

Los **Spyware** son aplicaciones cuyo objetivo es enviar información del sistema donde reside mediante la utilización de la conexión de red en forma oculta a empresas de publicidad en Internet.

Su objetivo principal es el envio de información de los usuarios en cuanto al comportamiento de navegación web y hábitos de consumos (compras online, hábitos de registro en páginas, newsfeeds, seguimiento de banners publicitarios) sin que el usuario tome conocimiento de esto. En función del análisis de este comportamiento las empresas dueñas de este software envían al cliente un aviso publicitario acorde a esa información.

Muchas veces, estos avisos publicitarios surgen en forma de popups.

Es software ilegitimo, contenido dentro de otro software útil o legitimado por el usuario. En algunos casos este software no solicita el consentimiento del usuario para instalarse.

Teniendo una gran similitud con los Troyanos, estos programas no presentan un peligro (manipulación o daño) para el sistema afectado, pero si violan la privacidad de la información.

Se introducen en los sistemas por un medio simple: la instalación de productos shareware por decisión propia de los usuarios que brindan alguna supuesta utilidad.

Son bibliotecas de vínculos dinámicos (.dll) con la funcionalidad de informar las webs visitadas, duración, banners, direcciones de mail, además modifican la registry para actuar.

La diferencia de funcionamiento con un virus, es que el Spyware generalmente no posee capacidades de replicarse a sí mismo.

Software Anti-Spyware:

El objetivo de este software es la remover y prevenir la ejecución del software espía o spyware, que se han convertido en una importante preocupación en cuanto a materia de

seguridad de la información, el 90% de las máquinas conectadas a Internet están infectadas con este software y que el 86% ha sufrido pérdidas económicas debido al Spyware.

Keylogger:

Es un software o hardware específico que se encarga de registrar las pulsaciones que se realizan en el teclado, para posteriormente memorizarlas en un archivo o enviarlas a través de internet.

SPAM:

Son mensajes no solicitados, habitualmente de tipo publicitario, enviados en cantidades masivas. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es la basada en el correo electrónico.

Generalmente el origen de estos correos son servidores fantasma y las direcciones de remitente son falsas.

Este tipo de envio de correo masivo son utilizados para el fraude electrónico tipo phishing.

Software y Appliances AntiSpam:

Su función es la del análisis de del contenido de los correos electrónicos para clasificarlos y determinar si estos cumplen con los requisitos para ser clasificados como SPAM y separarlos de los mails legítimos.

Este tipo de aplicaciones trabajan sobre los protocolos de correo electrónico (Pop3, ESMTP, SMTP, IMAP, etc.).

Existen listas de bloqueo llamadas “blacklists” donde figuran listados de direcciones de mail, dominios, y proveedores de Internet que realizan SPAM.

También pueden ser identificados por bloque de dirección IP (generalmente asociado a un ISP).

Centro de operaciones de seguridad (SOC):

Es una unidad centralizada compuesta por personas capacitadas, procesos y tecnologías que trabajan en conjunto para brindar capacidades de seguridad integrales.

Incluyen la prevención, detección e investigación, y respuesta a amenazas e incidentes de ciberseguridad.

Visibilidad centralizada de toda la actividad que ocurre en su entorno.

Un SOC proporciona las siguientes capacidades:

- Detección y respuesta de amenazas en tiempo real.
- Supervisión 24x7 de los datos del registro del sistema y del tráfico de la red.
- Una visión integral y centralizada de la postura de seguridad de una empresa.

- Caza e investigación de amenazas.
- Administración de usuarios, aplicaciones y procesos.

Monitores de seguridad (Endpoints – DLP):

Monitorizan centralizadamente la red, detectan dispositivos conectados y realizan varias tareas, como impedir la introducción de software malicioso o no autorizado.

Los **sistemas de ciberseguridad Endpoint**, que se pueden adquirir como software o como un dispositivo dedicado, sirven para descubrir, gestionar y controlar los dispositivos que solicitan acceso a la red corporativa de nuestra empresa. Evita la fuga y el robo de información mediante el control integral del acceso a dispositivos portátiles de almacenamiento con mínimo esfuerzo administrativo. Protege automáticamente equipos detectados desplegando un agente y una directiva de bloqueo predefinida.

Firewall Personal

Es una barrera de seguridad para el acceso a las comunicaciones de la terminal. Proporciona un balance óptimo entre seguridad y accesibilidad. Habilita o deshabilita el acceso a servicios.

