ConexPro

OCTUBRE · MES DE LA CIBERSEGURIDAD 2026



¿Tu empresa tiene una red o solo tiene Internet?

Guía para ordenar la red de tu negocio en 4 semanas, sin ser técnico

¿Quién diseñó tu red y cuándo se revisó por última vez?

conexpro.net

Contenido

01 Antes de empezar: 5 preguntas sobre tu red

02 ¿Red o solo Internet?

03 Las cifras que todo líder de negocio debe conocer

04 Tu red explicada en simple: las 5 piezas

05 Área 1: Seguridad y accesos

06 Área 2: Administración y seguimiento

07 Área 3: Continuidad del negocio

08 Tu plan de 4 semanas

09 Plantillas listas para usar

10 Mitos y realidades sobre la red de tu negocio

11 Cómo podemos ayudarte

12 Conclusión

CAPÍTULO 1

Antes de empezar: 5 preguntas sobre tu red

Responde sí o no. No necesitas saber nada técnico.

		Sí	No
1	¿Sabes quién diseñó tu red y cuándo se revisó por última vez?	☐	☐
2	¿Tu Wi-Fi fue diseñado, o fue creciendo con repetidores y equipos que se agregaron sobre la marcha?	☐	☐
3	¿Tus visitantes usan una red Wi-Fi distinta a la de tu equipo?	☐	☐
4	¿Las computadoras con datos de clientes están separadas de cámaras, impresoras y televisores?	☐	☐
5	¿Sabes qué hacer y a quién llamar si mañana se cae Internet?	☐	☐

5 «sí»

Tienes una red. Usa esta guía para mantenerla.

3 o 4 «sí»

Vas en camino. Empieza por las preguntas que respondiste con «no».

2 o menos

Probablemente tienes Internet, pero no una red. Esta guía es para ti.

CAPÍTULO 2

¿Red o solo Internet?

La mayoría de los negocios tiene Internet: llega la señal, las computadoras se conectan y el trabajo sale. Pocos tienen una red: un sistema pensado como un todo, con responsables y revisiones.

Pregúntate: **¿tu Wi-Fi fue diseñado o fue creciendo?** Un router del proveedor, un repetidor que alguien compró, la impresora nueva, una cámara, la clave que se compartió con un cliente. Cada pieza resolvió un problema del día, pero nadie las pensó juntas.

¿Quién diseñó todo esto y cuándo se revisó?

Si la respuesta es «nadie» o «no sé», no estás solo, y tiene arreglo.

Octubre es el Mes de la Concientización en Ciberseguridad, y el lema de este año de la National Cybersecurity Alliance lo resume bien: no se lo pongas fácil a quien busca una puerta abierta. Una red ordenada es exactamente eso.

Tu red es el camino por donde pasa todo: los cobros, las llamadas, los correos, las cámaras, los archivos de tus clientes. Si ese camino no está ordenado, ninguna otra protección funciona del todo.

La buena noticia: ordenar tu red no exige ser técnico. Exige saber qué tienes, quién lo controla y qué haces si algo falla. Eso es exactamente lo que vas a lograr con esta guía.

¿Ya hiciste tu Evaluación de red?

Cada tema de esta guía lleva el mismo nombre que en tu informe, ordenado en las mismas tres áreas. Busca los temas donde tu informe sugiere mejorar y empieza por los que podrían afectar el acceso a tus sistemas o detener tu operación.

¿Respondiste «No estoy seguro»? No es una mala respuesta: indica qué necesitas confirmar. En cada tema encontrarás la pregunta exacta para tu proveedor de Internet o tu técnico.

Escala del informe: 0–49 Riesgo elevado · 50–69 En riesgo · 70–84 Requiere atención · 85–100 Buenas prácticas

¿Aún no la haces? Son 18 preguntas y unos 5 minutos: **Haz tu Evaluación de red**

CAPÍTULO 3

Las cifras que todo líder de negocio debe conocer

Dos fuentes independientes coinciden: hoy la entrada más común de un ataque es una falla sin corregir en un equipo o programa, no solo el correo.

