Módulo 3. Inventario y descubrimiento

CÓRDOBA CREA FUTURO

Introducción

El inventario de activos y el descubrimiento de red son fundamentales en la ciberseguridad: no se puede proteger lo que no se conoce.

Se entiende por «inventario de activos» la lista de todos aquellos recursos (activos físicos, *software*, documentos, servicios, personas, instalaciones, etc.) que tengan valor para la organización y necesiten ser protegidos. En un equipo de TI, este registro incluye tanto *hardware* (servidores, PC, teléfonos, impresoras, etc.) como *software* (aplicaciones, servicios en la nube, licencias, etc.) y contiene información relevante sobre ubicación, propietario, estado, licencias y fase del ciclo de vida.

En el caso de las pymes, mantener el inventario actualizado resulta fundamental, dado que permite planificar compras, garantizar el cumplimiento normativo (por ejemplo, ISO

27001 exige inventarios actualizados) y facilita la identificación de brechas de seguridad y riesgos, como activos no autorizados. Dado que las amenazas evolucionan constantemente, las pymes deben combinar técnicas activas y pasivas para descubrir y catalogar sus recursos.

En este módulo abordaremos dos enfoques complementarios. En la primera unidad, nos centraremos en Nmap y explicaremos cómo descubrir *hosts* activos, puertos abiertos, servicios, versiones y sistemas operativos en la red. En la segunda, presentaremos buenas prácticas de gestión de inventarios, etiquetado y mantenimiento en pymes con recursos limitados. Cada unidad incluye explicaciones conceptuales, ejemplos prácticos adaptados a pymes y referencias actualizadas. Al final del módulo, se propone un laboratorio guiado, junto con una actividad práctica sencilla y un caso de estudio integrador.

CONTINUAR

Unidad 1. Nmap escencial

Nmap (Network Mapper, https://nmap.org/) es un programa de código abierto que permite efectuar rastreos de puertos. Fue escrito originalmente por Gordon Lyon y actualmente su desarrollo está a cargo de una comunidad. Se creó en un principio para Linux, aunque hoy es multiplataforma.

La herramienta Nmap es una aplicación de escaneo que puede utilizarse mediante una interfaz gráfica de usuario o una interfaz de línea de comandos. Permite detectar equipos en la red y escanearlos en busca de puertos abiertos. Muchos administradores de sistemas y redes también la utilizan para tareas como el inventario de red, la gestión de programas de actualización de servicios y la monitorización del tiempo de actividad de *hosts* o servicios.

Figura 1. Nmap

Fuente: captura de pantalla de Nmap (https://nmap.org/)

DADO QUE MUCHAS HERRAMIENTAS DE SEGURIDAD INFORMÁTICA UTILIZAN TÉRMINOS EN INGLÉS, A CONTINUACIÓN SE ACLARAN ALGUNAS TRADUCCIONES ADOPTADAS EN ESTE MÓDULO:

- ***Decoy***. Traducido como «señuelo».
- ***Fingerprinting***: «identificación por huellas» (en sentido digital). Se utiliza junto con la detección del sistema operativo, por lo que en algunos casos se reemplaza por este término o se reduce simplemente a «identificación».
- ***Host***: traducido habitualmente como «equipo» o «sistema».
- ***Port scan***: barrido de puertos.
- ***(To) probe***: traducido como «sondear» (o «sonda»).
- ***(To) scan***: traducido como «sondear» (o «sondeo») o «analizar» (o «análisis»). No se utiliza «escanear» (o «escaneo»), ya que este término alude literalmente a «pasar por el escáner».

- ***(To) spoof***: traducido como «falsificar».

Escaneos comunes

Hay una serie de razones por las que los profesionales de la seguridad prefieren Nmap a otras herramientas de análisis. Primero, Nmap ayuda a mapear rápidamente una red sin comandos ni configuraciones sofisticadas. También admite comandos simples (por ejemplo, para verificar si un host está activo) y secuencias Otras características de Nmap son las siguientes:

- Permite reconocer rápidamente todos los dispositivos conectados, incluidos servidores, *routers*, *switches*, dispositivos móviles, entre otros, en redes únicas o múltiples.
- Ayuda a identificar los servicios que se ejecutan en un sistema, como servidores web, servidores DNS y otras aplicaciones habituales. Nmap también puede detectar versiones de aplicaciones con un nivel razonable de precisión, lo que facilita la detección de vulnerabilidades existentes.
- Ofrece información sobre el sistema operativo que se ejecuta en los dispositivos, incluidas sus versiones, lo que resulta útil para planificar enfoques adicionales durante pruebas de penetración.

- Durante auditorías de seguridad y escaneos de vulnerabilidades, permite ejecutar scripts del motor de scripting de Nmap para atacar sistemas y obtener información más específica.
- Cuenta con una interfaz gráfica llamada Zenmap, que facilita el mapeo visual de la red, lo que mejora la usabilidad y la generación de informes. Nmap es, además, la herramienta gratuita más utilizada para el descubrimiento de red. Permite identificar qué dispositivos están activos y qué servicios se ejecutan en ellos. Por ejemplo, el comando `nmap -sP 192.168.1.0/24` (o `-sn` en versiones recientes) realiza un *ping scan* que lista los *hosts* activos dentro de la subred.

Una pyme podría emplear estas funciones para detectar rápidamente qué equipos responden dentro de su red local. A partir de esa lista, se pueden ejecutar escaneos de puertos sobre cada *host*. Entre los métodos básicos de escaneo TCP se encuentran los siguientes:

- **Escaneo SYN** (`-sS`): es el modo más común y rápido, también conocido como «semisigiloso», ya que no completa el *three-way handshake*. En lugar de establecer una conexión completa, envía una petición SYN y espera una respuesta. Si se recibe un SYN/ACK, el puerto se considera abierto; si llega un RST, se marca como cerrado. Por ejemplo, el comando `nmap -sS`

192.168.1.100 escanea los puertos TCP de la dirección IP indicada utilizando este método. Requiere privilegios de superusuario y permite realizar escaneos de manera rápida y discreta, ya que no genera registros en muchos sistemas de detección.

- **Escaneo de conexión** (-sT): cuando Nmap no se ejecuta con privilegios de superusuario, se utiliza este método, también conocido como «TCP connect». Realiza conexiones completas, por lo que es más lento y menos discreto, ya que registra la actividad en los registros del sistema. Sin embargo, resulta efectivo si no se cuenta con permisos de administrador.
- **Escaneo UDP** (-sU): se emplea para detectar servicios que utilizan el protocolo UDP, como DNS, SNMP o DHCP. Nmap envía cabeceras UDP vacías a los puertos objetivo. Si se recibe un mensaje ICMP de tipo 3/código 3 («puerto inalcanzable»), el puerto se marca como cerrado; si no hay respuesta tras varios reintentos, se clasifica como abierto o filtrado. Por ejemplo, el comando nmap -sU 192.168.1.0/28 permite escanear los puertos UDP de una red local pequeña. Dado que este tipo de escaneo puede ser lento —ya que retransmite para confirmar la falta de respuesta— y consume ancho de banda, es recomendable limitar los puertos con la opción -p.
- **Escaneos especiales**: Nmap también ofrece sondeos menos comunes, como NULL, FIN y XMAS (-sN, -sF, -sX), fragmentación (--mtu) o análisis de protocolo IP (-sO). No obstante, para la

mayoría de las pymes, suelen ser suficientes los modos estándar SYN y UDP. También existen escaneos *ping* o *ping sweep* para descubrir *hosts* activos de manera rápida (`-sL`, `-PR`, entre otros), y escaneos de protocolo (`-sO`). Por su versatilidad, el uso combinado de `-sS` y `-sU` suele cubrir la mayoría de los requerimientos en entornos corporativos.

