# Evaluación de redes

En el último tiempo, hemos visto una evolución y sofisticación de las amenazas que afectan a usuarios y empresas que utilizan servicios de Internet y de otras redes. Esto está convirtiendo en una necesidad el uso de medidas proactivas y ofensivas que permitan identificar vulnerabilidades, antes de que puedan ser aprovechadas por atacantes. Este enfoque busca conocer las motivaciones de los atacantes, así como las herramientas, métodos o vectores de ataque que utilizan para vulnerar las redes y sistemas informáticos, de manera que se puedan identificar las debilidades en la infraestructura tecnológica antes de que alguien ajeno a los recursos también pueda hacerlo.
En esta publicación abordaremos el tema de las auditorías de redes, como una manera de proteger los recursos -principalmente la información– en el contexto de amenazas cada vez más complejas y dinámicas. Además, distinguiremos entre los distintos tipos de revisiones que se pueden ejecutar.

## Auditorías de seguridad en la red corporativa

Las auditorías juegan un papel relevante ya que permiten mostrar el estado en el que se encuentra la protección de la información y de los activos dentro de las organizaciones. Además, involucra la identificación, análisis y evaluación de debilidades en las medidas de seguridad que han sido aplicadas, así como de los componentes tecnológicos de la empresa. Además, pueden tener distintas intenciones, por lo tanto las revisiones de seguridad varían de acuerdo a condiciones como el alcance, los criterios que se utilizan como parámetros de comparación, las personas que las llevan a cabo, los propósitos que se desean alcanzar, entre otros elementos que determinan el tipo de revisión. Así, se da lugar a distintas clasificaciones que abordaremos a continuación.
En el caso específico de las redes, la auditoría está relacionada con un método o un conjunto de ellos para verificar el cumplimiento de los requisitos de seguridad, necesarios dentro de una colección de dispositivos interconectados -como pueden ser routers, switches, hubs, computadoras y dispositivos móviles, entre otros.

## ¿Qué pueden considerar las auditorías de redes?

### Distintos tipos de evaluaciones ¿Física o lógica?

Cuando se considera la protección de la información y de los dispositivos de red, las auditorías pueden clasificarse en revisiones de seguridad física y lógica. Por un lado, la revisión de seguridad física está orientada en conocer y evaluar los mecanismos de protección del hardware y del cableado, mientras que las revisiones lógicas tienen como propósito verificar y evaluar las medidas de protección sobre la información y los procesos.
En este sentido, la auditoría de seguridad física en redes puede considerar la revisión de las conexiones y su apego a normas de cableado estructurado establecidas por organismos como ANSI o ISO, así como medidas que protegen tanto el cableado como los dispositivos de red, e incluso controles aplicados sobre los cuartos de servidores (sites).

En tanto, las evaluaciones lógicas consideran mecanismos de control de acceso a la red, privilegios de cuentas con autorización para conexiones o los protocolos utilizados, por mencionar algunos ejemplos.

Interna o externa.

Con base en la configuración de la red, la auditoría puede considerar revisones de red interna y externa.
Las revisiones externas son aquellas que se llevan a cabo desde fuera del perímetro y pueden incluir la evaluación de configuraciones, revisión de reglas en firewall, configuración de IP/IPsec[1], listas de control de acceso en routers, entre otras actividades.
La red interna, en cambio, puede considerar la revisión de la configuración de segmentos de red, protocolos utilizados, servicios desactualizados, o topologías empleadas, red cableada o inalámbrica.
Además, también es posible clasificar la revisión en función del tipo de red evaluada, por ejemplo si se trata de una revisión de red cableada o inalámbrica.
Si se trata de redes inalámbricas se deberá evaluar la conveniencia de los protocolos de cifrado utilizados para las comunicaciones entre los puntos de acceso y los dispositivos que se conectan a la red, así como el uso de llaves de cifrado extensas y complejas, que reduzcan la probabilidad de éxito de ataque de fuerza bruta o de diccionario.
En este sentido, también es importante llevar a cabo comprobaciones sobre la vulnerabilidad de los dispositivos relacionada con ataques comunes a redes inalámbricas, por ejemplo: suplantación de puntos de acceso o denegación de servicio DoS[2] (Denial of Service).
Ya hemos visto por que es importante este punto, si consideramos el peligro de la mala gestión del wifi en empresas.

Revisisiones técnicas o de cumplimiento

Otro tipo de auditorías estan relacionadas con las personas que llevan a cabo las revisiones y su especialización en el tema, por lo tanto se pueden llevar a cabo revisiones técnicas y de cumplimiento.
Las revisiones técnicas deben comprender conocimientos de los protocolos y dispositivos utilizados, de manera que las debilidades puedan ser identificadas y posteriormente corregidas. Para esto es importante aplicar la perspectiva ofensiva, en la cual se simulan ataques, claro está, siempre con la autorización debida y en ambientes controlados. Incluyen evaluaciones de vulnerabilidades o pruebas de penetración.
Las revisiones de cumplimiento o gestión permiten conocer el estado de apego en las prácticas que se llevan a cabo en las organizciones relacionadas con la protección de las redes en

[1] **IPsec** (abreviatura de Internet Protocol security) es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. **IPsec** también incluye protocolos para el establecimiento de claves de cifrado.
[2] un **ataque de denegación de servicio**, es un ataque a una red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad con la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema atacado.

comparación con lo que establecen documentos especializados, como puede ser estándares de seguridad, marcos de referencia o requisitos que deban ser cumplidos.

Finalmente, el propósito de las auditorías es la protección. Hemos enlistado, de manera general, este conjunto de enfoques que pueden ser utilizados para llevar a cabo auditorías de redes corporativas. Pero es importante mencionar que el objetivo de cada uno de ellos es el mismo: brindar información sobre el estado de las medidas de seguridad aplicadas para identificar fallas, evaluarlas y posteriormente corregirlas.

Por último, también resaltamos que no debe aplicarse una visión parcial de la auditoría, ya que en la actualidad, las distintas amenazas obligan a tener una perspectiva general de los problemas. De esta manera, es posible considerar los distintos enfoques y sobre todo los elementos involucrados, ya que ningún sistema se encuentra aislado desde dispositivos de red, equipos de cómputos, dispositivos móviles o cualquier otro que pueda conectarse a una red. Y esto, sin los análisis pertinentes, podría aumentar la gama de vulnerabilidades.