Módulo 1. Diseño de redes y segmentación

En este módulo se aborda el diseño seguro de redes y la segmentación de los sistemas de comunicación. Se hace hincapié en la estructuración de topologías y dominios de confianza que permitan aislar segmentos de red, mediante la aplicación de principios de seguridad como *zero trust* y prácticas de *hardening*. El objetivo es conformar redes resilientes, en las que cada segmento cuente únicamente con los accesos necesarios, lo que reduce al mínimo la exposición interna.

Unidad 1. Arquitectura segura

1.1 Topologías, subredes, VLAN y listas de control de acceso (ACL)

Una red está compuesta por una colección de nodos y enlaces que interconectan los nodos y permiten la comunicación entre ellos. Los nodos pueden incluir dispositivos como computadoras, teléfonos móviles, servidores, enrutadores y conmutadores.

La topología de red es la forma en que los nodos y enlaces conforman la red. Se visualiza, por lo general, mediante un gráfico que muestra cómo los enlaces establecen las conexiones entre los nodos. Esta topología describe la disposición física y lógica de los nodos y las conexiones dentro de una red. Las configuraciones topológicas determinan cómo están interconectados los dispositivos, cómo viajan los datos a través de la red y qué nivel de resiliencia presenta frente a fallos o ataques.

La topología de red puede entenderse como un **mapa físico o lógico que representa las interconexiones entre nodos.** Elegir la topología adecuada no solo permite optimizar la transmisión de datos, sino que influye de forma directa en la postura de ciberseguridad, la eficiencia operativa y la capacidad de respuesta ante incidentes de seguridad.

Las topologías de red están compuestas por diversos componentes que definen su funcionamiento. A continuación, se describen los principales tipos de nodos:

1. **Nodos**

En una red de datos, los nodos son puntos de conexión que envían, reciben o reenvían información. Se trata de dispositivos que generan, consumen o interactúan con los datos en la red. Se dividen, principalmente, en nodos finales y nodos intermedios.

- **Nodos finales (endpoints)**

Son dispositivos donde comienza o finaliza la comunicación. Algunos ejemplos son computadoras personales, teléfonos móviles, impresoras, servidores y dispositivos del *Internet of Things* (IoT). Estos nodos participan activamente en la red, ya que generan, reciben, transmiten o almacenan datos. En términos de uso, son los principales consumidores de los recursos de la red.

La seguridad de *endpoints* es una parte fundamental de la ciberseguridad, centrada en proteger estos dispositivos frente a posibles ataques. Resulta especialmente relevante en entornos corporativos, ya que estos equipos suelen ser gestionados por usuarios con conocimientos limitados en prácticas de seguridad digital. Además, suelen contener información sensible, como credenciales de acceso, datos de clientes o medios de pago corporativos, lo que los convierte en objetivos atractivos para actores maliciosos.

Con la generalización del trabajo remoto y el uso de servicios en la nube, los *endpoints* se encuentran cada vez más fuera del entorno de TI tradicional. Están distribuidos en hogares, espacios de coworking y otros entornos no controlados, lo que incrementa el riesgo de exposición. Esta situación favorece la mezcla entre usos personales y laborales en un mismo equipo, y dificulta que los equipos de TI puedan actuar de forma directa frente a incidentes. Contar con sistemas de protección específicos para *endpoints* permite detectar y responder automáticamente ante amenazas, lo que evita una carga constante sobre el personal y mejora la eficiencia organizacional.

- **Nodos intermedios**

Son los dispositivos que permiten que los datos viajen de un nodo final a otro, dirigiendo el tráfico de manera eficiente dentro de la red. No generan datos, sino que se encargan de reenviarlos, distribuyendo el flujo de información entre los distintos dispositivos. Entre los más comunes se encuentran los enrutadores (*routers*), que conectan redes diferentes y dirigen el tráfico entre ellas; los conmutadores (*switches)*, que organizan el tráfico dentro de una red local (LAN); y los concentradores o repetidores (*hubs* y *repeaters*), que retransmiten o amplifican señales sin aplicar inteligencia en la distribución.

Estos nodos cumplen una función clave en cualquier topología, ya que suelen incorporar herramientas de control como reglas de *firewall*, mecanismos de detección de intrusiones, segmentación mediante VLAN y monitoreo del tráfico. Por esta razón, requieren medidas de protección específicas, que incluyan controles de acceso, herramientas de seguridad para *endpoints* y la aplicación regular de actualizaciones, con el fin de minimizar su exposición frente a posibles amenazas.

2 Enlaces

Los enlaces son los medios de transmisión a través de los cuales se transportan los datos entre los nodos de una red. Pueden clasificarse en guiados —también llamados cableados—, como los cables UTP o las fibras ópticas que se utilizan en redes Ethernet; y no guiados —o inalámbricos—, como las señales electromagnéticas empleadas en redes *wifi*. La calidad, la velocidad y el tipo de enlace inciden directamente en la rapidez con que se transmite la información, así como en la capacidad de la red para resistir interrupciones o fallos.

3 Tarjetas de interfaz de red (NIC)

Las tarjetas de interfaz de red (NIC) son componentes de hardware instalados en los nodos, que permiten establecer la conexión con la red. Estas tarjetas gestionan el acceso

del dispositivo al medio de transmisión, controlan la emisión y recepción de datos y garantizan que la comunicación se realice conforme al protocolo correspondiente. Cada NIC posee una dirección MAC única, lo que permite su uso en procesos de autenticación, control de acceso y análisis forense en investigaciones de ciberseguridad.

Topología física vs. topología lógica

En el diseño de redes, se distinguen dos tipos de topologías: la física y la lógica.

La **topología física** se refiere a la disposición tangible de los componentes de la red, como cables, *switches* y *routers*. Representa la estructura real, visible y medible, de cómo están interconectados los dispositivos. Incluye la ubicación de los nodos, el tipo de medio de transmisión y las conexiones físicas entre los equipos. Por ejemplo, en una topología en estrella, todos los nodos se conectan a un nodo central mediante cables individuales.

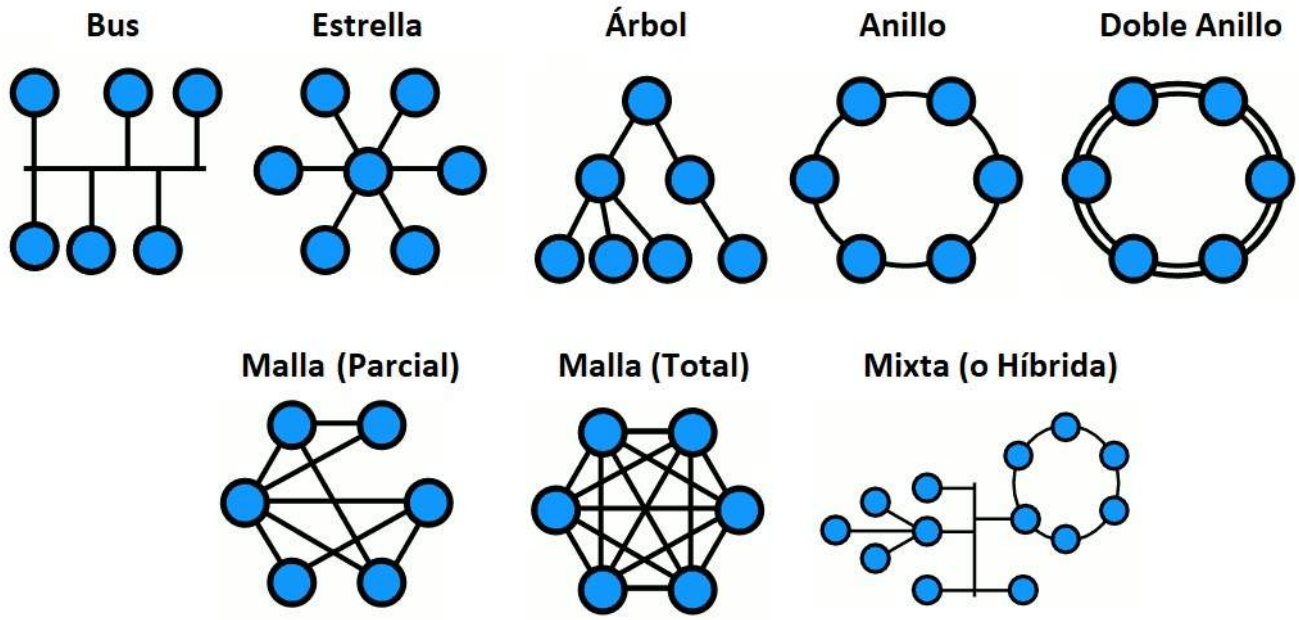
Por su parte, la **topología lógica** describe el flujo de los datos dentro de la red, sin considerar su diseño físico. Determina cómo se comunican los dispositivos, qué caminos siguen los paquetes de información y cómo se gestiona el tráfico entre los nodos. En este caso, los dispositivos se representan como nodos funcionales, y las conexiones se definen según las rutas que siguen los datos, más allá de cómo están conectados físicamente.

