GUÍA PARA PROTEGER TU NEGOCIO FRENTE A LOS CIBERRIESGOS

Fundación MAPFRE

Más información en:

www.segurosypensionesparatodos.org

Paseo de Recoletos, 23
28004 Madrid (España)
Tel.: +34 91 602 52 21

www.fundacionmapfre.org

Depósito legal: M-35438-2017

Vivimos en la sociedad de la comunicación. La tecnología ha hecho del mundo un lugar mucho más pequeño; todo es más inmediato e infinitamente más fácil. Las tecnologías de la comunicación, sin duda, han posibilitado que el bienestar general crezca y que las empresas mejoren su productividad, pero la dependencia que todos tenemos de ellas, una dependencia que crece día a día, abre nuevos escenarios de riesgo que debemos conocer y afrontar de manera adecuada.

Constituye un error frecuente el afirmar que los ataques informáticos sólo los sufren las grandes empresas, cuando la realidad demuestra que al margen del tamaño que tengan ninguna está a salvo.

Poco a poco nos damos cuenta de a qué nos enfrentamos. Las estadísticas cibercriminales son cada vez más alarmantes. Las pérdidas de las empresas, grandes o pequeñas, se cifran ya en millones de euros.

El objetivo de esta guía es concienciar tanto al pequeño y mediano empresario como al profesional autónomo de la existencia de los ciberriesgos y conocer las medidas preventivas que pueden adoptar para protegerse de ellos, además de informarles de que hay un seguro específico que puede proteger sus negocios frente a dichos problemas.

Este documento forma parte de la colección Guías Divulgativas que Fundación MAPFRE viene publicando desde 2014. Tanto esta que tiene en sus manos, como las anteriores, están a su disposición de manera gratuita, en formato pdf y epub, en nuestra web **www.fundacionmapfre.org** y en la del proyecto Seguros y Pensiones para Todos **www.segurosypensionesparatodos.org**

Fundación MAPFRE

SUMARIO

I

EL RIESGO CIBERNÉTICO: ORIGEN Y CONSECUENCIAS

¿QUÉ ES UN RIESGO CIBERNÉTICO O CIBERRIESGO?

Un ciberriesgo es cualquier amenaza que puede afectar a la tecnología, como por ejemplo a un sistema informático, así como al conjunto de datos contenido en el mismo, y que puede entrañar consecuencias negativas para nuestra empresa, para un conjunto de individuos o para nuestro modo de vida actual. Son los nuevos riesgos de la era digital.

Dichos riesgos pueden tener su origen en cualquier componente de nuestro sistema informático: equipos, aplicaciones, comunicaciones, etc.

Se puede producir como consecuencia de acciones intencionadas de personas (ataque de piratas informáticos, empleados, *hacktivistas* o ciberdelincuentes) o por errores y fallos de sistemas no diseñados a priori para causar un perjuicio (un fallo de alimentación eléctrica en un servidor).

Las consecuencias pueden ser diversas, entre ellas la revelación de datos a terceros no autorizados y la modificación, destrucción o pérdida de información digital.

A día de hoy existen muchos ejemplos:

- Robos de datos que pueden comprometer nuestro negocio, o datos sensibles de nuestros clientes.
- Los virus o la manipulación de información, a través de *hackers* o de empleados desleales, con el fin de obtener un beneficio propio, como la modificación de movimientos contables o transferencias a entidades financieras.

- Modificaciones de nuestro contenido web que no solo pueden dañar la reputación de nuestra empresa, sino también la de nuestros clientes y visitantes web.
- Robos de identidad de personas físicas para su uso posterior por delincuentes en diferentes tramas de delitos.
- Pérdidas de información sensible almacenada en portátiles, ordenadores o dispositivos de almacenamiento portable (como USB).
- Robo de propiedad intelectual o comercial para su posterior uso, así como supuestos de venta a la competencia o extorsión a la empresa afectada.

- Ataques de denegación de servicio que impidan el correcto funcionamiento de los sistemas que prestan un servicio a los clientes (individuos o empresas), paralizando una o varias actividades de la empresa.
- Secuestro de información o de sistemas informáticos para posteriormente solicitar una cantidad económica como rescate de la misma (comúnmente realizado por un determinado tipo de virus denominado ransomware).

¿QUIÉN ESTÁ EXPUESTO AL CIBERRIESGO?

Prácticamente toda la sociedad, tanto si usamos sistemas informáticos directamente como si utilizamos servicios de empresas que los utilizan (que a día de hoy son prácticamente la totalidad). Podemos incluir tanto a las familias como a las empresas como afectados potenciales, si bien las empresas presentan una mayor exposición a este riesgo, ya que los modelos operativos han ido evolucionando, generalizándose el uso de los sistemas informáticos y convirtiendo en muchas ocasiones el uso de la tecnología en un punto crítico para el buen funcionamiento del negocio.

CUALQUIER EMPRESA O NEGOCIO (NO IMPORTA EL TAMAÑO EN QUE OPERE NI EL SECTOR) QUE MANEJE DATOS Y USE SISTEMAS DE INFORMACIÓN ESTÁ EXPUESTO AL CIBERRIESGO.

Las empresas se benefician del uso de las nuevas tecnologías para mejorar su negocio. El uso de internet, de los sistemas in-

formáticos y de los dispositivos electrónicos no deja de crecer y cada vez tiene una mayor influencia en la gestión de las compañías, así como en la forma en que éstas prestan sus servicios, venden sus productos o se relacionan con sus clientes o proveedores, ya sean pymes o grandes empresas.

Como consecuencia, y debido a esta ampliación del uso de tecnología, se amplía el riesgo cibernético. A mayor uso, mayor dependencia y, por lo tanto, mayor riesgo.

¿CUÁLES SON LOS RIESGOS MÁS COMUNES?

Los riesgos que se producen con mayor frecuencia son:

- **Problemas de accesibilidad o disponibilidad:** Dificulta a los usuarios (empleados o clientes) que tengan permiso de uso de la información para consultar, modificar o trabajar con dichos datos.

  Por ejemplo, inhabilitando el sistema que los alberga o la red que da acceso, encriptando la información, etc.
- **Accesos NO autorizados o confidencialidad:** Alguien accede a información para la que no tiene permiso.

  Por ejemplo, realizando copias o extracciones no autorizadas mediante el robo de ficheros o bases de datos, o visualizando información sin contar con los permisos pertinentes.
- **Modificación deliberada de la información o integridad:** Alguien sin autorización modifica los sistemas de información o los datos que albergan estos, de forma que no reflejen la realidad.

Por ejemplo, instalando programas no permitidos o virus, o cambiando los programas de las empresas y los datos financieros, de clientes, de pedidos, etc.

¿QUÉ MÉTODOS USAN LOS CIBERDELINCUENTES?

