Tecnología
para los negocios

Protege tu información

Cómo proteger y reducir los riesgos de pérdida de información en tu empresa

Ciberataques

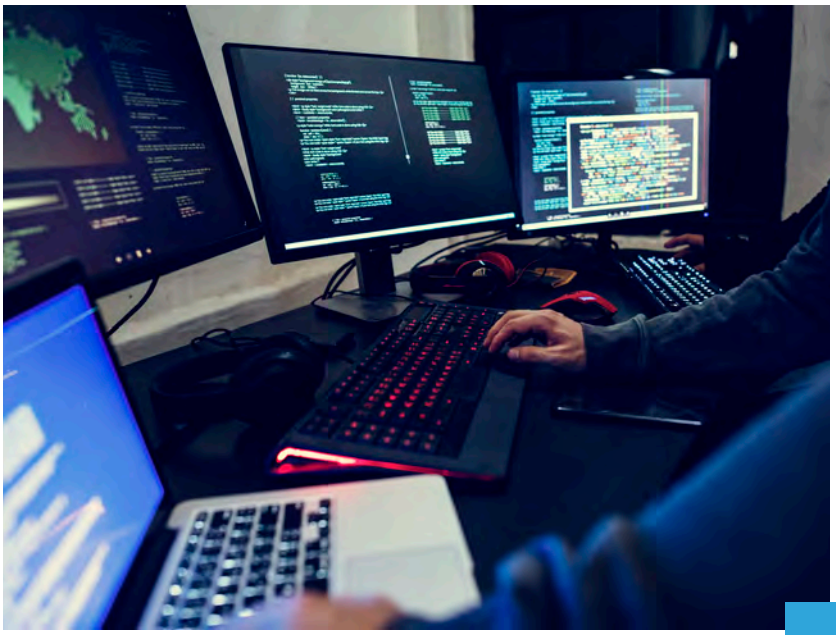
ticnegocios.es

Índice

¿Qué son los ciberataques? 1.

Nos encontramos en plena digitalización y constante evolución tecnológica. Estos avances tecnológicos que van de la mano de Inteligencia Artificial o Big Data ofrecen unas oportunidades únicas, pero consigo traen también un mundo que podríamos llamar más "vulnerable".

Actualmente está todo en internet, información muy importante de empresas, gobiernos e incluso personal, por ello aparecen los ciberataques.



Por lo que es realmente importante mantener nuestra empresa segura y protegida ante estos ataques, ya que no solo repercute en la infraestructura de nuestra empresa, sino que también se producen daños a terceros y mala reputación de la empresa que lo sufre.

1.1 Ciberataques la nueva forma de crear una guerra

El ciberataque es un conjunto de acciones contra sistemas de información o bases de datos de una entidad, organización o empresa, con el objetivo de perjudicar a dicha persona e institución y sacar en la mayoría de los casos provecho de ello.

↘¿Podríamos hablar de una nueva forma de guerra?
Se podría entender así, cómo una ciberguerra, ya que es un sistema que permite perjudicar de una forma más rápida y sencilla. Y esto se debe a su alta rentabilidad y a que exigen una infraestructura menos compleja, además de que es extremadamente difícil seguir su rastro y, por tanto, ser descubiertos.

1.2 España el 3º país que más ciberataques sufre

Cada dos minutos se produce el uso de datos privados con fines criminales, una cifra realmente sorprendente. Y es que actualmente España es el tercer país que más ciberataques sufre, solo por detrás de Estados Unidos y Alemania.

Una media de **40.000 ciberataques al día** se produjeron en 2021, ¡un aumento del 125% respecto al año anterior!.