Por ejemplo, una red puede tener una topología física en estrella, pero operar lógicamente como una topología en bus si las comunicaciones se manejan a través de un único canal compartido. Es decir, aunque físicamente los nodos estén conectados a un punto central, desde el punto de vista lógico los datos pueden circular como si lo hicieran por un bus común.

Además de describir la estructura física o el flujo lógico de los datos, cada tipo de topología influye directamente en el rendimiento de la red, su tolerancia a fallos y su comportamiento ante interrupciones. Por esta razón, tanto las disposiciones físicas como las lógicas deben considerarse al planificar la ciberseguridad, ya que pueden presentarse vulnerabilidades en cualquiera de los niveles.

En la siguiente figura se observan ejemplos de topologías de red comunes: *bus*, estrella, árbol, anillo, doble anillo, malla parcial (o parcialmente mallada), malla total (o totalmente mallada) e híbrida (o mixta). La topología de red define la disposición de los nodos y los enlaces. Esta clasificación es abstracta y puede aplicarse tanto al análisis de la topología física como al de la lógica, ya que una misma red puede adoptar una forma distinta según el enfoque desde el que se la examine.

Figura 1. Ejemplos de topologías de red físicas y lógicas



Fuente: [imagen sin título sobre topologías de red], (s.f.), https://goo.su/i9hjO

A continuación, se describen algunas topologías de red comunes, con sus características principales y consideraciones desde el punto de vista de la seguridad y la eficiencia.

Bus —

En una topología en bus, todos los nodos están conectados a una única línea de comunicación —generalmente denominada backbone— que actúa como canal compartido. Cada nodo funciona como una parada en esa ruta común. Aunque es una configuración económica y sencilla de implementar, presenta una escalabilidad limitada y una alta vulnerabilidad ante fallos: una interrupción en el cable puede afectar a toda la red. Es una estructura sensible a puntos únicos de falla, ya que cualquier corte en el enlace puede dejar la red fuera de servicio.

Estrella —

En esta configuración, cada nodo está conectado directamente a un concentrador o conmutador central (switch). Es una de las topologías más utilizadas por su simplicidad y facilidad de administración. La segmentación facilita la detección de fallos, ya que una caída en un nodo individual no afecta al resto de la red. Sin embargo, el nodo central representa un punto crítico de falla: si se ve comprometido o deja de funcionar, la red completa puede quedar inoperativa.

Árbol —

También llamada topología jerárquica, esta estructura puede entenderse como una combinación de redes en estrella organizadas en distintos niveles. A diferencia de la estrella, no cuenta con un único concentrador central, sino que tiene un nodo troncal —habitualmente un hub o switch— del cual se ramifican los demás nodos. Desde una perspectiva estructural, se asemeja a un árbol, lo que permite organizar la red en niveles y facilita la segmentación lógica.

Anillo —

En esta topología, cada nodo está conectado a otros dos, formando un bucle cerrado por el que circulan los datos en una única dirección. Esta estructura ofrece un flujo de información predecible, pero también introduce latencia y es vulnerable a interrupciones: si un enlace falla, se corta el circuito. Para reducir este riesgo, pueden emplearse variantes como el doble anillo, que proporciona un canal redundante para mejorar la tolerancia a fallos.

Malla —

Una topología en malla completa conecta cada nodo con múltiples otros nodos, creando una red altamente redundante. Esta interconexión mejora la tolerancia a fallos y garantiza rutas alternativas en caso de interrupción, aunque su implementación resulta costosa y compleja. Las topologías en malla parcial buscan un equilibrio entre redundancia y eficiencia, reduciendo los enlaces sin eliminar por completo la capacidad de recuperación.

Híbrida —

Las topologías híbridas combinan elementos de distintas configuraciones para adaptarse a necesidades específicas. Por ejemplo, una red puede utilizar una estructura en estrella dentro de cada departamento y conectarlas mediante una configuración en bus.

> Este tipo de diseño requiere una planificación cuidadosa, ya que cada subtopología introduce riesgos y características propias que deben contemplarse en las estrategias de ciberseguridad.

Además, pueden considerarse otras formas de conexión, como las punto a punto y las denominadas *daisy chain* —también conocidas como cadena margarita o en cascada—. Si bien estrictamente no constituyen topologías de red por sí mismas, las conexiones punto a punto suelen utilizarse como topología lógica superpuesta a una estructura física diferente. Por su parte, las conexiones en cascada suelen encontrarse en topologías físicas híbridas, o bien en la topología lógica de sistemas basados en *blockchain*.

Conexiones punto a punto

Las redes punto a punto se basan en una arquitectura en la que cada canal de datos conecta únicamente a dos computadoras. Estas conexiones permiten una comunicación directa y recíproca entre los dispositivos. Según la relación que se establece entre los nodos, pueden distinguirse dos tipos principales:

- **Redes punto a punto (no jerárquicas)**

  En este tipo de red, los dispositivos actúan como pares, sin jerarquías entre ellos. Cada uno puede asumir alternativamente el rol de emisor o receptor. Por ejemplo, en un momento determinado, el dispositivo A puede solicitar datos al dispositivo B, que responde enviando la información requerida. En ese caso, A actúa como receptor y B como emisor. Posteriormente, los roles pueden invertirse, manteniéndose una relación simétrica entre ambos. Esta estructura permite una comunicación directa y flexible, en la que no

existe una entidad central que controle o administre los intercambios.

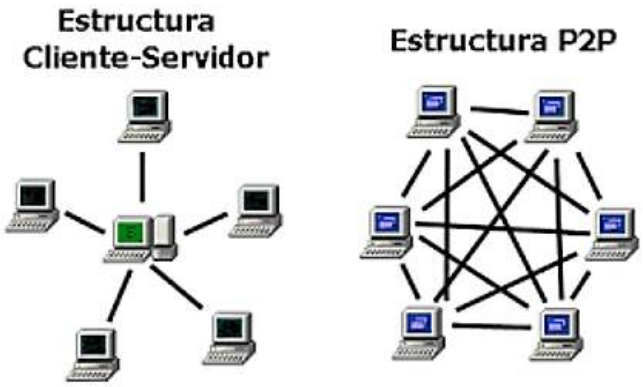
Figura 2. Red punto a punto entre dos routers

Fuente: [imagen sin título sobre red punto a punto], (s.f.), https://goo.su/EupOwDQ

- **Redes cliente-servidor (redes jerárquicas)**

  En contraste con el modelo anterior, las redes cliente-servidor se organizan de manera jerárquica. En este esquema, uno o más dispositivos actúan como clientes que solicitan servicios, mientras que un servidor centralizado responde a estas peticiones y administra recursos como archivos, aplicaciones y medidas de seguridad. Es el modelo predominante en Internet: por ejemplo, cuando se accede a una página web, el navegador del usuario (cliente) realiza una solicitud que el servidor procesa y responde con los datos solicitados. Este enfoque facilita la administración centralizada y puede ofrecer mayor control sobre la seguridad, aunque introduce una dependencia directa del servidor para el funcionamiento general de la red.

