sedian

Seguridad Digital
de Andalucía

Presentación

Securización de redes desde el perímetro hacia el interior (II)

26 de Noviembre de 2020

Junta de Andalucía

6.- Despliegue de infraestructura

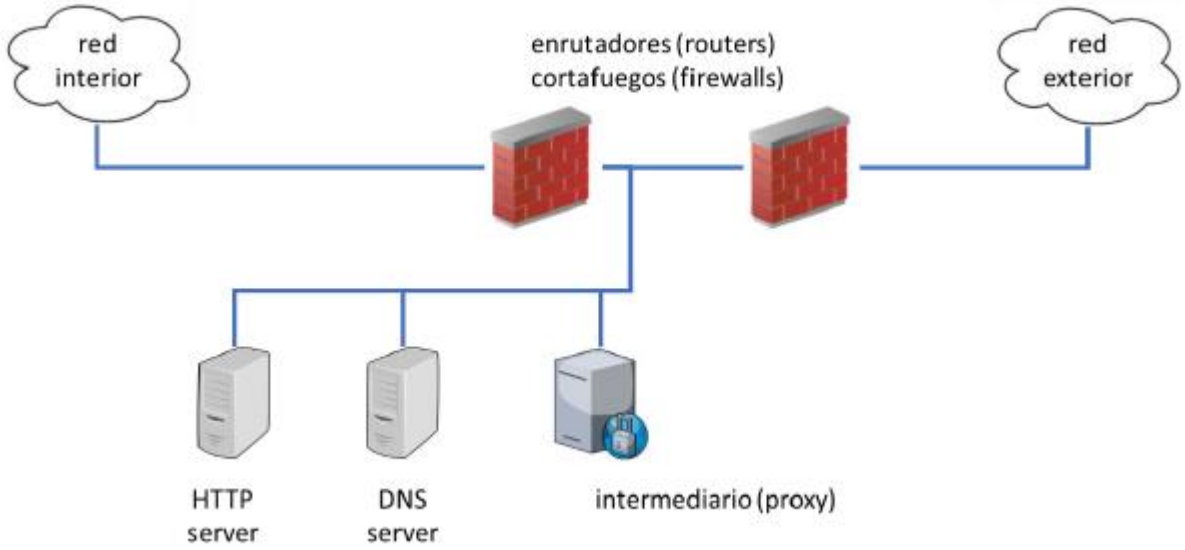
- Las arquitecturas descritas pueden ser desplegadas en diferentes esquemas de red para atender a las necesidades concretas del servicio. Dependiendo de cuales sean los flujos de información requeridos, la frontera debe adaptarse a las necesidades concretas sin mermar su capacidad de protección de la red interna.

- El acceso a los equipos de la frontera para su administración solo se podrá realizar desde dentro de la frontera, nunca desde el exterior

6.- Despliegue de infraestructura

6.1.- Servidores y servicios en la frontera

- Es habitual que elementos como servidores web se dispongan en la frontera para facilitar el acceso de usuarios internos sin necesidad de que penetren en la red interna. Son habituales: servidores HTTP y HTTPS de páginas web, servidores FTP de transferencia de ficheros, servidores DNS de resolución de nombres, etc.



6.- Despliegue de infraestructura

6.1.- Servidores y servicios en la frontera

- Todos ellos configurados de forma autónoma sin necesidad de establecer conexiones con la red interior para responder a las demandas de los usuarios externos. Si necesitaran establecer conexiones internas, pasarían a la categoría de servicios intermediados (proxies).

- Estos servicios deben configurarse de forma que los flujos de información desde el exterior atraviesen un cortafuegos y el intermediario. Debe considerarse la oportunidad de desplegar un proxy separado para estos servicios que no entran en la red interna.

6.- Despliegue de infraestructura

6.2.- Garantías de disponibilidad

- A fin de garantizar los niveles de seguridad requeridos por los servicios prestados a través de la interconexión, la frontera puede estar redundada. Varios cortafuegos, intermediadores (proxies) y servidores en la frontera pueden estar trabajando en paralelo para repartir carga y para evitar que el fallo de uno de ellos interrumpa el servicio. Incluso puede llegar a replicarse la frontera entera para evitar puntos únicos de fallo en equipamiento de red, elementos físicos y proveedores de servicio de Internet.

- Desde el punto de vista de seguridad, el control de los flujos de información deberá ser igual en todos los elementos redundados, concretamente en lo que respecta a flujos permitidos y herramientas de seguridad.

6.- Despliegue de infraestructura

6.3.- Frontera compartida

- Es relativamente frecuente el caso de que haya varias redes internas compartiendo una conexión al exterior. Bien sea por una segregación interna de la red, bien porque varios sistemas de información llegan a un acuerdo para compartir recursos.

