empresas

Guía completa de aspectos básicos de ciberseguridad en las empresas

Índice

INTRODUCCIÓN

Durante los últimos años el mundo ha sido testigo de un acelerado desarrollo tecnológico. La aparición y masificación de Internet -y de los dispositivos móviles- configuraron una nueva sociedad, una en la que la inmediatez y la conectividad se convirtieron en las bases del cotidiano.

En la actualidad se estima que existen cerca de **4.540 millones de internautas** -7% más que en 2019- lo que representa casi un 60% de la población global. Este dato permite entender el impacto que ha tenido Internet en la sociedad, posicionando el entorno digital como la base de diversos procesos cotidianos.

En ese sentido, vale la pena revisar algunas interesantes cifras que dan cuenta de cómo Internet se ha convertido en uno de los grandes pilares de la sociedad moderna:

6:30 HORAS DIARIAS — **27% DEL DÍA CONECTADO**

Promedio que pasa un internauta en la Web.

81% — **COMPRADORES MINORISTAS**

Realizan una investigación online antes de concretar la compra.

42% — **DE LA POBLACIÓN MUNDIAL UTILIZA LAS REDES SOCIALES**

54% — **De este grupo se vale de estas plataformas para investigar productos.**

86% — **DE LAS PERSONAS**

Utiliza Google Maps para encontrar la ubicación de una empresa.

40% — **DE LAS TRANSACCIONES ONLINE**

Se realizan a través de un dispositivo móvil.

95% — **DE LAS COMPRAS A NIVEL GLOBAL**

Se realizarían vía eCommerce para el 2040, según estimaciones.

Resulta evidente la importancia de la economía digital, el la cual los diversos actores del mercado utilizan la tecnología como base para la realización de sus procesos. Por ejemplo, durante 2017, la economía digital **constituyó el 30% de la expansión general de los Estados Unidos.**

¿Y a nivel local? Un estudio realizado por Accenture y Oxford Economics determinó que **la economía digital representa el 22,2% del Producto Interno Bruto** (PIB), cifra equivalente a unos US$55 mil millones.

Estos datos permiten graficar la importancia del entorno digital en la sociedad actual, más aún en la economía, entendiendo que las empresas se valen de Internet para -por ejemplo- realizar transacciones, alojar archivos y documentos, contactar a proveedores, seleccionar y reclutar personal y emitir facturas.

Lo anterior nos lleva a un punto de vital importancia para las empresas: **la protección de su información de valor.** Contraseñas, datos de los clientes, documentos e información financiera constituyen algunos ejemplos de lo que se alza como uno de los activos más valiosos para las organizaciones, por lo que su protección representa un asunto de carácter estratégico.

1. CIBERSEGURIDAD:
LOS DATOS QUE DEBES CONOCER

Aunque el entorno digital ofrece beneficios como agilidad en los procesos, mayor conectividad y rápido acceso a la información, también supone riesgos que las empresas deben considerar para evitar daños que pudieran comprometer sus operaciones.

Los siguientes datos reflejan la importancia de la ciberseguridad para el ecosistema empresarial:

62% DE LAS EMPRESAS DURANTE 2018

Fue víctima de phising (suplantación de identidad) y ataques de ingeniería social (manipulación).

+4,1 MIL MILLONES DE REGISTROS

Fueron expuestos el primer semestre de 2019 producto de la vulneración de datos.

-50% DE LAS EMPRESAS DEL MUNDO

Están preparadas para hacer frente a ciberataques.

1,6 MILLONES DE DÓLARES POR EMPRESA

Fue el costo de cada ciberataque durante 2018.

VULNERACIONES DE SEGURIDAD:

67% AUMENTO ENTRE 2014 Y 2019.

11% AUMENTO ENTRE 2018 Y 2019.

Un ciberataque puede ser nefasto para las organizaciones, especialmente considerando que -durante 2019- **identificar una brecha de seguridad demoró 206 días** (¡casi 7 meses!), y que el ciclo de vida promedio de cada incidente fue de 314 días desde su detección hasta su contención.

A nivel regional -y según un informe de Kaspersky-, entre julio de 2018 y julio de 2019 se registraron **45 intentos de ciberataques por segundo**, posicionando a Brasil como el país más atacado de Latinoamérica.