Figura 3. Red cliente-servidor vs. red punto a punto (P2P)



Fuente: [imagen sin título sobre red cliente servidor y red punto a punto], (s.f.), https://goo.su/9pVxQGm

- **Conexión daisy chain, cadena margarita o en cascada**

  Este tipo de conexión consiste en una sucesión lineal de enlaces, en la que un dispositivo A se conecta a un dispositivo B, B a un dispositivo C, C a un dispositivo D, y así sucesivamente. A diferencia de una red propiamente dicha, en esta configuración los dispositivos no están todos interconectados: por ejemplo, el dispositivo C no puede comunicarse directamente con el dispositivo A. Además, no existe un retorno desde el último dispositivo al primero, por lo que no se forma un lazo cerrado. La cadena margarita puede utilizarse para la transmisión de diferentes tipos de señales: alimentación eléctrica, señales analógicas, datos digitales o combinaciones de estos. Su aplicación depende del contexto y del tipo de sistemas involucrados.

Cada topología presenta características particulares en términos de rendimiento, tolerancia a fallos y facilidad de expansión. Por ejemplo, la topología en estrella —en la que todos los nodos se conectan a un nodo central— facilita el aislamiento de fallos, ya que una interrupción en un cable afecta únicamente al nodo correspondiente. Sin embargo, esta estructura depende críticamente del nodo central, que constituye un punto único de falla. Por otro lado, una topología en malla completa ofrece múltiples rutas redundantes, lo que mejora la tolerancia a fallos, aunque incrementa la complejidad y el costo de implementación.

En términos generales, la elección de la topología influye de forma directa en la capacidad de segmentar la red y en su resistencia frente a ataques o interrupciones.

A partir de una topología determinada, es posible redefinir la estructura lógica de la red mediante segmentación. Esta permite la creación de subredes lógicas que mejoran el control del tráfico y la seguridad. Con la incorporación de VLAN, además, se reorganizan los dominios de *broadcast*, lo que contribuye a una gestión más eficiente y segura de la red.

Subredes

Una subred es una porción lógicamente definida dentro de una red IP. Consiste en la división de una red mayor en segmentos más pequeños, cada uno con su propio rango de direcciones único. Por ejemplo, al dividir un bloque /16 en varias subredes /24, se logra aislar el tráfico interno y aplicar políticas específicas para cada segmento. Esta organización permite encaminar el tráfico de manera más eficiente dentro de una red local (LAN).

Segmentar una red en subredes más pequeñas ofrece múltiples ventajas. En primer lugar, optimiza el uso de direcciones IP, asignando rangos apropiados según las necesidades de cada sector. En segundo lugar, mejora el rendimiento general al reducir el dominio de *broadcast*, lo que disminuye la congestión de tráfico. Además, al aislar dispositivos o áreas críticas en subredes independientes, se refuerza la seguridad, ya que se limita la propagación de posibles ataques.

Esta segmentación también facilita la administración y el diagnóstico de problemas: las incidencias pueden localizarse y contenerse en una subred específica, lo que agiliza la solución de fallos.

En conjunto, el uso de subredes constituye una práctica fundamental en el diseño de redes IP, tanto para mejorar el rendimiento como para fortalecer la seguridad de la infraestructura.

VLAN (redes virtuales locales)

Las VLAN (*virtual* LAN) son redes lógicas independientes que operan sobre una misma infraestructura física. Permiten agrupar hosts como si se encontraran en el mismo segmento LAN, aunque estén conectados a *switches* distintos o se encuentren físicamente dispersos. Se configuran a nivel de *switch*, agrupando puertos o interfaces en dominios de *broadcast* separados, independientemente del cableado físico subyacente.

Configurar VLAN ofrece ventajas importantes:

- Este aislamiento lógico impide que dispositivos en VLAN diferentes intercambien tráfico de capa 2 de forma automática, incluso si están conectados al mismo *switch*. Por defecto, no se permite el flujo de tráfico entre VLAN a menos que se configure un enrutamiento inter-VLAN a través de un *router* o un dispositivo de capa 3.

- Las VLAN reducen los dominios de *broadcast* y permiten separar lógicamente distintos departamentos o funciones. Por ejemplo, pueden asignarse VLAN diferentes para Finanzas, Recursos Humanos, usuarios de oficina, impresoras o la red *wifi* de invitados.

- Esta separación disminuye la visibilidad entre segmentos de red: los equipos en distintas VLAN no pueden comunicarse entre sí, salvo que se establezca una política explícita que lo permita. Esto resulta útil para definir dominios de confianza diferenciados y limitar los movimientos laterales en caso de un ataque. Por ejemplo, puede ubicarse la red de usuarios internos, la red de invitados y la DMZ en VLAN independientes, actuando cada una como una «red separada» a nivel de tráfico local.

- Desde el punto de vista de la seguridad, cada VLAN puede tener reglas y accesos específicos. Es posible, por ejemplo, separar una VLAN de servidores críticos de la VLAN de usuarios comunes. El tráfico entre VLAN puede habilitarse o bloquearse mediante un *router* multicapa o *switches* de capa 3, de modo que cada VLAN funcione prácticamente como una subred aislada.

Listas de control de acceso (ACL)

Una lista de control de acceso (ACL) es un conjunto de reglas que se aplican en *routers*, *switches* de capa 3 o *firewalls*, con el fin de definir qué paquetes pueden ingresar o salir de un segmento de red según criterios establecidos. Estos criterios pueden basarse en direcciones IP de origen o destino, puertos o protocolos específicos. Las ACL

complementan la segmentación, ya que permiten aplicar un control fino sobre el tráfico que circula entre subredes o VLAN.

El funcionamiento típico de una ACL se basa en el principio de «denegar por defecto» (*deny by default*), lo que significa que solo se autoriza el tráfico expresamente permitido, mientras que todo lo demás es bloqueado. Por ejemplo, puede configurarse una ACL para permitir el acceso a un servidor únicamente desde ciertas subredes, impidiendo todas las demás conexiones. Este enfoque constituye uno de los mecanismos fundamentales para limitar el alcance de cada segmento y reducir la superficie de exposición.

En el perímetro entre la red interna y externa, una ACL configurada en un *router* puede establecer qué conexiones entrantes están autorizadas. Así, es posible permitir únicamente los puertos necesarios —como HTTP o SSH— y bloquear el resto, aplicando políticas de acceso estrictas en cada frontera de red. Del mismo modo, un *router* que conecta dos VLAN puede aplicar reglas de «permitir» o «denegar» para controlar la comunicación inter-VLAN, según lo requiera la política de seguridad definida.

En conjunto, la combinación de una topología de red bien planificada, subredes, VLAN y ACL permite aislar servicios críticos y contener posibles amenazas dentro de segmentos específicos, mejorando la seguridad general de la infraestructura.

Actualmente, se prefiere un diseño jerárquico de tres capas —acceso, distribución y núcleo—, en el que las VLAN y las políticas de filtrado se implementan en las capas inferiores. Esta estrategia favorece tanto la seguridad como la escalabilidad de la red.

1.2. Segmentación por dominio de confianza

La segmentación por dominios de confianza consiste en dividir la red en zonas con distintos niveles de confianza, estableciendo accesos controlados según el grado de riesgo o privilegio asignado a sus usuarios, dispositivos o sistemas.

Un diseño seguro define claramente los límites del perímetro de la red, diferenciando zonas como la LAN interna y la DMZ, y aplicando políticas de tráfico específicas entre ellas. Cada zona —o *trust zone*— cuenta con políticas de seguridad particulares que responden a su nivel de exposición y criticidad.

A continuación, se describen algunos ejemplos comunes de dominios de confianza:

- **Red interna (red de alta confianza).** Aloja activos críticos como equipos corporativos, servidores con datos sensibles y dominios internos. El acceso debe limitarse únicamente a empleados autorizados. El tráfico hacia y desde la DMZ o Internet se restringe mediante reglas estrictas, implementadas con ACL o cortafuegos. Por ejemplo, puede permitirse solo la salida de correo electrónico o el uso de VPN corporativa.

- **DMZ (zona desmilitarizada, red de confianza media):** es una subred intermedia, aislada entre la red interna y el exterior. Alberga servicios accesibles desde Internet, como servidores web, correo, DNS público o VPN. Se parte del supuesto de que los servidores en la DMZ pueden ser comprometidos; por tanto, su diseño se enfoca en contener posibles brechas y evitar que se propaguen a la red interna. Los sistemas en esta zona no deben comunicarse directamente con la LAN, y comúnmente se utilizan dos cortafuegos —uno entre Internet y la DMZ, y otro entre la DMZ y la red interna— para reforzar la separación.