Pasos típicos

Imaginemos un pequeño estudio contable con 20 equipos conectados en una red interna. A continuación, se describe un posible procedimiento de escaneo con Nmap:

- ***Ping sweep***. El comando `nmap -sn 192.168.0.0/24` permite identificar los equipos activos en la red.
- **Escaneo TCP básico**: para cada *host* activo, se puede utilizar `nmap -sS -p 1-1024 <IP>` para escanear los puertos más comunes. Esto ayuda a detectar, por ejemplo, si hay un servidor web interno en los puertos 80 o 443, o servicios de archivos en el puerto 445.
- **Detección de servicios**: al agregar la opción `-sV` (detección de versiones), se obtiene información adicional sobre los servicios detectados. Por ejemplo, `nmap -sS -sV -p 22,80,443 192.168.0.10` (véase la sección 1.4 para más detalles).

- **Escaneo UDP**: si se sospecha de servicios que utilizan UDP, como DNS local o un servidor DHCP, se puede ejecutar un comando como `nmap -sU -p 53,161,123 192.168.0.1`.
- **Reportar hallazgos**: es importante registrar los *hosts* identificados, los puertos abiertos y las aplicaciones detectadas (véase sección 1.4).

Estas tareas deben realizarse siempre con la debida autorización. Una pyme puede utilizar Nmap legalmente en su propia red sin costo alguno, ya que se trata de software libre. Se recomienda ejecutar los escaneos en horarios controlados para evitar la saturación de la red o interferencias con las tareas habituales.

Componente Nmap para ejecutar scripts Nmap Scripting Engine (NSE). Manejo básico

Una de las principales ventajas de Nmap es su motor de *scripting*, conocido como Nmap Scripting Engine (NSE). Este componente permite ejecutar *scripts* escritos en el lenguaje Lua, lo que facilita la automatización de tareas avanzadas durante el escaneo. Gracias al NSE, es posible realizar comprobaciones de vulnerabilidades, auditorías de servicios

específicos y consultas a fuentes externas, entre otras acciones. Este motor amplía significativamente las capacidades de Nmap, ya que permite llevar a cabo análisis mucho más detallados que un simple escaneo de red, automatizando buena parte del proceso necesario para detectar y gestionar amenazas de seguridad.

CATEGORÍAS DE SCRIPTS	DETECCIÓN DE SO (SISTEMA OPERATIVO)	SALIDAS Y PARSING

Los *scripts* del motor NSE están organizados en categorías fijas, definidas por los desarrolladores de Nmap según el propósito de cada *script*. Esta clasificación permite identificar rápidamente su función y nivel de intrusión. A continuación, se describen las principales categorías.

- **auth**: enfocados en la gestión de credenciales y autenticación. Evalúan la seguridad de servicios como FTP, SSH o HTTP mediante la prueba de combinaciones de usuario y contraseña. Son especialmente útiles en auditorías para verificar la solidez de las políticas de autenticación.
- **broadcast**: emplean consultas de difusión para descubrir *hosts* y servicios en una red local sin necesidad de especificar direcciones IP. Son efectivos para la detección masiva de dispositivos y servicios en entornos corporativos.
- **brute**: ejecutan ataques de fuerza bruta utilizando listas predefinidas de credenciales. Su objetivo es detectar contraseñas débiles, por lo que son

fundamentales en pruebas de penetración, siempre con la debida autorización.

- **default**: considerados seguros y útiles para la mayoría de los escaneos, proporcionan información adicional sobre los servicios detectados sin realizar acciones intrusivas. Se ejecutan automáticamente al usar la opción -sC.
- **discovery**: permiten recopilar información adicional del objetivo, como enumerar servicios, usuarios o recursos compartidos. Facilitan el reconocimiento previo al análisis más profundo.
- **dos**: simulan ataques de denegación de servicio, agotando recursos o explotando fallos conocidos. Deben utilizarse con extrema precaución y únicamente en entornos controlados.
- **exploit**: aprovechan vulnerabilidades conocidas para verificar si estas pueden ser explotadas. Se emplean en pruebas de penetración con autorización, ya que pueden comprometer la seguridad del sistema.
- **external**: interactúan con servicios o bases de datos externos, como consultas WHOIS o geolocalización, para obtener información sin afectar directamente el objetivo.
- **fuzzer**: envían datos aleatorios o malformados a servicios con el fin de detectar fallos en su implementación. Aunque eficaces, pueden causar inestabilidad y deben usarse con cuidado.
- **intrusive**: realizan acciones agresivas que podrían afectar la estabilidad del sistema o ser detectadas como maliciosas. Solo deben emplearse con autorización expresa.

- **malware**: buscan signos de infección o actividad maliciosa en el sistema objetivo. Resultan útiles en auditorías orientadas a la detección de compromisos.
- **safe**: recopilan información básica de manera no intrusiva. No alteran el sistema ni generan alertas, por lo que son ideales para escaneos preliminares.
- **version**: mejoran la detección de versiones de servicios mediante consultas específicas. Esto permite identificar con mayor precisión el software en ejecución, lo cual es clave para evaluar posibles vulnerabilidades.
- **vuln**: verifican si los servicios detectados están expuestos a vulnerabilidades conocidas y documentadas, como Heartbleed o Shellshock. Son fundamentales en auditorías de seguridad.

Las categorías de scripts del NSE no son excluyentes: un mismo script puede pertenecer a varias categorías según sus funciones. Los desarrolladores de Nmap asignan múltiples etiquetas cuando el propósito del script abarca distintos usos. Para consultar los scripts asociados a una categoría específica, se puede utilizar el comando `--script-help`. Por ejemplo, para visualizar todos los *scripts* de la categoría *discovery*, se utiliza el siguiente comando:

```
nmap --script-help "category:discovery"
```

También es posible ejecutar *scripts* específicos según las necesidades del análisis. A continuación, se presentan algunos comandos prácticos que pueden emplearse en entornos de pequeña escala, como una pyme:

- `nmap -sC -p 80,443 192.168.1.100`: ejecuta los *scripts* por defecto en los puertos 80 y 443 de un *host*.
- `nmap --script vuln -p 22,80 192.168.1.0/28`: busca vulnerabilidades conocidas en servicios SSH y HTTP dentro de una subred.
- `nmap --script smb-enum-shares.nse -p 445 192.168.0.10`: lista recursos compartidos de Windows en un servidor SMB.
- `nmap --script http-enum -p 80 192.168.0.20`: enumera posibles rutas y tecnologías web de un sitio interno.
- `nmap --script dns-brute 192.168.1.1`: intenta detectar subdominios comunes en un servidor DNS local.

Los *scripts* del NSE requieren privilegios apropiados y deben usarse con cuidado: los pertenecientes a las categorías *intrusive* o *dos* pueden afectar la red, por lo que siempre se debe contar con autorización. En resumen, el NSE potencia a Nmap para realizar auditorías automatizadas de vulnerabilidades y recolección de información en profundidad, algo muy útil para administradores de pymes con pocos recursos técnicos.

La detección del sistema operativo (SO) de los equipos escaneados es una de las funciones más reconocidas de Nmap. Esta técnica se basa en el análisis de huellas TCP/IP.