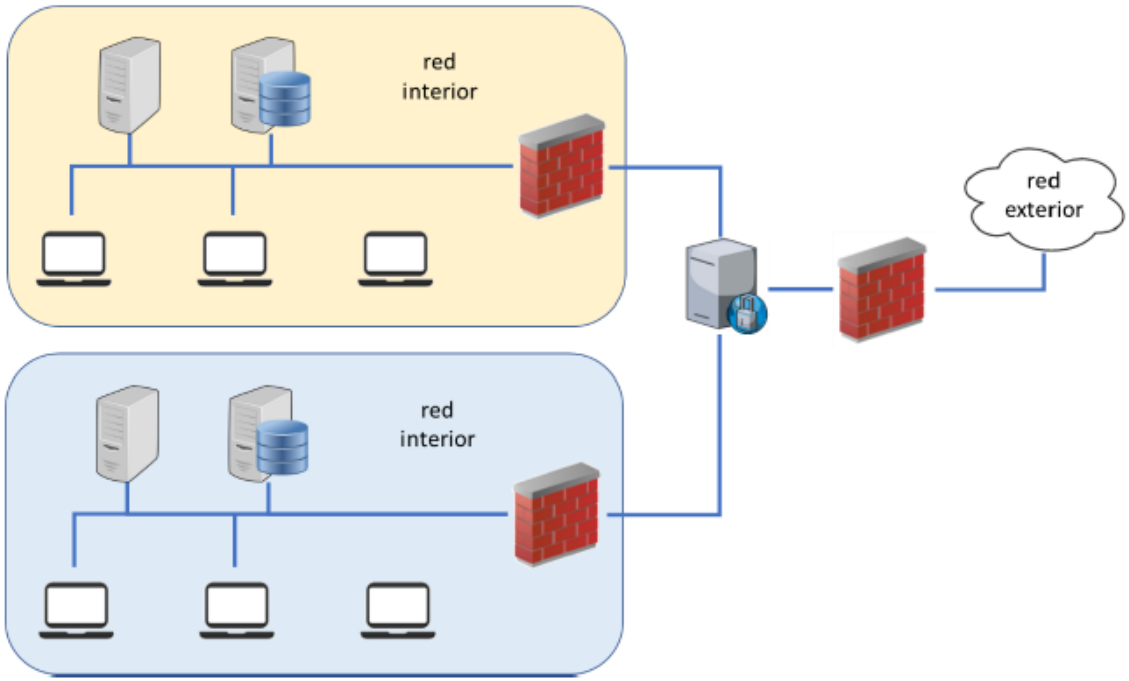
- En estos casos, se considera que hay tantas interconexiones como pares de redes conectados a la frontera compartida. En el ejemplo de la figura anterior, hay 3 interconexiones:
  - ✓ Red Interna-1 con Red Externa
  - ✓ Red Interna-2 con Red Externa
  - ✓ Red Interna-1 con Red Interna-2

6.- Despliegue de infraestructura

6.3.- Frontera compartida

- Y en cada una de las interconexiones se deben aplicar los principios básicos de la arquitectura de seguridad apropiada.

- A modo de ejemplo, se muestra un esquema que combina 2 redes internas compartiendo una salida al exterior, donde defendemos los flujos con el exterior, así como los flujos entre redes internas.



6.- Despliegue de infraestructura

6.4.- Redes privadas virtuales

- Las redes privadas virtuales (VPN, Virtual Private Networks) aparecen como un medio de comunicarse de forma segura a través de medios que no ofrecen garantías de seguridad.

- Por seguridad nos referimos a garantías de confidencialidad, integridad y autenticidad, según se recoge en las medidas de seguridad protección de la confidencialidad y protección de la autenticidad y de la integridad del ENS. Estas garantías son en buena parte criptográficas y se ajustarán a lo previsto en la guía CCN-STIC 807 Criptología de Empleo en el Esquema Nacional de Seguridad.

- Las características y requisitos de las redes privadas virtuales se tratan en detalle en la guía CCN-STIC 836 Seguridad en VPN en el marco del ENS.

- Las redes privadas virtuales conectan la red interior con otra red remota o con un nodo individual remoto, conexión vehiculada a través de una red externa.

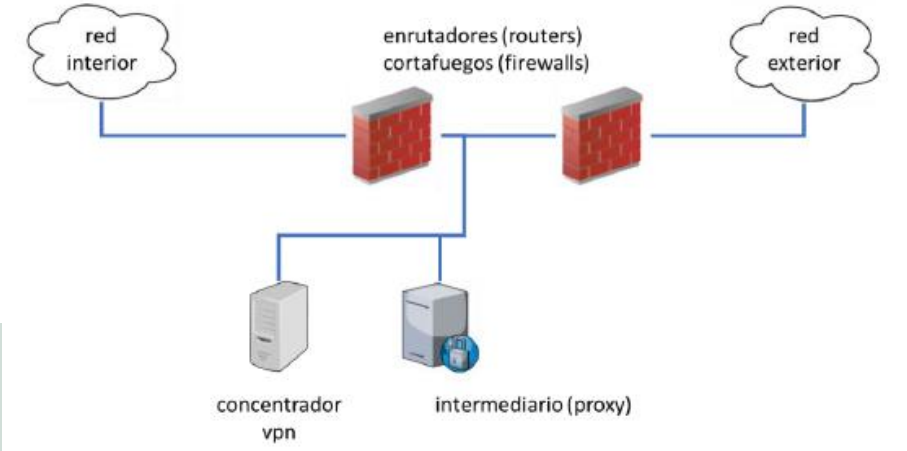
6.- Despliegue de infraestructura

6.4.- Redes privadas virtuales

- El concentrador de redes privadas virtuales (donde terminan las VPN) debe instalarse preferentemente en la zona desmilitarizada (DMZ) y todos los flujos de información, entrantes y salientes, deben pasar por el intermediador (proxy).

- Cuando sea necesario establecer la red privada desde un equipo interior y los datos aparezcan cifrados (negros) en la frontera, el equipo interior deberá disponer de un agente intermediador (proxy) que revise toda la información enviada o recibida a través de la red virtual.