- **Otras zonas (confianza media o baja)**: es posible crear VLAN específicas para invitados,

dispositivos IoT o proveedores externos, con reglas de acceso diferenciadas según el nivel de exposición. **Otras zonas (confianza media o baja)**: es posible crear VLAN específicas para invitados, dispositivos IoT o proveedores externos, con reglas de acceso diferenciadas según el nivel de exposición. A continuación, se detallan algunos casos frecuentes:

- **Red de invitados (red de baja confianza)**. VLAN con acceso limitado a Internet y sin comunicación con la red interna. Un ejemplo típico es la red *wifi* para visitantes, aislada de los recursos corporativos.
- **Segmentos especializados**. En entornos industriales o redes con dispositivos IoT, se recomienda aislar sistemas como SCADA, cámaras de videovigilancia o sensores en redes separadas, con políticas de acceso altamente restrictivas.

Este enfoque basado en zonas de confianza facilita la aplicación de la política de «mínimos privilegios», ya que cada segmento solo puede comunicarse con otros de acuerdo con reglas previamente definidas. Aislar dominios de confianza reduce el riesgo de propagación interna: si un atacante compromete un segmento, su alcance queda limitado y no puede acceder directamente a otras zonas. Un ejemplo clásico es la DMZ, que funciona como un amortiguador entre la red interna confiable y la red externa no confiable (Internet).

Cada zona se conecta con las demás exclusivamente a través de puntos de control que aplican políticas restrictivas. En la práctica, esta segmentación se implementa mediante cortafuegos y listas de control de acceso (ACL) situados entre zonas. Al segmentar según niveles de confianza, se definen reglas más estrictas en las fronteras de cada

dominio, permitiendo solo el tráfico necesario —por ejemplo, solicitudes HTTP hacia un servidor web— y bloqueando todo lo demás por defecto.

Esta estrategia contribuye a contener posibles brechas de seguridad: si un atacante accede a un segmento determinado, quedará confinado en esa zona y no podrá desplazarse lateralmente hacia otros sectores de la red interna.

En suma, la segmentación por niveles de confianza crea barreras internas de seguridad que complementan la defensa perimetral, logrando un aislamiento eficaz frente a fallos e intrusiones. De este modo, un error o una brecha en una zona de bajo riesgo puede ser contenido sin propagarse al resto de la red, lo que dificulta el acceso no autorizado a los activos más críticos.

Cada segmento opera casi como una red independiente, lo que reduce la superficie expuesta a posibles ataques. El tráfico entre zonas siempre debe pasar por dispositivos con controles de seguridad reforzados —como cortafuegos o *routers* con ACL—, en los que se aplican políticas de *deny by default* en cada frontera.

1.3 *Zero trust*: principios prácticos

El modelo de seguridad *zero trust* —también conocido como modelo de confianza cero — parte del principio de que ninguna entidad es confiable por defecto, ni siquiera dentro del perímetro de la red. En este enfoque, se asume que cualquier usuario, dispositivo o segmento —ya sea interno o externo— puede estar comprometido, por lo que nunca debe otorgarse acceso sin verificación previa. El principio fundamental es claro: «nunca confiar, siempre verificar».

Bajo este paradigma, todo intento de acceso debe someterse a una verificación continua. No existe confianza implícita basada en la ubicación de red o en el historial de conexiones. Cada solicitud se evalúa dinámicamente según múltiples factores, entre ellos la identidad del usuario o dispositivo, su nivel de seguridad, la ubicación y el contexto de la solicitud.

En la práctica, el modelo *zero trust* se basa en una serie de principios fundamentales que orientan su implementación. Entre los más relevantes, se destacan los siguientes:

- **Verificación explícita y continua.** Cada intento de acceso, ya sea de un usuario o de un dispositivo, debe autenticarse y autorizarse dinámicamente en tiempo real, sin importar desde dónde se origine la conexión. Se utilizan datos contextuales —como identidad, tipo de dispositivo, ubicación y nivel de riesgo— para tomar decisiones de acceso. No se asume que estar dentro de la red interna sea garantía de seguridad. En cambio, se adopta la mentalidad de «asumir la brecha», diseñando la seguridad bajo el supuesto de que un atacante ya se encuentra dentro del entorno.

- **Control de identidad y privilegios mínimos:** el modelo se centra en la identidad. A cada usuario o dispositivo se le asignan únicamente los permisos estrictamente necesarios para cumplir su función, y estos se limitan en alcance, duración y recursos. El acceso se concede solo tras verificar cada solicitud de forma individual. De este modo, incluso un actor legítimo dentro de la red no puede desplazarse libremente. Por ejemplo, un empleado debe autenticarse mediante mecanismos como la autenticación multifactor (MFA) incluso para acceder a un servidor interno.

- **Suponer violación:** el modelo parte del supuesto de que la red puede estar comprometida en cualquier momento. Por ello, se requiere monitoreo continuo de la

actividad, registro detallado de eventos y análisis constante en busca de comportamientos anómalos, como los movimientos laterales típicos de un atacante que ya logró ingresar.

- **Microsegmentación como mecanismo:** la red se divide en segmentos mucho más reducidos, incluso con respecto a la aplicación o el flujo de trabajo, lo que permite aplicar políticas de acceso granulares y contener cualquier incidente en un ámbito muy limitado. Esta estrategia no reemplaza las defensas perimetrales tradicionales, sino que las complementa. Tecnologías como la microsegmentación permiten establecer controles basados en identidad en cada recurso crítico, evitando confiar en bloques amplios como una VLAN completa. En este modelo, el perímetro deja de ser una frontera fija para transformarse en una burbuja dinámica que acompaña a cada usuario, dispositivo o dato.

- **Protección de datos:** todos los datos sensibles deben permanecer protegidos, tanto en tránsito como en reposo. El cifrado es obligatorio para impedir la interceptación o manipulación, y forma parte integral del diseño del modelo.

- **Monitoreo continuo y auditoría:** se registra y analiza todo el tráfico y los eventos de seguridad en tiempo real. Se supervisa permanentemente el estado de los dispositivos y servicios, con el objetivo de detectar cualquier anomalía. Dado que se

> asume que una vulneración puede ocurrir en cualquier momento, el sistema debe estar preparado para reaccionar automáticamente ante cualquier señal de comportamiento sospechoso. El control de acceso se reevalúa de forma constante en función del contexto

Estos principios se apoyan en tecnologías como la autenticación multifactor (MFA), la gestión de identidades y accesos (IAM), los cortafuegos internos y el análisis de comportamiento. En la práctica, *zero trust* transforma la red en un entorno «perimetrizado por segmentos», en el que cada paso dentro del flujo de comunicación requiere verificación y evidencia de seguridad. La filosofía central puede resumirse en una frase: «nunca confiar, siempre verificar». Esta perspectiva reduce de manera significativa la superficie de ataque y permite contener las amenazas de forma rápida y eficaz.

El modelo *zero trust* busca un equilibrio entre seguridad y productividad. Su objetivo es permitir que los usuarios desempeñen sus tareas sin barreras innecesarias, pero con controles rigurosos que impidan accesos no autorizados o usos indebidos de los recursos corporativos. Para lograrlo, se requiere la implementación de mecanismos como la autenticación multifactor, políticas de acceso basadas en el contexto —incluyendo dispositivo, ubicación o comportamiento— y un diseño de red segmentado, con controles de seguridad aplicados en cada frontera.

1.4. Modelos de referencia y dependencias

Para planificar arquitecturas de red seguras, se recurre a modelos de referencia que permiten comprender cómo fluye la información a través de las distintas capas de comunicación. Los más relevantes son el modelo OSI de siete capas y el modelo TCP/IP. Ambos estructuran la comunicación en capas —como física, de enlace, red, transporte, entre otras— y definen protocolos y estándares en cada nivel. Estos modelos fueron desarrollados precisamente para organizar y estandarizar los procesos de comunicación en red.