1.3 Las pymes las que mayor tasa de correos maliciosos reciben

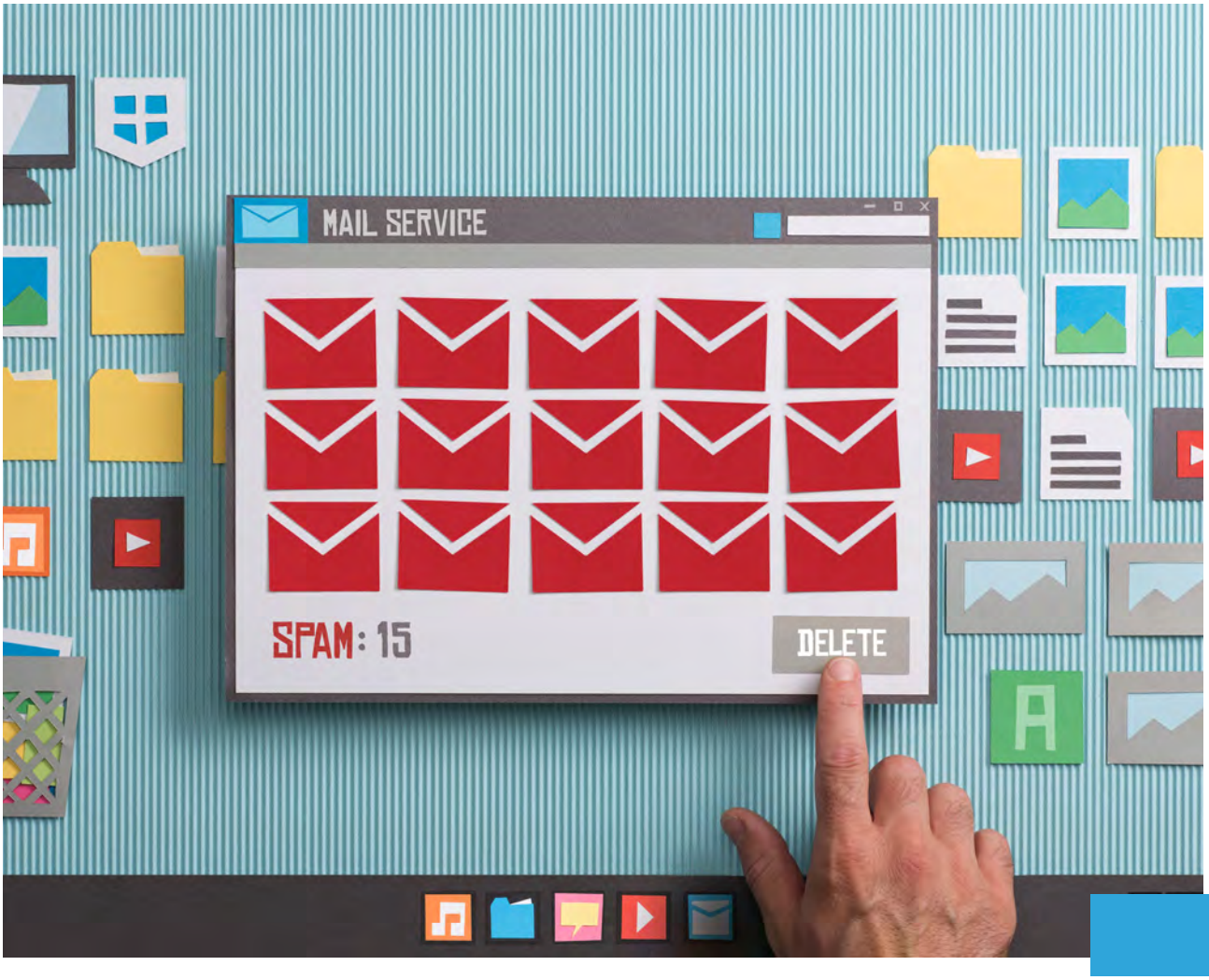
Actualmente las pymes reciben una mayor tasa de correos electrónicos maliciosos, ya que las pequeñas y medianas empresas suelen estar en la diana por tener menos sistemas de protección frente a estos ataques. Y según INCIBE el Instituto Nacional de Seguridad las pérdidas que se pueden producir por un ciberataque en una pyme pueden ir de los 2.000 a los 50.000 €.

Por ello es el momento de instalar un sistema seguro que cumpla con el Reglamento General de Protección De Datos (RGPD) y que además nos asegure que no tendremos esa pérdida de información.

