Machine Translated by Google
RCMOS – Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 1 de octubre de 2026 | Aceptación: 3 de octubre de 2026 | Publicación: 6 de octubre de 2026

Arquitecturas de conectividad para pymes: segmentación de red, VPN, virtualización y disponibilidad operativa.

Arquitecturas de conectividad para pymes: segmentación de red, VPN, virtualización y operativas.
Disponibilidad
Arquitecturas de conectividad para pymes: segmentación de red, VPN, virtualización y disponibilidad operativa.

Guilherme Gallo Zazeri

Profesional de las Tecnologías de la Información, consultor y emprendedor en infraestructura, conectividad y soluciones tecnológicas, con más de 25 años de experiencia profesional.

Resumen

Las redes corporativas de las pequeñas y medianas empresas (PYME) han evolucionado para dar soporte al acceso a aplicaciones locales y en la nube, el teletrabajo, la telefonía IP, los servicios virtualizados y la comunicación entre unidades. Este artículo examina los principios arquitectónicos para una conectividad segura y disponible, abordando la segmentación, los firewalls, las redes inalámbricas, las VPN, la redundancia de enlaces, la virtualización y la documentación. La investigación utiliza una revisión narrativa estructurada de libros de texto clásicos sobre redes, publicaciones del NIST y datos del Informe de Investigaciones de Violaciones de Datos de Verizon. Los resultados muestran que el rendimiento y la seguridad no deben considerarse objetivos contrapuestos: una arquitectura coherente reduce la superficie de exposición, limita la propagación de fallos, mejora el diagnóstico y crea las condiciones para la recuperación. Para las PYME, la estandarización y la simplicidad operativa son especialmente relevantes, ya que los entornos excesivamente complejos pueden aumentar los costes y la dependencia de especialistas.
Palabras clave: redes corporativas; conectividad; VPN; cortafuegos; virtualización; pequeñas y medianas empresas; disponibilidad.

Abstracto

Las redes corporativas de las pequeñas y medianas empresas ahora permiten el acceso a aplicaciones locales y en la nube, el trabajo remoto, la telefonía IP, los servicios virtualizados y la comunicación entre diferentes ubicaciones. Este artículo examina los principios arquitectónicos para una conectividad segura y disponible, abordando la segmentación, los firewalls, las redes inalámbricas, las VPN, la redundancia de enlaces, la virtualización y la documentación. El estudio utiliza una revisión narrativa estructurada de libros de texto de redes reconocidos, publicaciones del NIST y datos del Informe de Investigaciones de Violaciones de Datos de Verizon. Los hallazgos indican que el rendimiento y la seguridad no deben considerarse objetivos contrapuestos: una arquitectura coherente reduce la exposición, limita la propagación de fallos, mejora la resolución de problemas y crea las condiciones para la recuperación. Para las pymes, la estandarización y la simplicidad operativa son particularmente relevantes, ya que los entornos innecesariamente complejos pueden aumentar los costos y la dependencia de especialistas.
Palabras clave: redes corporativas; conectividad; VPN; cortafuegos; virtualización; pequeñas y medianas empresas; disponibilidad.

Introducción

Las redes corporativas ya no se limitan a conectar ordenadores dentro de una oficina. Hoy en día,

Integran aplicaciones en la nube, servidores virtualizados, telefonía IP, dispositivos inalámbricos, sucursales y...

profesionales remotos. Tanenbaum y Wetherall (2021) muestran que la comunicación en red es

construido a partir de capas y protocolos interdependientes, una característica que hace que el diseño arquitectónico

crucial para el rendimiento y la fiabilidad.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 1 de octubre de 2026 | Aceptación: 3 de octubre de 2026 | Publicación: 6 de octubre de 2026

La expansión de la conectividad también amplía el área de exposición. El informe DBIR 2025 de Verizon
Se identificó que, entre las pequeñas organizaciones consideradas en el informe, la intrusión en el sistema, social
Los ataques de ingeniería y los ataques básicos a aplicaciones web representaron en conjunto el 96% de las brechas de seguridad.
Los datos demuestran que las redes y el acceso no pueden gestionarse únicamente desde la perspectiva de
disponibilidad.
Este artículo analiza seis dimensiones de la arquitectura de conectividad para las PYMES: diseño y
Segmentación, cortafuegos, VPN, redundancia, virtualización y documentación. El objetivo de la discusión es...
para mostrar cómo se pueden aplicar los principios técnicos establecidos sin presuponer estructuras
equivalentes a las de las grandes corporaciones.