Gracias a esta organización, los profesionales pueden analizar cómo los dispositivos, enlaces y servicios de cada capa se relacionan y dependen entre sí. Por ejemplo, una regla de seguridad definida en la capa de red —como el enrutamiento IP— depende de que la capa de enlace de datos sea capaz de transportar correctamente los paquetes.

En particular, el modelo OSI clasifica y estandariza las funciones de hardware y software en siete niveles: física, enlace de datos, red, transporte, sesión, presentación y aplicación. Esta estructura facilita la visualización del flujo de datos desde la capa de aplicación hasta el medio físico, y permite identificar claramente las dependencias entre niveles. Cada capa solo interactúa directamente con la inmediatamente superior e inferior, lo que contribuye a aislar posibles fallos o ataques: una vulnerabilidad en una capa —por ejemplo, en la de aplicación— puede contenerse si las capas inferiores están correctamente configuradas.

Este enfoque en capas también permite abstraer funciones: las capas superiores se apoyan en las inferiores sin necesidad de conocer sus detalles técnicos. Así, un servidor web que opera en la capa de aplicación (capa 7) puede enviar datos sin preocuparse por cómo estos se fragmentan en paquetes IP (capas 3 y 4) o se encapsulan en tramas Ethernet (capa 2).

En el diseño de redes seguras, el enfoque por capas resulta especialmente útil, ya que permite aplicar controles de seguridad en distintos niveles —como cortafuegos, inspección profunda de paquetes o filtrado por identidad—, fortaleciendo así la resistencia general del sistema. Comprender cómo se organizan estas capas es fundamental en arquitecturas avanzadas, ya que cada tecnología o mecanismo de seguridad actúa sobre niveles específicos del modelo.

> Por ejemplo, las VLAN operan en la capa 2 (enlace de datos), el enrutamiento IP y las listas de control de acceso (ACL) actúan en la capa 3 (red), y los cortafuegos con capacidades de inspección de aplicaciones funcionan en capas superiores. Estas dependencias entre capas permiten determinar qué controles son necesarios y dónde aplicarlos. Así, si se segmenta una red mediante subredes (capa 3), será necesario implementar *routers* o cortafuegos de capas 3 o 4 para regular el tráfico entre ellas.

En definitiva, los modelos de referencia OSI y TCP/IP ofrecen un marco conceptual y un lenguaje común que facilitan tanto el diseño como la implementación de medidas de seguridad en la red.

Otro modelo de referencia útil para el diseño de redes seguras es la arquitectura jerárquica de tres capas, ampliamente utilizada en entornos Cisco. Esta estructura organiza la red en tres niveles funcionales: capa de núcleo (*core*), capa de distribución y capa de acceso.

La capa de núcleo reúne los *routers* y switches centrales de alto rendimiento, responsables de interconectar segmentos geográficos y transportar el tráfico de forma eficiente. La capa de distribución establece los límites de la red lógica y aplica las políticas de control, como las listas de control de acceso (ACL) o el enrutamiento entre VLAN. Finalmente, la capa de acceso conecta los dispositivos finales —como estaciones de trabajo, servidores o impresoras— y se orienta a la conectividad de *endpoints*.

Este modelo favorece la escalabilidad y simplifica la administración de la red. La capa de distribución actúa como punto de control para las políticas de seguridad, mientras que la capa de acceso se centra en la conectividad local de los usuarios.

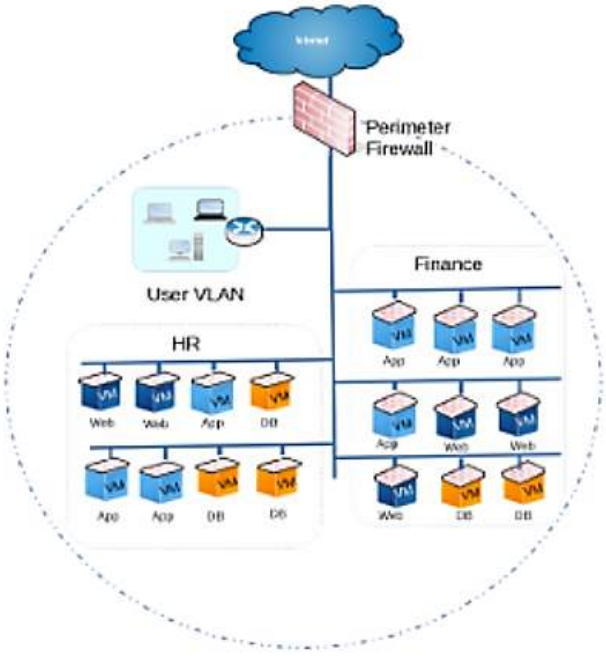
Conocer y aplicar estos modelos de referencia —como OSI, TCP/IP o la arquitectura jerárquica de tres capas— permite planificar adecuadamente las dependencias dentro de la red. Por ejemplo, al incorporar una nueva subred, estos esquemas ayudan a garantizar la interoperabilidad entre capas, documentar rutas de comunicación, establecer mecanismos de redundancia y definir los puntos donde se aplicarán los filtros de tráfico.

CONTINUAR

Unidad 2. Microsegmentación y endurecimiento (hardering)

En la siguiente figura se observa una red dividida en VLAN correspondientes a usuarios, Recursos Humanos y Finanzas, con un cortafuegos perimetral que controla el tráfico hacia Internet. La segmentación representada contribuye a contener posibles ataques, ya que permite aislar cada zona. Como se aprecia, cada segmento funciona casi como una red independiente, lo que refuerza la seguridad general del sistema. Fuente: Nile Secure.

Figura 4. Segmentación de red mediante VLAN y control perimetral



Fuente: Nile, s.f., https://goo.su/H8qnAX

La microsegmentación es una extensión avanzada de la segmentación de red. Su objetivo es aislar segmentos aún más pequeños —incluso a nivel de aplicación o carga de trabajo— dentro de la infraestructura. Cada carga de trabajo puede etiquetarse con políticas de seguridad específicas, de modo que solo pueda comunicarse con los servicios explícitamente permitidos.

Este enfoque permite establecer controles de seguridad altamente granulares. Por ejemplo, puede limitarse el tráfico entre dos máquinas virtuales alojadas en un mismo *host* exclusivamente al protocolo HTTP, y únicamente hacia el servicio requerido. Cuando se combina con el modelo *zero trust*, la microsegmentación permite un nivel de contención muy elevado: en caso de compromiso, el impacto queda confinado a la capa de aplicación afectada, sin posibilidad de propagarse a otros sectores de la red.

2.1 Políticas *deny by default*

La política *deny by default* establece que todo tráfico o acceso no autorizado explícitamente debe ser bloqueado. Es decir, por defecto se deniega todo, y solo se permite aquello que haya sido definido de manera expresa. Este enfoque contrasta con el modelo opuesto de «permitir por defecto», en el que todo lo no prohibido se acepta.

Desde el punto de vista de los cortafuegos, el NIST define esta política como «bloquear todo el tráfico entrante y saliente que no esté expresamente permitido por la política». Esta directriz se aplica a *firewalls*, *routers* y *switches*. En la práctica, los dispositivos de red se configuran con reglas permisivas específicas, seguidas por una regla implícita (o explícita) de denegación general. Esto significa que solo los servicios y flujos definidos como necesarios estarán disponibles, eliminando cualquier vía no autorizada. Las reglas deben formularse con el mayor nivel de restricción posible.

FIREWALL O ROUTER:	SWITCH DE CAPA 3:

se configuran las ACL para denegar todo tráfico por defecto, y luego se habilitan solo los puertos o protocolos requeridos. Por ejemplo, se puede permitir únicamente el acceso al puerto HTTPS de un servidor web, utilizando una regla como *access-list permit tcp any host X eq 443*. Esta regla autoriza tráfico HTTPS hacia el *host* X; todo lo demás se bloquea.

FIREWALL O ROUTER:

SWITCH DE CAPA 3:

además de la segmentación mediante VLAN (capa 2), se utilizan ACL de capa 3 para restringir el enrutamiento entre VLAN. Por ejemplo, puede bloquearse el tráfico entre la VLAN de usuarios y la de administración, salvo las excepciones justificadas.