2. Estadísticas e información sobre ciberataques a través de INCIBE

INCIBE es el Instituto Nacional de Seguridad en España, y este trabaja para procurar confianza y seguridad digital a los usuarios y empresas, a la vez que impulsa el mercado digital en España.

Gracias a la investigación y prestación de servicios de INCIBE, se consigue una mayor seguridad a nivel nacional. Además, la institución ofrece múltiples sugerencias y recomendaciones en su blog para poder hacer frente y evitar estos ciberataques.



2.1 En 2021 INCIBE recibió más de 100.000 incidentes en materia de ciberseguridad

El pasado año se recibieron más de 100.000 avisos de incidentes, de ellos 90.168 se realizaron a ciudadanos y empresas, con un total de 109.126 incidentes de ciberseguridad.

↘ Malware / Software malicioso: en un 29,88% siendo uno de los virus informáticos más comunes.

↘ Variantes de fraude: con un 28,60%.

↘ Ataques a sistemas vulnerables: con un 18,89%.

Es decir, los ataques más producidos son aquellos que más fácil pueden afectar a las empresas..

3. ¿Cómo afectan los ciberataques a las empresas?

La información es vital para las empresas, con ella podemos trabajar, contactar con proveedores, acceder a la cartera de clientes y a nuestra propia web. Por lo que una pérdida de esta información supondría un gran problema, y entre los más destacados podemos encontrar:

3.1 Bloqueo de los sistemas y la paralización de los sistemas de producción

Cuando se produce un ciberataque, sus efectos repercuten en toda la infraestructura empresarial bloqueando los sistemas, e incluso se puede paralizar el proceso de producción, y por consecuencia el funcionamiento normal de la empresa, por lo que puede generar graves repercusiones económicas.

3.2 Una pérdida de información

La pérdida de información de clientes, proveedores etc, supone enormes pérdidas económicas a los sufren. Las más conocidas son Everis, Cadena SER o Prosegur en 2019, que sufrieron ciberataques y pérdidas que paralizaron su actividad y suministro de servicios durante dos días.

3.3 Daños a terceros

Un ciberataque que implique el robo de datos de consumidores pone en riesgo no solo la empresa que lo recibe, sino los cimientos construidos durante años como la reputación y la confianza del cliente.

Por ello, es vital que las empresas se protejan de cara a un ataque, ya que cuando se produce un robo de datos es esencial conocer cómo actuar y mantener la confianza de los consumidores.

4. Tipos de ciberataques

Como hemos comentado anteriormente, los ciberataques se han convertido en los últimos años en un arma contra todo tipo de empresas.

Además cada vez la lista de ciberataques es más extensa, y sin excluir ningún tipo de negocio: pymes, pequeños autónomos o grandes empresas. Por ello es esencial que tus empleados y clientes conozcan que también están expuestos a sufrir un ataque informático, y cuáles son los más comunes según INCIBE.

A continuación describimos los ataques informáticos más comunes.

4.1 Ataques a las contraseñas

Los delincuentes utilizan nuestra contraseña a base de ensayo y error, probando diferentes combinaciones con nuestros datos personales, hasta que dan con el patrón correcto. Cuando tienen acceso pueden suplantar identidad, datos personales, cuentas bancarias…

Las contraseñas son un punto de acceso a los datos de cualquier empresa, por ello es esencial evitar:

- Utilizar las mismas contraseñas para diferentes servicios o servidores.
- Utilizar contraseñas débiles.
- Apuntarlas en otros documentos de fácil acceso.
- Hacer uso de patrones sencillos de letras o números.

4.2 Ataques por ingeniería social

Este tipo de ataques se caracterizan por ser suplantación de identidad en el correo, teléfono, mensajería… En ellos el ciberdelin-

cuente envía un mensaje suplantando una identidad (red social, web, o entidad pública). Estos mensajes suelen ser de carácter urgente o atractivo.

Lo más común es que contengan un enlace a una web fraudulenta, que ha podido ser suplantada, fingiendo ser un enlace legítimo, o un archivo adjunto malicioso para infectar con malware.

Entre los más comunes encontramos:

↘ **Phishing:** Suele emplearse el correo electrónico, redes sociales o aplicaciones de mensajería instantánea.

