CIBERRIESGOS: SU IMPACTO EN LAS PYMES

PREVENIR, MITIGAR, RECUPERAR

estamos seguros

cepreven

CEPYME
CONFEDERACIÓN ESPAÑOLA DE LA PEQUEÑA Y MEDIANA EMPRESA

UNESPA ASOCIACIÓN EMPRESARIAL DEL SEGURO

ÍNDICE

PRÓLOGO

Todas las empresas, incluso las de menor tamaño, están expuestas a los riesgos cibernéticos. Todas gestionan datos de carácter personal, dependen de sistemas informáticos y redes, contratan servicios a terceros y en la nube, generan y protegen su propiedad intelectual y, además, están sujetas al cumplimiento de una normativa sectorial, local, nacional y europea.

Por estas razones cualquier empresa, tenga el tamaño que tenga, debe tomar las medidas necesarias para preservar su competitividad y supervivencia frente ataques o incidentes cibernéticos.

Para afrontar esta situación puedes contar con el seguro. El trabajo de las aseguradoras es la gestión de riesgos y, por esta razón, son la mejor ayuda para que tu empresa pueda hacer frente a estos nuevos retos.

En esta guía encontrarás un conjunto de buenas prácticas que te permitirán proteger tu empresa de incidentes cibernéticos, minimizar su impacto, garantizar la recuperación de aquello que haya resultado dañado de alguna manera y, principalmente, asegurar la continuidad de tu negocio.

Mirenchu del Valle Schaan
Secretaria general de UNESPA

José Alberto González-Ruíz
Secretario general de CEPYME

Jon Michelena Muguerza
Director general de CEPREVEN

¿ESTÁ MI EMPRESA EXPUESTA A RIESGOS CIBERNÉTICOS?

Un empleado recibe un supuesto correo electrónico de una empresa de mensajería y hace clic en el enlace previsto para comunicarle el lugar de entrega de su paquete. En realidad, descarga, sin que él lo sepa, un programa de encriptación de datos (*ransomware*). En ese momento se encriptan y quedan totalmente inservibles todos los datos de la empresa. Los piratas informan a la compañía de que, para recuperar el acceso a esta información, debe pagar un rescate. Supuestamente, a cambio del desembolso de una cantidad de dinero mediante un soporte impersonal y en la nube (por ejemplo, en divisas virtuales). A cambio, la sociedad víctima del ataque cibernético recibe la clave de cifrado empleada por los ciberdelincuentes.

Los *hackers* o piratas informáticos aprovechan cualquier fallo de seguridad del sistema de información de un proveedor de servicios de comunicaciones electrónicas al público. De esta manera acceden a los datos de facturación de la base de clientes y prestadores de servicios. Los datos son revendidos a estafadores, quienes los podrán emplear para usurpar identidades y malversar fondos. Esto provoca que el servicio contable y comercial de la empresa se vea afectado durante varios días. Al considerarse estos datos como datos personales, la sociedad debe notificar el incidente e informar a sus clientes. Además, es posible que deba efectuar algunas compensaciones a los perjudicados. Todo esto genera pérdida de confianza por parte de algunos socios y clientes y, adicionalmente, provocará que tanto la empresa como sus directivos sufran las consecuencias de una investigación administrativa.

SI SUFRO UN INCIDENTE O ATAQUE, ¿CÓMO AFECTARÁ A MI EMPRESA?

- ¿Son de interés para alguien mis datos y la información que almaceno en mis dispositivos?
- ¿Está adecuadamente protegido mi sistema de información?
- Si sufro un ciberataque, ¿afectará a mi negocio?
- ¿Qué pasará si no puedo acceder a los datos o a mis equipos?
- ¿Podrá seguir funcionando mi negocio después del ataque? ¿Me recuperaré del impacto? ¿Estará en cuestión la propia supervivencia de mi empresa?
- ¿He implementado un plan de respuesta a incidentes o de continuidad del negocio si sufro un ataque?
- ¿Con quién debo ponerme en contacto en caso de sufrir un incidente o ataque cibernético?

