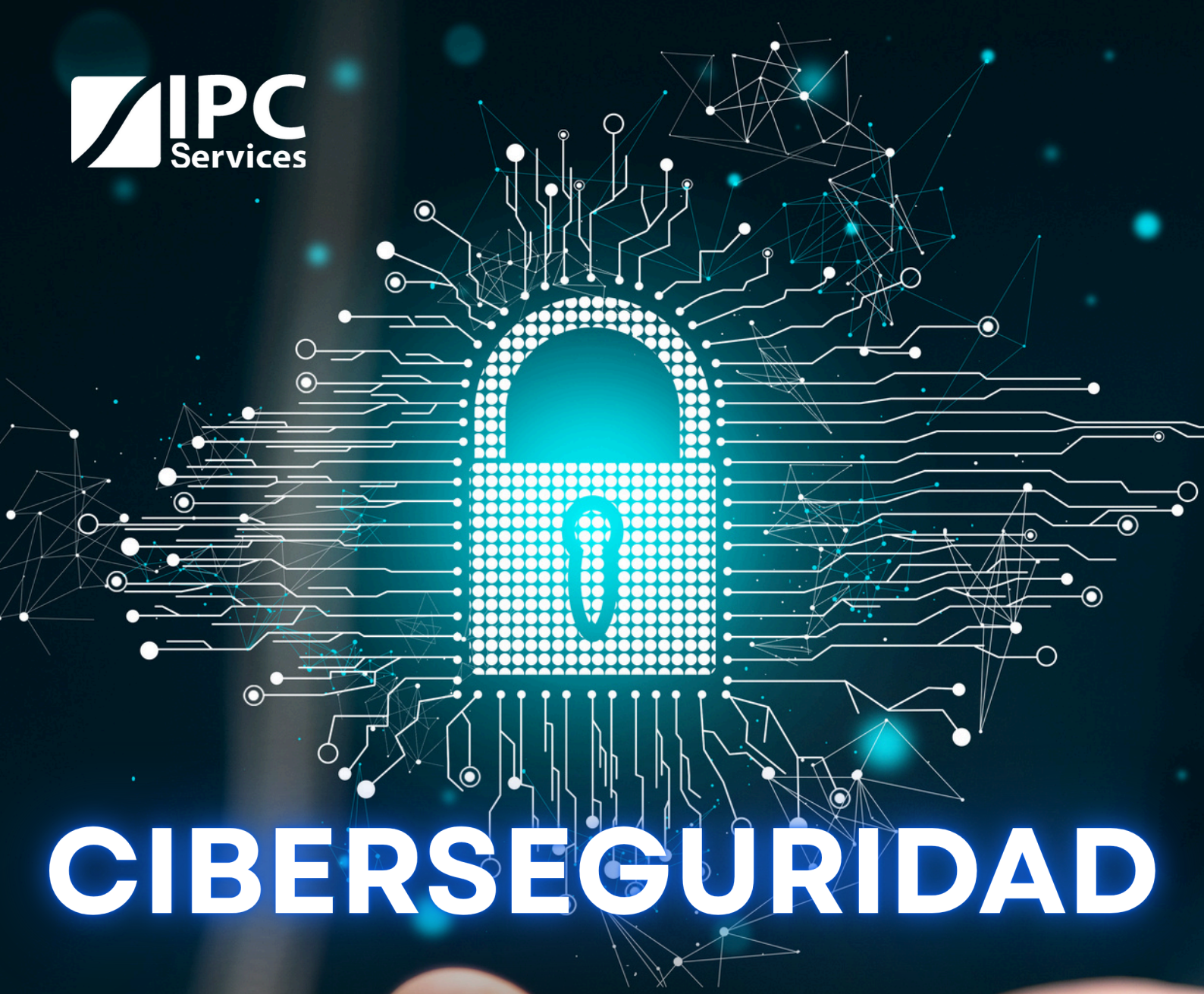
IPC Services



CIBERSEGURIDAD

Mapa de riesgos para el 2026

Cómo **neutralizar** la amenaza de la Inteligencia Artificial maliciosa en el **2026**

Contenido

¿TU EMPRESA CUENTA CON UNA ESTRATEGIA DE CIBERSEGURIDAD?