Nmap envía paquetes TCP y UDP específicos y analiza diversos aspectos de las respuestas —como el tiempo de vida (TTL), la identificación de paquetes, las opciones TCP, entre otros— para compararlos con una base de datos de huellas registrada (`nmap-os-fingerprints`). Si encuentra coincidencias, informa el sistema operativo detectado, incluyendo nombre, versión y fabricante.

En la práctica, esta función se activa con la opción `-O`. Por ejemplo, el comando `nmap -O 192.168.0.5` intenta identificar si el *host* escaneado ejecuta Windows, Linux, Cisco IOS u otro sistema.
Para obtener resultados precisos, se recomienda que el objetivo tenga al menos un puerto abierto y otro cerrado, ya que Nmap necesita respuestas contrastadas para realizar una comparación efectiva. Además, esta técnica suele requerir privilegios de superusuario (como el escaneo SYN) y tarda más que otros modos, pero ofrece información valiosa. Conocer si un servidor remoto utiliza, por ejemplo, Windows Server 2012, Linux Debian 10 o Android, permite identificar vulnerabilidades específicas y planificar actualizaciones.

En el contexto de una pyme, podríamos utilizar el comando `nmap -sS -O -p 22,80,443 192.168.1.0/24` para escanear la red interna mediante SYN scan e intentar detectar el sistema operativo de cada *host* que tenga puertos abiertos en servicios SSH o web. Al activar la salida detallada con `-v`, se indicará la probabilidad de acierto y el SO estimado. Si no se obtiene un nivel de confianza suficiente, Nmap incluso invita a contribuir enviando nuevas huellas.

En entornos pequeños, esta funcionalidad permite detectar, por ejemplo, equipos con Windows XP (obsoleto) o *routers* con *firmware* desactualizado.

En resumen, la opción `-O` resulta útil para enriquecer el inventario de activos con información sobre el sistema operativo que ejecuta cada dispositivo detectado.

CATEGORÍAS DE SCRIPTS	DETECCIÓN DE SO (SISTEMA OPERATIVO)	SALIDAS Y PARSING

Nmap ofrece múltiples formatos de salida para sus resultados, lo que facilita tanto la revisión manual como el análisis automatizado. Además, permite controlar el nivel de detalle de los informes, así como los mensajes de depuración. Las salidas pueden mostrarse en

la consola o guardarse en archivos, que pueden usarse posteriormente para reanudar escaneos interrumpidos.

De manera predeterminada, Nmap muestra la salida de forma interactiva en la consola. Sin embargo, utilizando las opciones `-o`, es posible guardar los resultados en distintos formatos de archivo:

- `-oN <fichero>` (normal). Guarda la salida en texto legible, similar a la que se muestra en pantalla. Por ejemplo, `-oN inventario.nmap` crea un informe de texto con todos los hallazgos.
- `-oX <fichero>` (XML): genera una salida estructurada en formato XML. Este formato es clave para procesar automáticamente los datos con otras herramientas o importarlos a bases de datos u hojas de cálculo. También permite aplicar hojas de estilo XSL para visualizar los resultados, por ejemplo, abriendo el archivo en un navegador.
- `-oG <fichero>` (*grepable*, obsoleto): fue un formato en el que cada línea representaba un *host*. Actualmente está en desuso en favor del XML, que ofrece mayor compatibilidad con analizadores modernos. No obstante, algunos scripts antiguos aún lo requieren.
- `-oA <prefijo>`: guarda simultáneamente en los tres formatos anteriores usando el mismo prefijo. Por ejemplo, `-oA reporte` generará los archivos `reporte.nmap`, `reporte.xml` y `reporte.gnmap`. Esta opción es útil para conservar todos los

formatos con un solo comando.

Las salidas pueden combinarse con opciones como `-v` (verbosidad) para aumentar el nivel de detalle, o `-d` (depuración) para analizar problemas técnicos. Además, al guardar en archivos, Nmap sigue mostrando la salida en pantalla, a menos que se indique lo contrario. Por ejemplo, `-oX -` envía el resultado en formato XML directamente a la salida estándar (*stdout*).

Parseo

Para procesar los resultados de Nmap, la opción más práctica es utilizar la salida en formato XML. Existen bibliotecas en lenguajes como Python o Perl (por ejemplo, `Nmap::Parser` o `libnmap`) que permiten extraer de forma sencilla los *hosts*, puertos y servicios detectados desde un archivo XML.

En el caso de una pyme sin personal de desarrollo, también es posible abrir el archivo XML directamente en Excel o emplear herramientas como `xsltproc` para convertirlo a otros formatos. De manera alternativa, la salida en formato normal (`-oN`) puede procesarse mediante comandos como `grep`, `awk` o `sed` en entornos Linux, por ejemplo, para filtrar puertos abiertos:

```
nmap -p 22,80,443 -oN output.txt 192.168.0.0/24
grep "open" output.txt
```

Sin embargo, el formato XML ofrece mayor precisión, ya que permite distinguir con claridad entre puertos abiertos, filtrados u otros estados, sin ambigüedades.

Otras opciones útiles para el manejo de salidas incluyen `--append-output`, que permite añadir resultados a un archivo en lugar de sobrescribirlo, y `--stats-every`, que informa del progreso del escaneo a intervalos regulares.

Estas posibilidades facilitan la integración de Nmap dentro de un flujo de trabajo de inventario: se ejecuta el escaneo, se guarda el resultado en un archivo con fecha en el nombre, y luego se importan los datos al sistema de inventario de la empresa. En resumen, se recomienda utilizar las opciones `-oX` y/o `-oA` para capturar los resultados de forma estructurada y permitir su análisis posterior mediante scripts o herramientas automatizadas.

CONTINUAR

Unidad 2. Inventario vivo

Para construir una arquitectura moderna y defendible, es fundamental que los propietarios y operadores de tecnología operativa (TO) de todos los sectores de infraestructura crítica cuenten con un inventario actualizado de activos de TO, complementado por una taxonomía clara de dichos activos.

El uso de estas herramientas permite identificar qué elementos del entorno deben ser protegidos y estructurar las defensas de manera adecuada, con el fin de reducir el riesgo que un incidente de ciberseguridad representa para la misión y la continuidad operativa de la organización.

Un inventario de activos es una lista organizada y actualizada de forma periódica que incluye los sistemas, el *hardware* y el *software* de una organización.

En entornos de tecnología operativa (TO), un aspecto clave para la creación de un inventario de activos es el desarrollo de una taxonomía específica: un sistema de categorización que organiza y prioriza los activos de TO. Esta clasificación facilita la identificación de riesgos, la gestión de vulnerabilidades y la respuesta a incidentes, al agrupar los activos según su función y nivel de criticidad.

La gestión del inventario es un proceso continuo. No basta con conocer los activos una sola vez; es necesario mantener un inventario vivo, que se actualice de forma permanente ante cualquier cambio.

Un inventario vivo en ciberseguridad es una lista dinámica y automatizada de todos los activos de una organización — ***hardware, software*****, datos y redes— que se actualiza en tiempo real o de forma continua. Este enfoque permite gestionar los riesgos de manera proactiva, garantizar el cumplimiento normativo (como ISO 27001) y mejorar la respuesta ante incidentes. Este enfoque supera el modelo tradicional basado en hojas de cálculo estáticas y se convierte en una herramienta estratégica de seguridad.**

Etiquetado de activos

Una medida básica para el control de activos consiste en asignarles identificadores únicos, ya sean físicos o digitales. En la Gestión de Activos Tecnológicos (*IT Asset Management*, ITAM), el etiquetado es la práctica de colocar identificadores únicos a los recursos tecnológicos para facilitar su rastreo y administración durante todo su ciclo de vida.