Por otro lado, un informe de la multinacional VU Security reveló que **45% de las empresas de la región sufrió un intento de ciberataque entre 2017 y 2019.** De estos, el phishing se posicionó como la modalidad más utilizada (51,9%), seguido por el malware (49,1%) y el ransomware (38%).

¿Cuál es la situación de Chile?

Durante 2019, en el país se registraron **más de 1,5 billones de intentos de ciberataques,** y su principal objetivo fue el sector de la banca. Esta cifra equivale a más de 4 millones de intentos diarios, dando cuenta de la envergadura de los riesgos presentes en el entorno digital.

Al respecto, el informe **"Ciberseguridad en las Empresas Chilenas"** -encargado por Microsoft a la consultora Ipsos- refleja cómo está la seguridad informática en el país:

4 DE CADA 10 EMPRESAS

Ha sido víctima de un ciberataque.

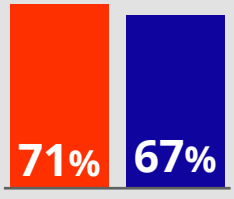
DE LAS EMPRESAS

Afirma tener la cantidad de personas suficientes para enfrentar un ciberataque.

LA ADQUISICIÓN DE SOFTWARE COMO ANTIVIRUS O FIREWALL

Se alza como la principal medida de protección ante este tipo de amenazas.

PRINCIPALES PREOCUPACIONES:



- Fuga de información.
- Eventual interrupción de la continuidad operacional.

Además, se estima que un **41% de las empresas chilenas no cuenta con políticas de ciberseguridad** o no las ha comunicado a sus trabajadores, evidenciando una profunda falta de cultura en la materia.

1.1. Pymes y ciberseguridad

Uno de los grandes errores en materia de ciberseguridad es creer que solo las grandes empresas pueden resultar afectadas. ¿Sabías que el **43% de los ataques informáticos son dirigidos a las pequeñas empresas**? Esto se explica, entre otras cosas, por la falta de recursos y de conocimiento sobre el tema, convirtiendo a las Pymes en un blanco fácil para las amenazas propias del entorno digital.

Estas entidades suelen ser parte de la cadena de suministro de las grandes compañías y, al ser vulnerables, constituyen el camino ideal para llegar a las entidades de mayor envergadura. Esto, desde luego, afecta la continuidad operativa y puede tener un impacto en las relaciones empresariales, siendo imprescindible adoptar los resguardos pertinentes.

Se estima que el 60% de las pequeñas y medianas empresas deja de operar **a los 6 meses de haber sufrido una vulneración informática.** Esto, además del factor económico, se explica por la pérdida de confianza con proveedores y clientes, indispensable en el mundo de los negocios.

Prevención: la base de una estrategia de ciberseguridad efectiva

Anticiparse a las amenazas constituye el camino más eficiente para disminuir los riesgos de un eventual ciberataque. En ese sentido, el primer paso para adoptar medidas de ciberseguridad en una empresa es **evaluar el nivel de riesgo de la red.**

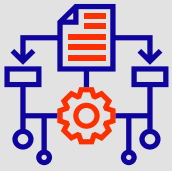
> Este análisis permite conocer el nivel de exposición de una empresa ante las amenazas informáticas, dando claridad a los tomadores de decisiones respecto a qué procesos seguir, qué soluciones tecnológicas adoptar, qué cargos se deben incorporar (en el mejor de los casos, crear un departamento TI) y cómo construir una cultura en ciberseguridad eficaz.

2. LA ESTRUCTURA ORGANIZACIONAL DE CIBERSEGURIDAD QUE LAS EMPRESAS NECESITAN

Entendiendo la importancia de proteger información, redes y sistemas, hay algunos perfiles de carácter estratégico que toda organización debería considerar, y que tienen a su cargo el resto de la estructura corporativa en materia de ciberseguridad:

CSO (Chief Security Officer)

Se trata del máximo cargo en lo que a seguridad corporativa respecta, incluyendo el área tecnológica. Puesto que se relaciona directamente con el CEO, debe mantenerse al tanto de las normativas y tendencias en lo que a seguridad respecta, ya que debe poseer una mirada macro del negocio y conocer las implicancias de cualquier movimiento en los protocolos.



CISO (Chief Information Security Officer)

Se trata del director de seguridad de la información, caro ejecutivo que depende y reporta directamente al CSO. En sus manos está la seguridad de los datos de la empresa, por lo que debe monitorear -en tiempo real- amenazas y riesgos con base en los activos y políticas de ciberseguridad de la empresa.