Introducción: La Ciberseguridad como Pilar Estratégico del Negocio

IPC Services

Introducción: La Ciberseguridad como Pilar Estratégico del Negocio

CONOCE A TU ENEMIGO

La ciberseguridad ha trascendido su tradicional rol técnico para consolidarse como un pilar para el éxito y la viabilidad económica de las empresas en la era digital.

La creciente dependencia tecnológica, junto con el aumento exponencial de las amenazas, ha evidenciado que una estrategia de seguridad robusta no es un lujo, sino una necesidad para proteger, no solo la información sensible, sino también la reputación y la continuidad del negocio.

El antiguo principio de Sun Tzu, "Conócete a ti mismo y conoce a tu enemigo", cobra vigencia en el contexto empresarial actual. "Conocerse a sí mismo" implica comprender a fondo la propia infraestructura, identificar vulnerabilidades y priorizar la protección de activos críticos. "Conocer al enemigo" exige estudiar las tácticas y técnicas de los ciberdelincuentes, quienes persiguen la información que se ha convertido en "el nuevo oro del siglo XXI".

Ante un panorama de amenazas en constante evolución, la prevención, detección y respuesta efectiva ya no son opcionales. Ignorarlos puede acarrear consecuencias devastadoras, desde pérdidas financieras directas hasta daños irreparables a la reputación corporativa.

Este informe ofrece un análisis de las tendencias que definieron el panorama de amenazas en 2025, los riesgos de negocio derivados y las soluciones estratégicas que las organizaciones deben adoptar para fortalecer su resiliencia de cara a 2026. A continuación, se desglosa el panorama de amenazas que marcará el próximo año.

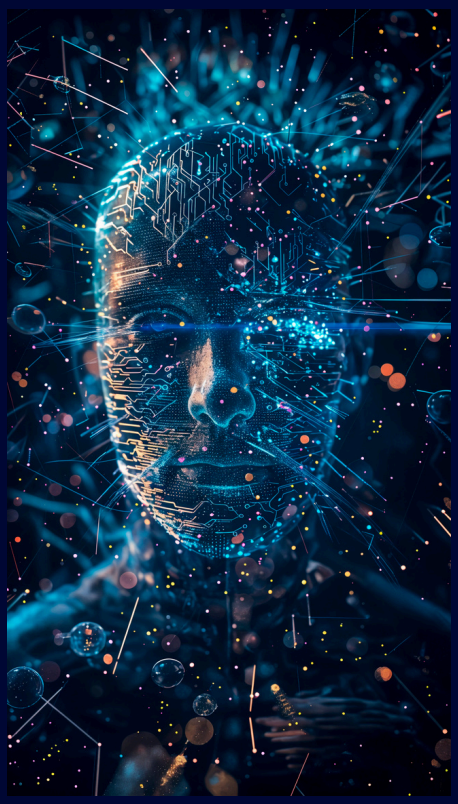
La ciberseguridad dejó de ser un asunto técnico: hoy es una condición de supervivencia empresarial.

El Panorama de Amenazas en el 2025

El panorama de amenazas cibernéticas se ha vuelto más complejo y dinámico que nunca, impulsado por una sofisticación tecnológica sin precedentes y una diversificación de los actores maliciosos. Desde grupos patrocinados por estados hasta ciberdelincuentes con motivaciones puramente económicas; las tácticas evolucionan a un ritmo vertiginoso. Esta sección desglosa las amenazas más críticas que las empresas enfrentaron en 2025.

LA INTELIGENCIA ARTIFICIAL GENERATIVA: UN ARMA DE DOBLE FILO

La inteligencia artificial (IA) generativa se ha consolidado como una de las tendencias de mayor impacto, actuando como un arma de doble filo. Mientras que las organizaciones la aprovechan para mejorar sus capacidades de defensa, los ciberdelincuentes la utilizan para automatizar y sofisticar sus ataques.