Si no tienes respuestas satisfactorias para estas preguntas... entonces eres vulnerable y, si eres vulnerable, debes protegerte...

LA SOLUCIÓN

Contrata un seguro frente a riesgos cibernéticos

¿QUÉ DEBO HACER EN CASO DE SUFRIR UN ATAQUE CIBERNÉTICO EN MI EMPRESA?

ANTE LOS PODERES PÚBLICOS

Presenta una denuncia:

- Si el ataque del cual has sido víctima constituye una infracción a las tecnologías de la información y las comunicaciones deberás denunciarlo en la comisaría de policía más próxima o ante una autoridad judicial.
- En caso de ataque probado o, incluso, ante la simple sospecha de haber sido víctima de un ataque informático, la empresa deberá recoger pruebas informáticas mediante comprobaciones técnicas.

Notificar el incidente:

- Según el nuevo *Reglamento General de Protección de Datos 2016/279* (RGPD) de la Unión Europea las organizaciones que gestionen datos de carácter personal de ciudadanos europeos deben informar de los ataques informáticos en un plazo de 72 horas, salvo aquellos en los que el responsable pueda demostrar en base al principio de "responsabilidad proactiva" la improbabilidad de que dicha violación de la seguridad constituya un riesgo para los derechos y libertades de las personas físicas (transposición del RGPD mayo 2018).

- La *Directiva UE 2016/1148 del Parlamento Europeo y del Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión Europea* (Directiva NIS) determina asimismo que los operadores de servicios esenciales y los proveedores de servicios digitales notificarán a la autoridad competente sin dilación indebida, a través del Equipo de Respuesta ante Emergencias Informáticas (CSIRT) de referencia, los incidentes que puedan tener efectos significativos en dichos servicios (NIS; mayo 2018).

ANTE MI ASEGURADORA

Contactar:

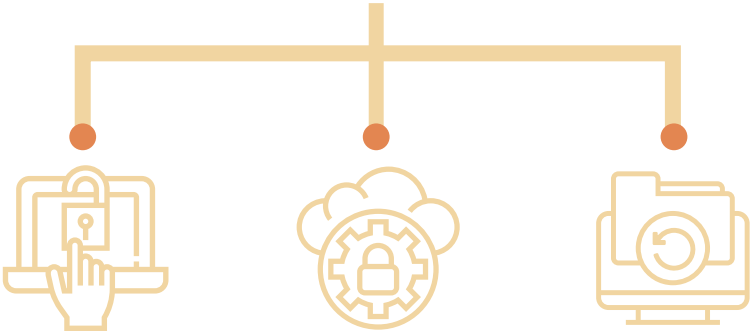
- Contacta sin demora con tu aseguradora; ella sabrá aconsejarte y ayudarte.
- En cualquier caso, no dejes de comunicarte con ella lo antes posible. Ten en cuenta que algunas decisiones pueden empeorar las cosas y agravar las consecuencias del incidente. Recuerda: cuanto antes te pongas en contacto con tu seguro, antes se resolverá el problema.

¿CÓMO PROTEJO MI EMPRESA?

La ciberseguridad de tu empresa depende de un análisis de los nuevos riesgos y la implementación de una política de gestión de esos riesgos. Todo esto hará posible trasladar a tu aseguradora el riesgo al que estás expuesto.

El proceso debe realizarse por una persona de la empresa, que se encargará de la aplicación y del seguimiento de la política de gestión del ciberriesgo, siempre con la aprobación de la alta dirección.

Esta política debe basarse en tres pilares:



FACTORES HUMANOS Y ORGANIZATIVOS

HERRAMIENTAS DE PROTECCIÓN

CAPACIDAD DE RECUPERACIÓN MEDIANTE HERRAMIENTAS DE RESILIENCIA

FACTORES HUMANOS Y ORGANIZATIVOS

Toda política de prevención requiere que la gente sepa qué actitud tomar ante los riesgos cibernéticos. Por eso:

- El personal de la empresa debe estar sensibilizado en la aplicación de las normas y las buenas prácticas.
- Se debe sensibilizar y formar a los subcontratistas y prestadores de servicios.

