TEMA 125

LA SEGURIDAD EN REDES. TIPOS DE ATAQUES Y HERRAMIENTAS PARA SU PREVENCIÓN: CORTAFUEGOS, CONTROL DE ACCESOS E INTRUSIONES, TÉCNICAS CRIPTOGRÁFICAS, ETC. MEDIDAS ESPECÍFICAS PARA LAS COMUNICACIONES MÓVILES.

Versión	30.1
Fecha de actualización	09/09/2024

1. La Seguridad en las Redes

Las infraestructuras TIC operan en un entorno hostil en el que las amenazas y riesgos comprometen su utilidad, en forma de ciberincidentes.

Los tipos de ataques en las redes son:

1. **Interrupción**: Ataque a la **disponibilidad** de un sistema con el fin de destruir o dejar inutilizable/no disponible.
2. **Interceptación**: Ataque a la **confidencialidad** donde no hay una alteración del sistema, uno de los ejemplos más conocidos es el acceso a la base de datos.
3. **Modificación**: ataque contra la **integridad** de un sistema en el que se accede a un recurso y se manipula.
4. **Suplantación** o Fabricación: ataque contra la **autenticidad** en la que el atacante añade información falsificada, por ejemplo suplantación de una dirección IP.

La **guía CCN-STIC 817 Gestión de ciberincidentes** resume en la siguiente tabla la clasificación de los ciberincidentes atendiendo a la ruta o camino que utiliza un atacante para tener acceso al activo atacado (vector de ataque).

Vector de ataque		Tipo de ciberincidente
Código dañino	Software cuyo objetivo es infiltrarse o dañar un ordenador, servidor u otro dispositivo de red, sin el conocimiento de su responsable o usuario y con finalidades muy diversas.	· Virus · Gusanos · Troyanos · Spyware · Rootkit · Ransonware · Remote Access Tools (RAT)

Disponibilidad	Ataques dirigidos a poner fuera de servicio los sistemas, al objeto de causar daños en la productividad y/o la imagen de las instituciones atacadas.	· Denegación de servicio (DoS) y Denegación de servicio distribuida (DDoS) · Fallo (HW/SW) · Error humano · Sabotaje
Obtención de información	Ataques dirigidos a recabar información fundamental que permita avanzar en ataques más sofisticados, a través de ingeniería social o de identificación de vulnerabilidades	· Identificación de vulnerabilidades (scanning) · Sniffing · Ingeniería social · Phishing
Intrusiones	Ataques dirigidos a la explotación de vulnerabilidades de diseño, de operación o de configuración de diferentes tecnologías, al objeto de introducirse de forma fraudulenta en los sistemas de una organización.	· Compromiso de cuenta de usuario · Cross-Site Scripting (XSS) · Cross-Site Request Forgery (CSRF, Falsificación de petición entre sitios cruzados) · Inyección SQL · Spear Phishing · Pharming · Ataque de fuerza bruta · Inyección de ficheros remota · Explotación de vulnerabilidad sw · Explotación de vulnerabilidad hw
Compromiso de la información	Incidentes relacionados con el acceso y fuga (Confidencialidad), modificación o borrado (Integridad) de información no pública.	· Acceso no autorizado a la información · Modificación y borrado no autorizada de información · Publicación no autorizada de información · Exfiltración de información

Fraude	Incidentes relacionados con acciones fraudulentas derivadas de suplantación de identidad, en todas sus variantes.	· Suplantación/Spoofing · Uso de recursos no autorizado · Uso ilegítimo de credenciales · Violaciones de derechos de propiedad intelectual o industrial.
Contenido abusivo	Ataques dirigidos a dañar la imagen de la organización o a utilizar sus medios electrónicos para otros usos ilícitos (tales como la publicidad, la extorsión o, en general, la ciberdelicuencia).	· Spam (Correo basura) · Acoso/ extorsión/ mensajes ofensivos · Pederastia/ racismo/ apología de la violencia, etc.
Política de seguridad	Incidentes relacionados por violaciones de usuarios de las políticas de seguridad aprobadas por la organización.	· Abuso de privilegios por usuarios · Acceso a servicios no autorizados · Sistema desactualizado
Otros	Otros incidentes no incluidos en los apartados anteriores.	

En base al art 33 del ENS, Para la gestión de los incidentes, depende del tipo de gravedad, hay que contar con el apoyo de:

- CCN-CERT: en el ámbito de AAPP´s y organismos públicos.
- CNPIC: para las infraestructuras críticas y servicios esenciales.
- INCIBE: Pymes y ciudadanos.
- Mando Conjunto del Ciberespacio, MCCE: en materia de ciberdefensa.

Para dar cumplimiento al RD 43/2021, se utilizará una única Plataforma Nacional de comunicación de incidentes para apoyar la coordinación y cooperación, y se creará una red nacional de SOCs.

1.1 Normativa de Seguridad

El **ENS** es normativa de **obligado cumplimiento** para el ámbito del sector público definido en la ley 40/2015, e **ISO/IEC 27000** es una familia de estándares de **certificación voluntaria**. No obstante, el ENS establece la obligatoriedad de establecer un proceso integral de seguridad, indicando en su artículo 27 que e*l proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua aplicándose criterios y métodos reconocidos en la práctica nacional*. En este sentido, la familia de normas ISO 27000 goza de gran reconocimiento, y contiene buenas prácticas para desarrollar, implementar y mantener los SGSI (Sistemas de gestión de la seguridad de la información). Se enfocan en procesos de mejora continua (círculo de Deming: Plan – Do – Check – Act.) Las principales normas de la familia 27000 relacionadas con seguridad en las redes, son:

ISO/IEC 27000	Vocabulario estándar para el SGSI. Introducción y base para el resto. No certificable.
ISO/IEC 27001	Establece un marco general para la gestión de la seguridad de la información, que incluye la protección de redes. **Certificable**
ISO/IEC 27002	Ofrece directrices detalladas sobre controles de seguridad, muchos de los cuales están directamente relacionados con la seguridad de redes, como la gestión de acceso, la protección de la red, y la seguridad de los datos en tránsito. No certificable
ISO/IEC 27005	Publicada en 2011 (primera edición), 2008 (segunda edición) y 2018 última versión. No certificable. Proporciona directrices para la gestión del riesgo en la seguridad de la información.
ISO/IEC 27033	Esta es la serie más específica en cuanto a la seguridad de redes dentro de la familia 27000. La ISO/IEC 27033 está dividida en varias partes que abarcan los conceptos generales de seguridad de redes, diseño y arquitectura segura, y directrices para la implementación de controles.

Dentro del **ENS** como normativa de obligado cumplimiento, deberemos atender a las medidas de seguridad en función de la categorización que hayamos obtenido. En relación con la seguridad en las redes podemos destacar las siguientes medidas:

Protección de las Comunicaciones (mp.com) Para proteger las comunicaciones en las redes, asegurando que los datos transmitidos sean seguros y confiables. Esto se conseguirá con un perímetro seguro que separe la red interna del exterior. Se tiene previsto una ITS de interconexión de redes para profundizar en los requisitos de estos perímetros.

Control de Accesos (op.acc) Para proteger el acceso a las redes y a los recursos que en ellas se encuentran, previniendo accesos no autorizados, implementando mecanismos de control de acceso a las redes, como autenticación de usuarios y dispositivos, listas de control de acceso (ACL) y segmentación de la red, para limitar el acceso solo a usuarios autorizados.

Monitorización del sistema(op.mon) Medidas destinadas a la monitorización continua de la red para detectar y responder a incidentes de seguridad. Por ejemplo mediante mecanismos que detecten intrusiones (IDS, IPS, sistemas de vigilancia, instauración de métricas que sirvan para evaluar la eficiencia del sistema...)

Gestión de la configuración de seguridad (op.exp.3) Para que las redes y sus componentes estén configurados de manera segura. Asegurando que los dispositivos de red, como routers y switches, estén configurados de manera segura, desactivando servicios innecesarios y aplicando contraseñas robustas y actualizadas.

Además, para la gestión de seguridad de las redes, destacan las siguientes guías:

Guía CCN-STIC-801 Responsibilidades y Funciones

Guía CCN-STIC 807 Criptología de empleo en el ENS

Guía CCn-STIC-811 Interconexión en el ENS

Guía CCN-STIC-817 Gestión de Ciberincidentes

MAGERIT es una metodología desarrollada por CCN para la gestión de riesgos en los sistemas de información, lo cual incluye la seguridad de las redes. Esta metodología proporciona un marco

estructurado para identificar, analizar y gestionar riesgos en cualquier componente del sistema de información, incluidas las infraestructuras de red. Además facilita el cumplimiento de normativas y estándares relacionados con la seguridad en redes, como ISO/IEC 27001 o la Directiva NIS

A nivel europeo, Estrategia de Ciberseguridad de la UE (2020) establece la dirección futura de las políticas y normativas de ciberseguridad en la UE, incluyendo la protección de redes y la cooperación transfronteriza. En el marco de la UE, además, destacan las normas de:

Directiva NIS2 (Directiva de Seguridad de Redes y Sistemas de Información): tiene como objetivo fortalecer la ciberseguridad en la Unión Europea. Se enfoca en proteger a las empresas y servicios esenciales, como los sectores de energía, transporte, salud, y otros.

Cybersecurity Act (Reglamento 2019/881) Fortalece el mandato de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) y establece un marco europeo de certificación de ciberseguridad.

2. Tipos de Ataques y Herramientas para su prevención

2.1 Tipos de Ataques

2.1.1 Ataques de Denegación de Servicio

Los ataques de denegación de servicio DoS afectan a la disponibilidad del sistema saturando el servicio o dejándolo inutilizado:

- ***DDoS (Distributed Denial of Service)***
- DRDoS (Distributed Reflection Denial Of Service)
- Connection Flood: inundación de conexiones
- SYN flooding: envío de mensajes SYN sin completar el proceso de conexión TCP
- ***Teardrop***: envío de fragmentos IP que el receptor no puede recomponer
- ICMP flooding
- UDP flooding
- ***Smurf***: envío de peticiones de eco ICMP (ping) a direcciones broadcast empleando como dirección de origen la dirección IP de la máquina a atacar (provoca saturación de tal dirección IP con las respuestas que se generan)
- **PING de la muerte**: envío de *ping request* de tamaño superior al permitido
- INVITE de la muerte (en protocolo SIP)
- ***Buffer overflow***

2.1.2 Ataques de suplantación

- Suplantación de identidad por medios técnicos: ***Spoofing***
  - MAC-spoofing
  - ARP-spoofing
  - IP-spoofing

  - DHCP-spoofing
  - DNS-spoofing
  - Mail-spoofing
  - Web-spoofing
  - ***Decoy***: simulación de interfaz web para obtener las contraseñas
  - Hijacking
- Suplantación de identidad mediante ingeniería social: ***Phising***