Toda organización que desee proteger sus datos, redes y sistemas debería contar con una estructura organizacional que permita abordar las necesidades empresariales en la materia desde etapas tempranas y, aunque ello depende de factores como tamaño y rubro de la empresa, el **Centro Canadiense de Ciberseguridad** **ha propuesto la siguiente estructura organizacional** en lo que a ciberseguridad respecta:

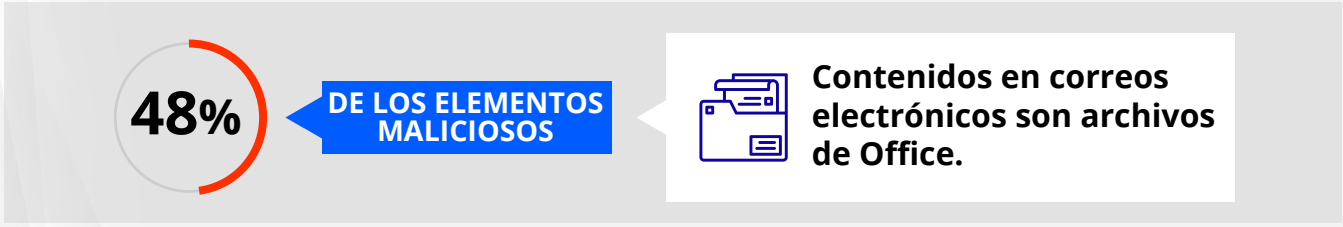
Cargo	Responsabilidades	Conocimientos requeridos	Puestos relacionados
Planificador estratégico	Desarrollo, implementación y evaluación de estrategias de ciberseguridad, alineadas con los objetivos organizacionales.	Especialización en seguridad informática.	• Coordinador de seguridad de TI. • Analista o gerente de seguridad.
Analista de políticas de seguridad	Análisis y desarrollo de políticas de seguridad, definiendo roles, responsabilidades, mecanismos de acción, monitoreo y evaluación de KPIs.	Administración de empresas o similares, idealmente con experiencia en área TI.	• Desarrollador de políticas de seguridad. • Asesor de seguridad.
Analista de requisitos	Evaluación de la efectividad de los controles de ciberseguridad, recomienda soluciones para falencias y deficiencias identificadas.	Especialización en seguridad informática, siempre interiorizado con las TI.	• Analista o gerente de seguridad.
Administrador del programa de seguridad	Garantizar la integración del programa de seguridad con otros protocolos organizacionales. Desarrollo, supervisión, monitoreo y evaluación del programa.	Especialización en seguridad informática.	• Gerente o coordinador de seguridad. • Gerente de seguridad de sistemas.
Autorizador del sistema	Verificar que los sistemas TI se ajusten a los requerimientos de seguridad de la empresa. Autoriza la utilización de determinados sistemas.	Experiencia en gestión de programas, deseable en control de riesgos.	• Director de información.
Planificador de recuperación de desastres	Desarrolla y evalúa el plan de recuperación de desastres, garantizando resistencia y continuidad operativa del sistema.	Especialización en seguridad informática.	• Gerente de continuidad TI. • Coordinador de continuidad comercial. • Coordinador de gestión de incidentes.
Asesor de seguridad de contratación y adquisiciones	Identificar requisitos de seguridad en relación con los bienes o servicios a adquirir. Revisión de cláusulas en contratos asociados a TI, garantizando su cumplimiento.	Especialización en seguridad informática.	• Analista de seguridad. • Gerente de proyectos. • Gestión de proveedores.

Desde luego, cada empresa debe evaluar la estructura organizacional de ciberseguridad más adecuada para sus condiciones y requerimientos. De los cargos anteriormente señalados se desprenden tareas concretas como **evaluación de vulnerabilidades y pruebas de penetración,** las cuales suelen recaer en un hacker ético.

Sin embargo, más allá de la estructura organizacional adecuada en materia de seguridad informática, hay un punto que constituye una responsabilidad transversal para toda la compañía: adoptar una cultura en ciberseguridad. Al hacerlo, es posible optimizar los esfuerzos y disminuir los factores de riesgo.