2. Metodología

La investigación adopta una revisión narrativa estructurada, reuniendo literatura sobre redes informáticas,
Seguridad perimetral, acceso remoto, virtualización y gestión de riesgos.
Se utilizaron como bases los trabajos de Tanenbaum y Wetherall (2021), Kurose y Ross (2021) y Stallings (2016).
Aspectos conceptuales de la arquitectura, los protocolos, el rendimiento y las redes modernas.
Las recomendaciones de seguridad se compararon con NIST SP 800-41 Rev. 1, NIST SP 800-46
Revisión 2, NIST CSF 2.0 y la guía del NIST para pequeñas empresas.
El informe DBIR 2025 de Verizon se incorporó como fuente empírica sobre patrones de violación, prestando especial atención a...
específicamente al segmento de pequeñas organizaciones presentado en el informe.
El análisis no evalúa marcas comerciales. Las tecnologías de firewall, Wi-Fi, hipervisor y túnel son...
Se analizaron en función de su función arquitectónica, con el fin de preservar la neutralidad y la aplicabilidad.
Los resultados se organizaron en seis ejes. Cada eje considera la disponibilidad, la seguridad,
Facilidad de mantenimiento e idoneidad para el tamaño de la organización.

3.1 Diseño de red y segmentación lógica

Tanenbaum y Wetherall (2021) explican que las redes están compuestas por sistemas interconectados cuyos
La organización influye en el rendimiento y la fiabilidad. En las empresas, el diseño debe reflejar las funciones.
distintos, como usuarios, servidores, telefonía, visitantes y dispositivos especializados.
La segmentación lógica permite separar grupos de activos y controlar la comunicación entre ellos. En lugar de
En una red plana, donde todos los dispositivos comparten un amplio alcance, los segmentos reducen la
Propagan fallos y limitan las rutas innecesarias.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 1 de octubre de 2026 | Aceptación: 3 de octubre de 2026 | Publicación: 6 de octubre de 2026

Kurose y Ross (2021) destacan la importancia de la derivación y las políticas que la determinan.
cómo los flujos atraviesan la red. En un contexto corporativo, estas decisiones deben documentarse y
asociado a necesidades de comunicación reales.

La segmentación no implica crear una complejidad ilimitada. Cada división adicional aumenta la necesidad.
de reglas, pruebas y diagnóstico. Para las PYMES, el equilibrio entre aislamiento y administración es parte de la
diseño.

Las redes inalámbricas también deben integrarse en la arquitectura. La separación entre el acceso corporativo y
Por ejemplo, evita que los visitantes se vean expuestos innecesariamente debido a la comodidad de la conectividad.
recursos internos.

Una arquitectura bien segmentada crea una base para las políticas de firewall, monitoreo y respuesta.
El diseño de la red comienza a expresar reglas de negocio, y no solo la disposición física de la misma...
equipo.

3.2 Cortafuegos y políticas de control de tráfico

Los cortafuegos actúan como puntos de aplicación de políticas entre diferentes redes o zonas de confianza.
Scarfone y Hoffman (2009), en NIST SP 800-41 Rev. 1, tratan la política del firewall como parte
esencial para la planificación y gestión de estos controles.

La efectividad depende de la calidad de las reglas. Los permisos acumulados a lo largo de los años pueden...
Crear excepciones cuyo propósito ya no existe. Las revisiones periódicas ayudan a eliminar reglas obsoletas y
Reduzca la exposición.

El principio de permitir solo lo necesario resulta especialmente útil. Los servicios publicados abren puertas.
El acceso administrativo debe corresponder a una necesidad identificada, con un origen y un destino específicos.
definido.

Los registros del firewall proporcionan evidencia para el diagnóstico y la investigación, pero su volumen requiere una consideración cuidadosa.
Los eventos relevantes deben conservarse y analizarse de manera coherente con el riesgo y la capacidad.
del equipo.

Los firewalls también participan en funciones de conectividad como NAT, VPN y conmutación por error.
La concentración hace que documentar las configuraciones y realizar copias de seguridad de los equipos forme parte del proceso.
continuidad operativa.