2.1.3 Ataques de Monitorización, Escucha y Manipulación

- *Port* ***Scanning*** (SYN Scan, RST Scan, TTL Scan): empleados para determinar si un puerto está abierto, cerrado o protegido por un cortafuegos.
- ***Sniffing***: análisis de tráfico capturado en las tarjetas de red
- ***MitM (Man In The Middle):*** interceptación de tráfico entre dos sistemas con posibilidad de inyección, modificación y repetición. Puede ser empleado para, ***replay attack, eavesdropping*** y ***hijacking*** entre otros
- ***Keylogger***: Herramientas que registran las pulsaciones del teclado para capturar información sensible como contraseñas o datos privados.
- ***Tampering o data diddling:*** Modificación no autorizada de datos durante su entrada o salida, alterando la información legítima para beneficio malintencionado.
- ***Malware***: Software malicioso diseñado para dañar, interrumpir, robar o causar impacto negativo en los sistemas informáticos. Incluye:
  - **Virus**: Programas que se insertan en otros archivos y se propagan cuando son ejecutados.
  - **Gusanos** (Worms): Programas autónomos que se replican en redes, consumiendo recursos y provocando caídas de sistemas.
  - **Troyanos**: Programas maliciosos que se disfrazan de software legítimo y permiten acceso no autorizado al sistema.
  - **Bombas Lógicas**: Código malicioso que se activa bajo ciertas condiciones, como fechas específicas o cambios en el sistema.

2.1.4 Ataques de Inyección

Estos ataques tienen como objetivo insertar código malicioso en sistemas o aplicaciones para alterar su funcionamiento o acceder a datos sensibles.

- **SQL Injection**: Inyección de código SQL en consultas a bases de datos para acceder, modificar o eliminar información no autorizada.
- **Code Injection:** Inserción de código malicioso en aplicaciones que se ejecutan en servidores o sistemas.
- **Cross-Site Scripting (XSS):** Inserción de scripts maliciosos en sitios web que se ejecutan en el navegador de la víctima, robando cookies o realizando acciones no autorizadas.

2.1.5 Ataques a Contraseñas

Consisten en obtener acceso no autorizado mediante el descubrimiento o robo de contraseñas.

- **Brute Force Attack:** Intento de adivinar contraseñas mediante pruebas exhaustivas de combinaciones posibles.
- **Dictionary Attack:** Uso de listas predefinidas de contraseñas comunes para acceder a cuentas.
- **Credential Stuffing:** Uso de combinaciones de usuario y contraseña robadas de otros servicios en múltiples plataformas para obtener acceso.

2.1.6 Ataques de Software y Sistema

Explotan vulnerabilidades en software o configuraciones de sistemas para acceder a recursos restringidos.

- **Exploits:** Código o técnicas que aprovechan vulnerabilidades conocidas en software para obtener acceso no autorizado o realizar acciones maliciosas.
- **Zero-Day:** Ataques que aprovechan vulnerabilidades desconocidas o sin parchear, lo que las hace especialmente peligrosas.
- **Ransomware:** Malware que cifra los datos del sistema y solicita un rescate para su liberación.

2.1.7 Contramedidas y Protecciones

Para protegerse contra estos ataques, es esencial implementar buenas prácticas de seguridad, como:

- **Actualización y Parcheo:** Mantener sistemas y software actualizados para cerrar vulnerabilidades conocidas.
- **Cifrado de Datos:** Proteger la información sensible con algoritmos de cifrado para prevenir accesos no autorizados.
- **Autenticación Multifactor (MFA):** Añadir capas adicionales de verificación para acceder a sistemas críticos.
- **Monitorización y Auditoría:** Revisar regularmente registros de actividad y tráfico de red para identificar y responder a comportamientos sospechosos.
- **Educación en Seguridad:** Capacitar a los usuarios y empleados sobre los riesgos de seguridad y cómo identificar posibles amenazas.

2.2 Herramientas de Prevención

2.2.1 Cortafuegos

Interconectan segmentos de red y establecen controles de acceso entre ellos. Cada vez incorporan más funcionalidades propias de otros dispositivos como **IDS** e **IPS**. La guía ***"CCN-STIC-811 Interconexión en el ENS"*** trata en profundidad los dispositivos de protección perimetral con especial atención a los cortafuegos.

MODO TÍPICO DE FUNCIONAMIENTO:

- Los firewalls disponen de una **lista de patrones** y acciones asociadas
  - Los patrones pueden basarse en campos de cabeceras o protocolos de aplicación, entre otros.
  - Las **acciones asociadas** pueden ser, entre otros, DENY o ACCEPT
  - La lista se encuentra priorizada, existiendo una **acción por defecto** que se aplica en caso de que el tráfico analizado no cumpla ninguno de los patrones. (DENY ALL o ACCEPT ALL)
- El firewall captura todo el tráfico recibido en las interfaces de red, compara el tráfico con los patrones de la lista y aplica la acción asociada o la acción por defecto

Al configurar los firewalls se puede optar por dos **tipos de políticas**:

- ***Política restrictiva*** (MÁS SEGURO): sólo se permite el tráfico explícitamente autorizado en un patrón de la lista, mientras que el resto se bloquea (la acción por defecto es ***deny all***).

- ***Política permisiva***: se permite todo el tráfico excepto el explícitamente bloqueado en alguno de los patrones (la acción por defecto es ***accept all***).

Además de realizar el filtrado de tráfico, los firewalls suelen proporcionar servicios adicionales como **NAT**, terminación túneles **VPN** o sistemas **IPS/IDS**.