Existe una multitud de métodos de ataque dirigidos a los sistemas de información que afectan a la protección, a la manipulación o al acceso tanto a la información como a los datos de las empresas.

Las variables de métodos usados por los ciberdelincuentes aumentan de forma exponencial, tanto por el propio incremento del uso de las tecnologías como por la complejidad de los mismos.

Algunos ejemplos de los más usados son:

- **Ataque de fuerza bruta:** Es un procedimiento para averiguar una contraseña. Consiste en ir probando de manera secuencial todas las combinaciones posibles hasta encontrar la combinación correcta para el acceso a una aplicación o sistema de información.
- **Denegación de servicio:** Es un conjunto de técnicas que tienen como objetivo dejar un servicio inoperativo. Mediante este tipo de ataques se busca una modificación o una sobrecarga de un servidor y de esta forma impedir que los usuarios legítimos puedan utilizar los servicios prestados por él.
- **Phishing:** Se trata de una estafa cometida a través de medios telemáticos mediante la cual el estafador intenta conseguir de usuarios legítimos información confidencial (contraseñas, datos bancarios, etc.) de forma fraudulenta. El estafador suplan-

ta en una comunicación electrónica la personalidad de una persona o empresa de confianza para que el receptor perciba dicha comunicación como aparentemente oficial o legítima (vía e-mail, fax, SMS o telefónicamente), creyendo en su veracidad y facilitando, de este modo, los datos privados que resultan de interés para el estafador.

- **Ransomware:** El ciberdelincuente, generalmente mediante un virus, toma control del equipo infectado y «secuestra» la información del usuario cifrándola, de tal forma que permanece inaccesible si no se cuenta con la contraseña de descifrado. De esta manera extorsiona al usuario pidiendo un rescate económico a cambio de esta contraseña para que, supuestamente, pueda recuperar sus datos.

- **Suplantación de identidad:** Es la actividad maliciosa por la que un atacante se hace pasar por otra persona para cometer algún tipo de fraude.
  Un ejemplo vigente en la actualidad es el denominado Fraude al CEO, en el que el ciberdelincuente envía un correo falso a una persona de una empresa haciéndose pasar por el CEO de la organización y urgiéndole a realizar una transferencia económica para la realización de una importante operación para la compañía, aludiendo a la confidencialidad de la misma para evitar revelarla a otros empleados.

¿QUÉ ES LA CIBEREXTORSIÓN?

En algunos casos, los ciberdelincuentes hacen uso de la violencia o de la intimidación a través de los medios informáticos, con el objetivo de que la víctima realice un pago o compensación económica a favor del delincuente.

El infractor y la víctima no suelen tener contacto directo más allá del mantenido en la red para pedir la cantidad a abonar.

Algunos ejemplos en los que suele ser normal la extorsión son:

- Bloqueo de la información o de programas informáticos que impida la realización normal de la actividad.
- Secuestro de acceso a teléfonos móviles.
- Bloqueo de cuentas personales en diferentes redes sociales.
- Amenazas de publicación de información obtenida de la víctima.
- Envío de comunicados solicitando información personal bajo amenazas.

- Amenazas de saturación de los servidores web para evitar que puedan prestar servicios a los clientes.

¿CÓMO PUEDEN EXTORSIONAR LOS CIBERDELINCUENTES?

La extorsión está muy relacionada con el *ransomware* (rescate de software). Éste consiste en el ataque a un ordenador seguido del bloqueo de archivos sensibles para el sistema o documentos importantes a través de un virus o *malware*[1] que cifra los ficheros con un objetivo claro de extorsión.

Malware: Es un programa informático que tiene efectos no deseados o maliciosos. Lo normal es que actúe sin que el usuario del equipo se dé cuenta. Suelen entrar a través del correo electrónico, la mensajería instantánea, descargas de software en sitios maliciosos o mediante la copia de ficheros en medios extraíbles (como dispositivos USB).

LO NORMAL ES QUE UN CIBERDELINCUENTE ENTRE EN UN ORDENADOR PERSONAL SIN QUE EL USUARIO SE DÉ CUENTA, BIEN A TRAVÉS DEL CORREO ELECTRÓNICO, BIEN AL DESGARGAR ALGÚN ARCHIVO DE UN SITIO MALICIOSO.

El programa *malware* se encarga de encriptar los archivos (pueden ser fotos, documentos, presentaciones, etc.) y de dejar un mensaje

[1] Combinación de dos palabras inglesas: *malicious* y software.

a la víctima con los pasos a seguir para el rescate, adjuntando la dirección o monedero electrónico donde debe depositar el dinero para que, posteriormente, se le entregue una herramienta o clave de descifrado que le sirva para poder recuperar los ficheros encriptados.

El sistema o los archivos encriptados son liberados si el usuario le paga un "rescate", normalmente en moneda "bitcoin", al ciberdelincuente.

Bitcoin: es una moneda virtual e intangible, y difícilmente trazable, que, sin embargo, puede utilizarse como medio de pago de la misma forma que la moneda tradicional. Esta moneda está fuera del control de cualquier Gobierno, institución o entidad financiera, ya sea de tipo estatal o privado, y su uso no revela la identidad de la persona que la utiliza.

¿QUÉ ES UNA BRECHA DE SEGURIDAD?

En algunas ocasiones, los sistemas informáticos en los que los ficheros de trabajo son almacenados y procesados se encuentran sujetos a posibles errores o fallos de funcionamiento, que, a veces, pueden terminar afectando negativamente a la actividad empresarial o a la información personal almacenada, posibilitando que personas no autorizadas puedan tener acceso a datos personales o ficheros de la compañía.

¿HAY EXIGENCIAS LEGALES PARA LAS EMPRESAS EN ESTA MATERIA?

Existe legislación específica relacionada con la ciberseguridad adaptada a determinados sectores empresariales.

Las instituciones europeas y los Estados miembros trabajan en la revisión e implantación de un marco legal para adecuarlo a las crecientes exigencias en materia de ciberseguridad en las áreas de los servicios esenciales (Directiva NIS, Ley PIC 8/2011 y el próximo Cybersecurity Act), la privacidad (regulaciones GDPR, e-Privacy) y organismos de soporte y coordinación en materia de ciberseguridad para organismos gubernamentales y empresas (Instituto Nacional de Ciberseguridad —INCIBE—, el CCN-CERT del Centro Nacional de Inteligencia y el Centro Nacional de Protección de Infraestructuras Críticas —CNPIC—).

Asimismo, se están implementando instrumentos legales a disposición de las autoridades judiciales y fuerzas de seguridad en la lucha en la red contra el crimen organizado y el terrorismo (Grupo de Delitos Telemáticos de la Guardia Civil, Brigada de Investigación Tecnológica de la Policía Nacional y la Fiscalía de Criminalidad Informática).