El Panorama de Amenazas en el 2025

ÁREAS EN LAS QUE SE INTENSIFICÓ EL USO MALICIOSO DE LA IA EN 2025:

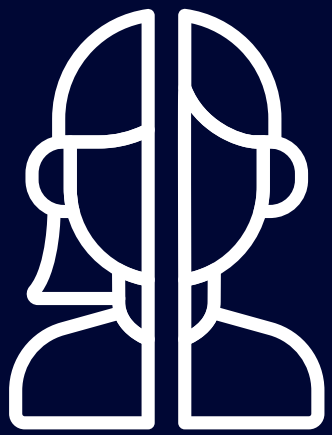
Spear-Phishing Avanzado:

La IA permite la creación automatizada de correos electrónicos y mensajes altamente personalizados y convincentes. Al analizar datos públicos y privados, estas herramientas pueden imitar a la perfección el tono y estilo de comunicación de una persona o entidad, haciendo que los mensajes fraudulentos sean casi indistinguibles de los reales y aumentando drásticamente la probabilidad de éxito del ataque.

Falsificación de Identidades (Deepfakes):

El uso de videos y audios falsos para suplantar a individuos está en auge. Los deepfakes se utilizan para cometer fraudes sofisticados, como la "estafa del CEO", donde se imita la voz de un alto ejecutivo para autorizar transferencias de fondos, o para llevar a cabo campañas de extorsión. Los riesgos empresariales más significativos de esta tecnología son el daño irreparable a la reputación de la marca y las pérdidas financieras directas.

> **Desde grupos patrocinados por estados hasta ciberdelincuentes con motivaciones puramente económicas, las tácticas evolucionan a un ritmo vertiginoso.**



El Panorama de Amenazas en el 2025

- **Creación y Automatización de Malware:** La IA generativa facilita la escritura de código malicioso polimórfico y ofuscado, capaz de evadir los controles de seguridad tradicionales. Esto no solo aumenta la sofisticación del malware, sino que también reduce las barreras técnicas para los ciberdelincuentes menos experimentados, lo que incrementa la escala y la velocidad de los ataques.
- **Propagación de Desinformación:** La capacidad de la IA para crear contenido falso (texto, imágenes y videos) de manera masiva y convincente se utiliza para manipular la opinión pública, socavar la confianza en las instituciones y afectar negativamente la reputación de las marcas a través de campañas de desprestigio.

IMPERATIVO ESTRATÉGICO:

La IA no solo automatiza ataques, sino que erosiona la confianza en las comunicaciones digitales.

Las defensas deben evolucionar para validar la autenticidad de las interacciones, no solo para detectar firmas de malware.

Vulnerabilidades y Riesgos Derivados del Negocio

01 | EL ANÁLISIS DE RIESGOS DEBE TRASCENDER LA TECNOLOGÍA.

La amenaza más probable no es una vulnerabilidad de software compleja, sino la confianza de un empleado. El verdadero impacto en el negocio se materializa a través de las vulnerabilidades organizativas, humanas y de procesos.

Esta sección evalúa los principales factores de riesgo que las empresas deben gestionar de forma prioritaria para construir una defensa sólida.

Las amenazas internas provocan el 43% de las brechas de seguridad, ya sea por sabotaje, negligencia o falta de concienciación sobre las políticas de seguridad.

La ingeniería social está directamente involucrada en aproximadamente el 98% de los ciberataques.

El error humano es la causa raíz del 95% de los problemas de seguridad.

02 | EL FACTOR HUMANO: LA PRIMERA LÍNEA DE DEFENSA Y EL ESLABÓN MÁS DÉBIL

A pesar de los avances tecnológicos, el ser humano sigue siendo el principal objetivo de los ciberdelincuentes y, a menudo, la principal causa de las brechas de seguridad. La falta de una cultura de ciberseguridad sólida es una vulnerabilidad crítica subyacente.