Este enfoque se alinea con el principio de mínimos privilegios, según el cual todo servicio o aplicación adicional —como SSH, SNMP o NTP— debe permanecer deshabilitado, salvo que exista una justificación clara para su habilitación. Al aplicar la política de deny by default, se reduce de forma significativa la superficie de ataque, ya que un atacante solo podrá establecer comunicación si el flujo correspondiente ha sido permitido de forma explícita.

Este modelo de control —basado en listas blancas de tráfico— es esencial en entornos seguros, ya que garantiza que ningún servicio nuevo ni una configuración errónea puedan habilitar accesos inadvertidos. Una política de denegación por defecto obliga a documentar y validar cada conexión que se permite, lo que fortalece el control sobre la infraestructura.

El beneficio es claro: se minimizan las oportunidades de ataque, ya que todo tráfico desconocido o no autorizado es bloqueado automáticamente. Solo los flujos necesarios —como HTTP hacia servidores web o SSH para el equipo de administración— reciben permiso explícito.

En redes complejas, el enfoque *deny by default* impone la necesidad de revisar cuidadosamente cada servicio habilitado, evitando configuraciones permisivas o poco seguras. Este principio también constituye la base de la microsegmentación: cada segmento de red o servicio expuesto debe estar definido como explícitamente permitido, mientras que todo lo demás permanece bloqueado por defecto. En la práctica, este modelo se implementa mediante ACL, reglas de *firewall* y listas blancas en cada frontera de la red.

2.2. Endurecimiento de *routers / switches*

El *hardening* de dispositivos de red consiste en aplicar medidas de seguridad adicionales que reduzcan al mínimo las vulnerabilidades presentes en *routers* y *switches*. En otras palabras, se refuerza cada equipo con el objetivo de disminuir su superficie de ataque. Entre las prácticas más recomendadas para este fin, se destacan las siguientes:

- **Desactivar servicios innecesarios.** Eliminar funciones no requeridas, como Telnet (en favor de SSH), SNMP v1/v2, servidores HTTP/FTP integrados u otros servicios prescindibles. Esto evita exponer puntos de acceso que no sean estrictamente necesarios.

- **Cambiar credenciales por defecto y usar contraseñas robustas:** modificar las claves de fábrica y aplicar políticas de acceso seguras, incluyendo autenticación basada en roles, contraseñas complejas y renovación periódica.

- **Uso de SNMPv3 o sistemas seguros de monitoreo:** si se necesita administración remota, deben emplearse protocolos seguros como SNMPv3 con cifrado, y restringirse los accesos por dirección IP o interfaz.

- **Aplicar actualizaciones y parches:** mantener actualizado el *firmware* de los dispositivos para corregir vulnerabilidades conocidas. La gestión regular de parches es fundamental para mitigar riesgos.

- **Configurar registro y auditoría:** habilitar el *logging* de eventos relevantes, como accesos, cambios de configuración e intentos fallidos de autenticación. Esto permite detectar conductas sospechosas o accesos no autorizados.

- **Limitar el acceso físico y por consola:** restringir el acceso físico a los equipos (racks, salas de servidores) y proteger las interfaces de consola mediante autenticación y parámetros de inactividad como *timeouts*.

- **Aplicar políticas de ACL internas:** además del control de tráfico externo, es recomendable implementar ACL en *switches* de capa 3 para segmentar la red internamente, limitando la comunicación entre VLAN según las políticas definidas.

- **Deshabilitar protocolos obsoletos:** eliminar protocolos o algoritmos criptográficos inseguros, como DES, MD5 o SNMPv1, que ya no cumplen con los estándares de seguridad actuales.

- **Configuración de SNMP y *logging* remoto:** enviar los registros de eventos a servidores centralizados para su almacenamiento y análisis. Esto evita que se pierdan datos si el dispositivo local se ve comprometido.

El *hardening* de dispositivos de red implica configurar los equipos de forma segura y eliminar vectores de ataque innecesarios. Algunas prácticas generales recomendadas —basadas en las guías de Cisco SAFE— son las siguientes.

Routers

- Desactivar Telnet y utilizar únicamente SSH con cifrado para administración remota. También se debe bloquear el uso de SNMP en versiones inseguras (v1 o v2), empleando SNMPv3 cuando sea necesario, o deshabilitándolo si no se requiere.

- Implementar autenticación centralizada mediante protocolos como TACACS+ o RADIUS (AAA), para controlar el acceso administrativo.

- Deshabilitar servicios y puertos de administración que no sean estrictamente necesarios, como HTTP, HTTPS o CDP. Asimismo, se debe restringir el acceso de gestión remota desde redes no confiables.

- Habilitar el registro de eventos (*logging*) y enviarlos a un servidor *syslog* centralizado. Es importante que estos registros incluyan información de auditoría, como los cambios de configuración realizados.

Switches

- Desactivar la autonegociación de enlaces troncales en puertos de acceso. En su lugar, configurar manualmente los enlaces troncales para evitar que un host no autorizado cree una conexión de este tipo.

- Asegurar la VLAN nativa de los enlaces troncales, asignándole un ID de VLAN que no se utilice en otras partes del *switch*. Esto evita

que tramas no etiquetadas circulen por la red sin ser procesadas por un *router*.

- Asignar todos los puertos inactivos a una VLAN «resguardada» o, preferiblemente, deshabilitarlos completamente. Esta medida impide que un atacante que acceda físicamente a un puerto libre pueda conectarse a la red.

- No utilizar las VLAN como único mecanismo de control de acceso entre subredes sensibles. Dado que no fueron diseñadas como medida de seguridad, es recomendable complementarlas con ACL o cortafuegos.

- En dispositivos que lo permitan, habilitar VLAN privadas (PVLAN) para aislar hosts dentro de una misma VLAN. Esta funcionalidad restringe la comunicación entre puertos aislados, lo que reduce el riesgo de propagación si un equipo es comprometido.

Fortalecer los dispositivos de red implica aplicar buenas prácticas de configuración para reducir al mínimo las vulnerabilidades. Algunas de estas medidas se detallan a continuación:

- **Credenciales y autenticación.** Cambiar de inmediato todas las contraseñas por defecto. Utilizar contraseñas robustas y, preferiblemente, autenticación basada en roles mediante protocolos como RADIUS o TACACS+. También se recomienda deshabilitar cuentas predeterminadas y administrar los

accesos siguiendo el principio de privilegio mínimo.

- **Acceso seguro:** desactivar servicios inseguros como Telnet o HTTP en las interfaces de administración y utilizar, en su lugar, SSH y HTTPS con certificados válidos. Configurar SNMPv3 con autenticación y cifrado en lugar de versiones anteriores. Limitar el acceso administrativo a direcciones IP o rangos autorizados.

- **Puertos y servicios inactivos:** deshabilitar los puertos Ethernet no utilizados y eliminar las VLAN vacías. También se deben desactivar protocolos innecesarios, como CDP o LLDP si no se utilizan, y SNMP si no es requerido. En *switches*, conviene activar funciones de seguridad por puerto, como 802.1X o *Port Security*, estableciendo un número máximo de direcciones MAC permitidas y listas de direcciones fijas.

- **Firmwares y parches:** mantener actualizado el sistema operativo de los dispositivos de red, aplicando sin demora los parches críticos de seguridad. Un dispositivo con software obsoleto representa un riesgo considerable, ya que puede ser explotado fácilmente.

- **Registros y monitoreo:** habilitar el registro de eventos relevantes (*syslog*), como intentos de acceso o cambios de configuración, y enviar estos registros a un servidor central. Además, configurar NTP para sincronizar los relojes de los dispositivos, garantizando que los registros sean útiles para tareas de auditoría.

- **Seguridad física:** restringir el acceso físico a *routers* y *switches*. El equipamiento debe estar alojado en salas cerradas y seguras, con acceso exclusivo para personal autorizado. En entornos críticos, se recomienda emplear autenticación física, como tarjetas o sistemas biométricos, para prevenir manipulaciones directas o robo de hardware.