Por último, debemos hacer referencia al Reglamento de la Unión Europea 2016/679, de tratamiento de datos personales y libre circulación de estos en el curso de una actividad profesional o comercial, que, según desarrollaremos posteriormente, establece una serie de obligaciones a las empresas en este ámbito, así como consecuencias legales derivadas de su incumplimiento.

¿QUÉ TIPO DE EMPRESAS SUFREN ATAQUES CIBERNÉTICOS?

En la actualidad ninguna empresa está libre de ser objetivo de los delincuentes, ya que es posible vender cualquier tipo de información tanto en el ciberespacio como a la competencia de dicha empresa.

La razón fundamental por la que una empresa se puede ver atacada reside en la capacidad que tenga el ciberdelincuente de obtener un beneficio del ataque perpetrado. Existen sectores que son más proclives a los ataques informáticos, como el bancario y el *retail*, o incluso el comercio minorista. La razón es que lo que pueden obtener es muy valioso; por ejemplo: venta de números de tarjeta, obtención de saldos bancarios, etc.

Además, existen amenazas globales que afectan a todos los que se encuentren en el ciberespacio tan sólo por el hecho de hacer uso de él. Las amenazas globales contra los sistemas de información afectan potencialmente a cualquier empresa, con independencia de que esta no se encuentre perturbada por ninguno de los factores anteriores.

¿CUÁLES SON LAS PRINCIPALES CONSECUENCIAS DE UN CIBERATAQUE?

Las consecuencias de un ciberataque pueden ser muy graves para la empresa. A través del acceso a los sistemas de información se puede estar expuesto a las siguientes situaciones:

Pérdida de datos

Los ataques cibernéticos normalmente intentan el robo de información sensible, datos de clientes, como investigaciones, estrategias empresariales, informes financieros... Las bases de datos digitales también están en el punto de mira de los delincuentes informáticos. Perder esta información privada puede suponer la quiebra de muchas empresas.

En multitud de ocasiones, las empresas elegidas para ser extorsionadas son aquellas que más cantidad de datos manejan, por una mera cuestión de relación entre el esfuerzo acometido por el ciberdelincuente y el beneficio obtenido de dicho ataque. En estos casos los ciberdelincuentes piden grandes cantidades de dinero a cambio de no atacar los sistemas corporativos, de dejar

de hacerlo o de revelar una información que previamente ha sido obtenida mediante un ataque exitoso.

Desembolso económico

En muchas ocasiones, la mera extorsión a la que son sometidas las empresas ya conlleva un impacto económico, bien por los costes de reparación y limpieza de las infraestructuras afectadas, bien por el posible desembolso directo de la extorsión.

En las empresas pequeñas las consecuencias son mayores debido al menor margen de maniobra con el que cuentan.

Cambio en el modelo de negocio

El cibercrimen puede tener consecuencias para las empresas más allá del aspecto económico. En ocasiones es necesario replantearse la forma en que se tratan, almacenan y protegen los datos y la información sensible para asegurarse de que los sistemas informáticos existentes no vuelvan a ser vulnerables.

De hecho, en ocasiones se opta por no volver a almacenar los datos personales especialmente sensibles, así como los datos financieros de sus clientes, tales como tarjetas de crédito o fechas de nacimiento, por el riesgo que ello conlleva de cara a las potenciales multas y sanciones.

Pérdida de confianza

Tras sufrir un ciberataque, la preocupación de los clientes, socios y accionistas puede afectar a la credibilidad y confianza de la empresa, cuestionado la capacidad de la misma para protegerse de este tipo de incidentes, pudiendo repercutir tanto en la reputación externa hacia los clientes como en la confianza de los socios y accionistas.

Por un lado, los empleados se sentirán inseguros y, lo más importante, los clientes podrían dejar de serlo, ya que se ha violado, aunque sea por medio de personas ajenas a la empresa, su privacidad al acceder a sus datos.

¿CÓMO TENGO QUE PROCEDER SI ACCEDEN A MI BASE DE DATOS DE CLIENTES?

Si una empresa tiene conocimiento de que se ha accedido a su base de datos de clientes, debe realizar dos acciones en paralelo. Por una parte, poner en marcha las medidas necesarias que le permitan contener la brecha de seguridad, siempre tratando de que no se pueda poner en peligro las evidencias legales necesarias para la toma de acciones legales.

Es difícil determinar las acciones específicas a llevar a cabo, ya que dependen en gran medida del incidente, el número y distribución de los sistemas informáticos afectados y el servicio que preste la empresa. Lo más habitual sería aislar los sistemas informáticos afectados y acudir a especialistas de seguridad para la extracción de información relevante que

permita esclarecer las causas, la autoría y el alcance de la brecha de seguridad, siempre tratando de no modificar evidencia alguna.

En paralelo a esa primera acción, es necesario dirigirse a las Fuerzas y Cuerpos de Seguridad del Estado (FCSE) para interponer la denuncia correspondiente de cara al inicio de las investigaciones que permitan esclarecer los hechos.

Según la legislación vigente, se deberán abrir los procesos de notificación pertinentes en los plazos establecidos. Por ejemplo, en el caso de la Directiva Europea GDPR (Reglamento de la UE 2016/679), se identifican dos procesos de notificación: una a la autoridad de control (Agencia de Protección de Datos) y otra a las personas afectadas, aunque este último proceso incluye exenciones en el caso de la existencia de medidas que contrarresten la vulneración de los datos de los afectados o la imposibilidad de que sean fácilmente identificables.

¿EN QUÉ GASTOS ECONÓMICOS PUEDO INCURRIR EN CASO DE SUFRIR UN ATAQUE?

Los principales gastos en los que puede incurrir una empresa como consecuencia de un ciberataque son:

- Daños causados a terceros como consecuencia de la vulneración, robo o deterioro de la información de éstos en poder de la empresa que ha sufrido el ciberataque.
- Costes de la restauración de los sistemas del software dañado.
- Costes de la restauración, así como de la recuperación de los datos robados.
- Costes de descontaminación del *malware* y de la restauración de los sistemas de control de acceso.
- Pérdidas económicas derivadas de la paralización de la actividad causada por un ciberataque.
- Extorsión por parte de los delincuentes.
- Costes de actualización de los sistemas de seguridad, como antivirus, *firewalls*, etc.

- Multas impuestas por parte de la Agencia de Protección de Datos derivadas de la vulneración de datos de carácter personal.
- Gastos derivados de la obligación de notificación a terceros por violación de su privacidad en base a lo establecido en el Reglamento de la UE 2016/679, de tratamiento de datos personales y libre circulación de estos en el curso de una actividad profesional o comercial.
- Gastos asumidos por la empresa para restituir su imagen dañada públicamente como consecuencia de la imposición de una sanción por la Agencia de Protección de Datos.