TIPOS DE FIREWALL SEGÚN EL NIVEL EN EL QUE OPERAN:

FIREWALL DE RED: el filtrado de paquetes se basa en información de cabeceras IP y TCP, como:

- Interfaz por la que se recibió el paquete
- Direcciones IP
- Protocolo superior: TCP, UDP, ICMP
- Flags TCP
- Puerto (80, 25, etc)

Existen dos tipos diferentes de firewall a nivel de red:

- ***Stateless packet filter (estático):*** analizan cada paquete de manera independiente y realizan el filtrado en función de campos de la cabecera del mismo. Es muy eficiente, pero no permite detectar ataques como el ataque TCP SCAN o TTL SCAN
- ***Statefull packet filter (dinámico):*** mantienen información sobre el estado de las sesiones que se están cursando, lo cual permite realizar el filtrado de los paquetes teniendo en cuenta no solo sus cabeceras, sino también la sesión a la que pertenece. Permite detectar más ataques de scan, pero supone una mayor carga.

FIREWALL DE NIVEL DE APLICACIÓN: reconstruyen los paquetes a nivel de aplicación y analizan protocolos específicos (ej. http, smtp, ftp, etc).

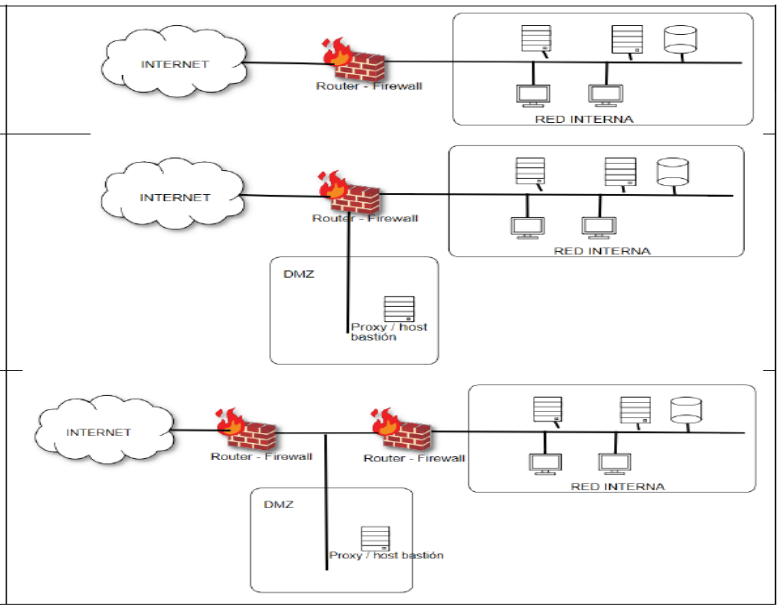
- Requieren una gran cantidad de recursos
- Permiten realizar análisis más exhaustivos y aplicar políticas más precisas. Ejemplos:
    - Análisis de detección de virus
    - Prohibición de descarga de archivos con extensión .exe
    - Verificador de formatos y esquemas XML

Un tipo concreto de firewall a nivel de aplicación son los ***proxies de aplicación***, los cuales son intermediarios entre los clientes y los servidores. De este modo, en caso de que se produzca un ataque, éste compromete al proxy, pero no al equipo final.

HOST BASTIÓN: sistema expuesto a posibles ataques desde el exterior, pero altamente securizado

Link interesante sobre firewalls:
https://www.youtube.com/watch?v=kH6oP6JUnHI&ab_channel=AlbertoLopezTECHTIPS

ARQUITECTURAS DE PROTECCIÓN PERIMETRAL:

Cortafuegos separando la red interna y externa	
DMZ construida con un único firewall (Se permite el tráfico entre la red externa y la DMZ, así como entre la DMZ y la red interna. Sin embargo, no se permite el tráfico directamente entre la red externa e interna)	
DMZ construida con dos firewalls en cascada	

2.2.2 Control de Accesos

2.2.2.1 Componentes del control de acceso

Autenticación, autorización y trazabilidad (accounting) son las tres componentes de un sistema de control de acceso y se refieren a las siguientes funciones:

- **Autenticación**: proceso mediante una entidad prueba su identidad ante otra.
- **Autorización**: proceso mediante el cual se conceden determinados derechos de acceso a activos de información a un usuario o entidad ya autenticada. Par ello se suelen utilizar sistemas LDAP que permiten definir perfiles de acceso para cada usuario. Una vez conocidos la identidad (autenticación) y el perfil del usuario, las aplicaciones pueden establecer en su lógica políticas de autorización.
- **Accounting** o **trazabilidad**: proceso mediante el cual se registra la actividad de los usuarios y sus operaciones en el acceso a activos de información.

2.2.2.2 Modelos de políticas de control de acceso

Las políticas de control de acceso hacen referencia a los mecanismos de autenticación y autorización de los usuarios que acceden a un sistema de información. Se distinguen 3 modelos:

- **Modelo de control de acceso discrecional** (DAC). Se le denomina así porque cada activo de información dispone de un propietario identificado que puede discrecionalmente determinar a qué usuarios concede derecho de acceso. La gestión de los accesos no está por tanto unificada sino que depende de cada propietario.
- **Modelo de control de acceso no discrecional o mandatorio** (MAC): el sistema protege los recursos de forma centralizada y permite el acceso a recursos si y sólo si el sujeto tiene el permiso adecuado, asignado normalmente mediante tags o etiquetas; por tanto debe disponer de un mecanismo para asignar derechos de acceso a cada recurso para cada usuario.

Los modelos DAC y MAC son ineficientes y poco prácticos. El DAC depende de la gestión de cada uno de los propietarios y el MAC es demasiado complejo y rígido. Por ello surgió a mediados de los 80 un tercer modelo: el control de acceso basado en roles.

- **Modelo de control de acceso basado en roles (RBAC)**: a cada usuario se le asigna un rol y a cada rol unos derechos. El sistema gestiona el control de acceso para cada perfil de forma centralizada, como en el MAC, pero no requiere establecer políticas para cada usuario, facilitándose la gestión del acceso.