- Se debe estudiar la oportunidad de desplegar un cortafuegos entre la terminación VPN y el proxy, a fin de limitar los paquetes que pueden atravesar esta interfaz.



6.- Despliegue de infraestructura

6.5.- Equipos remotos

- Se consideran equipos remotos aquellos equipos de usuario que se conectan a la red interior desde el otro lado de la frontera. Típicamente se utilizarán redes privadas virtuales para el acceso a través de redes públicas o de terceros.

- Los escenarios más típicos son:
  - ✓ teletrabajadores, que acceden a información y servicios proporcionados en la red interna; donde el equipo cliente puede ser propiedad del organismo o ser propiedad del usuario (BYOD – Bring Your Own Device)

  - ✓ empresas de mantenimiento remoto que proporcionan servicios de mantenimiento de software y de configuración a distancia

- A estos equipos remotos les serán de aplicación las medidas de seguridad del ENS que correspondan a la información que pueda estar o quedar almacenada en ellos. Se debe prestar atención, prioritariamente, a los requisitos de confidencialidad.

6.- Despliegue de infraestructura

6.5.- Equipos remotos

- Todos los equipos remotos deberán:

  - ✓ Disponer de un cortafuegos individual.
  - ✓ Atravesar el servicio proxy de la frontera en todos los accesos a la red interior.
  - ✓ Limitar al administrador de seguridad la instalación de software y la configuración de seguridad del equipo. La administración de la seguridad se realizará bajo la responsabilidad del Responsable de la Seguridad de la red interior.

- Si el sistema es de categoría MEDIA o superior,
  - ✓ El equipo remoto solamente podrá conectarse a sitios explícitamente autorizados (lista blanca).

- Si el sistema es de categoría ALTA,
  - ✓ Todas las comunicaciones entre el equipo y redes diferentes a la interior deberán ser a través del servicio proxy establecido en la frontera.

7.- Seguridad Wifi

- Se puede definir de forma general una red inalámbrica, como aquella formada por dispositivos con capacidades inalámbricas que se comunican entre sí a través de ondas electromagnéticas y sin necesidad de cableado (wireless).

- En este curso nos referiremos en exclusiva a las Redes de Área Local Inalámbricas, también conocidas como WLAN (Wireless Local Area Network) o Redes Wi-Fi. Estas redes inalámbricas se basan en el estándar IEEE 802.11, y será a este tipo, al que se hará referencia a partir de ahora como redes inalámbricas.

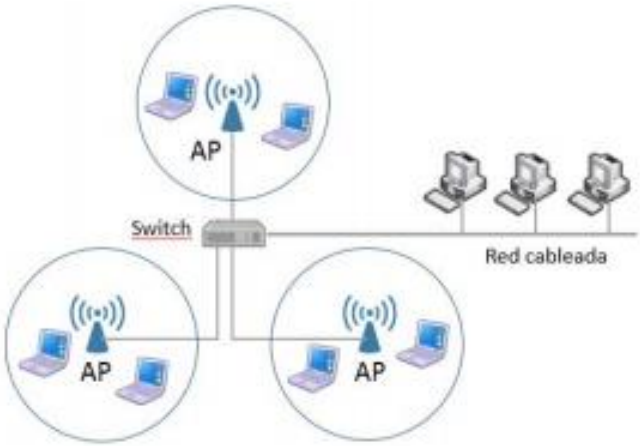
- Los componentes principales de una red inalámbrica son:

✓ **Dispositivos cliente**. Son los equipos de usuario que solicitan conexión a la red inalámbrica para realizar la trasferencia de datos de usuario. Pueden ser ordenadores portátiles, teléfonos inteligentes (smartphones), Smart TV, etc.

✓ **Puntos de Acceso (Access Points, AP)**. Son dispositivos que forman parte de la infraestructura inalámbrica, y se encargan de conectar los dispositivos cliente entre sí, o con la infraestructura de red cableada de la organización. A partir de ahora se hará referencia a estos dispositivos como AP.

7.- Seguridad Wifi

- Existen dos topologías de red inalámbrica: **modo Ad Hoc y modo Infraestructura**. En el modo Ad Hoc no existen los AP y los dispositivos cliente se comunican entre sí directamente. El modo Infraestructura, utilizan AP para conectar los dispositivos cliente entre sí o con el sistema de distribución de red.



7.- Seguridad Wifi

- Los AP pueden ser de dos tipos: **AP inteligentes y AP simples**. Los primeros realizan de forma independiente todas las tareas de cifrado y gestión de los dispositivos cliente conectados a ellos. En el caso de los segundos, AP simples, el cifrado y la política de seguridad se procesan de forma centralizada en un controlador de la infraestructura inalámbrica. La ventaja de una gestión centralizada, es que no se deposita en cada uno de los AP las claves criptográficas.

- Los riesgos de las redes inalámbricas son los mismos que afectan a las redes cableadas sumados a los riesgos específicos de un entorno inalámbrico. Existen multitud de fuentes de información donde se describen las amenazas y riesgos de las redes inalámbricas. En la siguiente lista se incluyen algunos de los más representativos.