Vulnerabilidades y Riesgos de Negocio Derivados

03 | LA EXPANSIÓN DE LA SUPERFICIE DE ATAQUE DIGITAL

La transformación digital, si bien ha sido un motor de innovación y eficiencia, también ha creado una "superficie de ataque" más amplia y difícil de proteger.

Las brechas en la nube suelen originarse por configuraciones incorrectas y una mala comprensión de la responsabilidad compartida.

El trabajo remoto y el uso de dispositivos personales elevan el riesgo al operar fuera del control de la empresa.

La rápida expansión de IoT y 5G aumenta los puntos vulnerables debido a dispositivos poco seguros y una red más abierta.

La IA introduce retos legales y éticos aún sin regulación clara: responsabilidad de decisiones autónomas, privacidad de datos, sesgos algorítmicos y propiedad intelectual del contenido generado.

La inversión en tecnología de seguridad es ineficaz sin una inversión paralela en la cultura de seguridad.

Exige la verificación constante y explícita de la seguridad para hacer negocios.

04 | RIESGOS DE TERCEROS Y DEPENDENCIAS EN LA CADENA DE SUMINISTRO

La falta de visibilidad y control sobre las prácticas de seguridad de los proveedores convierte sus vulnerabilidades en un riesgo directo e inmediato para la propia empresa. El riesgo de terceros ha sido identificado por el 49% de las organizaciones como una de sus principales preocupaciones para 2025.

Soluciones Estratégicas y Perspectiva para 2026

Para analizar el complejo panorama de 2025 y construir una postura de seguridad resiliente para 2026, las empresas deben abandonar los enfoques reactivos y adoptar una estrategia proactiva y multifacética.

La ciberseguridad ya no es un problema exclusivo del departamento de TI; es una responsabilidad de negocio que requiere una integración profunda de estrategia, cultura y tecnología.

Los siguientes cuatro pilares constituyen la base de una estrategia de ciberseguridad moderna y eficaz.

PILAR 1: ADOPTAR UNA ARQUITECTURA DE CONFIANZA CERO

El modelo de seguridad tradicional quedó obsoleto. Zero Trust lo está reemplazando con la regla “nunca confiar, siempre verificar”.

Esta arquitectura limita el movimiento lateral y responde a amenazas como ataques a la cadena de suministro, amenazas internas y ransomware.

Zero Trust se basa en microsegmentación, mínimo privilegio y autenticación multifactor. Por ello, el 97% de las empresas lo prioriza como estrategia clave contra el ransomware.

PILAR 2: CONSTRUIR UNA CULTURA DE CIBER-RESILIENCIA ORGANIZACIONAL

La tecnología por sí sola no es suficiente. La ciberresiliencia, definida como la capacidad de una organización para mantener su propósito frente a un ciberataque y recuperarse rápidamente, es un objetivo organizacional que debe cultivarse activamente:

GOBERNANZA Y LIDERAZGO:

La ciberseguridad debe ser una prioridad estratégica para la alta dirección. Actualmente, el 70% de las juntas directivas ya tienen alguna forma de supervisión de ciberseguridad, y el 50% de las organizaciones reportan trimestralmente a la junta sobre los riesgos cibernéticos, una tendencia que demuestra su creciente importancia ejecutiva.

EL EMPLEADO COMO SENSOR HUMANO:

Es necesario ir más allá de la formación básica anual. Las organizaciones deben implementar programas continuos de concienciación que incluyan simulaciones de phishing y ejercicios prácticos para transformar el comportamiento de los empleados y convertirlos en una primera línea de defensa activa.

PLANIFICACIÓN DE RESPUESTA A INCIDENTES Y CONTINUIDAD DE NEGOCIO:

La pregunta no es si ocurrirá un incidente, sino cuándo. Contar con planes de respuesta a incidentes y de continuidad de negocio probados y actualizados regularmente es crucial para minimizar el impacto de un ataque y garantizar la reanudación de las operaciones.