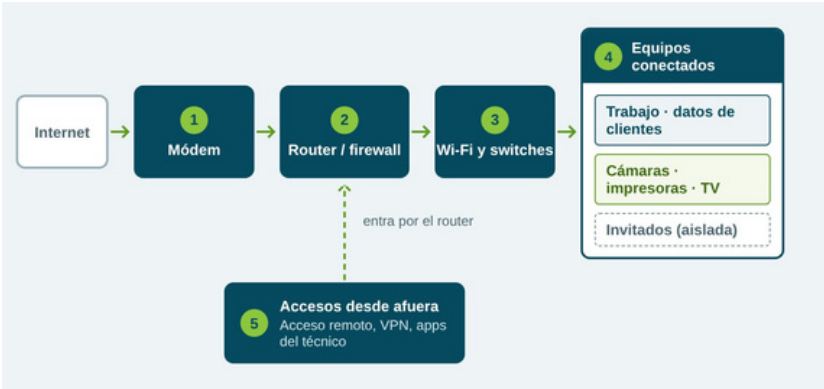
31%	**de las brechas empezaron aprovechando una falla sin corregir: la vía de entrada más común.** Actualizar el router y los equipos de red es tan importante como cuidar el correo. Fuente: Verizon DBIR 2026
32%	**de las intrusiones investigadas empezaron igual, en primer lugar por sexto año seguido.** Un segundo investigador, independiente de Verizon, llega a la misma conclusión. Fuente: Mandiant M-Trends2026
43 días	**tardan en promedio las empresas en corregir una falla crítica; solo el 26% las corrige por completo.** Mientras nadie actualiza, la puerta queda abierta. Por eso importa saber quién revisa tu router. Fuente: Verizon DBIR 2026
56%	**de las pequeñas empresas de EE. UU. sufrió al menos un ciberataque en el último año.** No es un problema solo de grandes empresas. Fuente: Hiscox Cyber Readiness Report 2026
69%	**de las víctimas de ransomware no pagó el rescate; el 66% de las empresas afectadas recuperó sus datos desde respaldos.** Prepararse funciona: buenos respaldos y un plan cambian el resultado. Fuente: Verizon DBIR2026 · Sophos State of Ransomware 2026

Lo que significa para ti: la red ya no es «cosa del técnico». Saber quién la controla y cada cuánto se revisa es una decisión de quien dirige el negocio, sea el dueño o el gerente.

CAPÍTULO 4

Tu red explicada en simple: las 5 piezas

Piensa en tu red como el edificio de tu negocio: tiene una puerta de entrada, pasillos, oficinas y una sala de visitas. Si sabes cuál es cada pieza, sabes qué preguntar.



Pieza	En palabras simples	Pregunta clave para quien dirige
1. Módem del proveedor	La conexión que llega de la calle. Normalmente pertenece a tu proveedor de Internet.	¿Quién es mi proveedor y cuál es su número de soporte para negocios?
2. Router o firewall	La puerta principal. Decide qué entra y qué sale de tu negocio.	¿Quién tiene la clave de administración y cuándo se actualizó por última vez?
3. Wi-Fi y switches	Los pasillos. Conectan computadoras, impresoras y teléfonos.	¿Cuántas redes Wi-Fi tengo y quién conoce cada clave?
4. Equipos conectados	Las oficinas: computadoras con datos de clientes, el software de taxes y el de cobros, cámaras, teléfonos IP, impresoras.	¿Tengo una lista de todo lo que está conectado?
5. Accesos desde afuera	Las llaves que entregaste: acceso remoto, VPN, apps del técnico o del proveedor. Entran por el router.	¿Quién puede entrar desde fuera de la oficina y cómo?

La regla de esta guía: cada pieza tiene un responsable, una clave que solo conoce quien debe y una fecha de última revisión

CAPÍTULO 5

Área 1: Seguridad y accesos

Controla quién puede conectarse a tu red y quién puede cambiarla. Aquí se concentran las puertas que los atacantes encuentran abiertas con más frecuencia.

La protección de la red y el acceso a la configuración

El riesgo	Routers con la clave de fábrica, sin actualizar o con la administración abierta desde Internet. Son exactamente el tipo de equipo que hoy más se ataca.
Tu primer paso	Anota marca y modelo del router y pregunta a tu proveedor o técnico: ¿quién lo administra?, ¿se actualiza solo?, ¿la administración remota está desactivada?
Vas bien cuando	Sabes quién tiene la clave y la fecha de la última actualización.