2.2.2.3 Factores de autenticación

Con el objeto de clasificar y ordenar los mecanismos y sistemas de autenticación se han definido una serie de categorías basadas en factores de autenticación. Son los siguientes:

- Sistemas basados en el "factor de conocimiento" (**algo que el usuario sabe**). Se trata de algo que el usuario conoce. Es el caso común de las contraseñas, preguntas para recordar contraseñas, PIN...
- Sistemas basados en el "factor de posesión" (**algo que el usuario tiene**). Se refiere a un elemento que el usuario posee. Por ejemplo, tarjetas criptográficas (como el DNIe) o los tokens digitales, donde un usuario presenta un elemento considerado como único, que le permite el acceso al sistema. Son similares a la posesión de una llave. En el caso del sistema Cl@ve se considera factor de posesión el terminal móvil del ciudadano, al que se puede enviar un código de autenticación.
- Sistemas basados en el "factor de inherencia" (**algo que el usuario es**). Se refiere a rasgos intrínsecos del usuario. Aquí entran todos los mecanismos biométricos, desde examen de iris, huellas dactilares o reconocimiento facial. Se diferencian entre los mecanismos fisiológicos (iris, facial,...) y los de conducta (voz, tipo de escritura en teclado,...).

ISO 19790 define un cuarto "factor de conducta" (algo que el usuario suele hacer), aunque es un sistema menos empleado.

Se habla de **autenticación fuerte** cuando un sistema de autenticación utiliza por lo menos dos de los tres factores citados anteriormente (dos distintos; no valen, por ejemplo, dos claves que el usuario sabe).

El ENS distingue diferentes mecanismos de autenticación **para usuarios externos** y para usuarios de la propia organización. Así, para usuarios externos, si bien permite el uso de una contraseña para nivel bajo, establece para niveles de protección medio o alto la obligación de disponer de sistemas de autenticación basados en dos factores (autenticación fuerte). Por otro lado, **para usuarios de la organización**, obliga tanto a nivel bajo, como medio y alto el uso de doble factor para accesos desde o a través de zonas no controladas (R8).

2.2.2.4 Protocolos de acceso y autenticación

Se resumen los protocolos y tecnologías de autenticación por el nivel OSI en que se realizan.

- **Protocolos soportados por el protocolo PPP (Point to Point Protocol) de nivel 2**

El protocolo de nivel de enlace PPP se emplea para acceso a redes y soporta mecanismos de autenticación típicamente antes de la asignación de la dirección IP al usuario. En concreto:

- **PAP** (Password Authentication Protocol). Basado en contraseñas. Muy inseguro.
- **CHAP** (Challenge Handshake Authentication Protocol). Utilizado por ISPs para el acceso a Internet. Es un protocolo de autenticación por desafío mutuo.
- **EAP** (Extended Authentication Protocol). No es en sentido estricto un protocolo de autenticación sino un marco (framework) para la negociación de los mecanismos de autenticación, denominados métodos. Existen alrededor de 40 métodos. Se emplea en IEEE 802.11 como parte de los mecanismos de control de acceso WAP y WPA2.

- **Acceso a redes WiFi**

  La norma IEEE 802.11 cuenta con diversos mecanismos para controlar la seguridad en el acceso. Se muestran los más importantes:

  - **WEP** (Wired Equivalent Privacy). Sistema de cifrado origina para el estándar IEEE 802.11. Se han descubierto muchas vulnerabilidades que permiten conseguir la clave de conexión en muy poco tiempo. IEEE declaró WEP obsoleto en 2004 y no se recomienda su uso.
  - **WPA** (Wi-Fi Protected Access). Sistema creado para corregir las deficiencias del anterior introducido como solución de contingencia. Emplea el cifrado con claves dinámicas. En WPA existen varias vulnerabilidades y se desaconseja su uso.

  En 2004 se introdujo la enmienda IEEE 802.11i que introduce el mecanismo WPA2:

  - **WPA-2**. Soluciona problemas de seguridad de la versión anterior y utiliza cifrado simétrico AES frente a WEP y WPA que utilizaban RC4. Es vulnerable no obstante a la fuerza bruta.

Sistema de encriptación	WEP	WPA	WPA2
Estándar	802.11b	802.11g	802.11i
Algoritmo	RC4	RC4TKIP	AES (Rijndael)
Características	Protección a redes inalámbricas vulnerables	IV extendido Llaves dinámicas (TKIP) Incluye MAC del emisor	Número algoritmo de mayor complejidad Tramas convertidas por operaciones matriciales
Longitud de claves	**64 (40) o 128 (104) bits**	**128 a 256 bits**	**128 a 256 bits**
Vulnerabilidad	IV muy corto Llaves estáticas Claves cortas Chequeo de integridad independiente de datos cifrados	Autenticación por handshake auditable. Claves en diccionario, o reconocibles por atacante	Claves conocidas Rondas cortas en información muy confidencial Uso de claves en diccionario o conocidas por atacante
Ataques conocidos	FMS, por estadística de IV, muy exitoso, obteniendo gran cantidad de tramas con IV	Por fuerza bruta comparando claves con handshake, éxito dependiente de tener la clave en el diccionario	Por fuerza bruta muy lenta comparando directamente con la red claves de diccionario, muy poco éxito en bastante tiempo de ataque

  - WPA-3: utiliza cifrado de 192 bits. Mejor protección aún con contraseñas simples. Configuración sencilla mediante códigos QR para dispositivos sin teclado/pantalla (WiFi Easy-Connect).

WPA3: Improved encryption?