Aplicar estas prácticas reduce de forma significativa los vectores de ataque: se evita la explotación de servicios innecesarios, el uso de credenciales débiles y la alteración de configuraciones sin detección. En conjunto, el *hardening* de dispositivos constituye una capa fundamental de defensa perimetral y periférica dentro de la red.

En resumen, el endurecimiento de dispositivos implica eliminar puntos de entrada inseguros —como Telnet, SNMP o servicios innecesarios— y reforzar la segmentación física y lógica mediante la gestión adecuada de puertos y el uso cuidadoso de VLAN. También es esencial mantener actualizado el *software* y el *firmware* con los parches de seguridad correspondientes.

El *hardening* de la infraestructura de red consiste en adoptar configuraciones seguras por defecto: eliminar funciones no requeridas, reforzar los mecanismos de autenticación y garantizar que cada componente solo ejecute lo estrictamente necesario. Estas medidas no solo previenen accesos no autorizados, sino que también aumentan la resiliencia del sistema frente a ataques dirigidos.

2.3. Visibilidad mínima entre VLAN

Uno de los objetivos fundamentales de una segmentación eficaz es reducir al mínimo la visibilidad y la conectividad entre VLAN o subredes distintas. Como se explicó previamente, las VLAN están aisladas por diseño: por defecto, no se permite el intercambio de tráfico entre VLAN.

En la práctica, esto implica que:

- dos redes lógicas diferentes no pueden verse entre sí a nivel de capa 2;
- ninguna trama de *broadcast* o tráfico no direccionado puede atravesar una VLAN sin un proceso explícito de enrutamiento.

Para habilitar la comunicación entre VLAN, es necesario implementar un punto de enrutamiento —como un *router* o *switch* de capa 3— que cuente con interfaces configuradas en cada VLAN involucrada. Incluso en estos casos, se recomienda aplicar listas de control de acceso (ACL) o cortafuegos que filtren los flujos de datos, permitiendo únicamente aquellos explícitamente autorizados.

De esta manera, la visibilidad inter-VLAN se limita estrictamente a lo necesario. Por ejemplo, si la VLAN de usuarios de oficina no requiere acceder a la VLAN de servidores de bases de datos, el *router* de frontera puede configurarse para impedir ese tráfico, o bien bloquearlo mediante ACL. Así, cada VLAN opera de forma similar a una red independiente, con fronteras bien definidas.

Este enfoque previene que un dispositivo comprometido en una VLAN de menor confianza —como una red de invitados— pueda escanear o comunicarse libremente con equipos ubicados en segmentos más críticos.

En entornos avanzados, particularmente bajo arquitecturas *zero trust*, la comunicación entre segmentos se reduce aún más, estableciendo únicamente túneles concretos y cifrados que permiten el paso exclusivo del tráfico legítimo y autorizado, reforzando la seguridad en cada límite de red.

La segmentación se fortalece al reducir al mínimo la comunicación entre VLAN. Cada VLAN debe operar casi como una red independiente, y solo se deben habilitar los flujos estrictamente necesarios. Esto implica adoptar una política de denegación por defecto para todo el tráfico inter-VLAN, y luego definir reglas puntuales para los servicios que requieran comunicación. A continuación, se presentan algunos ejemplos de buenas prácticas en este sentido:

- **Comunicación limitada entre usuarios y servidores críticos.** Se deben permitir únicamente las conexiones necesarias, como las que van desde estaciones de trabajo a servidores web a través de los puertos 80 o 443. Todo el tráfico no definido debe ser bloqueado mediante listas de control de acceso (ACL) de capa 3.

- **Filtrado del tráfico inter-VLAN mediante *firewalls* o *routers*:** se deben implementar reglas que regulen de forma precisa qué flujos están permitidos. Idealmente, las VLAN más sensibles —como aquellas que contienen bases de datos o sistemas críticos— no deberían iniciar conexiones hacia segmentos de menor nivel de confianza.

- **Evitar *broadcasts* entre VLAN y el uso compartido innecesario de recursos:** mantener el aislamiento completo entre VLAN contribuye a reducir la visibilidad interna. Una red segmentada bajo este enfoque mejora la seguridad general, ya que los incidentes quedan contenidos dentro del segmento comprometido y se impide el movimiento lateral del atacante.

En la práctica, estas medidas se aplican siguiendo el principio de *deny by default* en el enrutamiento interno: primero se bloquea todo el tráfico entre segmentos, y luego se introducen excepciones específicas y justificadas. Esta contención resulta fundamental para evitar accesos no autorizados entre zonas con distintos niveles de seguridad.

Cada VLAN debe funcionar como un dominio de red aislado. Por defecto, no debe permitirse la comunicación entre VLAN, salvo que sea estrictamente necesaria para el funcionamiento operativo. Para ello, se recomienda aplicar el principio de *deny by default* entre VLAN mediante listas de control de acceso (ACL) o cortafuegos internos. A continuación, se presenta un ejemplo típico de configuración:

- **VLAN de usuarios → VLAN de servidor SQL**. Permitir únicamente el tráfico destinado al puerto 1433 del servidor SQL.
- **Todo el tráfico restante**: debe ser bloqueado explícitamente.

De esta manera, una VLAN de producción no podrá comunicarse de forma automática con segmentos como la VLAN de gestión o la VLAN de invitados. Este nivel de aislamiento limita de forma significativa la posibilidad de movimientos laterales: si un *endpoint* en la VLAN 10 es comprometido, no podrá escanear ni afectar dispositivos en otras VLAN sin atravesar un control de seguridad.

Una topología correctamente segmentada, con cortafuegos y VLAN aisladas, permite contener intrusiones dentro de áreas limitadas de la red. En la práctica, se recomienda combinar la segmentación por VLAN con el uso de ACL. Algunas medidas son las siguientes:

- **Configurar dispositivos de capa 3 o cortafuegos virtuales** para filtrar el tráfico entre VLAN, asegurando que solo se habiliten los flujos estrictamente necesarios.
- **Verificar periódicamente** que no existan rutas indirectas que puedan generar visibilidad no deseada entre segmentos.

2.4 Bitácora de cambios y *rollback*

Un componente fundamental del endurecimiento de la red es la gestión de cambios. Esta consiste en registrar y versionar cada modificación aplicada a la configuración de los dispositivos. Se recomienda mantener una bitácora o sistema de gestión donde quede documentado quién realizó cada cambio, en qué momento y sobre qué dispositivo. Cada ajuste —como modificaciones en las ACL, reglas de *firewall*, actualizaciones de *firmware* o cambios en parámetros del sistema— debe quedar registrado de forma precisa.

Además, es esencial validar y probar los cambios antes de implementarlos en entornos de producción. Contar con un sistema de control de versiones para las configuraciones —por ejemplo, gestionando archivos en un repositorio Git— permite recuperar una versión anterior en caso de error o impacto no deseado.

En la práctica, se acostumbra a exportar y almacenar copias periódicas de la configuración de *routers* y *switches*. Esto facilita la restauración del estado anterior tras un incidente o una configuración incorrecta. Muchas plataformas de gestión de red ofrecen notificaciones en tiempo real ante cambios, y permiten realizar *rollback* de forma automática.

Según los principios de gestión de configuración, toda modificación debe estar debidamente registrada y verificada. El archivado de versiones anteriores garantiza la reversibilidad de los cambios y contribuye a la continuidad del servicio en caso de falla.

Llevar un registro detallado de todos los cambios realizados en la red es esencial tanto para la seguridad como para la gestión operativa. Según la norma ISO 27001, toda organización debe conservar la configuración de sus dispositivos de red y registrar el historial de cambios, incluyendo quién realizó cada modificación y en qué momento. Contar con esta bitácora permite auditar las acciones administrativas y revertir configuraciones problemáticas en caso de incidentes.

Para facilitar esta tarea, se recomienda automatizar las copias de seguridad de las configuraciones. A continuación, se presentan algunas herramientas ampliamente

utilizadas en la comunidad técnica:

- **RANCID y Oxidized.** Son programas de código abierto que se conectan periódicamente a *switches* y *routers*, recopilan la configuración en ejecución y la almacenan en un repositorio, normalmente Git. Permiten detectar cambios entre versiones y generan alertas ante cualquier modificación.