Esta práctica resulta esencial para mejorar la visibilidad, la seguridad y el cumplimiento normativo. Sin un sistema de etiquetado adecuado, el seguimiento del *hardware*, el *software* y otros recursos informáticos puede volverse caótico.

En la práctica, se aplica del siguiente modo:

- ***Hardware*** (*laptops*, servidores, *routers*, impresoras). Se colocan etiquetas adhesivas con un número de inventario único (por ejemplo, «IT-001», «IT-002»), que pueden ser códigos de barras o QR. En entornos muy grandes se utiliza tecnología RFID, pero en pymes suelen ser suficientes etiquetas de papel o plástico.

- ***Software* y licencias**: se asignan códigos o números de licencia dentro de un registro digital. No se utilizan etiquetas físicas, sino campos en la base de datos de inventario.
- **Activos intangibles**: bases de datos, cuentas críticas u otros recursos que no se etiquetan físicamente, pero deben ser registrados y gestionados de manera adecuada.

Las etiquetas deben incluir, como mínimo, el identificador único del activo, y opcionalmente pueden contener otros datos relevantes, como el código de ubicación o el departamento al que pertenece. Al escanear o leer estas etiquetas, el personal de TI puede identificar rápidamente el activo en el sistema de inventario.

El etiquetado contribuye a mejorar la organización y la visibilidad de los recursos, ya que facilita el seguimiento de activos y reduce el riesgo de pérdida o extravío. Además, en entornos dinámicos, permite cumplir con requisitos normativos —como vincular correctamente cada licencia a su equipo— y fortalece la seguridad, al dejar claro quién es responsable de cada dispositivo.

Cinco ventajas de etiquetar activos en la empresa —

La implementación del etiquetado de activos como parte de una estrategia de gestión de activos tecnológicos (ITAM) ofrece

múltiples beneficios. Entre ellos, se destacan los siguientes:

- **Mejora de la organización**. Permite un seguimiento rápido y eficaz de los activos, lo que reduce el riesgo de pérdida o extravío y asegura un control más preciso de toda la infraestructura tecnológica.
- **Simplificación de la gestión por grupos**: cuando las etiquetas están asociadas a registros digitales, es posible agrupar y administrar los recursos según criterios como ubicación, departamento, estado o nivel de riesgo. Esto facilita la aplicación de acciones en bloque, la supervisión segmentada y la organización a gran escala.
- **Precisión en la información**: este método proporciona datos consistentes y confiables. Si el seguimiento es automatizado, el proceso se vuelve aún más eficiente al requerir una intervención mínima.
- **Rastreo del ciclo de vida**: desde la adquisición hasta la baja, las etiquetas permiten supervisar cada etapa del activo, lo que facilita la planificación de actualizaciones, reemplazos o mantenimiento.
- **Mayor visibilidad y generación de reportes**: al contar con una visión integral del entorno, es posible elaborar informes precisos

sobre el uso de los activos, su historial de mantenimiento y el cumplimiento normativo.

En una pequeña clínica, por ejemplo, cada computadora, impresora y *router* cuenta con una etiqueta identificadora. El personal de TI registra ese código en una planilla de Excel junto con información relevante como la descripción del activo, modelo, fecha de alta y usuario asignado. Esta práctica permite verificar físicamente cada equipo frente a su registro digital en caso de una auditoría, ya sea externa o interna, y refuerza el control general sobre los recursos tecnológicos disponibles.

¿Qué tipos de recursos informáticos deben etiquetarse?

Si bien es posible hacer un seguimiento de todos los activos informáticos, el verdadero valor del etiquetado reside en centrarse en aquellos que aportan mayor rendimiento, visibilidad y control para la organización. Priorizar los activos adecuados permite reducir riesgos y optimizar costos sin perder tiempo en elementos de bajo impacto.

A continuación, se enumeran los principales tipos de activos tecnológicos que conviene etiquetar:

- ***Hardware***. Activos tangibles, de alto valor y frecuentemente críticos para las operaciones, como laptops, computadoras de escritorio, servidores, equipos de red y periféricos.
- ***Software* y licencias**: aplicaciones, sistemas operativos, soluciones empresariales y suscripciones SaaS. Es fundamental realizar un seguimiento de su uso, fechas de renovación y cumplimiento.
- **Servicios en la nube y activos virtuales**: aunque no sean físicos, pueden generar costos recurrentes y presentar vulnerabilidades ocultas. Incluyen máquinas virtuales, almacenamiento en la nube y servicios en línea.
- **Consumibles y periféricos**: elementos de menor costo —como teclados, cables, *mouses* o adaptadores— que, al fallar, pueden generar interrupciones y cuellos de botella en las operaciones.
- **Máquinas especializadas o específicas del sector**: dispositivos que requieren mantenimiento, calibración o cumplimiento normativo, como equipos médicos o de laboratorio, o cualquier recurso con un alto costo de sustitución.
- **Cuentas de redes sociales y la información contenida en ellas**: aunque intangibles, también representan activos que deben gestionarse con cuidado por su valor reputacional y su exposición a riesgos de seguridad.

Para facilitar el manejo y mantenimiento del inventario, es recomendable clasificar los activos por categorías, de acuerdo con su naturaleza y función. Esta organización permite una gestión más eficiente, tanto operativa como estratégica. Entre las categorías más utilizadas se encuentran las siguientes:

- **Datos**. Incluyen toda la información generada, recogida, gestionada, transmitida o eliminada, en cualquier formato. Ejemplos: bases de datos, documentación técnica, manuales de usuario, contratos, normativas, entre otros.
- **Aplicaciones**: abarcan el *software* utilizado para la gestión de procesos. Se incluyen aquí los sistemas SCADA, herramientas de desarrollo de HMI, aplicaciones desarrolladas a medida, sistemas operativos y *firmware* de dispositivos.
- **Hardware industrial**: equipos físicos necesarios para las operaciones industriales, como terminales remotas, PLC, IED, computadoras personales, servidores y dispositivos móviles o portátiles.
- **Red**: dispositivos de conectividad, tales como *routers*, *switches*, concentradores, pasarelas, entre otros elementos que conforman la infraestructura de red.

- **Tecnología**: otros equipos necesarios para la gestión de las personas y del negocio, como servidores, equipos de usuario, teléfonos, impresoras, *routers* o cableado estructurado.
- **Personal**: incluye tanto al personal interno de la organización como a contratistas, personal de mantenimiento y cualquier otra persona con acceso, directo o indirecto, a los sistemas industriales.
- **Instalaciones**: espacios donde se alojan los sistemas relevantes, como oficinas, edificios, instalaciones eléctricas o vehículos utilizados en la operación.
- **Equipamiento auxiliar**: comprende activos que dan soporte a los sistemas de información, pero que no encajan en las categorías anteriores, como equipos para destrucción de datos, sistemas de climatización o unidades SAI.

