TRANSFORMATION TRENDS

Glosario de ciberseguridad para PyMEs

Cada término en dos frases: qué es, y por qué le importa a tu negocio. La segunda es la que casi nunca te explican.

25 términos · septiembre de 2026
transformationtrends.com/glosario

Tu correo

Tu dirección de correo es la identidad de tu empresa frente a clientes y proveedores. Estos cuatro registros son los que impiden que alguien la use en tu nombre.

SPF

Una lista publicada en tu dominio que dice qué servidores tienen permiso de enviar correo a nombre tuyo.

Por qué te importa: Sin ella, cualquier servidor del mundo puede mandar correos que digan venir de tu empresa, y el de tu cliente no tiene forma de notar la diferencia.

DKIM

Una firma invisible que tu servidor le pone a cada correo que sale, y que el servidor que lo recibe puede comprobar.

Por qué te importa: Es lo que demuestra que el mensaje salió de ti y que nadie lo modificó en el camino. Sin firma, tus correos legítimos también tienen más probabilidad de caer en spam.

DMARC

Una regla que le dice a los servidores de correo qué hacer con los mensajes que dicen venir de tu dominio pero no pasan las comprobaciones de SPF y DKIM.

Por qué te importa: Sin ella, alguien puede mandar facturas falsas a nombre de tu empresa y tú ni te enteras. Con ella, esos correos se rechazan antes de llegar a tu cliente.

Spoofing (suplantación)

Falsificar el remitente de un correo para que parezca que lo mandó una persona o una empresa de confianza.

Por qué te importa: Es la técnica detrás del fraude de factura: llega un correo que parece tuyo, con tus datos, pidiendo que depositen a otra cuenta. Lo que lo frena es DMARC.

Phishing

Un mensaje diseñado para que alguien entregue una contraseña, haga un pago o abra un archivo, creyendo que se lo pide alguien de confianza.

Por qué te importa: Es la puerta de entrada más común, y no depende de tu tecnología sino de tu equipo. Por eso se entrena a la gente, no sólo se configuran servidores.

Tu sitio web

Tu sitio es la cara pública de tu negocio y, casi siempre, lo primero que alguien revisa desde afuera.

SSL / HTTPS

El candado del navegador: cifra lo que viaja entre tu sitio y quien lo visita, para que nadie en medio pueda leerlo.

Por qué te importa: Si el certificado vence, tu visitante ve una pantalla roja de advertencia antes de entrar. Muchas ventas se pierden ahí, sin que nadie te avise.

Cloaking

Cuando un sitio le muestra una cosa a Google y otra distinta a las personas.

Por qué te importa: Es la señal clásica de que alguien metió contenido ajeno en tu sitio. Tú lo abres y lo ves normal; Google ve otra cosa y te puede sacar de los resultados.

Malware

Cualquier programa metido en un sistema para hacer algo que su dueño no autorizó.

Por qué te importa: En un sitio web casi nunca se nota por dentro: se nota porque Google lo marca como peligroso, o porque tus clientes empiezan a reportar cosas raras.

Hardening (endurecimiento)

Cerrar todo lo que un sistema trae abierto de fábrica y no necesitas.

Por qué te importa: La mayoría de los servidores llegan configurados para que todo funcione fácil, no para que sea difícil entrar. Endurecer es la diferencia entre las dos cosas.

WAF / firewall

Un filtro delante de tu sitio que bloquea peticiones con pinta de ataque antes de que lleguen a tu servidor.

Por qué te importa: Te da tiempo. No arregla la falla de fondo, pero frena los intentos automáticos mientras tú actualizas lo que haya que actualizar.

CMS

El programa con el que se administra un sitio sin programar. WordPress es el más común.

Por qué te importa: Hace fácil publicar, y también hace que tu sitio se parezca a millones de otros. Quien busca sitios vulnerables busca versiones, no empresas.

Plugin (complemento)

Un pedazo de software de terceros que le agrega funciones a tu CMS: formularios, tienda, galerías.

Por qué te importa: Cada uno es código de alguien más corriendo dentro de tu sitio. La mayoría de los sitios comprometidos lo fueron por un complemento sin actualizar, no por el CMS.

Tus datos y la ley

Si guardas datos de clientes, empleados o proveedores, en México tienes obligaciones concretas.

LFPDPPP

La Ley Federal de Protección de Datos Personales en Posesión de los Particulares: la ley mexicana que regula cómo las empresas privadas pueden tratar datos personales. La versión vigente se publicó el 20 de marzo de 2025 y sustituyó a la de 2010.