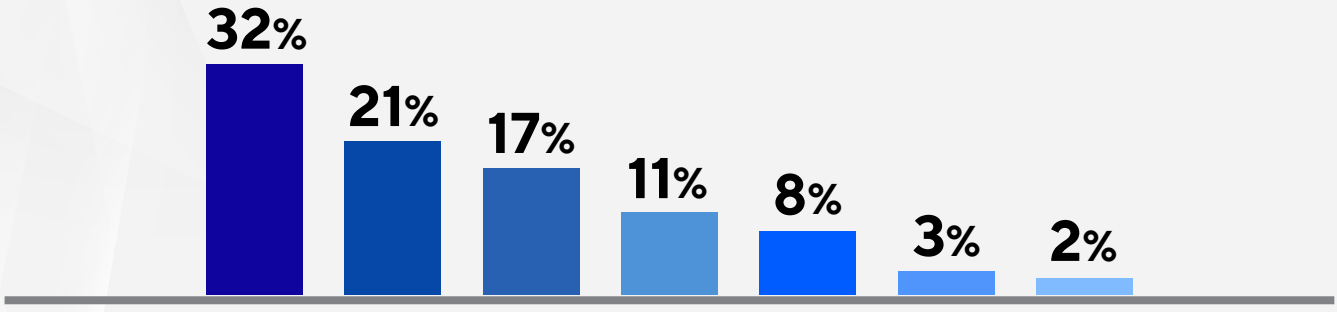
3. CULTURA EN CIBERSEGURIDAD:
LA BASE PARA DISMINUIR LOS RIESGOS

Resguardar los datos, redes y sistemas de una empresa va más allá de contar con la infraestructura adecuada o tener cargos como los descritos anteriormente: **requiere de la colaboración de todos los integrantes de una organización,** pero ¿por qué?



Fuente: Varonis.com

Causas más comunes tras un ciberataque



- De las vulneraciones tiene que ver con divulgación accidental de información.
- Se relaciona con robo o pérdida de equipos.
- Se debe al actuar de hackers, lo que puede disminuirse con una cultura en ciberseguridad sólida.
- De las fallas tiene su causa en el actuar malintencionado de algún trabajador.
- Tiene su origen en brechas de proveedores que los atacantes aprovechan para acceder a los sistemas y datos de la empresa contratante.
- De los ataques tiene su origen en la ingeniería social, es decir, manipulación para conseguir información confidencia.
- Responde al colapso de la red por causa de acciones contra los servidores, como los ataques DDoS (Distributed Denial of Service, o ataque de denegación de servicio).

Más allá de las diferentes causas tras las vulneraciones de ciberseguridad, gran parte de estas tiene como factor común el elemento humano. Por eso, es fundamental implementar una cultura en ciberseguridad que permita a los colaboradores saber cómo actuar ante ataques o sospechas de intentos de vulneración.

Como trabajador, ¿cómo puedes prevenir un ciberataque?

- No descargues archivos contenidos en correos electrónicos desconocidos.
- No hagas click en links de correos desconocidos.
- No ingreses información confidencial -como usuarios o contraseñas- en enlaces de correos desconocidos.
- No entregues información a desconocidos, ya sea por fono, correo electrónico o cualquier otro canal.
- No entregues datos bancarios a través de llamadas, y siempre verifica el remitente de los correos.

Se estima que el 95% de los ciberataques radican en fallas humanas, dando cuenta de la importancia que tiene establecer, adoptar y promover una cultura en ciberseguridad. Para lograrlo, no basta con generar un documento y distribuirlo a cada área o departamento de la empresa: es necesario evaluar constantemente la efectividad de las estrategias.

Plan de concientización: que tus trabajadores no sean un factor de riesgo

92% **DE LOS ATAQUES DE MALWARE**

Se perpetúan a través de correo electrónico, lo que evidencia la importancia de contar con una cultura en ciberseguridad.

Fuente: Irmsecurity.com

Diseñar y comunicar un plan de acción es la base para que una empresa adopte una cultura en ciberseguridad. Sin embargo, ¿cómo garantizar que los trabajadores están preparados para actuar ante un intento de vulneración?

Es aquí cuando un **plan de Awareness** -o concientización- cobra especial relevancia, ya que permite a las empresas saber si sus trabajadores han comprendido las medidas preventivas previamente difundidas, y evaluar de qué forma responden ante determinados escenarios. Para ello, este plan debe contemplar acciones como:

Capacitación efectiva

Además de informar las políticas de ciberseguridad, las empresas deben ofrecer capacitación a sus trabajadores que contemple ejercicios prácticos.