Cinco tipos de etiquetas para los activos tecnológicos

Cuando se habla de etiquetas para activos tecnológicos, generalmente se hace referencia a las etiquetas físicas adheridas directamente a los dispositivos. Esta es la forma más común de identificar y rastrear equipos de tecnología. A continuación, se describen los principales tipos de etiquetas utilizadas:

- **Etiquetas con código de barras**. Son económicas y fáciles de implementar, aunque requieren escáneres específicos para su lectura.
- **Etiquetas QR**: permiten almacenar mayor cantidad de información y pueden ser escaneadas con teléfonos inteligentes o *tablets*.
- **Etiquetas RFID**: utilizan ondas de radio para realizar el seguimiento inalámbrico. Son ideales en entornos con gran volumen de activos, ya que no requieren contacto visual directo.
- **Etiquetas NFC**: variante de la tecnología RFID, con menor alcance. Se emplean para identificación rápida mediante dispositivos móviles compatibles.
- **Etiquetas GPS**: incorporan funciones de geolocalización y permiten el seguimiento en tiempo real de los activos, independientemente de su ubicación. Por su costo, no son comunes en entornos informáticos tradicionales, pero resultan útiles para recursos móviles o de alto valor que requieren visibilidad permanente.

Más allá de las etiquetas físicas, muchas plataformas modernas de gestión de activos (ITAM) incorporan **etiquetas digitales**. Estas no se colocan en los dispositivos, sino que funcionan como

clasificaciones internas dentro del sistema, permitiendo agrupar, filtrar y administrar activos según criterios como ubicación, departamento, tipo de licencia o nivel de riesgo. La combinación de etiquetas físicas y digitales proporciona un mayor nivel de control y visibilidad sobre la infraestructura tecnológica.

¿Cómo es el procedimiento de etiquetado de activos de información?

Aunque el etiquetado de activos tecnológicos puede realizarse de forma manual, lo más eficaz es gestionar el proceso mediante una plataforma especializada de seguimiento. Este tipo de software no solo agiliza las tareas, sino que también reduce los errores humanos y permite automatizar partes del flujo de trabajo. Además, muchas de estas herramientas incluyen campos estandarizados para registrar los datos de cada bien, lo que facilita una estructura de etiquetado coherente en todo el inventario.

A continuación, se describe el procedimiento paso a paso para el etiquetado de activos físicos de información:

- **Definición de normas para las etiquetas**. Establecer qué información deben contener (tipo de activo, identificador único, número de serie, ubicación, usuario asignado). También es

importante definir convenciones claras de nomenclatura para garantizar la coherencia en todo el inventario.

- **Carga en el sistema**: registrar los bienes en la plataforma, completando los perfiles con los datos básicos. Esto constituye la base para un seguimiento preciso.
- **Generación e impresión**: crear los códigos de barras, QR u otros identificadores a partir de la información registrada, e imprimir las etiquetas correspondientes para cada equipo.
- **Colocación de las etiquetas**: adherirlas en una zona visible y accesible, asegurándose de que sean lo suficientemente duraderas como para resistir el uso cotidiano.
- **Vinculación y validación**: escanear las etiquetas para asociarlas correctamente a los perfiles registrados en el sistema y verificar que la información sea precisa y esté actualizada.
- **Auditorías periódicas**: revisar que las etiquetas permanezcan intactas, que los datos sean correctos y que los bienes retirados se eliminen del sistema.

De forma complementaria, también es posible añadir **etiquetas digitales** dentro del *software* de gestión. Estas se basan en metadatos y permiten agrupar activos según criterios como

departamento, ubicación, estado de la licencia o fase del ciclo de vida, aportando mayor flexibilidad y visibilidad al inventario.

Ejemplos de etiquetado de activos

En términos prácticos, el etiquetado de activos IT puede implementarse de las siguientes maneras:

- ***Laptops* o computadoras con códigos QR**. Cada equipo entregado a los empleados incorpora un código QR. Al escanearlo, se accede de inmediato al perfil del activo, que contiene información relevante como el usuario asignado, la fecha de compra y el estado de la garantía. Esto facilita el seguimiento, especialmente en organizaciones con personal distribuido.
- **Servidores con códigos de barras**: durante las auditorías de rutina, los técnicos escanean las etiquetas para verificar la ubicación, el historial de mantenimiento y los parámetros de configuración. Este procedimiento garantiza precisión sin requerir intervenciones manuales extensas.
- **Equipos de red con etiquetas RFID**: dispositivos como conmutadores o *firewalls* pueden ser etiquetados con chips RFID, lo que permite recolectar información de múltiples activos simultáneamente. Esto acelera las tareas de control de

inventario en entornos de gran escala y disminuye el riesgo de extravíos.

Planillas y ciclos de revisión

Para que un inventario de activos aporte valor en la evaluación de la seguridad y en la gestión de riesgos, debe contener información suficiente tanto para responder ante incidentes como para planificar futuros proyectos. Además, debe ofrecer una visión precisa del valor de cada activo, lo que permite establecer criterios adecuados para realizar un análisis de riesgos.

PARA CUMPLIR CON ESTE PROPÓSITO, EL INVENTARIO DEBE REGISTRAR LA INFORMACIÓN RELEVANTE DE CADA SISTEMA:	EN LA PRÁCTICA DE LAS PYMES, SE SUGIERE APLICAR LAS SIGUIENTES MEDIDAS:	ALTA / BAJA / CAMBIO

- **Nombre**. Puede incluir la marca, el modelo o una denominación descriptiva que facilite su identificación.
- **Descripción**: no es necesario que sea extensa, pero debe indicar claramente el uso del activo dentro de la organización.
- I**dentificador**: código único asignado al activo, siguiendo un patrón definido por la empresa.

- **Tipo**: categoría a la que pertenece el activo (por ejemplo, hardware, software, red, etc.).
- **Propietario**: persona responsable de tomar decisiones sobre el activo, como su reemplazo o retiro.
- **Responsable**: encargado de mantener el activo operativo y de gestionar los accesos al mismo. En algunos casos, puede coincidir con el propietario.
- **Ubicación**: lugar físico donde se encuentra el activo. En el caso de activos lógicos, la ubicación hace referencia al sistema físico que los contiene.
- **Valoración del activo**: permite evaluar su impacto en el sistema. Esta valoración puede basarse en distintos parámetros:
    - **Disponibilidad**: grado de importancia que tiene la ausencia del activo, expresado cualitativa o cuantitativamente.
    - **Integridad**: consecuencias para el negocio ante una modificación no autorizada del activo.
    - **Confidencialidad**: nivel de protección que requiere la información asociada al activo.
    - **Criticidad**: grado de dependencia del proceso con respecto al activo. A mayor criticidad, mayores serían las consecuencias ante su pérdida.

- **Costo**: valor económico del activo.

Muchas pymes gestionan sus inventarios mediante hojas de cálculo —como Excel, LibreOffice Calc o Google Sheets— debido a que son herramientas accesibles y de uso generalizado. Lo importante es que estas planillas estén correctamente estructuradas para facilitar su mantenimiento y análisis.

Una hoja de inventario típica puede incluir columnas como identificador del activo, tipo (PC, *switch*, etc.), modelo, ubicación, usuario responsable, valor, fecha de compra, vida útil estimada, fecha de alta en inventario y observaciones, entre otras.

Existen plantillas gratuitas disponibles en línea —por ejemplo, en plataformas como Smartsheet— aunque muchas de ellas se encuentran en inglés. Lo fundamental es adaptar la planilla a las necesidades del negocio local. Esto puede incluir campos específicos como la versión del *firmware* o del software, o bien la clasificación del activo según el nivel de confidencialidad de la información que gestiona.