Por lo tanto, un cortafuegos no debe considerarse un dispositivo que automáticamente garantiza la seguridad de la red.
Su valor depende de la arquitectura, las reglas, el mantenimiento y la monitorización.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google
RCMOS - Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 1 de octubre de 2026 | Aceptación: 3 de octubre de 2026 | Publicación: 6 de octubre de 2026

3.3 VPN y conectividad entre unidades remotas y profesionales

El acceso remoto y la interconexión de unidades requieren canales que protejan los datos en tránsito y controlen...
quién puede acceder a los recursos internos. Souppaya y Scarfone (2016), en NIST SP 800-46 Rev. 2,
Analizan la seguridad del teletrabajo y el acceso remoto como una combinación de tecnologías, políticas y...
gestión.

Las VPN pueden establecer túneles entre sitios web o conectar usuarios individuales. La elección depende de...
Topología, aplicación, rendimiento y modelo de autenticación.

El cifrado de túnel protege el tráfico, pero por sí solo no resuelve el riesgo del punto final. Un dispositivo
Una persona con acceso no autorizado y comprometida puede introducir amenazas en la red.

Por lo tanto, el diseño de acceso remoto debe aplicar privilegios compatibles con el rol. No todos
El usuario remoto debe poder acceder a todos los segmentos o servicios.

También es necesario considerar la disponibilidad. Dependencia de un único enlace, equipo o
Los servicios de autenticación pueden convertir el acceso remoto en un punto crítico.

Por lo tanto, las VPN son componentes de una arquitectura más amplia. La seguridad depende de la combinación de...
Identidad, segmentación, actualización, monitorización y reglas de acceso.

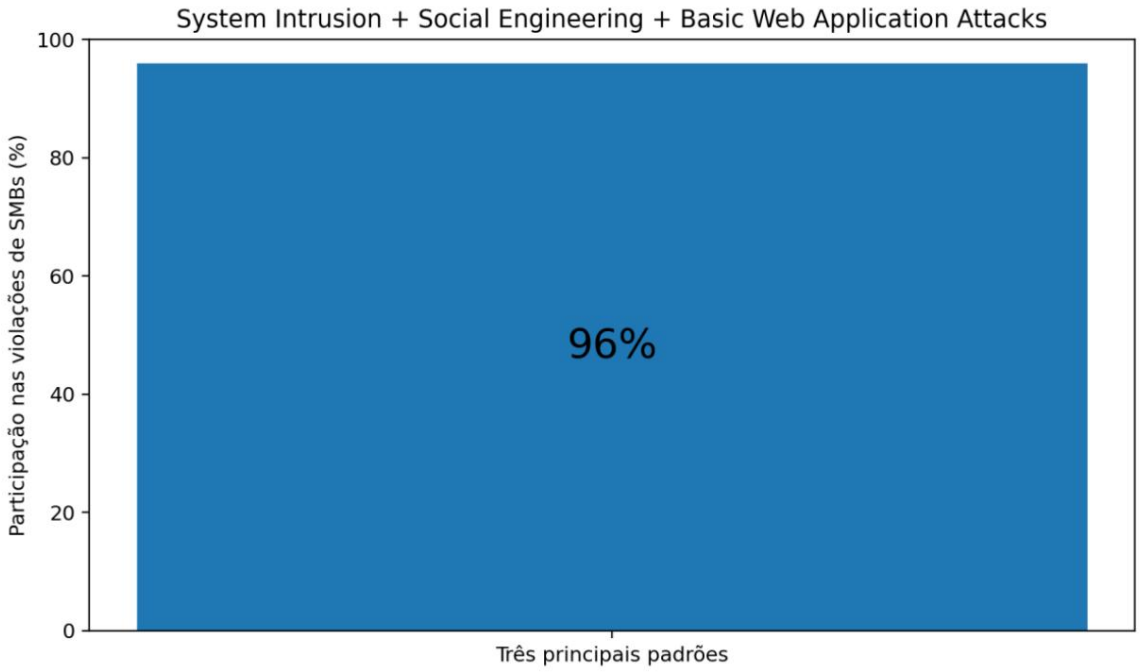

Figura 1. Participación conjunta de los tres principales patrones de violación en organizaciones pequeñas:
Intrusión en sistemas, ingeniería social y ataques básicos a aplicaciones web. Fuente: Elaboración propia del autor.
basado en Verizon (2025).

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 1 de octubre de 2026 | Aceptación: 3 de octubre de 2026 | Publicación: 6 de octubre de 2026

3.4 Redundancia de enlaces y continuidad de la conectividad

La conectividad externa se ha convertido en una dependencia fundamental para las empresas que utilizan SaaS, correo electrónico y otros servicios.
Computación en la nube, telefonía IP y trabajo remoto. Una interrupción de internet puede afectar a múltiples servicios.
simultáneamente.