- **Git:** utilizar repositorios Git —por ejemplo, en un servidor interno— para versionar los archivos de configuración garantiza un historial detallado. Esto permite conocer con precisión quién modificó qué, y volver fácilmente a una versión anterior si es necesario.

- **Sistemas de registro (*logs*) y SIEM:** centralizar los registros de cambios a través de *syslog*, y analizarlos con herramientas como Graylog, ELK u OSSIM, permite auditar de forma efectiva las acciones realizadas sobre los dispositivos. Estos sistemas también facilitan la correlación de eventos en contextos de seguridad.

Además, se debe establecer un procedimiento claro de *rollback*. Antes de aplicar cualquier cambio crítico, es fundamental guardar una copia de la configuración actual. Si el nuevo ajuste provoca fallos o expone vulnerabilidades, se puede restaurar rápidamente el estado previo. Muchas plataformas modernas incorporan funciones de reversión inmediata. En dispositivos Cisco, por ejemplo, se puede utilizar el comando «rollback» para restaurar una configuración sin necesidad de reiniciar el equipo por completo.

Es fundamental documentar y controlar cada cambio de configuración en la infraestructura de red. Para ello, se debe mantener una bitácora en la que se registre quién realizó cada modificación, en qué momento y con qué propósito. Además, es necesario conservar copias de seguridad de la configuración actual —como los archivos *running-config* de *switches* y *routers* — tras cada ajuste.

Herramientas de control de versiones, como Git, o soluciones especializadas como RANCID y Oxidized, permiten automatizar estas tareas. Estas herramientas recopilan las configuraciones, detectan diferencias entre versiones y facilitan el seguimiento de cambios de manera centralizada.

Cuando un cambio provoca problemas —como interrupciones de rutas, bucles o pérdida de conectividad—, debe ejecutarse un *rollback*: la restauración de la última configuración funcional conocida. Muchos dispositivos de fabricantes como Cisco o Juniper ofrecen comandos específicos para revertir a una versión anterior sin reiniciar el equipo. Como señala una guía especializada, «en el ámbito de las redes, los administradores pueden recurrir al *rollback* cuando los cambios en la configuración generan problemas de conectividad».

Gracias a los respaldos y registros adecuados, es posible recuperar rápidamente un estado operativo, sin necesidad de deducir manualmente los parámetros anteriores. Este tipo de respuesta evita tiempos de inactividad prolongados y mejora la resiliencia operativa.

En resumen, una gestión de cambios eficiente incluye los siguientes elementos esenciales:

- guardar configuraciones base;
- registrar cada modificación;
- validar los cambios en un entorno de pruebas antes del despliegue;
- y disponer de un plan de contingencia (rollback) ante posibles fallos.

Estas prácticas garantizan que la red se mantenga segura y operativa, incluso tras reconfiguraciones accidentales o ataques dirigidos. Contar con una bitácora de cambios y un mecanismo efectivo de *rollback* es imprescindible en redes seguras, ya que proporciona trazabilidad total y capacidad de recuperación ante errores humanos o incidentes de seguridad. Así, cualquier modificación se vuelve reversible sin comprometer la estabilidad del sistema.

CONTINUAR

Referencias

[Imagen sin título sobre topologías de red], (s.f.). https://247tecno.com/topologia-de-red-tipos-caracteristicas/#google_vignette

[Imagen sin título sobre red punto a punto], (s.f.). https://natverksteknologier.diginto.se/datalankskikt/topologier/

[Imagen sin título sobre red cliente servidor y red punto a punto], (s.f.). https://shareaza.sourceforge.net/mediawiki/P2P_network/es

Nile, (s.f.). *A Network Segmentation Diagram Cheat Sheet*. https://nilesecure.com/network-design/network-segmentation-diagram

Referencias bibliográficas de consulta

Amazon Web Services. (s. f.). *¿Qué es el modelo OSI?* https://www.aws.amazon.com/es/what-is/osi-model/

Azion. (s. f.). *¿Qué son los modelos OSI y TCP/IP?* https://www.azion.com/es/learning/network-layer/que-son-los-modelos-osi-y-tcp-ip/

Canle, E. (2021). *Modelo jerárquico de capas Cisco.* Tokio School. https://www.tokioschool.com/noticias/modelo-jerarquico-capas-cisco/

Cimas Cuadrado, G. (2024). *Topología de redes informáticas: tipos, características y aplicaciones*. OpenWebinars. https://openwebinars.net/blog/topologia-de-redes-informaticas/

Cisco. (s.f.). *Cisco SAFE: un modelo de seguridad para las redes de las empresas (PDF)*. https://www.cisco.com/c/dam/global/es_es/assets/docs/safe_wp1.pdf

Cloudflare. (s.f.). *Qué es Zero Trust*. https://www.cloudflare.com/es-es/learning/security/glossary/what-is-zero-trust/

De Luz, S. (2025). *VLANs: qué son, tipos y para qué sirven*. RedesZone. https://www.redeszone.net/tutoriales/redes-cable/vlan-tipos-configuracion/

ESET Digital Security Guide. (2022). *Nunca confíes: siempre verifica — la confianza cero explicada*. https://digitalsecurityguide.eset.com/es/nunca-confies-siempre-verifica-la-confianza-cero-explicada

Fortinet. (s.f.). *¿Qué es el modelo OSI?* https://www.fortinet.com/lat/resources/cyberglossary/osi-model/

Illumio. (2025). *Ciberseguridad 101: ¿Qué es la segmentación de red?* https://www.illumio.com/es-mx/cybersecurity-101/network-segmentation/

Interlir. (2024). *Cómo crear una subred y configurar el enrutamiento*. https://interlir.com/es/2024/11/11/como-crear-una-subred-y-configurar-el-enrutamiento/

Instituto Profesional IPP. (2024). *¿Qué es rollback en el sector TI?* https://ipp.cl/tecnologia-y-desarrollo/que-es-rollback-en-el-sector-ti/

Kaspersky, E. (2012). *Denegar por defecto significa negarlo todo*. https://eugene.kaspersky.es/2012/10/03/denegar-por-defecto-significa-negarlo-todo/

Kass, J. (s.f.). *Mejore la ciberseguridad de su empresa con segmentación de red*. Rockwell Automation. https://www.rockwellautomation.com/es-mx/company/news/magazines/mejorelaciberseguridad.html

Lee, J. (2026). *¿Qué es la topología de red?* Trend Micro. https://www.trendmicro.com/es_es/what-is/network-security/network-topology.html

Netwrix. (2025). *Zero Trust*. https://netwrix.com/es/cybersecurity-glossary/architectural-concepts/zero-trust/

Netwrix. (s.f.). *Mejores prácticas de seguridad de red* (guía). https://netwrix.com/es/resources/guides/network-security-best-practices/

Peters, S. (2025). *Configuration management (ISO/IEC 27001, Anexo A 8.9)*. ISMS Online. https://es.isms.online/iso-27001/annex-a-2022/8-9-configuration-management-2022/

Rojas Campo, J. (s.f.). *¿Qué es la seguridad perimetral informática? Guía completa*. TecnoSeguro. https://www.tecnoseguro.com/faqs/seguridad-perimetral-informatica-que-es

Sargeant, S. (2025). *¿Qué es Endpoint Security?* Trend Micro. https://www.trendmicro.com/es_es/what-is/endpoint-security.html

Startup Defense. (2025). *Segmentación de red: la clave para mejorar la seguridad y el rendimiento de los datos*. https://www.startupdefense.io/es-us/blog/segmentacion-de-red-la-clave-para-mejorar-la-seguridad-y-el-rendimiento-de-los-datos

Trend Micro. (2026). *Cuáles son los aspectos básicos de la seguridad de red?* https://www.trendmicro.com/es_es/what-is/network-security/network-security-basics.html

UNIR. (2023). *¿Qué es el hardening de sistemas en informática?* https://www.unir.net/revista/ingenieria/hardening-que-es/

Utimaco. (s.f.). *¿Cuáles son los principios básicos de un modelo Zero Trust?* https://utimaco.com/es/servicio/base-de-conocimientos/zero-trust/cuales-son-los-principios-basicos-de-un-modelo-zero-trust

CONTINUAR