¿PUEDE TENER CONSECUENCIAS LEGALES PARA UNA EMPRESA EL HECHO DE SUFRIR UN CIBERATAQUE?

Como indicábamos anteriormente, en este momento hay un debate sobre la necesidad de una mayor regulación legal en esta materia, de tal forma que se genere una mayor seguridad jurídica.

Un ejemplo de ello es la homogeneización de la regulación legal en materia de Protección de Datos llevada a cabo por parte de la Unión Europea a través del mencionado Reglamento de la UE 2016/679, de cumplimiento obligatorio para los Estados miembros a partir del 25 de mayo de 2018.

Este nuevo Reglamento europeo establece una serie de obligaciones legales que las empresas deben cumplir en materia de protección de datos, estableciendo asimismo las consecuencias derivadas de su incumplimiento y que se materializan, por ejemplo, en la imposición de multas.

¿CUÁLES SON LAS OBLIGACIONES MÁS RELEVANTES?

El artículo 33 de dicho reglamento establece la obligación de notificar una violación de la seguridad de los datos personales a la autoridad de control por parte del responsable de los datos, sin dilación, y a más tardar 72 horas después de haber tenido conocimiento de la violación de seguridad de los datos personales.

Asimismo, el artículo 34 establece la obligación de comunicar una violación de la seguridad de los datos personales al interesado siempre que entrañe un alto riesgo para los derechos y libertades de las personas físicas.

Además, el reglamento establece un nuevo régimen sancionador. Las multas económicas se incrementan respecto de los rangos establecidos hasta la fecha en nuestra normativa nacional recogida en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y que deberá adaptarse a las exigencias del reglamento europeo, y pueden alcanzar hasta 20 millones de euros o hasta el 4% del volumen de negocio mundial, pudiendo elegir la autoridad competente la imposición de la cifra más elevada.

¿LOS PROVEEDORES ME PUEDEN INFECTAR?

Uno de los factores que más complican el escenario actual es la denominada hiperconectividad. Es un factor que afecta a toda la sociedad. Todas las personas están conectadas en todo momento con muchas otras personas por diferentes medios (Whatsapp, Facebook, Twitter, etc.). La tecnología ha cambiado la forma de relacionarse entre las personas.

Además, esta hiperconectividad también afecta de manera general a las empresas, puesto que éstas también están hoy en día mucho más conectadas entre sí. Este nuevo escenario presenta grandes ventajas competitivas a las empresas, puesto que mejora la colaboración entre ellas en todos los campos, acortando tiempos de espera, costes, etc.

Sin embargo, este escenario de amplia conectividad también conlleva una serie de riesgos, ya que, al estar una empresa conectada con sus proveedores, las amenazas de ciberseguridad que puedan afectar a éstos también pueden trasladarse a la empresa.

Por ejemplo, un virus que afecte a un terminal podrá propagarse de una empresa a otra si no se han tomado las medidas de filtrado de red adecuadas.

II

MEDIDAS PREVENTIVAS ANTE LOS CIBERRIESGOS

¿QUÉ MEDIDAS PUEDO ADOPTAR PARA PREVENIR UN CIBERATAQUE?

Aunque no es posible hablar de una protección completa en el ámbito de los ciberriesgos, existen algunas prácticas que las empresas pueden aplicar para tratar de reducir la posibilidad de verse afectadas:

- **Concienciar a los usuarios:** Mantenerlos informados de los riesgos a los que está expuesta la empresa, de los impactos que puede conllevar la materialización de los ciberriesgos y de las medidas mínimas que deben aplicar en el ejercicio de sus funciones en la empresa.
- **Definir políticas de seguridad de la empresa y de uso adecuado de los equipos informáticos:** La política de seguridad fija la posición de la dirección de la empresa con respecto a los ciberriesgos. Todas las acciones que se realicen en la empresa deberán ir alineadas con dicha política de seguridad. Adicionalmente, la política de uso de los sistemas informáticos de la empresa permite definir reglas de uso en la normativa y en los sistemas de seguridad que ayudan a prevenir los ciberriesgos.

  Por ejemplo, se puede asignar una serie de reglas de navegación web que controlen la reputación de los sitios a los que se tiene pleno acceso, evitando que un empleado navegue por sitios maliciosos.
- **Diseñar una solución de seguridad a medida:** No existen fórmulas mágicas en el ámbito de la seguridad. Cada empresa requiere sus propios niveles de seguridad adaptados a sus procesos, sistemas y modelo de negocio. Por ello, se recomienda el asesoramiento profesional externo para la identificación y obtención de las medidas de seguridad que necesita la organización (en algunos casos dependerá de las capacidades económicas o de personal).

- **Construir capacidades preventivas y mitigadoras frente a los ciberriesgos:** Hay que tener en cuenta tanto la puesta en marcha de medidas para disminuir el riesgo de sufrir un incidente de seguridad como otras medidas que doten a la organización de capacidad de respuesta cuando se haya producido un ciberataque. En función de las capacidades y estrategia de la empresa se podrán construir dentro de ésta o externalizarlas con apoyo de proveedores.
- **Asegurar una línea base de seguridad que sea sencilla y suficiente:** A pesar de no suponer una garantía cien por cien segura para no sufrir ataques, es más adecuado tener una línea base mínima de seguridad que se cumpla que abordar muchas iniciativas que no se lleguen a cumplir nunca.

¿QUÉ LÍNEA BASE DE SEGURIDAD PODRÍA ADOPTAR?

Una línea base que se emplea en muchas empresas se centra en los siguientes aspectos:

- **Disponer de un inventario de sistemas y aplicaciones:** No se puede proteger lo que no se sabe que existe.
- **Aplicar una plantilla de seguridad mínima sobre los equipos y sistemas informáticos,** de forma que se establezcan las funcionalidades mínimas o aceptables que deben de cumplir, evitando riesgos innecesarios.
- **Disponer de software antivirus:** Aunque no es garantía, y los ratios de detección de los antivirus ha disminuido sensiblemente en los últimos años, sigue siendo un software mínimo del que no se debe prescindir.
- **Actualización permanente:** La tecnología es imperfecta y con el tiempo se convierte en insegura. Es fundamental disponer de una política de actualización tanto de parches como versiones que garanticen que los equipos y sistemas están dentro de un ámbito de actualización razonable.
- **Realizar copias de seguridad periódicamente:** Tanto los fallos de los sistemas como los incidentes de seguridad pueden conducir a una eliminación o pérdida de información. Ante este tipo de situaciones, la práctica más efectiva y eficiente consiste en realizar copias de seguridad de los datos y sistemas con una periodicidad suficiente que garantice el funcionamiento futuro de una empresa (tras su restauración).