Además, la protección de tu empresa depende de factores organizativos como:

1. La seguridad del acceso físico y remoto

La gestión de los derechos de acceso, tanto físicos como informáticos, debe adaptarse a la situación de tu empresa y a las funciones de los colaboradores afectados.

Para evitar que se usurpen fácilmente, las contraseñas deben ser:

- Individuales.
- Secretas.
- Fuertes (complejas).
- Cambiarse regularmente.

Es útil definir un nivel mínimo de seguridad como, por ejemplo, claves con ocho caracteres que combinen mayúsculas, minúsculas, cifras y símbolos.

2. Una adecuada concienciación del personal y de los socios y colaboradores

Debe sensibilizarse a todos los colaboradores sobre la importancia de los ciberriesgos. Ya sea personal con contrato temporal, estudiantes en prácticas, etc. Deben recordarse regularmente normas simples como:

- Evitar la utilización de aparatos personales (USB o discos duros externos), así como los accesos remotos o móviles no protegidos (wifi, bluetooth…).

¿CÓMO PROTEJO MI EMPRESA?

**EN CASA, NO ABRES LA PUERTA A CUALQUIERA.
EN EL CIBERESPACIO, ¡NO ABRAS TUS SISTEMAS DE INFORMACIÓN A CUALQUIERA!**

- No dejar a la vista contraseñas en los lugares de trabajo.
- Establecer una política de utilización segura del correo electrónico (documentos adjuntos dudosos, hipervínculos o enlaces extraños, extensiones .pif, .com, .exe, .bat, .ink).

Esta política también debe compartirse con el conjunto de los socios, proveedores y prestadores de servicios.

3. La actualización de programas y aplicaciones de operación, gestión, proceso y producción:

Los fallos de los programas son vías de acceso para las intrusiones maliciosas. Estos fallos deben corregirse a medida que se identifican.

HERRAMIENTAS DE PROTECCIÓN

Destacan las siguientes herramientas de protección:

1. Antivirus / Cortafuegos:

Son la base de la protección indispensable de todos los sistemas de información. Deben actualizarse de forma regular, mejor diariamente, y de manera automática.

2. Herramientas de filtrado:

Los antivirus y cortafuegos se complementan con herramientas del tipo de Sistema de Detección de Intrusiones (IDS) y Sistema de Protección de Instrusiones (IPS) que filtran las entradas y salidas para detectar y descartar algunas intrusiones maliciosas.

3. Herramientas de detección del comportamiento:

Las intrusiones maliciosas no bloqueadas por las herramientas de filtrado pueden detectarse con el análisis de descargas y otras acciones sospechosas.

CAPACIDAD DE GESTIÓN DE CRISIS: HERRAMIENTAS DE RESILIENCIA

La capacidad de la empresa para volver a ponerse en marcha después de un ataque es más rápida si se han previsto dos aspectos:

1. Las copias de seguridad

Pautas a seguir en relación a las copias de seguridad:

- Organizar una copia de seguridad frecuente de los datos, preferentemente diaria, en soportes y sistemas independientes de los sistemas de información. Verificar periódicamente que estas restauraciones funcionan.
- Evitar localizar las copias de seguridad en el mismo sitio donde se almacenan los sistemas y datos a proteger.
- Las copias de seguridad de los sistemas operativos y programas deben seguir las prescripciones de los editores y las de los proveedores de servicios informáticos.

2. Plan de continuidad del negocio

Implementar un plan de respuesta a incidentes y de continuidad del negocio. Dicho plan debe incluir:

- Cómo calificar los datos, sistemas y aplicaciones críticas en términos de sensibilidad, confidencialidad o privacidad.
- Aplicar un procedimiento de gestión de crisis en caso de ataque.
- Designar a los colaboradores (responsables, expertos e informadores) y asignar tareas de urgencia.

¿PUEDO ASEGURAR MI EMPRESA?