El mantenimiento del inventario debe realizarse de forma periódica. Es recomendable que un equipo responsable revise el inventario al menos una vez al año y también cada vez que se incorpore o retire un activo

PARA CUMPLIR CON ESTE PROPÓSITO, EL INVENTARIO DEBE REGISTRAR LA INFORMACIÓN RELEVANTE DE CADA SISTEMA:	EN LA PRÁCTICA DE LAS PYMES, SE SUGIERE APLICAR LAS SIGUIENTES MEDIDAS:	ALTA / BAJA / CAMBIO

- **Revisión trimestral o semestral**. Consiste en comparar la planilla con la infraestructura física y la red real. Se verifica si hay equipos faltantes o si existen dispositivos no registrados. Por ejemplo, utilizando herramientas como Nmap, es posible detectar cámaras IP, impresoras u otros dispositivos conectados que no figuran en el inventario. Una vez verificados, deben ser incorporados.
- **Actualización tras cambios**: cada vez que se adquiere un nuevo equipo o se retira uno existente, la información debe actualizarse de inmediato en el inventario. Esto evita inconsistencias o datos obsoletos. En este sentido, la norma ISO 27001, en su control A.8.1.1, exige un inventario documentado y actualizado ante cualquier cambio.
- **Ciclo de vida**: es importante planificar la renovación de los activos con anticipación. Por ejemplo, si una computadora cumple cinco años, se puede marcar en el inventario para su reemplazo futuro. Esta práctica evita decisiones urgentes y costosas.

Para organizaciones con recursos limitados, las hojas de cálculo representan una opción viable para gestionar el inventario, siempre que se mantenga una disciplina administrativa constante. Como alternativa o complemento, existen herramientas gratuitas de gestión de activos que automatizan escaneos y generación de reportes, como OCS Inventory y GLPI, ambas de código abierto.

OCS Inventory permite desplegar agentes en los equipos, los cuales envían de forma periódica información detallada de hardware y software a un servidor central. Esto mantiene actualizada la base de datos de inventario sin intervención manual. Además de capturar información, permite crear configuraciones y desplegarlas en los equipos. Se compone de cuatro servicios principales, que pueden instalarse en un único equipo o distribuirse:

- **Servicio de base de datos**. Almacena los datos recolectados.
- **Servicio de comunicaciones**: gestiona el intercambio de datos por HTTP entre los agentes y la base de datos.
- **Consola de administración**: interfaz web que permite a los administradores consultar y gestionar el inventario.
- **Servicio de despliegue**: almacena y distribuye configuraciones a los dispositivos gestionados.

GLPI, por su parte, es una aplicación web que ofrece una gestión integral del inventario informático, incluyendo además un sistema de gestión de incidencias (*ticketing*). Puede instalarse en entornos LAMP (Linux, Apache, MySQL, PHP), y también es compatible con servidores Windows. Su instalación y uso son simples, lo que facilita la implementación incluso en entornos con equipos reducidos.

Esta herramienta combina la gestión de activos (equipos, servidores, periféricos, licencias, topología de red, reservas de recursos, entre otros) con la gestión de soporte técnico. Esto permite vincular cada intervención a usuarios y dispositivos, generando un historial completo de mantenimiento.Ambas soluciones pueden integrarse: OCS Inventory recopila y actualiza los datos, y GLPI los gestiona desde una interfaz centralizada.

Su uso conjunto permite ahorrar tiempo frente a la gestión manual y proporciona una visión mucho más precisa de la infraestructura tecnológica. No obstante, cuando no se cuenta con personal dedicado, una estrategia sencilla basada en planillas y escaneos regulares con Nmap puede ser suficiente para mantener un inventario actualizado en el día a día.

PARA CUMPLIR CON ESTE PROPÓSITO, EL INVENTARIO DEBE REGISTRAR LA INFORMACIÓN RELEVANTE DE CADA SISTEMA:	EN LA PRÁCTICA DE LAS PYMES, SE SUGIERE APLICAR LAS SIGUIENTES MEDIDAS:	ALTA / BAJA / CAMBIO

El proceso de alta, baja y cambio (ABC) de activos constituye el pilar del mantenimiento del inventario. Documentar correctamente cada uno de estos movimientos permite conservar un registro actualizado y confiable.

- **Alta de activos**

Cada vez que ingresa un nuevo equipo, debe asignársele de inmediato un identificador único, colocarse su etiqueta correspondiente (véase apartado 2.1) y registrarse en el inventario con todos los datos relevantes: modelo, ubicación, usuario asignado, fecha de adquisición, costo, entre otros. Por ejemplo, al incorporar una computadora de escritorio, se le genera un código como «IT-025», se coloca la etiqueta física en la carcasa, y se registra en la planilla: «IT-025 – PC escritorio – Dell Optiplex – Oficina Norte – Juan Pérez – 15/03/2025». Con estos pasos, el equipo queda formalmente incorporado al inventario.

- **Baja de activos**

Ya sea por obsolescencia, extravío o robo, la baja de un equipo debe reflejarse en el inventario. Se actualiza el estado como «dado de baja», se consigna la fecha de retiro y, en algunos casos, se traslada el registro a otra hoja para mantener el historial.

Por motivos normativos, es importante conservar los registros de baja, ya que pueden ser requeridos en auditorías o reclamos ante seguros. Además, el equipo debe retirarse físicamente del entorno de producción, lo cual incluye tareas como eliminar cuentas de usuario asociadas o borrar configuraciones sensibles. Es fundamental no reutilizar el mismo identificador en otro dispositivo. En caso de reciclar físicamente el equipo (por ejemplo, tras una reparación), se le asigna un nuevo código y se etiqueta nuevamente.

- **Cambio de activos**

En caso de **cambio**, como puede ser la reasignación de un equipo a otro usuario, la modificación de un componente interno o la reubicación física, se debe actualizar la información correspondiente en el inventario: responsable, ubicación, especificaciones técnicas, entre otros campos.

Por ejemplo, si un servidor cambia de rack, se actualiza el campo de ubicación; si se amplía la memoria RAM, se añade el dato en la descripción técnica. Toda modificación relevante —como instalaciones de software o actualizaciones de versión— también debe registrarse. Este proceso controlado permite mantener la sincronización entre el inventario y la realidad operativa.

Por lo general, estas operaciones son documentadas por el área de TI o personal administrativo mediante procedimientos internos. Cada una de estas acciones debe disparar una actualización inmediata del inventario. Además, el área de TI o de seguridad debe coordinarse con compras para registrar nuevos equipos, y con el área contable o financiera para documentar adecuadamente las bajas. En algunos países, como Argentina, los libros contables requieren control formal sobre la baja de bienes.

Para facilitar la gestión, herramientas como hojas de cálculo o plataformas como GLPI y OCS Inventory permiten marcar los activos por estado (activo/inactivo), generar reportes y filtrar información relevante, reduciendo el riesgo de omisiones.

Revisión periódica

Mantener un inventario vivo requiere realizar revisiones y conciliaciones de forma periódica. Es fundamental disponer de un registro actualizado y validado con regularidad, ya que cualquier desvío entre el inventario y la realidad puede derivar en problemas de seguridad o gestión.

En la práctica, esto se implementa mediante auditorías internas, al menos una vez al año, y también cada vez que

ocurre un evento relevante, como una incorporación o baja de activos, o cambios de personal clave. El objetivo es detectar diferencias entre lo documentado y lo que realmente está en uso. Por ejemplo, al realizar un escaneo de red con *Nmap*, pueden detectarse dispositivos conectados que no figuran en la planilla de inventario. Ante esto, es necesario determinar si se trata de equipos legítimos no registrados o posibles intrusos, y actuar en consecuencia.