7.- Seguridad Wifi

- ✓ **Eavesdropping.** Cuando un individuo no autorizado utiliza alguna herramienta (normalmente antenas de gran alcance) para capturar de forma pasiva el tráfico inalámbrico. Este tráfico le sirve para espiar información (en caso de que no vaya cifrada) y para detectar patrones de comportamiento.
- ✓ **Denegación del Servicio (DoS).** Cuando la infraestructura inalámbrica queda incapacitada para ofrecer el servicio. Por ejemplo, cuando un individuo no autorizado inyecta peticiones masivas de asociación a los AP dejándolos incapacitados para responder a las peticiones de los clientes legítimos.
- ✓ **Man-in-the-middle**. Cuando un individuo no autorizado se coloca en medio de la comunicación inalámbrica entre emisor y receptor, suplantando a una de las partes y haciendo creer a la otra que está hablando con el comunicante legítimo. El más conocido de estos ataques es el de Rogue AP (falso AP), que se produce cuando un individuo no autorizado logra suplantar a un AP legítimo con uno falso de las mismas características y mayor potencia de señal, haciendo que los clientes soliciten asociación en primer lugar al Rogue AP. A partir de aquí, se pueden ejecutar multitud de ataques posteriores (captura de credenciales, de tráfico, etc.).

7.- Seguridad Wifi

- ✓ **Ataques por fuerza bruta.** Consisten en métodos para averiguar las claves criptográficas probando todas las combinaciones posibles. En caso de que la red inalámbrica no utilice algoritmos criptográficos y claves con la suficiente fortaleza, se pueden realizar este tipo de ataques ya que existen multitud de herramientas gratuitas que lo permiten.

- ✓ **MAC Spoofing.** Los AP pueden tener configurada una lista de direcciones MAC permitidas. Sin embargo, un individuo no autorizado puede suplantar una dirección MAC autorizada para lograr el acceso.

- ✓ **Acceso de dispositivos no autorizados** que están conectados al dispositivo cliente autorizado y que a través de él pueden lograr acceso a la red inalámbrica y por ende a la red cableada de la organización pudiendo introducir software dañino.

7.- Seguridad Wifi

7.1.- Medidas organizativas

- La red inalámbrica deberá incluirse en la Normativa, Procedimientos y Procesos de la organización.

  ✓ **Normativa**: Dentro de la Normativa, deberá existir una Política de seguridad de la red inalámbrica, que junto con las decisiones que tome la organización para forzar su cumplimiento, será la base para todas las medidas de seguridad.

  ✓ Dentro de esta Política deberán incluirse, al menos, los siguientes aspectos:

  • **Uso aceptable de la red inalámbrica**. Aspectos relacionados con el uso apropiado e inapropiado de la red inalámbrica y las medidas disciplinarias correspondientes. Se indicará lo que se puede hacer a través de la red inalámbrica y a qué recursos se puede acceder. Se incluirán los requisitos de autenticación de usuario para el acceso a la red inalámbrica, requisitos sobre los dispositivos cliente, requisitos específicos de la conexión, etc.

7.- Seguridad Wifi

7.1.- Medidas organizativas

- **Requisitos de seguridad de la infraestructura inalámbrica**. Aspectos relativos a la asignación de roles y responsabilidades para la dirección, gestión y explotación de la red inalámbrica; tipo de información que podrá y que no podrá ser transmitida por la red inalámbrica; requisitos de seguridad física para los componentes de la infraestructura; configuración de seguridad de los elementos de la infraestructura; mecanismos de protección de la comunicación inalámbrica, incluyendo requisitos sobre cifrado, autenticación y gestión de claves criptográficas; etc.

- **Requisitos de seguridad de los dispositivos cliente**. Aspectos relacionados con las condiciones de uso permitido de los dispositivos clientes, es decir, cómo, cuándo y dónde se pueden utilizar para acceder a la red inalámbrica; tipos de dispositivos cliente autorizados; configuraciones de seguridad, etc.

- **Evaluaciones de seguridad periódicas.** Aspectos relacionados con el alcance y periodicidad de las auditorías de seguridad que revisan el estado global de la seguridad de la infraestructura inalámbrica.

7.- Seguridad Wifi

7.1.- Medidas organizativas

- ✓ **Procedimientos**: También deberán existir los Procedimientos correspondientes a la red inalámbrica, que serán acordes con los procedimientos relativos a la infraestructura general de la organización. Algunos de estos procedimientos son los siguientes:

• **Operación y mantenimiento de la infraestructura inalámbrica.** Se incluirán aspectos relativos a la actualización de parches, alta de nuevos dispositivos y usuarios, instalación y configuración de AP, actualización y gestión del inventario, etc.

• **Gestión de eventos y registros de log.** Se incluirán aspectos como la información a registrar, cuánto tiempo debe conservarse, cada cuánto tiempo debe revisarse, envío de copias de los eventos a servidores centralizados de gestión, etc.

• **Gestión y respuesta a incidentes de seguridad en la red inalámbrica.** Se analizará cómo los componentes de la infraestructura inalámbrica pueden verse afectados por los incidentes, para documentar las actividades que den respuesta a estos incidentes de forma efectiva y eficiente.

7.- Seguridad Wifi

7.1.- Medidas organizativas

- **Respuesta y actuación frente a pérdidas o robos de dispositivos inalámbricos.**
- **Monitorización de seguridad continua, que atienda a los ataques y las vulnerabilidades de la red inalámbrica**.
- **Auditorías periódicas de la infraestructura inalámbrica**. Se definirá la periodicidad y alcance de las auditorías, cuyo objetivo será verificar que la red cumple con la política de seguridad de la organización.