SI TENGO UN ANTIVIRUS, ¿ESTOY TOTALMENTE PROTEGIDO?

Los sistemas antivirus son principalmente software que se desarrolla en paralelo a los sistemas operativos (Windows, Mac, etcétera). Su finalidad es detectar el uso de software malicioso. Se trata de una medida que se viene aplicando desde prácticamente el principio del uso del ordenador personal.

A pesar de ser una medida imprescindible de protección frente a los ciberriesgos, no es una medida totalmente efectiva sobre la que se pueda centrar exclusivamente nuestra estrategia de seguridad.

Por ejemplo, durante el año 2016 se identificaron 127 millones diferentes de muestras de virus, lo que viene a ser un virus nuevo cada 4 segundos. Los fabricantes de antivirus actualizan como mucho entre dos y tres veces al día los ficheros de detección de virus, por lo que, aunque se diera por hecho que los antivirus detectaran todos los virus, siempre quedaría una ventana por la que podrían entrar esos virus y los equipos se encontrarían desprotegidos (la ventana entre actualización y actualización).

La seguridad debe ser aplicada desde un punto de vista estratégico y técnico, que debe abordarse desde diferentes líneas de acción. De la misma manera que para la protección contra el fuego de un edificio una empresa no se limita a colocar extintores, sino que define una estrategia que suele pasar por la implantación de diversas medidas como un sistema de extinción de incendios, sistemas de detección, empleo de puertas y materiales resistentes al fuego, una estrategia de seguridad informática implica la definición e implantación de diferentes medidas como cortafuegos o *firewalls,* redes segregadas, aplicación de plantillas de seguridad, contraseñas robustas, etc.

¿QUÉ PUEDO HACER PARA PROTEGER EL CORREO ELECTRÓNICO?

El correo electrónico es uno de los principales medios de comunicación utilizados hoy en día, tanto a nivel particular como profesional. El correo electrónico se basa en una tecnología que se definió en 1982 cuando el escenario de la tecnología era muy diferente al que tenemos hoy en día. Los ordenadores se contaban por millares a nivel mundial, cuando hoy el número de dispositivos según algunas consultoras llega casi a los 9.000 millones.

Esta tecnología utilizó los mismos principios sobre los que se basaba el correo ordinario, sin entrar en los posibles malos usos que se podían derivar, y no se tuvo en cuenta que mientras el correo ordinario presenta una serie de barreras de entrada por coste, en el correo electrónico estas barreras desaparecían, ya que es posible enviar tantos correos electrónicos como la cantidad de tiempo

que se necesite en generarlos. Así, el correo electrónico presenta en la actualidad varias amenazas, las más relevantes son:

- Información en claro: A la hora de enviar un correo, toda la información que lleve éste en el cuerpo, asunto, destinatarios o adjuntos, es accesible por cada uno de los puntos por los que ese correo pasa a través de internet.
- Ausencia de mecanismos de control de alteración del contenido: Al igual que en el punto anterior, un correo electrónico puede ser manipulado sin conocimiento de ninguna de las partes (emisor y receptor) en cada uno de los puntos por los que pasa durante su transmisión.
- Imposibilidad de legitimar la fuente: El campo del emisor o *sender* es un texto en claro que puede ser rellenado a voluntad de la propia persona que envía el correo (igual que un sobre enviado por correo ordinario).
- Envío masivo de correo no deseado o malicioso: El bajo coste[2] que supone enviar correos electrónicos ha propiciado el empleo de este medio como propagación de publicidad no deseada, fraudes e intentos de estafa, e incluso la distribución de virus.

Estas amenazas han provocado que, a pesar de que el correo electrónico presenta unas características potenciales muy interesantes para la relación cliente-empresa, no haya sido explota-

[2] Sin desembolso económico directo, tan sólo es necesario un equipo informático, una base de datos de e-mails y una conexión a internet. A diferencia del correo ordinario, no existen prestadores de servicio exclusivos y/o autorizados, puesto que ello iría en contra del principio base de neutralidad de Internet.

do en su totalidad e incluso haya sido abandonado por algunos sectores como el bancario.

Existen diferentes medidas que, de alguna manera, ayudan a mitigar la situación, aunque han tenido un nivel de implantación desigual. No obstante, durante los últimos años se ha potenciado el uso de estos mecanismos para tratar de revertir la situación:

- **Sistemas de filtrado de correos** *(antispam):* Este tipo de sistemas utiliza diferentes mecanismos para determinar si el correo electrónico recibido se corresponde con un correo no deseado. Aunque la efectividad de estos sistemas no es total, su uso previene gran parte de los incidentes de seguridad que puede tener una empresa.
- **Sistemas de cifrado de información** (PGP, SMTP SSL y DKIM): Se trata de tecnologías que cifran la información que se transmite. Algunas de estas tecnologías ofrecen también mecanismos de control ante la alteración del contenido.
- **Sistemas de comprobación de identidad del emisor** (SPF, PGP y DMARC): Son medidas de seguridad que pueden ayudar a garantizar al emisor (persona que escribe el correo) en diferentes grados, desde un dominio entero (por ejemplo, @midomnio.com) hasta un usuario en particular.

No obstante, la implantación de estas medidas no es sencilla y requiere un análisis por parte de la organización. Además, las empresas a las que se destinan los correos también deben adoptar las mismas medidas, ya que, en caso contrario, estas no serán efectivas.

¿CÓMO ME PUEDO PROTEGER FRENTE A LA ENCRIPTACIÓN DE ARCHIVOS O RANSOMWARE?

Ya hemos visto que el *ransomware* es un tipo de virus que se centra en la encriptación de ficheros de un equipo informático con una clave secreta con el objeto de solicitar posteriormente un dinero por la revelación de la clave.

La protección contra este tipo de virus es compleja, ya que la manera en la que un *ransomware* funciona no dista mucho de cómo funciona un sistema de compresión de datos[3].

La situación complicada y excesivamente dinámica de los virus, como anteriormente se ha expuesto, y la dificultad de detección hacen que el tratamiento de las amenazas del *ransomware* sea difícil tanto en el ámbito empresarial como en el doméstico. Esto hace que, adicionalmente a las medidas básicas de seguridad que se han comentado anteriormente, se ponga especial atención en las siguientes:

[3] En muchos casos el encriptado de datos es muy similar a una compresión. En líneas generales el funcionamiento del software Winzip® y Winrar® puede entenderse como parecido al de un *ransomware*.