↘ **Vishing:** Se lleva a cabo mediante llamadas de teléfono.

↘ **Smishing:** El canal utilizado son los SMS.

↘ **Spam:** Es el envío de grandes cantidades de mensajes o campañas publicitarias a través de Internet sin haber sido solicitados. La mayoría tienen una finalidad comercial, aunque puede haberlos que contengan algún tipo de malware.

4.3 Ataques a las conexiones

Estos ataques son muy comunes, en ellos los ciberdelincuentes saltan las medidas de seguridad para tomar o infectar los dispositivos.

Se suele suplantar el DNS, es decir, la dirección IP a la que accedemos como un dominio seguro y acceden a nuestros datos. Por lo que es fundamental blindar la seguridad del router, restringiendo las conexiones remotas.

Los ataques a conexiones más usados son:

↘ **Redes trampa:** en ella los ciberdelincuentes crean una red wifi falsa idéntica a la de acceso seguro, con ella podrán robar los datos nada más acceder. Es muy importante tener en cuenta las redes públicas, ya que es el caso más común.

↘ **Spoofing:** es la suplantación de una web segura por una web con malware, por ello siempre debemos de acceder a web con una capa de protección de seguridad (Certificado de seguridad SSL)

↘ **Ataque a cookies:** Las cookies se envían de un servidor a otro, pero al acceder a una web sin certificado de seguridad, es decir (http), este intercambio puede llegar a ser visible para los ciberdelincuentes. Robando toda la información que contienen (datos de navegación, el idioma, la zona horaria, dirección de correo electrónico, etc)

4.4 Ataques por malware

Los ataques por malware son programas maliciosos que pretenden realizar acciones dañinas en el sistema informático, y pretenden robar información o causar daños en el equipo para obtener un beneficio económico. Dependiendo del modus operandi, y de la forma de infección, existen distintas categorías de malware, entre las que encontramos:

↘ **Virus:** Estos están diseñados para copiarse a sí mismos y propagarse a tantos dispositivos como les sea posible, son capaces de modificar o eliminar los archivos almacenados en el equipo, y pueden transmitirse por servicios web, dispositivos extraíbles o archivos adjuntos.

↘ **Spyware:** Este se instala en nuestros equipos y comienza a recopilar información, supervisando toda su actividad para luego compartirlo con un usuario remoto, suelen ejecutarse a la vez que otro software infectado.

↘ **Keyloggers:** Los Keyloggers realizan un seguimiento y registran cada tecla que se pulsa en un equipo sin nuestro consentimiento, su objetivo es monitorizar nuestra actividad y recoger datos que el atacante pueda utilizar para robar cuentas, información y perpetrar otro tipo de ataques.

Además podemos encontrar otros más modernos como:

↘ **Cryptojacking:** en él los ciberdelincuentes utilizan nuestros dispositivos sin nuestro consentimiento para llevar a cabo "extracciones" de criptomonedas. En este caso no suelen tener interés en acceder a nuestros datos personales, sino en utilizar nuestros recursos para el minado de criptomonedas y obtener un beneficio económico.

↘ **Apps Maliciosas:** Las Apps maliciosas se hacen pasar por aplicaciones verificadas, y una vez instaladas en el dispositivo, nos pedirán una serie de permisos abusivos o, por el contrario, harán un uso fraudulento de dichos permisos.

5. Medidas de protección frente a ciberataques

Como hemos visto existen multitud de tipos de ciberataques a los que nuestra empresa se expone todos los días, por ello es crucial contar con recomendaciones como:

5.1 Protege tus dispositivos

Utiliza un antivirus para analizar todas las descargas y archivos sospechosos, y siempre actualizado, revisa el configurado del VPN para acceder de manera remota y comprobar que el software y el hardware de cada equipo.

5.2 Cuenta con un seguro ante ataques cibernéticos

Otra buena forma de cubrirse ante estos ataques es con un seguro para riesgos cibernéticos es una práctica herramienta que ayuda a que las empresas y asociaciones puedan proteger su patrimonio ante:

- Ataques de hackers
- Fugas de seguridad
- Virus informáticos
- Robo de identidad y otras eventualidades

5.3 Contraseñas seguras

Utiliza contraseñas robustas y diferentes para proteger todas tus cuentas, con la verificación en dos pasos utiliza la verificación en dos pasos u otro factor de autenticación.