✓ **Autorización**: Finalmente, deberán elaborarse los Procesos de Autorización necesarios para atender las necesidades de la red inalámbrica relativas a autorizaciones. Al menos los siguientes:

- **Autorización de usuarios y dispositivos para el uso de la red inalámbrica.**
- **Autorización para el despliegue de nuevos componentes de la infraestructura inalámbrica** (por ejemplo, AP).

7.- Seguridad Wifi

7.1.- Medidas organizativas

- ✓ **Autorización**: Finalmente, deberán elaborarse los Procesos de Autorización necesarios para atender las necesidades de la red inalámbrica relativas a autorizaciones. Al menos los siguientes:

    - **Autorización de usuarios y dispositivos para el uso de la red inalámbrica.**

    - **Autorización para el despliegue de nuevos componentes de la infraestructura inalámbrica** (por ejemplo, AP).

7.- Seguridad Wifi

7.2.- Medidas operacionales

- ✓ **Arquitectura de seguridad**: La Arquitectura de Seguridad, tal y como se indica en la guía CCN-STIC-804 (Apartado 4.1.2), esta medida es básicamente documental y descriptiva de cómo es la arquitectura de la red inalámbrica y su sistema de gestión.

Los aspectos específicos de una red inalámbrica relacionados con la arquitectura de seguridad, que se deben tener en cuenta, son los siguientes:

- **Cobertura de los puntos de acceso antes de ubicarlos físicamente**, con objeto de minimizar la radiación de estos fuera del perímetro controlado por la organización. La ubicación física se deberá combinar con la configuración de las antenas de los AP para controlar la dirección y potencia de radiación y, por lo tanto, la cobertura final de la red inalámbrica.
- **La red inalámbrica deberá ser modo infraestructura**. No son recomendables las redes Ad Hoc. En la red tipo infraestructura, la configuración de seguridad se puede estandarizar y desplegar a los AP. En la red Ad Hoc los dispositivos cliente se conectan entre sí directamente y ejercen diversos roles de configuración más difíciles de controlar.

7.- Seguridad Wifi

7.2.- Medidas operacionales

- ✓ **Autenticación** : Dentro del diseño de la autenticación de una red inalámbrica, hay que determinar los aspectos que se definen a continuación.

a) **Tipo de autenticación de la red inalámbrica**. El estándar IEEE 802.11i (RSN) permite utilizar dos tipos de autenticación: basado en claves pre-compartidas (PSK) y basado en protocolo 802.1X/EAP.

b) **Mecanismos de autenticación.** Mecanismos empleados para la autenticación del servidor (AS) y para la autenticación del cliente (en caso de realizar autenticación mutua). En general, el servidor se autentica frente el cliente a través de certificado, mientras que para la autenticación del cliente se podrán usar múltiples mecanismos (contraseñas, tokens, biometría, etc.) o una combinación de ellos.

c) **Método EAP.** EAP es el protocolo encargado del transporte, encapsulado y seguridad del proceso de autenticación. Existen diferentes métodos EAP con distintos mecanismos de autenticación y con distintas características de seguridad.

7.- Seguridad Wifi

7.2.- Medidas operacionales

- ✓ **Acceso Local para Administración de los AP**

Nivel Medio / Alto [I C A T]

El acceso a la infraestructura inalámbrica desde la red cableada de la organización (acceso local) realizado con la finalidad de administración y gestión de los dispositivos, además de atender a las indicaciones realizadas en la guía CCN-STIC-804 (Apartado 4.2.6) sobre el acceso local [op.acc.6], debe contemplar los siguientes aspectos específicos a la red inalámbrica:

En el caso de que las dimensiones de: integridad [I], confidencialidad [C], autenticidad [A] y trazabilidad [T] alcancen nivel Medio o Alto, el protocolo usado para la gestión de la infraestructura inalámbrica debe ser un protocolo de gestión seguro, como puede ser SSH, SSL/TLS o SNMPv3. Este será el único protocolo de gestión habilitado, debiendo de estar deshabilitado cualquier otro protocolo de gestión inseguro que tenga el AP entre sus funcionalidades como, por ejemplo, SNMPv1, SNMPv2, HTTP, etc.

7.- Seguridad Wifi

7.2.- Medidas operacionales

- ✓ **Acceso Local para Administración de los AP**

<u>Nivel Medio / Alto [I C A T]</u>

Además, atendiendo al principio de segregación de tareas y roles indicado el acceso local para administración del AP, solo estará disponible para los administradores autorizados a realizar estas funciones.

Los accesos, así como las actividades realizadas durante los mismos, deben quedar registrados.

El mecanismo de control de acceso para la administración de los dispositivos, dependerá del nivel exigido en las dimensiones de seguridad [I C A T]

7.- Seguridad Wifi

7.2.- Medidas operacionales

- ✓ **Monitorización**:

Categoría Básica

La monitorización de la seguridad es un aspecto fundamental en todas las redes y sistemas, pero aún adquiere mayor importancia en las redes inalámbricas, que están sujetas a las mismas amenazas y a otras específicas del entorno inalámbrico.

Debe llevarse a cabo una monitorización continua, que permita mantener un conocimiento constante del estado de la seguridad de la red inalámbrica, de forma que sea posible identificar y reaccionar de la forma más inmediata posible, a ataques, fallos en las configuraciones de seguridad, y cualquier otro problema en la seguridad de la red inalámbrica.