Control de puertos:

Los Firewalls actuales controlan los puertos actuando sobre los paquetes y aplicaciones. Consiste en controlar puertos abiertos mediante una aplicación de seguridad en memoria.

Pueden configurarse en forma manual o automática.

Firma digital

Es un conjunto de datos asociados a un mensaje digital que permite garantizar la identidad del firmante y la integridad del mensaje. Sus beneficios son la garantía de procedencia, seguridad de no intervención, e identificación del firmante.

No es una firma escrita, es un software basado en algoritmos (como Diffie Hellman, RSA, DSA, PGP, etc.).

Todos los algoritmos se basan en un mismo método:

- Se utilizan dos claves, una pública y otra privada.
- Encriptado/Desencriptado de claves.
- Operaciones matemáticas con números primos.

Aplicaciones de Firma Digital:

- Mensajes con autenticidad asegurada.
- Contratos comerciales electrónicos.
- Factura electrónica.
- Transacciones comerciales electrónicas.
- Dinero electrónico.

Seguridad de la Firma Digital:

- Autenticación.
- Imposibilidad de suplantación.
- Integridad.
- No repudio.
- Auditabilidad.
- Acuerdo de claves secretas.

El remitente se encarga de:

- Escritura del mensaje.
- Hashing del texto (con un algoritmo).
- Encriptación con clave privada.
- Firma Digital.
- Envío del texto con la Firma Digital.

Y el destinatario de:

- Recepción del texto del mensaje y firma.
- Hashing del texto (con la clave pública).
- Desencriptado de la firma.
- Comparación de los mensajes (igualdad de mensajes).
- Remitente válido.
- Mensaje sin alteraciones.

Métodos criptográficos:

- **Método simétrico:** Es un algoritmo de encriptación tal que la clave para encriptar es la misma que para desencriptar. Algunos de estos algoritmos son: DES, 3DES, RC2, RC4, IDEA, etc.
- **Método asimétrico:** Es un algoritmo que utiliza claves distintas para encriptar y para desencriptar. Son los únicos métodos que permiten identificar al emisor de un mensaje, y por lo tanto los únicos que permiten implementar la firma digital. Algunos de estos algoritmos son: RSA, DSA, etc.

Ventajas y desventajas de los algoritmos simétricos y asimétricos:

- Los **algoritmos simétricos** son mucho más rápidos que los asimétricos, pero tienen el problema de que es necesario distribuir las claves, dado que el emisor y el receptor deben usar las mismas en cada comunicación.
- Los **métodos asimétricos** usan claves distintas, con lo que se evita el problema de la distribución, pero son lentos.
- La solución usada universalmente es llegar a claves comunes con un método asimétrico y luego cambiar a uno simétrico para la transmisión masiva.

Firma electrónica:

La firma electrónica es una manera de representación y confirmación de la identidad de un sujeto en el medio electrónico. Técnicamente, es un conjunto de datos únicos encriptados.

Diferencias entre una firma digital y una firma electrónica:

FIRMA ELECTRÓNICA	FIRMA DIGITAL
No hay transformación.	*Es la transformación de la firma de un mensaje.*
No se usan claves.	*Se utiliza una clave pública y otra privada.*
Se utiliza para identificar a su emisor (signatario).	*Asegura la autoría.*
No asegura su integridad.	*Asegura la integridad del mensaje.*
Puede ser la representación electrónica de una firma hológrafa.	*No es una representación electrónica de una firma hológrafa.*
Puede ser estampada por medio de elementos de Digitalización.	*Es una subcategoría dentro de la firma electrónica.*
Lo electrónico se vincula con otras tecnologías como la mecánica, magnética, eléctrica, óptica.	*No se vincula con otra tecnología especifica.*
En caso de ser desconocida corresponde a quien la invoca acreditar su validez.	*Se presume válido, salvo prueba en contrario.*

Certificado de Seguridad:

Imagine que envía cartas por correo en un sobre transparente, cualquiera que tenga acceso a él podrá ver los datos. Si parece valiosa, pueden hacerse con esa información o modificarla.

La **autoridad de certificación** es la encargada de emitir los certificados, verifican el nombre de dominio y la existencia de su empresa, la propiedad del nombre de dominio y su potestad para solicitar el certificado. Una entidad autorizada, denominada autoridad de certificación, es la encargada de emitir los certificados SSL.

Un **certificado SSL** establece un canal de comunicaciones privado que permite cifrar los datos durante su transmisión. El cifrado codifica los datos, fundamentalmente creando un sobre que preserva la confidencialidad del mensaje.