PARA PROTEGER LO QUE ME PERTENECE: MI PATRIMONIO Y MIS ACTIVOS

Hay varios tipos de seguros que pueden proteger tu patrimonio y tus activos:

- Los contratos contra daños a bienes (multirriesgos y pérdidas de explotación) cubren generalmente las consecuencias (gastos de investigación de la causa, reparaciones, pérdidas de explotación consecutivas…) de los accidentes (incendios, fenómenos naturales…), de los errores humanos (imprudencia, negligencia…) o de los actos malintencionados (robo, sabotaje…), que impliquen daños materiales a sus edificios y/o a su contenido.
- Los contratos cibernéticos cubren generalmente las mismas consecuencias (gastos de investigación, de recuperación de datos, pérdidas de explotación consecutivas…), aunque estas sean consecuencia de hechos de origen informático, sin daño material y de alguna de las siguientes naturalezas:
  - Accidental: debidos a un error humano.
  - Voluntaria: por actos malintencionados tales como virus, acceso ilícito a datos personales o confidenciales, programas de encriptación (*ransomware*), ataques por denegación de servicio (*Distributed Denial of Service* o DDoS), o cualquier otra intrusión digital no autorizada para robar datos personales u otros activos.

Como complemento, los contratos cibernéticos pueden cubrir igualmente:

- Los gastos de notificación resultantes del ataque, robo o extracción de datos personales y/o confidenciales que hayan sido confiados, tales como los gastos ocasionados por la denuncia del incidente al organismo regulador los gastos de información y de prevención a los titulares de los datos apropiados y los gastos inducidos por la investigación administrativa.

- Los gastos de gestión de crisis, como los gastos de comunicación y/o de preservación de la reputación y de la imagen de la sociedad.
- Los gastos de consultores especializados con el fin de acabar con una ciberextorsión.

PARA ASEGURAR MI RESPONSABILIDAD FRENTE A TERCEROS

Hay varios tipos de seguros que pueden protegerte frente a reclamaciones de terceros:

- Los contratos de responsabilidad civil cubren tu responsabilidad frente a daños causados a terceros (clientes, vecinos, asalariados…), ya sean daños corporales, materiales e/o inmateriales. Estos contratos pueden cubrir igualmente los gastos de retirada, así como los de desmontaje y montaje.
- Algunos contratos de responsabilidad civil pueden excluir o limitar la garantía de su responsabilidad frente a terceros por los daños puramente inmateriales cuando son consecuencia de abuso informático. Esta misma garantía puede cubrirse con un contrato cibernético.
- En el caso de ataque o incidente cibernético pueden cubrir responsabilidades frente a terceros por privacidad de datos, cobertura legal frente a un procedimiento administrativo iniciado por un organismo regulador por un incumplimiento de la normativa de protección de datos de carácter personal, cobertura económica parta gastos de gestión de incidentes, etc.

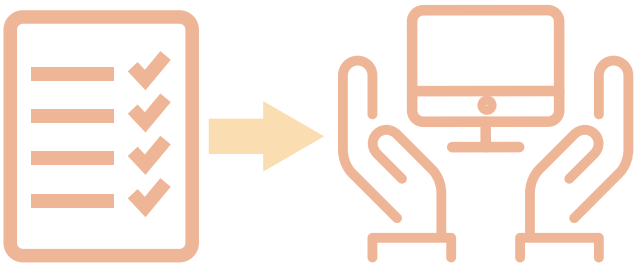
PARA ASEGURAR MI RIESGO DE FRAUDE

El seguro también da protección frente a casos de fraude:

- Los contratos contra fraudes cubren generalmente las pérdidas financieras causadas por fraudes, malversación de fondos (extorsiones, abuso de confianza, estafas…) o por algunos actos de abuso informático.
- Este mismo fraude ocasionado por actos de abuso informático también puede cubrirse por una extensión en un contrato cibernético.

¿ME PROPORCIONA EL SEGURO COBERTURA DE CIBERRIESGOS PARA MI EMPRESA?

Comprueba el ámbito y la extensión de tus seguros en vigor con el fin de asegurarte de que estás protegido de forma adecuada en caso de que se produzca un incidente informático y, más concretamente, un ciberataque.