7.- Seguridad Wifi

7.2.- Medidas operacionales

- ✓ **Monitorización**:

La monitorización de seguridad que se realice, debe atender al menos a estos dos aspectos:

a) **Monitorización de los posibles ataques**, tanto los específicos de redes inalámbricas, como aquellos que afectan a redes cableadas (ya que también afectan a redes inalámbricas). Se atenderá especialmente a los ataques activos, en los que un individuo no autorizado, no se limita a monitorizar el tráfico, sino que genera, altera o interrumpe las comunicaciones inalámbricas.

b) **Monitorización de vulnerabilidades**, a llevar a cabo sobre los componentes de la infraestructura inalámbrica, de la misma forma que se realice para la red cableada. Identificar y aplicar parches, verificar las configuraciones de seguridad y ajustarlas cuando sea necesario. Estas acciones deberían ser realizadas al menos con la misma frecuencia que se realicen en los componentes de la red cableada.

7.- Seguridad Wifi

7.2.- Medidas operacionales

- ✓ **Detección de intrusión**:

<u>Categoría Media / Alta</u>

En caso de que la categoría sea Media o Alta, la monitorización de seguridad se llevará a cabo de forma automática a través de Sistemas de Detección de Intrusión Inalámbrica WIDS (Wireless Intrusion Detection Systems) y/o Sistemas de Prevención de Intrusión Inalámbricos WIPS (Wireless Intrusion Prevention Systems). Estos sistemas disponen de sensores que se despliegan en localizaciones determinadas dentro de las instalaciones de la organización. Los sensores realizan un barrido de frecuencias en las bandas y canales de la red inalámbrica, y seleccionan muestras del tráfico capturado, para analizarlo en busca de posibles ataques o vulnerabilidades. En el Anexo E se detalla el funcionamiento de estos sistemas.

El sistema WIDS o WIPS debe tener la misma cobertura que la red inalámbrica, para evitar que individuos no autorizados se instalen en zonas donde puedan eludir el sistema de detección.

7.- Seguridad Wifi

7.2.- Medidas operacionales

✓ **Detección de intrusión**:

Es recomendable que la monitorización de la infraestructura inalámbrica sea capaz de detectar, al menos, lo siguiente:

- **Dispositivos inalámbricos no autorizados**, incluyendo falsos AP (rogue AP) y dispositivos cliente.

- **Dispositivos desconfigurados**, o con una configuración de seguridad que no sea la estándar de la organización.

- **Patrones de uso de la red inalámbrica anormales**. Por ejemplo, un elevado número de dispositivos cliente utilizando un mismo AP, volumen de tráfico anormal procedente de un dispositivo cliente, un elevado número de intentos fallidos de conexión a la red en un corto periodo de tiempo, etc.

7.- Seguridad Wifi

7.2.- Medidas operacionales

✓ **Detección de intrusión**:

- **Escáneres activos que puedan estar generando tráfico ilícito a la red inalámbrica.** Por ejemplo, las herramientas que individuos no autorizados utilizan para escanear redes inalámbricas realizadas en movimiento.

- **Ataques DoS.** Por ejemplo, registrando el número de eventos de terminación de conexiones en la red inalámbrica, y alertando cuando se supere un umbral, ya que eso puede significar un ataque DoS.

- **Ataques de suplantación y man-in-the-middle.** Por ejemplo, algunos WIDS pueden detectar cuando un dispositivo está tratando de suplantar la identidad de un cliente autorizado.

7.- Seguridad Wifi

7.2.- Medidas operacionales

- ✓ **Auditorías de seguridad:** La red inalámbrica deberá ser incluida en las Auditorías de seguridad periódicas que la organización realizará sobre sus sistemas e infraestructuras. De esta forma, podrá verificarse que la red inalámbrica cumple con las políticas y normativa de seguridad establecidas.

Las auditorías de la red inalámbrica deberán contemplar, al menos, los siguientes aspectos:

- Análisis de vulnerabilidades y medidas técnicas implantadas.
- Análisis del rango de cobertura y potencia de radiación de los AP.
- Análisis del estado de configuración de los AP.
- Análisis de los incidentes producidos y medidas correctoras aplicadas.

7.- Seguridad Wifi

7.2.- Medidas operacionales

- ✓ **Auditorías de seguridad:**

La periodicidad con la que deberán realizarse las auditorías la determina la organización. En el caso de la red inalámbrica, deberán tenerse en cuenta los siguientes factores:

- La localización de las instalaciones de la organización. En caso de que se encuentren cerca de áreas públicas concurridas y de fácil acceso, aumentará el riesgo de amenazas a la red inalámbrica.
- El nivel de seguridad de la información transmitida a través de la red inalámbrica.
- Cambios físicos en las instalaciones, que puedan afectar a la propagación y potencia de la señal inalámbrica.

7.- Seguridad Wifi

7.3.- Medidas de protección

- Protección de las instalaciones e infraestructuras:

Categoría Básica

✓ Es especialmente importante restringir el acceso a los AP para evitar su manipulación, de forma que al menos estén fuera del alcance, como, por ejemplo, por encima del falso techo.

✓ Adicionalmente, es recomendable también que el botón de reset de los AP se encuentre protegido, para evitar su pulsación de forma accidental o mal intencionada. Si la configuración de seguridad no es robusta, esto podría causar que el AP vuelva a su configuración de fábrica, deshabilitando todas las medidas de seguridad.

7.- Seguridad Wifi

7.3.- Medidas de protección

- Protección de las instalaciones e infraestructuras:

Categoría Media / Alta

✓ En el caso de que sean los AP los que realizan las funciones de seguridad, como gestión del tráfico de autenticación, generación de claves criptográficas y cifrado, es recomendable que sean ubicados en CPD, salas de servidores, armarios o dependencias similares con controles de acceso físico apropiados.