En muchos casos, se recomienda iniciar la revisión por los activos conectados a Internet, ya que representan un mayor riesgo. Esto es especialmente útil luego de períodos prolongados de trabajo remoto: revisar qué servidores permanecen activos, qué dispositivos IoT se conectaron y si existen accesos externos habilitados que deberían haberse cerrado. En el caso de una pequeña empresa, como una clínica o estudio contable, este control podría revelar que un servidor antiguo aún tiene acceso remoto habilitado por un empleado que ya no forma parte del equipo.

La frecuencia de revisión varía según el tamaño y la madurez de la organización. Algunas empresas realizan auditorías trimestrales o semestrales, mientras que otras más pequeñas pueden comenzar con revisiones anuales combinadas con controles manuales tras movimientos

importantes. Lo más importante es establecer una metodología documentada: por ejemplo, generar informes que comparen el resultado del último escaneo con la planilla de activos. Esto no solo ayuda a mantener el control actualizado, sino que también sirve como respaldo para auditorías externas y mejora la disciplina interna.

Resumen de buenas prácticas en revisión

Para que el inventario de activos de tecnología sea una herramienta útil y confiable en materia de seguridad, no alcanza con armarlo una sola vez: requiere revisiones periódicas y un mantenimiento sistemático. A continuación, se presentan algunas buenas prácticas clave para realizar esa revisión de forma eficaz:

1. **Planificación fija.** Asignar fechas para auditorías de inventario. Marcar en el calendario corporativo (por ejemplo, al cierre del año o cada tres meses).
2. **Reconciliación:** usar Nmap y otras herramientas (*ping*, SNMP) para descubrir dispositivos en la red, y cotejar con el listado del inventario.
3. **Verificación física:** si es posible, cruzar con inspección física, especialmente en oficinas con gran cantidad de equipos.

4. **Acciones correctivas:** para cada discrepancia encontrada, actualizar el inventario o corregir la red (quitar equipos no autorizados, dar de baja licencias olvidadas, etc.).
5. **Documentación:** mantener registros de la revisión (quién la hizo, cuándo, qué se ajustó). Incorporar esta información al proceso de gestión de cambios de la empresa.

De esta forma, el inventario evoluciona con la organización, convirtiéndose en una fuente confiable para la seguridad informática. Vale la pena recordar que los escáneres de vulnerabilidades y los equipos de respuesta solo cubrirán los activos listados en el inventario. Así que mantenerlo actualizado es evitar que «activos desconocidos» se vuelvan agujeros de seguridad.

¿Qué es un inventario de activos de TI?

Un inventario de activos de tecnología de la información (TI) es una herramienta que permite a los equipos técnicos registrar, organizar y gestionar todos los recursos tecnológicos que utiliza una organización. Su objetivo es garantizar que esos recursos estén disponibles, funcionen de manera eficiente y se administren de forma rentable.
Este inventario reúne datos relevantes de cada activo:

- Ubicación y usuarios asignados

- Historial de mantenimiento y soporte
- Documentación técnica
- Rendimiento y estado operativo
- Licencias y cumplimiento normativo
- Coste y fase del ciclo de vida

Los activos incluidos suelen dividirse en dos grandes categorías:

- ***Hardware.*** Servidores, computadoras, portátiles, teléfonos, impresoras, dispositivos de red, etc.
- ***Software*:** aplicaciones instaladas, plataformas en la nube, servicios SaaS, entre otros.

Desde el punto de vista de la **seguridad informática**, este inventario adquiere un rol aún más estratégico. Una auditoría de seguridad efectiva debe priorizar la visibilidad completa de todos los activos conectados a internet y que podrían quedar expuestos a riesgos. Esto abarca no solo el *hardware* y el *software* tradicional, sino también datos sensibles, entornos en la nube y dispositivos IoT e IIoT (Internet de las Cosas e Internet Industrial de las Cosas).

En definitiva, cualquier elemento que esté conectado o accesible, ya sea dentro de las instalaciones, en la nube o en un entorno híbrido,

debe figurar en el inventario. Solo así es posible proteger lo que realmente se tiene.

¿Por qué es importante contar con un inventario de activos de TI?

Contar con un inventario completo y actualizado de activos de TI es fundamental porque permite a los equipos de seguridad (SecOps) detectar y corregir vulnerabilidades antes de que sean explotadas por atacantes. Hoy en día, esa tarea es cada vez más compleja. Las superficies de ataque se expanden, los activos se multiplican y las amenazas evolucionan con rapidez. En ese escenario, no se puede proteger lo que no se conoce. Sin un inventario confiable:

- muchos activos pueden quedar fuera del radar: dispositivos obsoletos, mal configurados o instalados sin aprobación;
- se amplifica el fenómeno de la informática en la sombra, donde empleados incorporan soluciones sin intervención del área de TI;
- algunos activos gestionados por terceros o proveedores externos pueden reconectarse sin aviso, generando nuevas brechas de seguridad.

Por eso, un buen inventario no es solo una herramienta de gestión: es una condición básica para la seguridad. Saber qué activos

existen, dónde están, cómo funcionan y quién los usa es el primer paso para proteger la infraestructura tecnológica de una organización.

¿Por qué debe cambiar la gestión de activos?

La gestión de activos siempre se ha realizado sobre la base de un inventario manual y se ha configurado como una auditoría puntual mensual o trimestral. Sin embargo, esta gestión tiene dos grandes inconvenientes: no solo consume una gran cantidad de tiempo y resulta enormemente laboriosa, sino que, por naturaleza, el inventario resultante está plagado de errores y queda obsoleto enseguida.

Esto es muy peligroso, ya que el inventario que utilizan los equipos de seguridad determina la precisión de otros procesos. Los escáneres de vulnerabilidades o antivirus/*antimalware* solo analizan los activos que figuran en el inventario. Por lo tanto, los activos no registrados se convierten rápidamente en riesgos y exposiciones sin identificar. Además, los *red teams* tendrán dificultades para evaluar la gravedad, porque las pruebas de penetración y demás procedimientos requieren una fuente única de información confiable sobre todos los activos.

¿**Cómo gestionar el inventario?**

Teniendo en cuenta los retos que plantea una superficie de ataque moderna, la forma de controlar los activos y mantener un inventario exhaustivo consiste en garantizar que, en todo momento, se detectan y supervisan todos los activos conectados a internet, ya sean de hardware o de software, locales o en la nube. Este modelo de gestión de activos permite contar con una única fuente de información fidedigna, sin importar su ubicación o si pertenecen a un *partner* o a un proveedor.

Conviene considerar que ni toda la gestión de la superficie de ataque (*attack surface management*, ASM) ni todo el software de gestión de activos son equivalentes. Una solución de ASM debe contribuir a garantizar el cumplimiento normativo, reducir los costes asociados a la prevención de ataques y mejorar la eficiencia de SecOps, de modo que se requiera menos intervención humana para identificar y mitigar los riesgos de la superficie de ataque.

Una solución de ASM también debe detectar las exposiciones y ofrecer los datos contextuales necesarios para identificar a quién pertenece el activo y a quién le corresponde corregir los problemas. Sería conveniente que esos avisos y datos pudieran transferirse fácilmente a una herramienta de orquestación, automatización y respuesta de seguridad (SOAR), encargada de automatizar las medidas correctivas.

Para garantizar que un inventario incluya todos los activos, es necesario escanear desde el exterior hacia el interior. Esta perspectiva resulta relevante porque, por un lado, permite encontrar todos los activos y obtener los datos sin necesidad de recurrir a otras herramientas o aplicaciones de software de gestión de activos y, por otro, coincide con el enfoque que un adversario tendría sobre la superficie de ataque.