Standard	WEP	WPA	WPA2	WPA3
Release	1997	2003	2004	2018
Encryption	RC4	TKIP with RC4	AES-CCMP	AES-CCMP & AES-GCMP
Key Size(s)	64 and 128-bit	128-bit	128-bit	128 and 256-bit
Cipher Type	Stream	Stream	Block	Block
Authentication	Open System & Shared Key	Pre-Shared Key (PSK) & 802.1x with EAP variant	Pre-Shared Key (PSK) & 802.1x with EAP variant	Simultaneous Authentication of Equals (SAE) & 802.1x with EAP variant

- **Autenticación en la capa IP (nivel 3): IPsec**
  IPsec es un conjunto de protocolos de nivel 3 que permiten la autenticación, la integridad y la confidencialidad así como la protección frente al ataque *replay*. Funciona sobre IPv4. IPv6 lo soporta de forma nativa.

  Puede funcionar en modo transporte o modo túnel y está compuesto a su vez por 3 protocolos:

  - IKE: generar claves temporales.
  - AH: integridad, y no repudio en origen.
  - ESP: confidencialidad y es opcional tanto la autenticidad de origen como la integridad.

- **Autenticación en la capa de transporte: TLS**
  TLS (Transport Layer Security) es un protocolo cliente-servidor (típicamente entre el browser del usuario y el servidor web si se emplea bajo el protocolo HTTP) de nivel de transporte que se sitúa por encima del protocolo TCP y por debajo del protocolo de aplicación (HTTP, IMAP, etc.) Su última versión es la 1.3.

  En la actualidad la versión mínima del protocolo recomendada es la TLS1.2, aunque se recomienda ir pensando en la implementación de la 1.3, ya que mejora la seguridad de la versión anterior.

  TLS proporciona:

  - Confidencialidad e integridad (esta última desde TLS 1.2). Cifrado hasta el límite de la cabecera de la aplicación (por ejemplo, HTTP)
  - Autenticación mutua entre las partes (aunque la autenticación de cliente es opcional). En la forma más común de aplicación el servidor se autentica sin requerir la autenticación del cliente.

  El protocolo proporciona 4 funciones principales: autenticación de servidor y cliente (este último opcional), el negociado de algoritmos (Cipher Suite), el intercambio de claves con autenticación, y el cifrado simétrico de los mensajes. Los algoritmos típicos son:

  - Autenticación: Soporta PKI y certificados X.509. Para el intercambio de claves: RSA, DSA, Diffie Hellman (mínimo 2048 bits). El reglamento 910/2014 eIDAS contempla un tipo de certificado para autenticación de servidores web mediante TLS (Certificado de autenticación de sitio web).
  - Integridad: Hash HMAC-SHA256/384.

- Confidencialidad: Cifrado AES, Camellia (mínimo 128 bits).

En cuanto a la arquitectura del protocolo, TLS define un formato de mensaje entre las partes TLS RECORD) que aporta confidencialidad e integridad a las comunicaciones y que puede ser de 3 tipos en función de su contenido:

- Handshake: autenticación y negociación de la "cipher suite" (tecnologías y características del cifrado) en el establecimiento de la sesión de transporte.
- Change Cipher Spec: paso a comunicación cifrada, una vez acordada la tecnología de cifrado mediante el protocolo anterior.
- Alert: excepciones; control de la sesión TLS.
- Aplication: encapsulamiento de los datos de la aplicación.

Se recomienda ver documentación adicional sobre el protocolo TLS.

- **Protocolos de autenticación AAA de nivel de aplicación (Authentication, Authorization and Accounting)**

  - Remote Authentication Dial In User Service (RADIUS)

    RADIUS es un protocolo cliente-servidor de la capa de aplicación que emplea tanto UDP como TCP. Proporciona servicios de AAA centralizados para usuarios que acceden a una red. Se emplea típicamente por los ISPs para acceso a Internet. Emplea PAP, CHAP o EAP para autenticación.

  - TACACS+ (Terminal Access Controller Access Control)

    Desarrollo por CISCO. Es un protocolo de autenticación remota. Es similar a RADIUS.

  - DIAMETER

    Análogo a RADIUS. pensado para la actual generación de IP móvil y redes inalámbricas.

  - Kerberos

    Kerberos es un protocolo de AAA de aplicación para control de acceso a recursos mediante tickets que se emplea principalmente en dominios corporativos. Para más información ver tema 123 *Acceso remoto a sistemas corporativos: gestión de identidades, single sign-on y teletrabajo*.

- **Otros protocolos de nivel de aplicación para autenticación**

En el tema 130 *Acceso remoto a sistemas corporativos: gestión de identidades, single sign-on y teletrabajo* se ven las siguientes tecnologías de autenticación:

- Tecnologías para la federación de identidades: SAML, WS-*, Windows Cardspace.
- Tecnologías de Single Sign On multidominio (Internet): OAuth, OpenID, OpenID Connect, Facebook Connect.

2.2.3 Técnicas Criptográficas

Las técnicas criptográficas se ven en el tema *79 El cifrado. Algoritmos de cifrado simétricos y asimétricos. La función hash. El notariado*. Aquí se señalarán únicamente la técnicas apropiadas para cada nivel de seguridad definido en el ENS según se indica en la guía **CCN-STIC 807 *Criptología de empleo en el Esquema Nacional de* Seguridad** de abril de 2017

- **Longitudes de clave simétrica para AES y TDEA establecidas por la guía**
  Nótese que sólo se mencionan TDEA y AES. El resto de los algoritmos de cifrado no se recomiendan.