En caso de que sean otros los elementos que realizan estas funciones de seguridad (por ejemplo, switches de la red inalámbrica), serán éstos los que deberán protegerse físicamente de la forma anteriormente indicada..

7.- Seguridad Wifi

7.3.- Medidas de protección

- Segregación de redes: En el diseño de la seguridad de la red inalámbrica, debe tenerse en cuenta cómo esta red puede afectar a otras redes con las que tenga conexión (normalmente la red cableada de la organización), y a las que se puede acceder a través de ella.

Categoría Básica/Media

- ✓ La red inalámbrica deberá estar segmentada en caso de que existan diferentes dominios de seguridad. Por ejemplo, segmentos de red distintos para el acceso de invitados (personal externo a la organización) y el acceso de personal interno.

- ✓ Una práctica recomendable es segregar el tráfico de la red inalámbrica del tráfico de la red cableada a través de VLAN dedicadas. El uso de estas VLAN facilita la implementación de listas de control de accesos a la red, permitiendo identificar los protocolos y servicios autorizados a pasar desde la red inalámbrica a la red cableada.

7.- Seguridad Wifi

7.3.- Medidas de protección

- Segregación de redes:

<u>Categoría Alta</u>

- La red inalámbrica deberá estar segmentada a través de un dispositivo lógico o físico asegurado y mantenido de la forma apropiada, para acotar el acceso a la información y la propagación de incidentes.

    - Formación y concienciación:

Categoría Básica / Media / Alta

- La organización debe asegurarse de que todos los usuarios y el personal técnico que vaya a utilizar o a administrar la infraestructura inalámbrica dispone de la formación adecuada y es conocedor de las políticas y procedimientos.

7.- Seguridad Wifi

7.3.- Medidas de protección

- Formación y concienciación:

✓ Se debe concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad de la red inalámbrica alcance los niveles exigidos.

✓ Tal y como se indica en la guía CCN-STIC-804, es necesario refrescar regularmente:

- La normativa de seguridad relativa al buen uso de la red inalámbrica.
- La identificación de incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado.
- El procedimiento de reporte de incidencias de seguridad, seas reales o falsas alarmas.

7.- Seguridad Wifi

7.3.- Medidas de protección

- Formación y concienciación:

  - ✓ Los administradores de la red inalámbrica deben ser plenamente conscientes de las amenazas y los riesgos de seguridad a los que se expone la red. Deben trabajar para asegurar el cumplimiento de la política de seguridad, y deben conocer perfectamente los procedimientos de configuración de seguridad de la infraestructura inalámbrica, los de gestión de incidentes de seguridad y otros procedimientos relativos a la red inalámbrica.

  - ✓ Es recomendable que los administradores estén al día sobre nuevas vulnerabilidades y ataques a la infraestructura inalámbrica, para lo cual pueden consultar multitud de fuentes que publican este tipo de información.

7.- Seguridad Wifi

7.3.- Medidas de protección

- Borrado y destrucción: Los dispositivos inalámbricos almacenan información sensible relacionada con contraseñas, PSK, información de configuración, etc. Esta información puede ser utilizada por individuos no autorizados de forma muy provechosa para realizar ataques a la red inalámbrica.

Nivel Bajo [C]

En el caso de que la confidencialidad [C] alcance un nivel Bajo, los dispositivos inalámbricos que se vayan a reutilizar deberán ser objeto de borrado seguro. En el caso de los AP, habrá que eliminar como mínimo, la siguiente información:

- Claves PSK.
- Configuración de seguridad (hacer un reset a la configuración de fábrica).
- Registros de actividad y eventos.
- Cuentas de administración.

7.- Seguridad Wifi

7.3.- Medidas de protección

- Borrado y destrucción:

Nivel Medio / Alto [C]

- En el caso de que la confidencialidad [C] alcance un nivel Medio o Alto, los dispositivos inalámbricos que se vayan a dar de baja, deben ser objeto de destrucción segura según se indica en el Apartado 5.5.5 de la guía CCN-STIC-804.

8.- Criptología de empleo en la ENS

7.3.- Algoritmos acreditados

- **Protección de Confidencialidad, Autenticidad e Integridad**

✓ El estándar IEEE 802.11i (RSN) puede utilizar dos suites criptográficas para la protección de la comunicación inalámbrica: TKIP y CCMP.

✓ TKIP es la suite que implementa WPA de forma obligatoria, y su algoritmo central es RC4. CCMP es la suite que implementa WPA2 de forma obligatoria y su algoritmo central es AES.

✓ TKIP utiliza los algoritmos RC4 y Michael (como código de integridad de mensaje). Ambos algoritmos tienen vulnerabilidades de seguridad conocidas a día de hoy, por lo que TKIP no se considera adecuado para entornos con requisitos de seguridad elevados. Para estos entornos, CCMP es un mecanismo más seguro, pero requiere más recursos de computación.

8.- Criptología de empleo en la ENS

7.3.- Algoritmos acreditados

- **Protección de Confidencialidad, Autenticidad e Integridad**

Nivel Bajo [I C A]

✓ En caso de que las dimensiones de integridad [I], confidencialidad [C] y autenticidad [A] tengan todas ellas un nivel Bajo, no establecen ningún requisito sobre el cifrado de la comunicación inalámbrica.