La redundancia de enlaces reduce esta dependencia cuando los proveedores, las rutas y los equipos son...
Diseñado para evitar un único punto de fallo. Sin embargo, la existencia de dos contratos no garantiza
independencia física o lógica.

El balanceo de carga y la conmutación por error tienen objetivos diferentes. El primero distribuye el tráfico; el segundo...
En segundo lugar, busca mantener el servicio cuando una ruta deja de funcionar. La arquitectura debe permitir...
Está claro qué comportamiento se espera.

Es necesario realizar pruebas porque la conmutación automática puede fallar debido a problemas de DNS, sesión, enrutamiento u otros.
Dependencia de la megafonía pública. La disponibilidad debe considerarse desde el punto de vista de
solicitud.

La telefonía IP pone de relieve este desafío. Incluso si la centralita telefónica (PBX) permanece operativa, la pérdida de
La conectividad a troncales externas puede impedir las llamadas. Kurose y Ross (2021) muestran cómo.
Las aplicaciones en tiempo real son sensibles a los retrasos, las pérdidas y la disponibilidad de la red.
Por lo tanto, la redundancia efectiva depende de la diversidad, la configuración, las pruebas y la monitorización. Duplicar
Los componentes que no validan la ruta completa solo pueden crear una apariencia de resiliencia.

3.5 Virtualización y consolidación de servidores

La virtualización separa la ejecución lógica de los sistemas del hardware físico subyacente. Stallings (2016)
relaciona la virtualización con la evolución de las infraestructuras modernas, en las que los recursos informáticos
Pueden abstraerse y gestionarse con mayor flexibilidad.

Para las PYMES, consolidar las cargas puede reducir la cantidad de equipos necesarios y facilitar el aprovisionamiento.
Las máquinas virtuales se pueden copiar, migrar y organizar de forma diferente a los servidores.
exclusivamente físico.

La consolidación también concentra el riesgo. Cuando varios servicios dependen del mismo host,
Las fallas físicas pueden afectar diversas funciones. Capacidad, almacenamiento, energía y estrategia de
La recuperación debe ir a la par con la densidad de carga.

La virtualización no sustituye a las copias de seguridad. Las instantáneas pueden servir para el mantenimiento a corto plazo o para revertir cambios.
pero no deben confundirse automáticamente con una estrategia de protección independiente y
retención.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 1 de octubre de 2026 | Aceptación: 3 de octubre de 2026 | Publicación: 6 de octubre de 2026

La estandarización del entorno facilita el soporte. Plantillas, nomenclatura, documentación y criterios para...

La asignación hace que los cambios sean más predecibles y reduce las configuraciones improvisadas.

De este modo, la virtualización crea valor cuando integra capacidad, continuidad y gobernanza.

El objetivo no es maximizar el número de máquinas por host, sino obtener una infraestructura manejable.

y recuperable.

3.6 Seguimiento operativo, documentación y diagnóstico

Las redes complejas generan señales en enrutadores, cortafuegos, puntos de acceso, servidores y aplicaciones.

El sistema de monitorización convierte algunas de estas señales en información operativa, lo que permite su reconocimiento.

indisponibilidad, saturación y comportamiento anómalo.

Tanenbaum y Wetherall (2021) muestran que los problemas de red pueden surgir en diferentes capas.

Un diagnóstico eficaz requiere distinguir entre fallas físicas, problemas de direccionamiento, problemas de enrutamiento, resolución de nombres,

transporte y aplicación.

La documentación reduce el tiempo necesario para esta investigación. Diagramas, inventarios,

El direccionamiento, las reglas esenciales y las dependencias ayudan a reconstruir la ruta del tráfico.

El informe DBIR 2025 de Verizon refuerza la importancia de mantener la visibilidad del entorno. En la sección correspondiente...

Para las organizaciones pequeñas, existen tres patrones principales: intrusión en el sistema, ingeniería social y navegación web básica.

Los ataques a las aplicaciones representaron el 96% de las brechas de seguridad.

Estos datos no significan que cada incidente sea causado por la arquitectura de la red. Demuestran,

Sin embargo, la conectividad, los sistemas y la identidad están integrados en un escenario donde la exposición y

Es necesario supervisar el acceso de forma continua.