Pruebas o trampas de seguridad

Esta es la mejor forma de evaluar qué tan involucrados están los trabajadores con la cultura de ciberseguridad adoptada en la empresa. ¿Cómo hacerlo?

Enviar correos trampa que contengan enlaces no autorizados. Si el trabajador lo abre, se genera una respuesta con copia a su jefe, invitando a elevar las medidas de precaución.

Ejercicios de phishing. Las simulaciones de este tipo de amenazas permiten a las empresas saber cómo se enfrentan sus trabajadores ante este tipo de riesgos, pudiendo fortalecer las medidas de ciberseguridad.

Advertir las fallas. Por ejemplo, poniendo notas con un llamado a tener más cuidado sobre pantallas abiertas sin bloquear.

Retirar dispositivos abandonados

Suele ocurrir que los trabajadores dejan equipos corporativos en áreas comunes o sin cuidado. Cuando esto ocurre, puedes retirar el equipo dejando una nota para retirarlo en determinada oficina.

Comunicación permanente

Para que los trabajadores tomen conciencia sobre el papel que tienen en la ciberseguridad de la empresa, no basta con un correo electrónico mensual: es necesaria una comunicación permanente y entregarles información actualizada que permita incorporar el tema en el cotidiano desde una vereda proactiva y preventiva.

4. PROCESOS Y TECNOLOGÍAS A ADOPTAR

PARA QUE UNA EMPRESA PERMANEZCA SEGURA

Para que una empresa pueda protegerse de los riesgos propios del entorno digital, es importante que adopte los procesos y la tecnología necesaria para ello.

Procesos

Se refiere a todos los procedimientos y acciones orientadas a proteger la integridad de datos, redes y sistemas. Aunque siempre dependerán de la infraestructura y requerimientos de cada empresa, hay algunos de son de carácter transversal:

- **Actualización de sistemas y equipos.** Las actualizaciones permiten que dispositivos y software puedan repeler intentos de vulneración. Al respecto, es conveniente realizar revisiones periódicas a todos los recursos corporativos para garantizar que cuenten con las debidas actualizaciones.
- **Cambio permanente en credenciales,** especialmente de las cuentas corporativas, puntos de acceso a la red, sistemas, etc.
- **Procesos higiénicos de TI,** entre los cuales vale la pena destacar la gestión de archivos, de parches, de vulnerabilidades, investigación ciberforense, etc.
- **Desarrollo seguro,** tanto de las plataformas internas como en la integración de nuevas herramientas.
- **Realizar copias de seguridad,** indispensable para garantizar la continuidad operativa.
- **Conexiones remotas seguras,** para lo cual debe garantizarse el acceso a redes y sistemas desde una VPN.

Tecnologías

Aquí se consideran todas las soluciones adquiridas o desarrolladas por la empresa para proteger sus datos, sistemas y redes. Algunas de las más importantes son:

- **Antivirus.** Indispensable para detectar intromisiones de malware y similares, además de permitir monitorear amenazas potenciales, como archivos contenidos en correos electrónicos.

- **Firewall.** También llamado cortafuegos, esta herramienta es fundamental para proteger la red privada de una empresa **al gestionar el tráfico de acuerdo con estándares preestablecidos,** evitando que terceros accedan a las redes internas.