PREGUNTAS FRECUENTES

¿QUÉ ES UN DATO DE CARÁCTER PERSONAL?

Constituye un dato de carácter personal toda información relativa a una persona física identificada o que pueda identificarse, directa o indirectamente, por referencia a un número de identificación o a uno o varios elementos que le sean propios. Así lo establece el artículo 4.1 del *Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales* (RGPD).

¿CUÁLES SON LOS ATAQUES MÁS FRECUENTES?

Los ataques más frecuentes son la denegación de servicio o *Denial of Service* (DoS), los programas de encriptación (*crypotlockers*) y programas de secuestro de datos (*ransomwares*), así como los programas maliciosos (*malware*).

¿QUÉ ES UNA DENEGACIÓN DE SERVICIO?

Un ataque de denegación de servicio o ataque de denegación de servicio distribuido (en inglés, *Distributed Denial of Service* o DDoS) es una forma de ataque que consiste en saturar las capacidades de tratamiento de un sistema de información o de un sitio internet a partir de otras máquinas previamente infectadas.

¿QUÉ ES UN PROGRAMA DE ENCRIPTACIÓN O UN PROGRAMA DE SECUESTRO DE DATOS?

Se trata de un programa malicioso que encripta los datos de un sistema de información. La clave de descifrado se obtiene a cambio del pago de una suma, frecuentemente, en divisas virtuales.

PREGUNTAS FRECUENTES

¿QUÉ ES UN PROGRAMA MALICIOSO?

Los programas maliciosos son programas que afectan al funcionamiento de un sistema de información. Pueden designarse con el nombre de virus, gusanos, troyanos o caballos de Troya...

¿ESTOY ADECUADAMENTE PROTEGIDO SI MI SISTEMA OFIMÁTICO ESTÁ PROTEGIDO?

No. Según los objetivos que pretendan, los *hackers* pueden igualmente atacar la informática de gestión, como la contabilidad, los ficheros de personal, así como la informática de proceso (autómatas...), o incluso las instalaciones de seguridad y protección.

¿EXISTEN RIESGOS RELACIONADOS CON EL *WIFI* O EL *BLUETOOTH* O, EN GENERAL, CON LOS OBJETOS CONECTADOS?

Si los datos entrantes y salientes del sistema de información no están encriptados con un nivel de seguridad suficiente, estos serán fácilmente accesibles. En concreto, se podrá llegar a ellos a través del *wifi* y el *bluetooth*. Los objetos conectados aumentan las vías de acceso a los datos y a los sistemas de información de la empresa. Por consiguiente, son puntos que los *hackers* pueden aprovechar para realizar ataques.

¿QUÉ ES EL BYOD Y CUÁLES SON LOS RIESGOS INHERENTES A LA UTILIZACIÓN DE ESTAS HERRAMIENTAS?

BYOD es el acrónimo de *Bring Your Own Device*. Esto puede traducirse como «traiga sus propios dispositivos» y constituye la práctica de permitir a la gente utilizar sus propios equipos personales para uso profesional. Esta mezcla de la esfera personal —que se presume mucho menos protegida y que, en todo caso, se encuentra fuera del control de

la empresa— con la esfera profesional multiplica los riesgos. El BYOD aumenta las vías de acceso a los datos y a los sistemas de información de la empresa. Por lo tanto, la práctica del BYOD en una empresa constituye otro punto débil que los *hackers* pueden aprovechar.

¿CUÁLES SON LOS RIESGOS DE LA NUBE?

La informática en la nube o *cloud computing* es la utilización de sistemas virtuales por medio de redes, especialmente, internet. Se trata de contratar servicios de alojamiento de datos, utilización de aplicaciones o plataformas y sistemas ubicados en servidores remotos. Esta externalización de datos y servicios por parte de la empresa es susceptible de comprometer su control sobre los mismos. La empresa deberá analizar los riesgos de esta externalización, así como las condiciones y herramientas necesarias para garantizar el nivel de confianza y de seguridad que espera de la empresa prestadora de servicios.

¿SOBRE QUÉ FUNDAMENTO JURÍDICO PUEDO PRESENTAR UNA DENUNCIA?