Equipos y actualizaciones

El riesgo	Equipos que nadie actualiza, o que tienen más de 5 años y el fabricante ya no corrige. Una falla conocida en el router puede quedar abierta para siempre.
Tu primer paso	Anota marca, modelo y año aproximado de compra de cada equipo de red. Pregunta si se actualizan solos, cuándo fue la última vez y si el fabricante sigue publicando actualizaciones. Programa las actualizaciones fuera del horario de trabajo.
Vas bien cuando	Cada equipo tiene fecha de última actualización y ninguno está fuera de soporte; si alguno lo está, ya tiene fecha de reemplazo.

Wi-Fi de visitantes y contraseña del Wi-Fi del negocio

El riesgo	Compartir la clave principal con clientes, proveedores o familiares. Cualquier celular conectado queda al lado de las computadoras con datos de tus clientes.
Tu primer paso	Crea una red de invitados aislada, con otra clave. Cambia la clave principal y reconecta solo los equipos del negocio.
Vas bien cuando	Nadie fuera del equipo conoce la clave principal.

La separación de los equipos

El riesgo	Cámaras, impresoras y televisores en la misma red que las computadoras con datos de clientes. Si un equipo débil cae, los demás quedan expuestos.
Tu primer paso	Anota dónde está conectado cada equipo y pide a tu técnico separar redes (lo que los técnicos llaman VLAN) en al menos tres grupos: trabajo, invitados y dispositivos (cámaras, televisores, teléfonos).
Vas bien cuando	El software de taxes y el de cobros no comparten red con las cámaras ni con los invitados.

Los accesos de exempleados y proveedores

El riesgo	Cuentas, claves de Wi-Fi y accesos remotos que siguen activos meses después de que alguien se fue.
Tu primer paso	Haz una lista de exempleados y proveedores anteriores y de lo que usaban. Desactiva o cambia lo que ya no corresponde y define quién lo revisa en cada salida.
Vas bien cuando	Cada salida tiene una lista de cierre firmada por un responsable.

El acceso remoto

El riesgo	Programas de escritorio remoto instalados «para emergencias», sin segunda verificación ni control central. Es una de las vías favoritas del ransomware.
Tu primer paso	Pregunta a tu equipo y a tus proveedores cómo trabajan o dan soporte desde fuera. Distingue las aplicaciones en la nube (correo, software de taxes en línea) del acceso a las computadoras de la oficina, que es el más delicado. Elimina las herramientas que nadie usa y exige verificación en dos pasos en las demás.
Vas bien cuando	Todo acceso remoto pasa por un método administrado, con verificación en dos pasos y un registro de quién entró.

CAPÍTULO 6

Área 2: Administración y seguimiento

No puedes proteger lo que no sabes que tienes. Esta área convierte tu red de «algo que funciona» en algo que conoces y controlas.

El inventario de equipos

El riesgo	Sin lista, nadie sabe qué equipo necesita actualización, cuál es viejo o quién lo instaló.
Tu primer paso	Una hoja de cálculo con seis columnas: equipo, ubicación, marca y modelo, uso, responsable y fecha de última revisión. Usa la Plantilla 1 de esta guía.
Vas bien cuando	La lista existe, está bajo control del negocio y se actualiza cada vez que entra o sale un equipo.

La documentación de la red

El riesgo	Cuando algo falla, se pierden horas averiguando a quién llamar o dónde está el router.
Tu primer paso	Una hoja con contactos del proveedor y del técnico, ubicación de los equipos, fotos de sus etiquetas y los servicios que dependen de Internet (cobros, cámaras, llamadas). Sin contraseñas. Guarda una copia impresa. Usa la Plantilla 2.
Vas bien cuando	Cualquier persona del equipo puede encontrar a quién llamar en menos de cinco minutos.

La detección de equipos desconocidos

El riesgo	Un dispositivo extraño conectado durante semanas sin que nadie lo note.
Tu primer paso	Compara tu inventario con la lista de dispositivos conectados que muestra el router o la app de tu proveedor. Pregunta si puedes recibir un aviso cuando se conecte un equipo nuevo.
Vas bien cuando	Alguien revisa esa lista una vez al mes y sabe qué hacer si aparece algo desconocido.