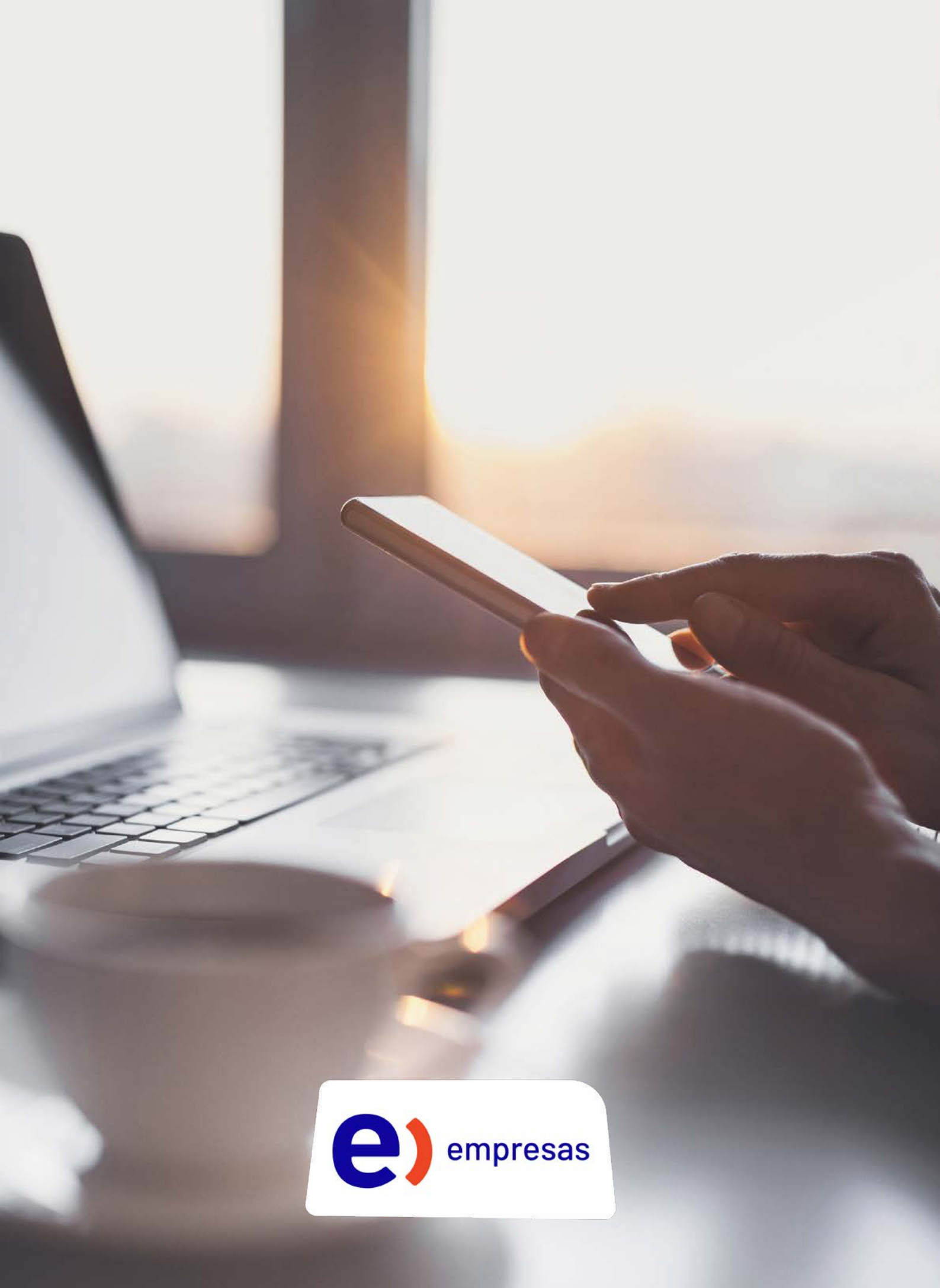
- **EDR.** Acrónimo de Endpoint Detection and Response, este término se refiere a herramientas que permiten **monitorear y hacer un seguimiento continuo de equipos y redes.** Ideales para complementar la seguridad otorgada por soluciones como antivirus y firewall, alertando ante la más mínima sospecha de amenaza.

- **VPN.** Las redes privadas virtuales (Virtual Private Network) son determinantes para proteger a la empresa cuando hay trabajadores operando de forma remota, pues permiten crear una red blindada dentro de la pública. Así, las empresas pueden incentivar la flexibilidad y agilizar los procesos sin descuidar la protección de sus datos.

Aunque un ciberataque puede generar daños considerables a nivel económico, de infraestructura, de imagen y confianza, vale la pena considerar que un **80% de las infracciones de datos pueden evitarse con medidas básicas,** como las que hemos revisado en este documento.

Siendo así, está en tus manos adoptar los resguardos necesarios para proteger a tu empresa de los riesgos propios de Internet. Ya diste el primer paso: te informaste, conociste los principales aspectos que -como directivo- debes manejar para tomar las decisiones acertadas.

Ahora, debes evaluar el nivel de seguridad de tu infraestructura TI y, con ello, puedes comenzar a integrar las soluciones necesarias para brindar a tu empresa la protección necesaria para operar con tranquilidad, disminuyendo al máximo los riesgos y manteniendo un control permanente sobre tus redes, equipos y datos críticos.


empresas