- **Concienciación de los usuarios** ante situaciones sospechosas. Las formas más habituales que propician la entrada de *ransomware* en las empresas son los correos con contenido malicioso y la descarga de software de sitios maliciosos o infectados. Es crucial que los empleados estén alerta y notifiquen cualquier situación que les pueda parecer sospechosa.
- **Copias de seguridad** con suficiente periodicidad. Una vez que un *ransomware* ha encriptado la información, no existe garantía alguna de que ni aun pagando se pueda recuperar la información, por lo que la única esperanza es la recuperación mediante copia de seguridad. Para garantizar que esta estrategia sea adecuada la empresa tiene que hacer el ejercicio mental de ponerse en situación de determinar cuál sería el daño de perder una información y tener que funcionar con un *backup* o copia de seguridad.
- **Sistemas de detección,** haciendo especial hincapié en el software antivirus, sistemas de filtrado de emails y sistemas de filtrado web.

Ninguno de ellos es efectivo al cien por cien, aunque una combinación puede ayudar a evitar la mayoría de las amenazas.

¿ES OBLIGATORIO EL USO DE CONTRASEÑAS?

El empleo de contraseñas es una de las medidas básicas de seguridad, pero, al igual que pasa con todas las medidas, no es suficiente para garantizar una seguridad total.

TODO SISTEMA DE SEGURIDAD CUYO ACCESO NO DEBA SER UNIVERSAL DEBERÁ DISPONER DE UN CONTROL DE ACCESO.

El sistema de control de acceso más básico y de uso generalizado es el de usuario personal[4] y contraseña. Aunque este sistema presenta ciertas carencias, se puede reforzar su seguridad siguiendo las siguientes pautas:

- Longitud mínima de 8 caracteres.
- Cambio periódico cada 3 meses.
- Bloqueo tras 10 intentos de uso.
- Combinación de uso de mayúsculas, minúsculas y números u otros signos de puntuación.

La aplicación de estas medidas se puede ajustar en función de la realidad de la empresa. El objetivo que se persigue es el de evitar que una tercera persona pueda tratar de adivinar una contraseña.

El uso de usuarios personales y contraseñas, como se ha dicho, es un sistema que presenta ciertas carencias y que hace no recomendable su uso en todos los escenarios. Estos pueden ser sistemas críticos, sistemas con información especialmente sensible o accesos remotos a redes internas. En estos escenarios se recomienda el uso de otras tecnologías adicionales, que deberán valorarse de acuerdo con el escenario particular de la empresa.

¿PUEDEN ACCEDER A MI SISTEMA A TRAVÉS DE LA WEB?

Todo sistema conectado a Internet es susceptible de ser traspasado tras un ciberataque. Ello no quiere decir que el riesgo sea inmi-

[4] Se entiende por usuario personal aquel que identifica de manera inequívoca a un individuo.

nente, pero no hay que olvidar que los servidores web están basados en tecnología que con el paso del tiempo se torna en insegura, bien porque queda obsoleta, bien porque se van descubriendo vulnerabilidades de seguridad que hacen necesario que se deban aplicar parches de seguridad para solventar esta situación.

Internet es uno de los pilares fundamentales sobre los que se desarrollan las nuevas tendencias en tecnología. Para que un sistema pueda interactuar con los clientes a través de Internet este sistema debe estar conectado.

¿QUÉ SE PUEDE HACER PARA REDUCIR LOS RIESGOS A TRAVÉS DE LA WEB?

Podemos reducir los riesgos aplicando las siguientes medidas:

- **Publicar sólo lo estrictamente necesario:** Si se reduce la superficie de exposición (o publicado en web), se minimizan los riesgos. Una medida que se suele aplicar para reducir los riesgos en la web es la implantación de sistemas cortafuegos (o *firewall*) que limitan los accesos masivos o bloquean a aquellos usuarios no autorizados. Adicionalmente, se pueden limitar los accesos a páginas web o a servicios que deben estar disponibles para el buen funcionamiento de la compañía.
- **Hacer pruebas sustantivas de *hacking*:** La mejor forma de conocer las posibles vías de infección consiste en hacer intentos de intrusión o pruebas de *hacking* sobre los sistemas publicados para poder localizar vulnerabilidades que identifiquen posibles vías de acceso. Lo normal es que una empresa se apoye en proveedores específicos especializados en test de intrusión.

- **Aplicar plantillas de seguridad:** Una empresa debe prever que su sistema pueda llegar a ser tomado por un ciberdelincuente, por lo que hay que tratar de garantizar que esta situación no ponga en peligro el resto de sistemas de las redes internas de la empresa. Es habitual la limitación de capacidades o accesos a un sistema tras la aplicación de plantillas de seguridad. No obstante, es aconsejable adaptar las guías de seguridad al escenario particular de cada empresa mediante capacidades internas, o apoyándose en proveedores especializados en seguridad.
- **Proteger las redes internas:** De forma complementaria a la medida anterior, es muy recomendable limitar el acceso

a redes internas mediante la implantación de cortafuegos o *firewalls*, que bloquean el acceso a usuarios no autorizados a las redes internas de la empresa.

- **Disponer de medios de detección:** Como medio de control adicional, y cada día más necesario, las empresas deben disponer de medidas que les permitan identificar y responder ante actividades fraudulentas o potencialmente peligrosas sobre los sistemas que se encuentren accesibles desde internet.

No obstante, las distintas medidas que se pueden adoptar dependen de distintos factores, como, por ejemplo, del tipo de empresa, de los sistemas conectados a internet, de que la información publicada sea crítica para la compañía, de que los servicios que presta se realicen a través de internet, etc.

¿QUÉ HACER EN CASO DE SUFRIR CIBEREXTORSIÓN?

Las medidas a adoptar siempre van a depender del reclamo del ciberdelincuente, pero, como norma general, se recomienda en primer término la interposición de una denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado, que es un paso fundamental para que los delitos puedan ser perseguidos y juzgados.

Debemos recordar que el pago inmediato ante cualquier amenaza no garantiza la erradicación de la extorsión. Generalmente, los ciberdelincuentes suelen acudir de forma recurrente a las mismas empresas que acceden al pago de las cantidades, solicitando más dinero en cada una de sus solicitudes, hasta que finalmente la empresa deja de pagar y el ciberdelincuente procede a

materializar su amenaza. Por ello, la recomendación es no pagar bajo ninguna circunstancia.

Adicionalmente a la interposición de la denuncia, la empresa deberá poner en marcha los protocolos de gestión de incidentes de seguridad, comenzando por realizar un análisis de lo ocurrido lo antes posible para intentar volver a la normalidad. Esta medida suele pasar por la restauración de la información y de los sistemas, de tal forma que se garantice la inexistencia de software no autorizado.

En el caso de que la empresa no disponga de medios o capacidades de respuesta a incidencias de seguridad, se recomienda que la empresa acuda a solicitar soporte de proveedores de seguridad especializados.

III

EL SEGURO DE CIBERRIESGOS

¿EXISTEN SEGUROS EN EL MERCADO ESPAÑOL PARA DAR COBERTURA A ESTE TIPO DE RIESGOS?