✓ Por lo tanto, se permite el uso de TKIP y, consecuentemente, de WPA. Esto favorece el uso de equipamiento antiguo que puede no soportar la carga computacional que supone el uso de CCMP (AES) con WPA2. Sin embargo, si el equipamiento inalámbrico lo permite y aunque no sea requisito exigido, se recomienda el uso de WPA2.

8.- Criptología de empleo en la ENS

7.3.- Algoritmos acreditados

- **Protección de Confidencialidad, Autenticidad e Integridad**

✓ **<u>Nivel Medio [I C A]</u>**

- En caso de que las dimensiones de integridad [I], confidencialidad [C] y autenticidad [A] tengan alguna de ellas nivel Medio y ninguna nivel Alto, las medidas y aplicadas a la red inalámbrica, establecen que la suite criptográfica usada para la protección de las comunicaciones, deberá emplear algoritmos acreditados por el Centro Criptológico Nacional (CCN).
- Este requisito descarta el uso de TKIP, ya que RC4 (su algoritmo central), no pertenece a los algoritmos acreditados por el CCN según la guía CCN-STIC-807 – Criptografía de empleo en el ENS. Se requiere por lo tanto el uso de CCMP, cuyo algoritmo central es AES, que sí pertenece a la lista de algoritmos acreditados por el CCN. Los dispositivos inalámbricos deberán utilizar por lo tanto WPA2, ya que el uso de CCMP en WPA no es obligatorio y el dispositivo puede no implementarlo. Además, dentro de la configuración de seguridad del AP y del dispositivo cliente deberá inhabilitarse el uso de TKIP, para que en ningún momento (por precaución ante reinicios del equipo) se utilice esta suite criptográfica.

8.- Criptología de empleo en la ENS

7.3.- Algoritmos acreditados

* **Protección de Confidencialidad, Autenticidad e Integridad**

✓ **Nivel Medio [I C A]**

- En el caso de equipamiento inalámbrico obsoleto que no pueda utilizar CCMP, y solo de forma temporal hasta que sea sustituido por la organización, se podrá utilizar TKIP si se utiliza una red privada virtual (VPN) para la protección de la comunicación. Esto exige que la organización disponga de infraestructura VPN (concentradores VPN).

- La VPN se establecerá entre el dispositivo cliente (que deberá por lo tanto disponer de un software cliente de VPN) y el concentrador VPN que se encontrará en la red interna, y por lo tanto detrás del AP. La VPN deberá utilizar una suite criptográfica compuesta por algoritmos acreditados por el CCN.

8.- Criptología de empleo en la ENS

7.3.- Algoritmos acreditados

* **Protección de Confidencialidad, Autenticidad e Integridad**

✓ **<u>Nivel Alto [I C A]</u>**

- En caso de que las dimensiones de integridad [I], confidencialidad [C] y autenticidad [A] tengan alguna de ellas un nivel Alto, las medidas y aplicadas a la red inalámbrica, establecen que los dispositivos inalámbricos deberán utilizar WPA2 y además deberán ser productos certificados conforme a lo establecido en la medida.

- Siguiendo las indicaciones descritas en la medida operacional, deberá utilizarse un dispositivo inalámbrico cuyas funcionalidades de seguridad y cuyo nivel, hayan sido evaluados conforme a normas europeas o internacionales, y cuyos certificados estén reconocidos por el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información. Tendrán la consideración de normas europeas o internacionales, ISO/IEC 15408 u otras de naturaleza y calidad análogas.

8.- Criptología de empleo en la ENS

7.3.- Medidas de seguridad

- IEEE 802.11i (RSN) utiliza dos jerarquías de claves, una para la protección del tráfico unicast (clave Pairwise Master Key), y otra para la protección del tráfico multicast / broadcast (clave Group Master Key). En cada jerarquía se deriva la clave maestra (PSK o GMK) a partir de una clave raíz, que puede ser una clave pre-compartida, PSK, o una clave generada por el Servidor de Autenticación, MSK. De las claves maestras se derivan el resto de claves para la protección de la comunicación.

Categoría Básica

En caso de que se utilicen claves pre-compartidas PSK, estas deberán generarse en medios aislados de los medios de explotación.

Se recomienda el uso de una PSK de al menos 12 caracteres, y generada de forma automática a través de algún dispositivo de generación de claves aleatorias PRNG (Pseudorandom Number Generator). La PSK deberá renovarse de forma periódica.

8.- Criptología de empleo en la ENS

7.3.- Medidas de seguridad

Categoría Básica

Se recomienda la configuración de un tiempo de vida máximo (life time) de las claves PMK (para tráfico unicast) y GMK (para tráfico multicast) no superior a 24 horas.

La distribución de la MSK del Servidor de Autenticación (AS) al AP deberá realizarse a través de un canal seguro, para lo que se requiere el uso de una VPN (Virtual Private Network). Se recomienda el uso de IPsec v3, o TLS 1.2.

Categoría Alta

Los dispositivos inalámbricos deberán usar WPA2 y además deberán ser productos certificados.

Deberá utilizarse un dispositivo inalámbrico cuyas funcionalidades de seguridad y cuyo nivel, hayan sido evaluados conforme a normas europeas o internacionales, y cuyos certificados estén reconocidos por el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información. Tendrán la consideración de normas europeas o internacionales, ISO/IEC 15408 u otras de naturaleza y calidad análogas.

sedian Seguridad Digital de Andalucía