↘ Las más recomendadas son aquellas que están formadas por caracteres aleatorios en las que se intercalan mayúsculas con minúsculas y aparecen símbolos.

↘ También se debería hacer cada cierto tiempo un cambio de contraseña, por si acaso han sido comprometidas de alguna manera.

5.3 Protección web

Utiliza sólo webs seguras con https y certificado digital certificado SSL (lo podremos identificar con el icono del candado). Este tipo de página se caracteriza por enviar la información de manera cifrada; así, ningún atacante podrá acceder a la misma, ni tan siquiera leerla. y utiliza el modo incógnito cuando no quieras dejar rastro.

5.3 Backup o copia de seguridad

Las pequeñas y medianas empresas son las que mayor tasa de correos electrónicos maliciosos reciben, sin embargo, solo un 16% de las pymes realiza copias de seguridad, algo esencial para ellas, ya que la pérdida de datos por ciberataques puede suponer pérdidas de entre 2.000 y 50.000 euros para las pymes, según Incibe.

Las copias de seguridad ofrecen:

↘ Mantener al menos tres copias de sus datos (para evitar que un incidente individual destruya todas sus copias).

↘ Almacenar los datos en al menos dos formatos distintos (por ejemplo, discos, cintas, la nube, etc.)

↘ Guardar una copia en una ubicación externa para protegerla del fuego, inundaciones, robos y otros desastres físicos entre otros.

6. Las herramientas para la transformación digital industrial protegidas

Las tendencias y herramientas para la transformación digital han evolucionado ante el crecimiento de los ciberataques. Por lo que en los procesos de transformación digital y con la necesidad de mejorar la protección deben implantarlas.

Para ello te dejamos unas claves para que la transformación digital de tu empresa sea segura:

6.1 Claves para una transformación digital segura

↘ Contar con profesionales en digitalización y ciberseguridad, en la que en el proceso se utilicen las herramientas adecuadas para la protección de los datos.

↘ La actualización de los software siempre actualizado como hemos comentado anteriormente.

↘ La gestión de datos debe ser gestionada por profesionales y con herramientas seguras, con derechos de

acceso y la protección necesaria.

↘ Formación de todo el equipo, es muy importante este punto, para que cualquier trabajador de la empresa pueda identificar cualquier error y pueda detectarlo a tiempo.

6.2 Tendencias ciberseguridad 2022

Entre las tendencias que más se prevé que se empleen en 2022 encontramos:

Externalización de los servicios de ciberseguridad:

Los sistemas de seguridad son uno de los elementos más adecuados para confiar a proveedores externos, ya que permite a la empresa ahorrar costes en materia de innovación y desarrollo tecnológico.

La inteligencia artificial

El Big Data en una empresa permite procesar gran cantidad de información, así como el machine learning, que gestionan datos y pueden analizar escenarios cambiantes y situaciones de riesgo identificando patrones de comportamiento.

Además de incorporar sistemas más seguros en Cloud en la nube y el cumplimiento íntegro del RGPD, la regulación general de protección de datos.

7. Conclusiones

La ciberseguridad en las empresas como hemos podido observar es uno de los puntos más importantes. Ninguna empresa está exenta de sufrir un ataque cibernético y las pérdidas tras sufrirlo pueden ser realmente perjudiciales.

Proteger y reducir al máximo los riesgos de pérdida de información, así como subsanar las vulnerabilidades que se encuentren debe ser algo obligatorio en el entorno digital de cualquier empresa durante 2022.

Esta inversión de ciberseguridad será sin ninguna duda, una inversión beneficiosa ofreciendo la integridad de todos los datos de la empresa, una mejora en la imagen corporativa y confianza de los clientes, nos permitirá aumentar la productividad y ahorrar en gastos, así como una mayor recuperación ante cualquier imprevisto.

¡Protege a tu empresa de los ataques cibernéticos!

ticnegocios.es