Cifrado simétrico: TDEA y AES	Nivel Bajo	Nivel Medio	Nivel Alto
2.5. Protección de la confidencialidad	No se aplica	Permitido Claves ≥ 112 bits	Permitido Claves ≥ 128 bits
2.6. Protección de la autenticidad y de la integridad	No se aplica	Permitido Claves ≥ 112 bits	Permitido Claves ≥ 128 bits
2.7. Cifrado de la información	No se aplica	No se aplica	Permitido Claves ≥ 128 bits
2.8. Protección de las claves criptográficas	Permitido Claves ≥ 112 bits	Permitido Claves ≥ 128 bits	Permitido Claves ≥ 128 bits

RESUMEN DE LONGITUDES DE CLAVES DE CRIPTOSISTEMAS DE CIFRADO EN BLOQUE PARA EL ENS

Longitudes de claves para cifrado asimétrico

Cifrado simétrico: RSA	Nivel Bajo	Nivel Medio	Nivel Alto
2.5. Protección de la confidencialidad	No se aplica	Claves ≥ 2048 bits	Claves ≥ 3072 bits
2.6. Protección de la autenticidad y de la integridad	No se aplica	Claves ≥ 2048 bits	Claves ≥ 3072 bits
2.7. Cifrado de la información	No se aplica	No se aplica	Claves ≥ 3072 bits
2.8. Protección de las claves criptográficas	Claves ≥ 2048 bits	Claves ≥ 2048 bits	Claves ≥ 3072 bits

LONGITUDES DE CLAVE PARA ALGORITMO RSA

Cifrado simétrico: ECC	Nivel Bajo	Nivel Medio	Nivel Alto
2.5. Protección de la confidencialidad	No se aplica	Permitido Claves: 224-255 bits	Permitido Claves: ≥ 256 bits
2.6. Protección de la autenticidad y de la integridad	No se aplica	Permitido Claves: 224-255 bits	Permitido Claves: ≥ 256 bits
2.7. Cifrado de la información	No se aplica	No se aplica	Permitido Claves: ≥ 256 bits
2.8. Protección de las claves criptográficas	Permitido Claves: 224-255 bits	Permitido Claves: 224-255 bits	Permitido Claves: ≥ 256 bits

LONGITUDES DE CLAVE PARA ALGORITMOS ECC

- **Resumen de longitudes de claves de criptosistemas asimétricos y tipos funciones resumen en esquemas de firma electrónica para el ENS**

2.9. Firma electrónica	Nivel Bajo	Nivel Medio	Nivel Alto
RSA	Claves ≥2048 bits	Claves ≥ 2048 bits	Claves ≥ 3072 bits
ECC	Claves: 224-255 bits	Claves: 224-255 bits	Claves: 256-283 bits
MD5	No permitido	No permitido	No permitido
SHA-1	No permitido	No permitido	No permitido
RIPEMD-160	No permitido	No permitido	No permitido
SHA-2	Permitido	Permitido	Permitido
SHA-3	Permitido	Permitido	Permitido

Algoritmos y longitud de claves para firma electrónica (criptografía asimétrica y función huella).

2.2.4 Detección y Prevención de Intrusiones

Este tipo de herramientas trabajan normalmente analizando el tráfico de red y comparándolo con bases de datos de patrones de ataque conocidos, es por ello que la frecuencia de actualización de este tipo de herramientas, es uno de los factores importantes a tener en cuenta.

La seguridad perimetral se aborda en la guía **CCN-STIC-432 *Seguridad perimetral IDS***

Estas herramientas se pueden agrupar en las categorías:

a. **Detección de intrusiones (IDS):** herramientas cuya funcionalidad es la detección de intrusiones en curso o ya logradas, así como la generación de algún tipo de alarma o notificación. Son herramientas con carácter pasivo, su función es detectar y notificar a otras herramientas o personas para que puedan tomar las acciones correctivas necesarias.

b. **Prevención de intrusiones (IPS)**: herramientas cuya funcionalidad es la prevención de intrusiones, así como la generación de algún tipo de alarma o notificación. Son herramientas con carácter activo, su función es prevenir las intrusiones antes de que se materialicen para lo cual disponen de capacidad de acción bien directa, bien mediante notificación a herramientas de terceros. Un ejemplo de acción de este tipo de herramientas sería la ejecución de un script para introducir una regla en un cortafuegos y así bloquear a un atacante.

IDS/IPS: herramientas que integran las funcionalidades de los dos conjuntos anteriores.

Además, son fundamentales los **gestores de eventos (SIEM)** para la gestión centralizada de logs de los diferentes sistemas incluidos IDS e IPS.

También si la organización utiliza servicios basados en la nube, hay que tener en cuenta el enfoque de cero confianza (zero trust network, ZTN) que promueve la mutua autenticación, incluyendo la verificación de identidad e integridad de los dispositivos, independientemente de la ubicación, y garantizando el acceso a las aplicaciones y servicios estribando en la confianza de la identidad del dispositivo, en combinación con la autenticación del usuario. Incluso contratar servicios CASB (cloud access security broker) para monitorizar la actividad del usuario, notificar a los administradores sobre las acciones potencialmente peligrosas del mismo, aplicar las políticas de seguridad definidas y prevenir acciones dañinas.

3. Medidas específicas para las Comunicaciones Móviles

Existe una guía de seguridad **CNN-STIC 496 para Sistemas de Comunicaciones Móviles seguras**. En ella se define la obligación de cada organismo de implementar una política para los sistemas de información en movilidad, que debe estar alineada con la política de seguridad de la información de la organización.