El monitoreo y la documentación completan el ciclo arquitectónico. Una red bien diseñada, pero no

Si es observable o comprensible para quienes lo gestionan, pierde una parte importante de su capacidad.

Permanecer disponibles y seguros.

3.7 Telefonía IP, calidad de servicio y convergencia de las comunicaciones

La convergencia de voz y datos ha alterado el papel de la red corporativa. Sistemas de telefonía IP

Comparten infraestructura con aplicaciones, acceso a internet y servicios internos, lo que provoca que...

Una degradación de la conectividad puede afectar simultáneamente a los sistemas de comunicación y a los sistemas empresariales.

Kurose y Ross (2021) explican que las aplicaciones en tiempo real tienen sus propios requisitos específicos.

Retraso, variación del retraso y pérdida de paquetes.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 1 de octubre de 2026 | Aceptación: 3 de octubre de 2026 | Publicación: 6 de octubre de 2026

En una red sin criterios de priorización, el tráfico de gran volumen puede competir por los recursos con las llamadas.
voz. La percepción del usuario es inmediata: retrasos, cortes y pérdida de inteligibilidad. La gestión de
La calidad del servicio busca abordar esta diferencia de sensibilidad sin asumir que cada aplicación
Requiere el mismo comportamiento de red.

Stallings (2016) vincula la calidad del servicio y la calidad de la experiencia con la evolución de las redes modernas.
En entornos corporativos, esto significa que las métricas técnicas deben interpretarse desde...
Efecto en la actividad: se puede disponer de conexión y, al mismo tiempo, ofrecer experiencia.
No apto para videoconferencias o llamadas de voz.

La telefonía IP también aumenta la importancia de la segmentación. Separar lógicamente los dispositivos y
Las transmisiones de voz pueden facilitar la aplicación de políticas, el diagnóstico y el control de la difusión. La decisión,
Sin embargo, debe seguir siendo compatible con la capacidad de gestión del equipo.

Otro aspecto es la dependencia externa. Los troncales SIP, el DNS, internet y la energía eléctrica pueden integrarse en la cadena.
El funcionamiento del sistema telefónico. La redundancia debe tener en cuenta estas relaciones; mantener la centralita telefónica (PABX) activa.
No se puede solucionar una interrupción del servicio si la ruta externa necesaria para las llamadas permanece inaccesible.

La documentación cobra especial relevancia en entornos con un gran número de extensiones.
La numeración, los grupos, las rutas, las reglas de entrada y salida y las dependencias de los transportistas deben ser...
Registrado para que los cambios e incidentes puedan gestionarse de forma predecible.

La convergencia también cambia el diagnóstico. Los problemas percibidos como fallas telefónicas pueden
Puede tener su origen en la pérdida de paquetes, la saturación, el DNS, el enrutamiento, el cortafuegos o la configuración del punto final.
Tanenbaum, Feamster y Wetherall (2021) muestran por qué un análisis por capas sigue siendo útil.
incluso en la arquitectura moderna.

Por lo tanto, la telefonía IP no debe gestionarse como un sistema aislado. Se integra en la arquitectura de
conectividad y necesidades para compartir los mismos principios de disponibilidad, segmentación,
Se aplicaron medidas de monitorización, documentación y recuperación al resto de la infraestructura.

3.8 Estandarización arquitectónica y escalabilidad en entornos distribuidos

Empresas que crecen mediante la creación de nuevas unidades, el teletrabajo o la adopción de servicios en la nube.
Se enfrentan a un problema adicional: las configuraciones caso por caso tienden a producir entornos
Difícil de mantener. La estandarización reduce las variaciones innecesarias y crea puntos de referencia para la implementación.
y diagnóstico.

La estandarización no significa hacer que todas las unidades sean idénticas. Significa establecer principios repetibles.
para direccionamiento, segmentación, acceso remoto, denominación, registros, actualización y copias de

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 1 de octubre de 2026 | Aceptación: 3 de octubre de 2026 | Publicación: 6 de octubre de 2026

configuración. Kurose y Ross (2021) muestran que la predictibilidad del comportamiento de la red
Depende de reglas claras para el enrutamiento y la comunicación.
Las plantillas y las listas de verificación pueden reducir las omisiones durante las nuevas implementaciones. En redes distribuidas,
La repetición disciplinada de criterios también facilita la comparación del rendimiento entre ubicaciones y la identificación
desviaciones.