Por qué te importa: Aplica a cualquier empresa que guarde datos de personas, sin importar su tamaño. Con la ley de 2025 la autoridad dejó de ser el INAI y pasó a la Secretaría Anticorrupción y Buen Gobierno.

Aviso de privacidad

El documento donde le dices a una persona qué datos suyos vas a recabar, para qué, y cómo puede pedirte que los corrijas o los borres.

Por qué te importa: Es obligatorio en México y tiene que estar disponible en el momento en que pides el dato, no escondido en el pie de página. Un formulario sin aviso es un dato recabado sin base.

Fuga de datos

Cuando información que debía estar resguardada acaba publicada o en manos de alguien más.

Por qué te importa: Casi nunca empieza en tu empresa: empieza en otra donde tu gente se registró con el correo del trabajo. Por eso esas listas se revisan aunque tú no hayas tenido ningún incidente.

Respaldo (backup)

Una copia de tu información guardada en otro lado, que puedes restaurar si la original se pierde.

Por qué te importa: Un respaldo que nadie ha probado a restaurar no es un respaldo, es una esperanza. La prueba de restauración es la parte que casi siempre falta.

RGPD / GDPR

El reglamento europeo de protección de datos, la referencia mundial en la materia.

Por qué te importa: Te toca si tienes clientes o usuarios en Europa, aunque tu empresa esté sólo en México. Y muchos clientes grandes piden ese nivel aunque la ley no los obligue.

Lo que puede pasar

Cuatro términos que vas a oír cuando alguien te hable de riesgo, explicados sin dramatismo.

Ransomware

Un programa que cifra tus archivos y pide dinero a cambio de devolvértelos.

Por qué te importa: Lo que decide si tumba tu operación o no es tu respaldo, no tu antivirus. Con una copia reciente y probada, dejas de tener que negociar.

Pentest (prueba de intrusión)

Un ejercicio autorizado en el que alguien intenta entrar a tus sistemas para mostrarte por dónde se puede.

Por qué te importa: Es distinto de un análisis externo como Ciber-Scan: el análisis mira lo que está expuesto sin tocar nada, el pentest sí intenta aprovecharlo y necesita permiso por escrito.

Vulnerabilidad

Una falla conocida en un programa que permite hacer algo que no debería poder hacerse.

Por qué te importa: Se publican en catálogos abiertos, con versión y fecha. Eso significa que quien busca sitios vulnerables ya tiene la lista: lo que te protege es ir por delante de ella.

Parche (actualización)

La corrección que publica el autor de un programa para cerrar una falla.

Por qué te importa: Entre que se publica el parche y que tú lo aplicas hay una ventana, y esa ventana es cuando ocurren los ataques automáticos. Actualizar rápido es casi todo el trabajo.

Cómo se gestiona

Los marcos y conceptos con los que se ordena todo lo anterior y se demuestra ante un cliente o una licitación.

ISO/IEC 27001

El estándar internacional para gestionar la seguridad de la información: no es una lista de productos, es una forma de decidir qué proteger y comprobar que lo estás haciendo.

Por qué te importa: Cada vez más clientes grandes y licitaciones lo piden como requisito para contratar. Tener la ruta empezada te abre puertas que no se abren de otra forma.

ISO/IEC 42001

El estándar equivalente, pero para sistemas de gestión de inteligencia artificial.

Por qué te importa: Si tu empresa ya usa IA para trabajar, es el marco con el que se demuestra que la usa de forma responsable y trazable. Es reciente y hoy es un diferenciador.

Continuidad del negocio

El plan que define cómo sigues operando cuando algo falla: un servidor, un proveedor, un sistema.

Por qué te importa: Convierte una crisis en un procedimiento. La pregunta útil no es si algo va a fallar, sino cuánto tiempo puedes estar sin eso antes de que te duela.

Riesgo residual

El riesgo que queda después de haber aplicado todo lo que decidiste aplicar.

Por qué te importa: Nunca llega a cero, y ese es el punto: se trata de decidir a conciencia cuánto aceptas, no de aspirar a eliminarlo. Un riesgo aceptado por escrito se gestiona; uno ignorado, no.

¿Cuáles de estos te aplican hoy?

Ciber-Scan revisa tu dominio desde afuera y te dice cuáles de estos puntos están abiertos en tu negocio. Es gratis y no instala nada en tu sitio.

ciberscan.transformationtrends.com