En ella se definen una serie de bloques funcionales del sistema y las recomendaciones a adoptar en cada uno de ellos:

- **Dispositivo**: Punto más crítico del sistema. Hardware y software de confianza y mecanismo de autenticación fuerte con la red corporativa.
- **Red móvil**: Se considerará como potencialmente comprometida o no fiable.
- **Red corporativa** que por lo general está ya desplegada y habrá que adaptar a la nueva red móvil
- **Router**: Separa el tráfico con destino en la red corporativa. Posible inclusión de un IPS.
- **Firewall red móvil**: Primera barrera de protección bajo control de la organización.
- **Firewall externo DMZ**: Únicamente tráfico con entrada o salida en el terminado VPN y bajo determinados protocolos.
- **Firewall interno DMZ:** Final de la DMZ externa. Protege el terminado VPN de envíos no legítimos desde la red corporativa interna.
- **VPN**: Actúa como extremo VPN en la sede de la organización.

- **Proxy / pasarela de servicios corporativos**: Proxy de servicios internos proporcionados a movilidad (correo electrónico, file manager, web).
- **Servidor SIP**: Gestión de identidades y permisos para mensajería entre dispositivos.
- **Pasarela de telefonía**: Conexión con la red de telefonía corporativa.
- **Zona de gestión interna**: Gestión de usuarios desde el punto de vista de la organización.
- **Firewall de red corporativa**: Inicio de la red corporativa.

En la actualidad, tanto la AGE como las corporaciones privadas están introduciendo herramientas **MTD** (Mobile Threat Defense) para la protección de los dispositivos móviles y no solo de las comunicaciones, un dispositivo móvil está expuesto a estos vectores de ataque:

- Ataques de acceso físico al dispositivo (fuerza bruta, móviles sin pantalla de bloqueo).
- Explotaciones de vulnerabilidad del SO o de las apps instaladas.
- Aplicaciones maliciosas (apps disponibles incluso en las tiendas oficiales y que pueden contener malware ya que escapan de los controles de Google y Apple).
- Ataques de red

Las herramientas MTD se suelen integrar con herramientas de gestión de la movilidad corporativa (**EMM**) para la distribución de políticas a todos los terminales de la organización. Realizan detección de anomalías, análisis inteligente por perfiles de comportamiento, prevención de intrusiones, firewall de host, etc. Con todo ello se intenta mitigar la posible pérdida/robo de información corporativa valiosa y posibles accesos a la red interna de la organización que puedan originarse desde terminales corporativos.

OWASP (Open Web Application Security Project), que se centra principalmente en la seguridad de aplicaciones web y móviles, en 2024 ha lanzado una actualización de los top 10 mobile risks, entre los que se incluyen medidas y recomendaciones para evitar vulnerabilidades respecto a la seguridad de las redes en este tipo de infraestructuras (móviles)

- M1: **Uso inadecuado de credenciales**: Los usuarios no autorizados pueden obtener acceso a información o funciones confidenciales dentro de la aplicación móvil o sus sistemas backend. Esto puede provocar filtraciones de datos, pérdida de privacidad del usuario, actividad fraudulenta y posible acceso a funciones administrativas.
- M2: **Seguridad inadecuada de la cadena de suministro:** Los binarios de las aplicaciones generalmente se pueden descargar de las tiendas de aplicaciones o copiar desde dispositivos móviles, por lo que los ataques binarios son fáciles de configurar.
- M3: **Autenticación/autorización insegura**: Aunque el principal problema es la autenticación, también impacta la seguridad de la red, ya que un acceso no autorizado puede llevar a la explotación de otras vulnerabilidades de red, como conexiones no seguras o APIs expuestas.
- M4: **Validación de entrada/salida insuficiente**: La falta de validación adecuada de los datos de entrada puede permitir inyecciones de comandos que exploten las comunicaciones de red, manipulando las solicitudes y respuestas que pasan a través de la red móvil. Esto puede llevar a ataques como inyecciones SQL o comandos en sistemas backend.
- M5: **Comunicación insegura**: falta de cifrado o el uso inadecuado de cifrado en las comunicaciones de las aplicaciones móviles. Esto incluye el uso de protocolos inseguros o la ausencia de verificación de los certificados del servidor, lo cual puede facilitar ataques de Hombre en el Medio (MitM), escuchas no autorizadas, y la interceptación de datos sensibles en tránsito.
- M6: **Controles de privacidad inadecuados:** La información de identificación personal siempre debe procesarse teniendo en cuenta la posibilidad de que un atacante pueda acceder a los medios de comunicación y almacenamiento.

- M7: **Protecciones binarias insuficientes**: Los binarios de las aplicaciones generalmente se pueden descargar de las tiendas de aplicaciones o copiar desde dispositivos móviles, por lo que los ataques binarios con ingeniería inversa o alteración del código son fáciles de configurar.
- M8: **Mala configuración de seguridad:** Directamente relacionado con la seguridad de la red, ya que una configuración incorrecta puede permitir a los atacantes acceder a la infraestructura de red, explotar puertos abiertos, o realizar ataques de red no detectados.
- M9: **Almacenamiento de datos inseguro**: Aunque se enfoca en la seguridad de los datos almacenados en el dispositivo, puede afectar a la red si la información sensible (como credenciales de red o tokens de autenticación) es almacenada y luego capturada por un atacante que tenga acceso a la red o al dispositivo móvil. Esto puede derivar en accesos no autorizados a servicios de red.
- M10: **Criptografía insuficiente:** Estas debilidades pueden incluir el uso de algoritmos de cifrado débiles o longitudes de clave inadecuadas, prácticas deficientes de gestión de claves, manejo inadecuado de claves de cifrado, generación insegura de números aleatorios, implementación defectuosa de protocolos criptográficos o vulnerabilidades en bibliotecas o marcos criptográficos. Los atacantes pueden explotar estas debilidades para eludir el cifrado, realizar ataques criptográficos, manipular datos u obtener acceso no autorizado a información cifrada.

Ver link https://owasp.org/www-project-mobile-top-10/