La administración de la red

El riesgo	Llamar al técnico solo cuando algo se rompe, o dejar la red en manos de un empleado que «sabe de tecnología» pero no tiene tiempo ni función asignada. En ambos casos, nadie revisa entre una falla y otra.
Tu primer paso	Acuerda por escrito qué se revisa cada mes (actualizaciones, accesos, alertas) y quién lo hace. Lleva un registro sencillo de fecha, trabajo realizado y pendientes.
Vas bien cuando	Tienes un calendario de revisiones y un respaldo si tu técnico no está disponible.

La revisión de alertas de la red

El riesgo	El router o la app avisan de algo extraño y nadie lo ve.
Tu primer paso	Confirma qué alertas genera tu equipo y a qué correo llegan. Define cuáles requieren acción inmediata (accesos desconocidos, cambios de configuración) y cuáles pueden esperar.
Vas bien cuando	Cada alerta importante llega a una persona con nombre y apellido.

CAPÍTULO 7

Área 3: Continuidad del negocio

Tarde o temprano la conexión falla o aparece un problema de seguridad. La diferencia entre un mal rato y una semana perdida es tener un plan antes de que ocurra.

La conexión de respaldo

El riesgo	Si se cae Internet, se caen los cobros, las llamadas y las aplicaciones en la nube.
Tu primer paso	Responde dos preguntas: ¿qué tareas no pueden detenerse? y ¿cuántas horas aguanta el negocio sin conexión? Con eso, evalúa un respaldo: un segundo proveedor, un router con conexión celular o, como mínimo, un plan de datos móvil para las computadoras que no pueden parar.
Vas bien cuando	Probaste el respaldo al menos una vez y sabes cuánto tarda en activarse.

La estabilidad de la conexión

El riesgo	Caídas frecuentes que se «arreglan» reiniciando el equipo, sin corregir la causa.
Tu primer paso	Durante dos semanas anota fecha, hora, duración y qué se afectó en cada falla (Plantilla 3). Entrega ese registro a tu proveedor y pide un diagnóstico por escrito.
Vas bien cuando	Las fallas tienen causa identificada y un plan de corrección con fecha.

Cómo responder a problemas de la red

El riesgo	El plan solo existe en la cabeza de una persona. Si no está, nadie sabe qué hacer.
Tu primer paso	Escribe una hoja con cuatro bloques: 1. **A quién llamar:** proveedor de Internet, técnico o ConexPro, banco y aseguradora. 2. **Quién decide:** nombre de la persona que autoriza desconectar equipos o avisar a clientes. 3. **Cómo distinguir:** una caída de Internet (todo deja de cargar) frente a un posible ataque (archivos bloqueados, mensajes de rescate, accesos que nadie reconoce). 4. **Qué hacer primero en un posible ataque:** no apagar ni borrar nada, desconectar del cable o del Wi-Fi el equipo afectado, no pagar rescates y llamar a tu técnico.
Vas bien cuando	La hoja está impresa, accesible sin Internet y el equipo la revisó al menos una vez.

Los respaldos de información

El riesgo	El ransomware cifra también las copias que están conectadas a la misma red.
Tu primer paso	Aplica la regla 3-2-1: tres copias de tus datos, en dos tipos de almacenamiento, una de ellas fuera de la oficina o desconectada. Prueba recuperar un archivo una vez al mes.
Vas bien cuando	Recuperaste un archivo real del respaldo en los últimos 30 días.

CAPÍTULO 8

Tu plan de 4 semanas

Una hora por semana es suficiente para tener tu red en orden en un mes. Este plan retoma las tres áreas que trabajamos anteriormente en la guía: Seguridad y accesos, Administración y seguimiento, y Continuidad del negocio. Empieza la semana en que recibas esta guía y marca cada casilla al completarla.

Semana 1 · Conoce tu red

Área 2 Administración y seguimiento

- □ Haz el inventario de equipos con la plantilla
- □ Anota marca y modelo del router y el contacto de tu proveedor
- □ Compara la lista de dispositivos conectados con tu inventario

Semana 2 · Cierra las puertas

Área 1 Seguridad y accesos

- □ Crea la red de invitados y cambia la clave principal del Wi-Fi
- □ Confirma quién tiene la clave de administración del router
- □ Pide que se actualice el router y se desactive la administración desde Internet

Semana 3 · Revisa las llaves

Área 1 Seguridad y accesos

- □ Lista exempleados y proveedores anteriores y retira sus accesos
- □ Identifica cada herramienta de acceso remoto y activa la verificación en dos pasos
- □ Separa las computadoras con datos de clientes de las cámaras y los invitados

Semana 4 · Prepárate para fallar bien

Área 3 Continuidad del negocio

- □ Escribe tu plan de una página y compártelo con el equipo
- □ Prueba recuperar un archivo del respaldo
- □ Define tu conexión de respaldo y pruébala

Bonus: repite la Evaluación de red al terminar las 4 semanas y compara tu puntaje.