Los actores de amenazas pueden automatizar los análisis de internet para localizar activos vulnerables en menos de una hora, y la gestión del inventario debería realizarse, como mínimo, a esa velocidad. La gestión moderna de la superficie de ataque puede ser eficiente y eficaz, lo que permite detectar, evaluar y mitigar los riesgos, incluidos aquellos que afectan a la nube y a entornos pertenecientes a proveedores o a empresas fusionadas o adquiridas. Además, ASM permite priorizar los riesgos y facilita que los equipos se concentren en los más relevantes.

¿Por qué los responsables de la defensa necesitan inventariar los activos?

Existe otra razón por la cual resulta importante contar con un inventario de activos completo y actualizado: los atacantes no dejan de buscar formas de acceder a los entornos, y

actúan con rapidez. Son capaces de analizar toda la red internet en busca de sistemas vulnerables en menos de una hora.

Además, saben aprovechar los anuncios de vulnerabilidades y exposiciones comunes (CVE, por sus siglas en inglés). Apenas se publica un anuncio de este tipo, suelen tardar entre 15 y 60 minutos, o incluso menos, en comenzar la búsqueda de la vulnerabilidad. El 2 de marzo de 2021, Microsoft anunció vulnerabilidades en Microsoft Exchange Server y Outlook Web Access (OWA). Muchos actores de amenazas comenzaron a realizar análisis para detectarlas en menos de cinco minutos.a

Propuestas prácticas complementarias no obligatorias

LABORATORIO GUIADO | ACTIVIDAD PRÁCTICA

A modo de práctica libre, se propone un laboratorio utilizando una máquina virtual Linux (por ejemplo, Ubuntu) con Nmap instalado. El

objetivo es realizar un inventario básico de una red local de pruebas. En el siguiente listado se describen los pasos a seguir:

1. Configurar red local de laboratorio. Montar dos máquinas virtuales (una servidora y otra atacante) en VirtualBox, utilizando el adaptador de red «Solo anfitrión» u «Host-only». Asignar direcciones IP estáticas (por ejemplo, 192.168.56.101 y 192.168.56.102).
2. Instalar Nmap. En la máquina atacante (Linux), ejecutar el comando `sudo apt update && sudo apt install nmap`.
3. Descubrir *hosts*. Ejecutar el siguiente comando para identificar *hosts* activos:
   `nmap -sn 192.168.56.100/30`. Deberían aparecer ambas direcciones IP.
4. Escanear puertos. Desde la máquina atacante, correr los siguientes comandos:

   - `nmap -sS 192.168.56.101` (controlador)
   - `nmap -sS 192.168.56.102` (servidor Linux)

Observar los puertos abiertos que se muestran.

5. Detectar sistema operativo. Probar con los siguientes comandos:

- `sudo nmap -O 192.168.56.101`
- `sudo nmap -O 192.168.56.102`

Comparar los resultados con los sistemas conocidos (uno corresponde a Windows y el otro a Linux).

6. Guardar salida en fichero. Ejecutar `nmap -sS -O -oX reporte.xml 192.168.56.101-102` y verificar el contenido del archivo «reporte.xml».
7. Interpretar resultados. Explorar el archivo utilizando un navegador o con el comando `grep` en Linux para extraer información, por ejemplo, `grep "<portid>22"`. Esto permite comprobar si aparece el puerto 22.

Este laboratorio muestra cómo Nmap permite mapear una red pequeña. Es gratuito (solo se requiere Nmap, disponible en los repositorios de Linux) y resulta aplicable a cualquier pyme que disponga de un servidor de pruebas o una red local cerrada.

Como actividad libre de aplicación, se propone realizar un inventario simple utilizando Nmap y una hoja de cálculo en Excel o LibreOffice.

Objetivo: utilizar Nmap para descubrir los dispositivos activos en una red de ejemplo (puede ser una red doméstica o de laboratorio) y documentarlos en una hoja de cálculo.

Instrucciones

A continuación, se describen los pasos para llevar a cabo la actividad:

1. Configurar Nmap en caso de no estar instalado (Linux o Windows).
2. Identificar el segmento de red local mediante el comando correspondiente:

- En Windows, `ipconfig`
- En Linux, `ifconfig`

3. Ejecutar `nmap -sn <red>` para listar los *hosts* activos. Anotar estas direcciones IP en una tabla.
4. Para cada IP, hacer un escaneo rápido con `nmap -sS -sV <IP>`. Registrar los puertos abiertos y los servicios detectados. En la tabla se pueden incluir las siguientes columnas: «IP», «Dispositivo (si se conoce)», «Puertos abiertos» y «Servicios».

5. Opcionalmente, probar la detección de sistema operativo con `-O` y completar la columna «SO aproximado».
6. Clasificar cada activo en una categoría (por ejemplo, PC, *router*, móvil, impresora) y anotarlo en la tabla.

Resultado: una planilla con una fila por cada dispositivo detectado, que sirva como inventario inicial de la red.

Esta actividad demuestra que, con Nmap y una hoja de cálculo, es posible generar un inventario básico de la red mediante escaneo y registro. Además, permite familiarizar al equipo con el uso de estas herramientas libres.

CONTINUAR

Referencias

Cybersecurity and Infrastructure Security Agency [CISA]. (2025). *Foundations for OT cybersecurity: Asset inventory guidance for owners and operators*. https://www.cisa.gov/resources-tools/resources/foundations-ot-cybersecurity-asset-inventory-guidance-owners-and-operators

Ibidem Translations. (2022). *Tutorial de Nmap, la mejor herramienta de escaneo de todos los tiempos*. https://www.ibidem-translations.com/edu/traduccion-nmap-escaneo-red/

INCIBE. (2016). *Inventario de activos y gestión de la seguridad en SCI*. https://www.incibe.es/incibe-cert/blog/inventario-activos-y-gestion-seguridad-sci

INCIBE. (2025). *Explorando el módulo de scripts de Nmap*. INCIBE-CERT. https://www.incibe.es/incibe-

cert/blog/explorando-el-modulo-de-scripts-de-nmap

Graglia, I. (2023). *Etiquetado de activos IT: Cómo taguear el software y el hardware*. InvGate Blog. https://blog.invgate.com/es/etiquetado-de-activos-it

Nettix. (s.f.). *Guía completa de OCS Inventory y GLPI*. https://www.nettix.com.pe/documentacion/soporte-documentacion/guia-completa-de-ocs-inventory-y-glpi

Nmap. (s.f.). *Nmap Output*. https://nmap.org/book/man-output.html

Marker, A. (2025). *Plantillas gratuitas de inventario de Excel*. Smartsheet. https://www.smartsheet.com/es/plantillas-gratuitas-de-inventario-de-excel

Revista Ciberseguridad. (2022). *Los muchos peligros del protocolo de escritorio remoto*. https://www.revistaciberseguridad.com/2022/06/los-muchos-peligros-del-protocolo-de-escritorio-remoto/

Palo Alto Networks. (s.f.). *¿Qué es un inventario de activos de TI?* https://www.paloaltonetworks.es/cyberpedia/what-is-it-asset-inventory

Toro, G. (Comp.). (2008). *Guía de referencia de Nmap*. http://we.riseup.net/assets/77169/Manual-de-uso-de-Nmap.pdf

CONTINUAR

Lección 5 de 5

Descarga en PDF

PDF

Módulo 3. Inventario y descubrimiento.pdf

2.9 MB