En los últimos años se ha producido un incremento del interés del mercado asegurador español por dar cobertura a estos riesgos mediante el seguro de ciberriesgos. Si bien en origen estos seguros eran demandados por grandes empresas y los productos existentes se focalizaban en ellas, la generalización de los ataques a pequeñas y medianas empresas ha originado una demanda de seguro de ciberriesgos en este segmento empresarial.

En España son varias las compañías aseguradoras que han lanzado recientemente un producto específico, normalmente con coberturas paquetizadas, para cubrir los riesgos generados por un ciberataque, tanto para las pequeñas como para las medianas empresas.

Sin embargo, las grandes empresas requieren de productos especializados y elaborados de forma mucho más específica, según sus necesidades concretas.

Es importante remarcar que la gestión de los ciberriesgos es uno de los retos más complejos que afrontarán las empresas en los próximos años. Debe existir por parte de la empresa una planificación en su ciberseguridad en la que el seguro sea un elemento más en dicha gestión de riesgos, y no configurarse únicamente con un elemento paliativo.

¿CUÁLES SON LOS REQUISITOS PARA LA CONTRATACIÓN DE UN SEGURO DE CIBERRIESGOS?

Los requisitos de contratación varían en función de la dimensión de la empresa analizada, siendo en ocasiones necesaria la valoración in situ de los sistemas informáticos o el acceso informático remoto a los mismos.

Como tónica general, las aseguradoras solicitan la cumplimentación de un cuestionario en el que se recogen preguntas relativas a:

- Detalle de sus sistemas de protección informática, así como la madurez de los mismos.
- Tipología de información que obra en sus sistemas informáticos y que por tanto podría ser objeto de vulneración: información de carácter sanitario, afiliación, religión, datos bancarios, datos de tarjetas de crédito...
- Confirmación sobre si la empresa efectúa copias de seguridad de su información crítica y periodicidad de dichas copias. Las copias de seguridad son especialmente relevantes para poder restaurar esta información con la mayor celeridad posible tras un ciberataque, reduciendo de esta forma el tiempo de paralización de la actividad de la empresa.
- Incidentes informáticos que haya sufrido y detalle de los mismos.

Entre los requisitos mínimos de contratación se encuentran tanto disponer de un software antivirus original actualizado en todos sus equipos y servidores como contar con sistemas *firewall* para los servidores accesibles desde internet.

¿QUÉ INFORMACIÓN DE MI NEGOCIO DEBO PROPORCIONAR AL ASEGURADOR?

La información a facilitar varía en función de los parámetros de análisis de cada compañía aseguradora, si bien existen algunas variables comunes en los riesgos de pequeñas y medianas empresas:

- Tipología de actividad que desarrolla la empresa, puesto que en función de este dato el riesgo se configurará como sencillo, agravado e incluso excluido.
- Volumen de facturación de la empresa.
- Cumplimentación del cuestionario en el que recogerán los sistemas de protección informática de la empresa y su grado de madurez.
- Suma asegurada que se desea contratar, entre otras cuestiones.

¿CUÁLES SON LAS COBERTURAS MÁS HABITUALES EN EL SEGURO DE CIBERRIESGOS?

- Cobertura de **Responsabilidad Civil**
  La configuración de la cobertura de Responsabilidad Civil varía en función del seguro analizado y es la más habitual. En general, da cobertura a los daños y perjuicios causados a terceros, e incluso a empleados propios de la empresa asegurada, como consecuencia del daño, robo, pérdida o revelación de los datos de carácter personal de dichos terceros, y, en ocasiones, de información de carácter confidencial, causados por un ataque cibernético.

- Cobertura de **Daños Propios**
  Daños propios son los daños que se producen en el bien asegurado. Entre las coberturas de daños propios más habituales destacan:
  – Daños a los sistemas informáticos del asegurado, que englobaría los costes de restauración o recuperación de datos dañados o robados, los costes de descontaminación y limpieza del virus *malware* y la restauración de los siste-

mas de control de acceso al sistema informático del asegurado, entre otros. En este punto, es importante que la compañía aseguradora no se limite a la asunción del coste sino que preste el servicio urgente de un proveedor de servicios tecnológicos especializados en este tipo de eventos, de tal forma que se acompañe al asegurado en este proceso desconocido para él, simplificando la restauración del daño sufrido.

- Pérdidas económicas del asegurado derivadas de la interrupción del negocio provocada por un ciberincidente.
- Gastos de notificación a terceros por violación de la privacidad de los mismos.
- Garantía de multas y sanciones impuestas por la autoridad competente en materia de protección de datos derivado de un incumplimiento legal.
- Gastos derivados de restitución de la imagen por sanciones impuestas por la agencia de protección de datos.

¿EXISTEN GARANTÍAS ESPECÍFICAS QUE AMPAREN LAS EXIGENCIAS ESTABLECIDAS POR LA LEY?

Es habitual la incorporación de dos coberturas que responden a las exigencias contenidas en el Reglamento de la UE 2016/679, de tratamiento de datos personales y libre circulación de éstos, mencionados en el punto anterior:

- Cobertura de notificación de violación de la privacidad de terceros, que da respuesta a la obligación de comunicación de un quebranto de la seguridad de los datos personales al interesado siempre que entrañe un alto riesgo para los derechos y li-

bertades de las personas físicas, y que se recoge en el artículo 33 del citado Reglamento.

En dicha cobertura se engloban, entre otros, gastos de asesoramiento legal para evaluar la violación de datos de terceros y asesorar sobre las medidas más apropiadas a adoptar, gastos de redacción por parte de un asesor legal de la notificación a cualquier tercero afectado por la violación de datos, así como los gastos de envío de dichas notificaciones, gastos de establecimiento de un servicio de atención telefónica para gestionar las llamadas en relación con la violación de datos o gastos de una investigación forense de los Sistemas Informáticos del Asegurado si fuera requerida por ley u organismo oficial.

- Cobertura de multas y sanciones impuestas por la Agencia de Protección de Datos como consecuencia de la vulneración de la normativa de protección de los datos de carácter personal.

IV

DECÁLOGO PARA PROTEGERSE FRENTE A LOS CIBERRIESGOS

DECÁLOGO PARA PROTEGERSE **FRENTE A LOS CIBERRIESGOS**

1 PREVENIR

Frente a cualquier riesgo, se deben adoptar las actuaciones necesarias para evitarlo o intentar minimizar sus consecuencias. El primer paso es una mayor concienciación en relación a los ciberriesgos y los daños que pueden provocar a todos los niveles de una empresa.

2 ADOPTAR MEDIDAS REALES Y EFICACES

El empresario debe establecer las medidas técnicas y organizativas necesarias de protección que permitan minimizar las probabilidades de sufrir un incidente de seguridad. Es necesario que la empresa adopte las medidas básicas de ciberseguridad especificadas en el capítulo II de la presente guía.