Soluciones Estratégicas y Perspectiva para 2026

PILAR 3: APROVECHAR LA TECNOLOGÍA PARA UNA DEFENSA PROACTIVA

La innovación tecnológica es un aliado indispensable en la lucha contra el cibercrimen. Las empresas deben invertir en herramientas avanzadas que les permitan pasar de una postura defensiva a una proactiva.

La misma IA que utilizan los atacantes puede ser un poderoso aliado para la defensa. Se emplea para la detección de anomalías en tiempo real, la propuesta de respuestas automatizadas en los centros de operaciones de seguridad y el análisis forense para acelerar la investigación de incidentes.

La seguridad de datos (DLP) protege información sensible en endpoints, red, nube y email mediante controles segmentados.

Un SGSI ayuda a establecer políticas y evaluar riesgos. La implementación de marcos de referencia reconocidos, permite a las organizaciones gestionar la seguridad de una forma estructurada, continua y auditable.

PILAR 4: INVERSIÓN ESTRATÉGICA Y PLANIFICACIÓN

La planificación debe basarse en una evaluación realista del riesgo y del potencial impacto de un incidente.

Como referencia, el presupuesto de ciberseguridad en las PYMES suele situarse entre el 5% y el 10% del presupuesto total de las tecnologías de la información.

La combinación estratégica de una arquitectura Zero Trust, una cultura de resiliencia, tecnología proactiva y una inversión bien planificada es la clave para navegar con seguridad en el complejo entorno digital del futuro.

El 93% de las empresas consideran la inteligencia artificial como una prioridad de inversión.

ESCRITO POR IPC SERVICES

Conclusión: Preparación para un Futuro Digital Interconectado y Complejo

WWW.IPCSERVICES.MX

Conclusión: Preparación para un Futuro Digital Interconectado y Complejo

El análisis presentado reafirma que 2025 estuvo marcado por una creciente sofisticación de las amenazas impulsadas por inteligencia artificial, una mayor exposición a través de las cadenas de suministro y una presión regulatoria cada vez más estricta.

Los ciberdelincuentes continuarán innovando, explotando tanto las vulnerabilidades tecnológicas como el factor humano para alcanzar sus objetivos.

En este contexto, la respuesta para 2026 no puede ser puramente tecnológica. Las empresas que prosperarán serán aquellas que adopten un enfoque sistémico, integrando la ciberseguridad en su estrategia de negocio, fomentando una cultura de resiliencia que involucre a todos los niveles de la organización y aprovechando la tecnología, no solo para defenderse, sino para anticiparse a las amenazas.

Además, al mirar al futuro, las organizaciones deben comenzar a monitorear el impacto de tecnologías emergentes como la computación cuántica en la criptografía actual (PQC).

Este desarrollo representa un cambio que podría dejar obsoletos los métodos de cifrado actuales, lo que subraya la necesidad de una vigilancia tecnológica continua y una planificación a largo plazo. Por tanto, es imperativo que las empresas adopten un enfoque proactivo, colaborativo y resiliente para fortalecer sus defensas digitales y proteger su patrimonio en un entorno cada vez más complejo y sofisticado.

Anticipar amenazas es la verdadera ventaja competitiva.

Sobre IPC

En IPC Services nos especializamos en proteger lo más valioso de las organizaciones: su información, su continuidad operativa y su reputación.

Somos una firma de consultoría en ciberseguridad enfocada en grandes corporativos, empresas altamente reguladas y entornos tecnológicos críticos.

> **Protegemos la infraestructura digital de las empresas que lideran el futuro**

CONSULTORÍA DE CIBERSEGURIDAD PARA EMPRESAS

Más de 25 años integrando tecnología, ciberseguridad e infraestructura para empresas que buscan eficiencia operativa, conectividad segura y continuidad de negocio.

www.ipcservices.mx
ventas@ipcservices.net

811352-2600