CAPÍTULO 9

Plantillas listas para usar

Tres hojas que puedes imprimir o llenar aquí mismo. Ninguna debe contener contraseñas.

Plantilla 1: Inventario de equipos

Equipo	Ubicación	Marca y modelo	Uso	Responsable	Última revisión
Ej.: Router principal	Oficina, rack	(marca / modelo)	Conexión a Internet	Proveedor X	(fecha)
Ej.: PC con software de taxes	Recepción	(marca / modelo)	Cobros	Gerente	(fecha)

Plantilla 2: Ficha de mi red

Dato	Respuesta
Proveedor de Internet y teléfono de soporte	
Número de cuenta o contrato	
Técnico o empresa de soporte y su alternativa	
Ubicación del módem y del router	
Redes Wi-Fi que existen (nombres, no claves)	
Servicios que dependen de Internet	
Quién tiene la administración del router	
Herramientas de acceso remoto en uso	
Conexión de respaldo y cómo se activa	

Plantilla 3: Registro de fallas e incidentes

Fecha / hora	Qué pasó	Duración	Qué se afectó	A quién se avisó	Acción tomada

CAPÍTULO 10

Mitos y realidades sobre la red de tu negocio

Mito	Realidad
«El router lo puso el proveedor, así que está seguro.»	El proveedor lo instala para que funcione, no siempre para que sea seguro. Pregunta qué protección incluye y quién lo actualiza.
«Si Internet funciona, la red está bien.»	Una red puede funcionar perfecto y tener puertas abiertas. Funcionar no es lo mismo que estar protegida.
«Darle el Wi-Fi a los clientes es buen servicio.»	Lo es, siempre que sea una red de invitados separada. La clave principal es solo para el negocio.
«Mi técnico se encarga de todo.»	Llamar cuando algo falla no es lo mismo que prevenir. Acuerda revisiones periódicas por escrito.
«Reiniciar el router lo arregla.»	Recupera el servicio, pero no corrige la causa. Registra cada falla y pide un diagnóstico.

CAPÍTULO 11

Cómo podemos ayudarte

No tienes que hacerlo todo solo. En ConexPro combinamos telecomunicaciones, TI y ciberseguridad para que tu red funcione bien y esté protegida.

1 **Evaluación de red gratuita**
18 preguntas, unos 5 minutos. Recibes tu puntaje de 0 a 100 y un informe con recomendaciones en las mismas tres áreas de esta guía.

2 **Revisión de resultados**
Un especialista revisa tu informe contigo y te dice qué atender primero.

3 **Implementación guiada**
Separación de redes, Wi-Fi de invitados, firewall administrado, acceso remoto seguro y conexión de respaldo.

4 **Monitoreo y soporte continuo**
Revisiones periódicas para que tu red no dependa de que algo se rompa.

OFERTA PARA LECTORES DE ESTA GUÍA

Completa tu Evaluación de red y recibe una revisión de resultados sin costo con un especialista.

Haz tu Evaluación de red

¿Prefieres hablar con alguien? Escríbenos **RED** por Instagram o WhatsApp.

CAPÍTULO 12

Conclusión

Tu red es la base de todo lo que haces en línea. No necesitas ser técnico para protegerla: necesitas saber qué tienes, quién lo controla y qué hacer cuando algo falla.

Empieza con una hora esta semana, sigue el plan de cuatro semanas y mide tu avance repitiendo la Evaluación de red. Al terminar, tu negocio no solo tendrá Internet: tendrá una red.

¡Actúa hoy y da el siguiente paso hacia un negocio más seguro!

ConexPro

www.conexpro.net · +1 346 413 8825 · info@conexpro.net
32607 FM2978 PMB 1, Magnolia, TX 77354

Fuentes de las cifras: Verizon Data Breach Investigations Report 2026; Mandiant M-Trends 2026; Hiscox Cyber Readiness Report 2026; Sophos State of Ransomware 2026.