3 ANALIZAR SOLUCIONES ASEGURADORAS

La empresa debe analizar los riesgos; tanto los que decide asumir como los que decide transferir, y valorar las necesidades reales de protección de cada negocio y actividad, y, en base a ello, seleccionar las diferentes soluciones aseguradoras. Para que el seguro que se contrate sea el adecuado se deben analizar conjuntamente las coberturas ofrecidas, la solvencia y solidez de la entidad aseguradora, los servicios adicionales ofrecidos por el seguro y, finalmente, el precio.

En el seguro de ciberriesgos es especialmente relevante que la compañía aseguradora cuente con un proveedor tecnológico especializado que preste una inmediata respuesta a la empresa asegurada en caso de que se produzca un ciberataque.

4 ASESORARSE

Se recomienda el asesoramiento de los profesionales del seguro. Es importante establecer en la póliza capitales asegurados suficientes y realistas, para lo cual es recomendable un análisis reposado que contemple todas las necesidades a cubrir.

5 RESOLVER

Antes de suscribir el seguro se deben resolver todas las dudas que surjan. Por su propia finalidad, las pólizas son documentos extensos y bastante técnicos; es importante conocer y comprender el significado de las diferentes coberturas y condiciones.

6 ARCHIVAR

Se debe conservar la documentación relativa a las pólizas, así como las sucesivas comunicaciones con la compañía. Resulta recomendable conservar en formato electrónico todos los documentos y contar con una copia de seguridad o almacenamiento en la nube.

7 ACTUALIZAR

Hay que mantener los contratos de seguros actualizados, ya que los riesgos cambian con el paso del tiempo, y en materia informática los cambios se producen con mayor celeridad. Estos cambios deben recogerse en las pólizas para que estemos tranquilos con las coberturas contratadas.

8 CONTACTAR

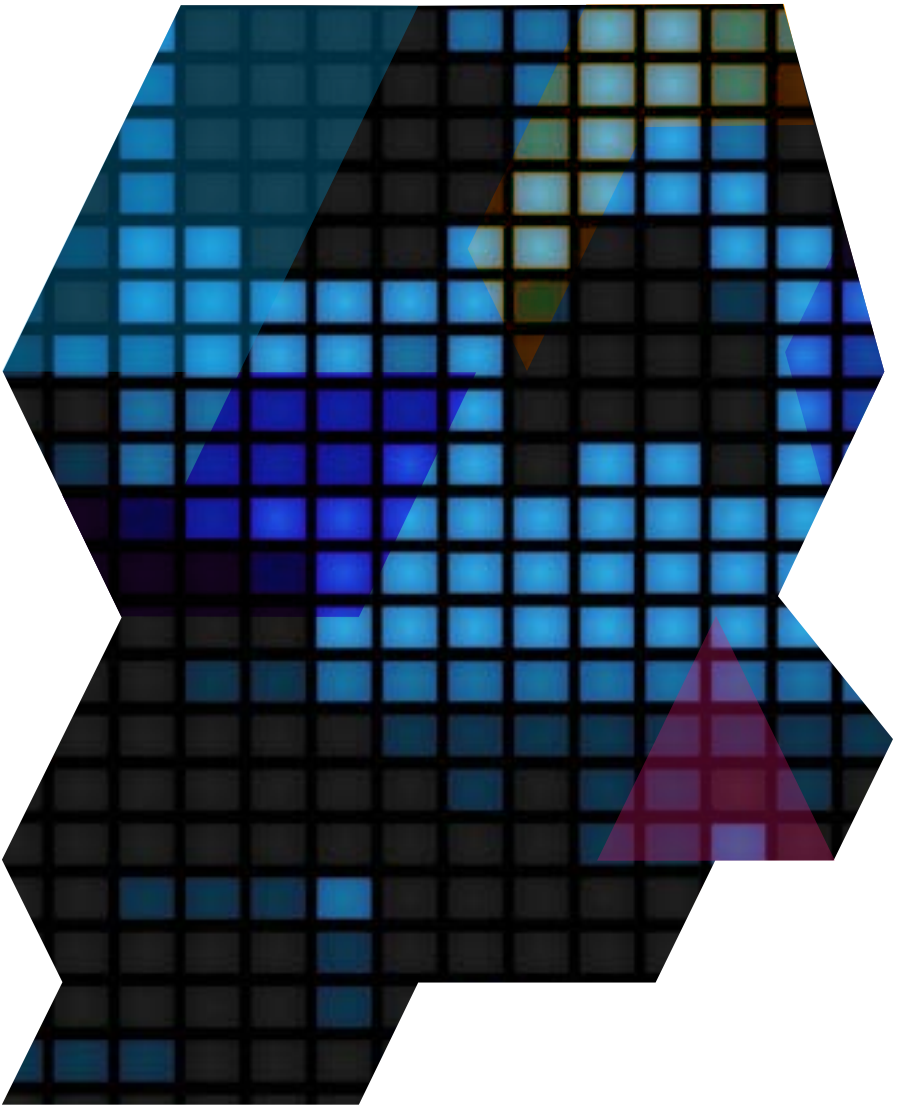
Informar a la compañía aseguradora, tan pronto como sea posible, de todos los cambios que afecten a las pólizas, como cambios en la actividad asegurada, en la tipología de información almacenada, etc.

9 ACTUAR

En caso de siniestro, las actuaciones a seguir se resumen en: primero, intentar mitigar el daño; seguidamente, dirigirse a las Fuerzas y Cuerpos de Seguridad del Estado (FCSE) para interponer la denuncia correspondiente. A su vez, notificarlo a la aseguradora urgentemente para que ponga a disposición del asegurado a los profesionales especializados en materia cibernética que puedan analizar el siniestro e iniciar de forma inmediata las acciones de restauración de los sistemas informáticos. En caso de que otras personas o bienes de terceros hayan sido perjudicados, comunicarles la existencia de un seguro.

10 CONFIAR

Hay que confiar en la protección que ofrece el seguro. Y para cualquier cuestión que surja, ponerse en contacto con la compañía o con su agente de seguros de confianza. Aunque no seamos conscientes, el seguro funciona desde el momento en que se contrata; y si no tenemos que comunicar ningún posible siniestro, ¡es la mejor señal de que todo va bien!



CENTRO DE DOCUMENTACIÓN

Todas nuestras publicaciones a tu alcance

Además del acceso gratuito a nuestro fondo documental especializado en:

- Seguros
- Gerencia de riesgos
- Prevención

Fundación MAPFRE

Centro de Documentación

www.fundacionmapfre.org/documentacion

Fundación **MAPFRE**

Síguenos en:

www.**fundacionmapfre**.org
Tel. **(+34) 91 602 52 21**