El NIST CSF 2.0 (PASCOE; QUINN; SCARFONE, 2024) enfatiza los resultados de seguridad
Deben ser comprendidos, priorizados y comunicados. Una arquitectura estandarizada facilita esto.
Este proceso permite asociar controles con patrones conocidos en lugar de reconstruir el entorno desde cero.
cada evaluación.
La escalabilidad incluye la capacidad de operación humana. Una solución que requiere intervención manual.
Por cada nuevo usuario, un túnel o unidad puede operar a pequeña escala y volverse insostenible.
Con el crecimiento, la automatización y la estandarización también deben evaluarse teniendo en cuenta este efecto.
La documentación estandarizada reduce aún más la dependencia del profesional que realizó la implementación.
original. Cuando la topología, las reglas y los parámetros esenciales siguen un modelo común, otros
Los miembros del equipo pueden comprender el entorno con un menor coste de transición.
Finalmente, la estandarización crea una base más segura para la innovación. Las nuevas tecnologías pueden...
Evaluado en base a una arquitectura conocida, lo que permite comparar beneficios y riesgos sin introducir nuevas tecnologías.
Cambios simultáneos en todas las capas.
Por lo tanto, ampliar la conectividad no se trata solo de agregar equipos y enlaces. Se trata de preservar
comprensibilidad, seguridad y mantenibilidad a medida que la red crece y se hace más grande.
más ampliamente distribuido.

Conclusión

La conectividad de una PYME respalda servicios que antes eran independientes y, por lo tanto, necesita ser...
Se trata como arquitectura crítica. La segmentación ayuda a organizar los flujos y limitar la exposición, siempre que
El nivel de complejidad sigue siendo manejable. Los cortafuegos son mecanismos de aplicación de políticas;
Su efectividad depende de la calidad y el mantenimiento de las reglas, no solo de la presencia de
Las VPN mejoran la movilidad y la integración entre unidades, pero deben combinarse con otros equipos.
con identidad, privilegio y seguridad del dispositivo. La redundancia del enlace debe probarse mediante
Ruta de aplicación completa. Dos circuitos no representan continuidad si comparten una ruta.
Dependencias ocultas. La virtualización ofrece flexibilidad y consolidación, a la vez que...
Requiere prestar atención a la concentración de carga, la capacidad y la recuperación.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 1 de octubre de 2026 | Aceptación: 3 de octubre de 2026 | Publicación: 6 de octubre de 2026

La monitorización y la documentación hacen que la arquitectura sea observable y reducen el tiempo de diagnóstico.

Además de reducir la dependencia del conocimiento individual, se concluye que las redes resilientes para

Las PYMES se basan en una combinación de simplicidad, segmentación y controles de acceso.

Redundancia proporcional y operación disciplinada. El dibujo técnico gana valor cuando se mantiene...

Comprensible, comprobable y sostenible a lo largo del tiempo.

Referencias

TANENBAUM, Andrew S.; FEAMSTER, Nick; WETHERALL, David J. Redes de computadoras. 6.ª ed. Harlow: Pearson, 2021.
KUROSE, James F.; ROSS, Keith W. Redes de computadoras: un enfoque de arriba hacia abajo. 8.ª ed. Hoboken: Pearson, 2021.
STALLINGS, William. Fundamentos de las redes modernas: SDN, NFV, QoE, IoT y la nube. Boston: Addison-Wesley, 2016.
PASCOE, Cherilyn; QUINN, Stephen; SCARFONE, Karen. El Marco de Ciberseguridad (CSF) 2.0 del NIST. NIST CSWP 29. Gaithersburg: Instituto Nacional de Estándares y Tecnología, 2024.
ELIOT, Daniel. Marco de Ciberseguridad 2.0 del NIST: Guía de inicio rápido para pequeñas empresas. NIST SP 1300. Gaithersburg: Instituto Nacional de Estándares y Tecnología, 2024.
VERIZON. Informe de investigaciones de filtraciones de datos de 2025. Basking Ridge, 2025.
SCARFONE, Karen; HOFFMAN, Paul. Directrices sobre cortafuegos y políticas de cortafuegos. NIST SP 800-41 Rev. 1. Gaithersburg: Instituto Nacional de Estándares y Tecnología, 2009.
SOUppAYA, Murugiah; SCARFONE, Karen. Guía para el teletrabajo empresarial, el acceso remoto y la seguridad de los dispositivos personales en el trabajo. NIST SP 800-46 Rev. 2. Gaithersburg: Instituto Nacional de Estándares y Tecnología, 2016.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.