En España se ha promulgado un marco legal y jurídico que protege a todas las partes interesadas en el uso de estas tecnologías y el intercambio y tratamiento de la información a través de ellas dado el creciente uso de las nuevas tecnologías.

Este marco abarca todo un entramado legal distribuido por distintos organismos ministeriales del que merece la pena destacar las siguientes normativas:

- ***Ley Orgánica de Protección de Datos de carácter personal***[1] (LOPD): es una transposición de la *Directiva Europea 95/46* que tiene por objeto proteger todos los datos de carácter personal, para que no sean utilizados de forma inadecuada, ni tratados o cedidos a terceros sin consentimiento del titular. Para ello se establecen obligaciones para toda persona física o jurídica que posea archivos o ficheros con datos personales.

1. *Ley 15/1999, de 13 de diciembre*

PREGUNTAS FRECUENTES

- ***Real Decreto del Reglamento de desarrollo de la LOPD***[2].
- ***Ley de Servicios de la Sociedad de la Información y Comercio Electrónico***[3] (LSSI-CE): su finalidad es regular el funcionamiento de los prestadores de servicios de la sociedad de la información, empresas que realizan comercio electrónico y aquellas que hacen publicidad por vía electrónica, como correo electrónico o SMS.
- ***Ley de Firma Electrónica***[4] (LFE): regula la firma electrónica[5], su eficacia jurídica y la prestación de servicios de certificación.
- ***Real Decreto de Ley de Propiedad Intelectual*** (LPI)[6]: regulariza, aclara y armoniza las disposiciones vigentes en la materia.
- ***Ley General de Telecomunicaciones***[7]: su objeto es la regulación de las telecomunicaciones que comprenden la explotación de las redes y la prestación de los servicios de comunicaciones electrónicas. Entre otros objetivos esta ley fomenta la competencia efectiva de los mercados de las empresas de telecomunicaciones, promueve el desarrollo del sector y defiende los intereses de los ciudadanos.
- ***Ley de Acceso de los Ciudadanos a los Servicios Públicos***[8]: a través de esta norma se reconoce el derecho de los ciudadanos a relacionarse con las Administraciones Públicas por medios electrónicos. Además, regula los aspectos básicos de la utilización

2. *Real Decreto 1720/2007, de 21 de diciembre*
3. *Ley 34/2002, de 11 de julio*
4. *Ley 59/2003, de 19 de diciembre*
5. Firma electrónica: conjunto de datos asociados que sirve para identificar a una persona en transacciones electrónicas.
6. *Real Decreto Legislativo 1/1996, de 12 de abril*
7. *Ley 32/2003, de 3 de noviembre*
8. *Ley 11/2007, de 22 de junio*

de las tecnologías de la información en la actividad administrativa, en las relaciones entre las Administraciones Públicas, así como en las relaciones de los ciudadanos con las mismas.

- ***Ley de Medidas de Impulso a la Sociedad de la Información***[9]: en este texto se introduce una serie de modificaciones tanto de la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico, como de la Ley de Firma Electrónica, que constituyen dos piezas angulares del marco jurídico en el que se desenvuelve el desarrollo de la sociedad de la información.
- ***Ley Orgánica 1/2015***[10] por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal (Reforma del Código Penal).

Asimismo, existe una normativa de la Unión Europea en la que destacan:

- ***Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales*** (RGPD). Este reglamento es de obligado cumplimiento desde el 25 de mayo de 2018.
- ***Directiva UE 2016/1148 del Parlamento Europeo y del Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión Europea*** (Directiva NIS).

9. *Ley 56/2007, de 28 de diciembre*
10. *Ley 01/2015, de 30 de marzo*

CEPREVEN
Avda. del General Perón, 27, 5ª. 28020 Madrid
Teléfono 91 445 73 81

CEPYME
Diego de León, 50, 28006 Madrid
Teléfono 91 411 61 61

UNESPA. Asociación Empresarial del Seguro
Núñez de Balboa, 101. 28006 Madrid
Teléfono 91 745 15 30