¿Qué impacto puede tener en tu empresa un ciberataque?

En un entorno cada vez más conectado, en el que las tecnologías de la información y las comunicaciones han venido ganando un creciente protagonismo, como también lo está haciendo el avance de la digitalización y la red de infraestructuras digitales, la empresa no puede permanecer ajena al alcance de los ciberriesgos y ha de realizar una adecuada gestión de la ciberseguridad.

Ana Domínguez

La hiperconectividad existente ha traído importantes ventajas a las empresas, así como a la economía y la sociedad en su conjunto, permitiendo una mayor accesibilidad a la información, a bienes y servicios y a nuevos mercados, a la par que una más fácil difusión del conocimiento e incluso una mayor democratización de las capacidades para innovar y competir. Pero para aprovechar estas ventajas es necesario moverse en un terreno confiable, ya que con el proceso de digitalización están aflorando nuevos riesgos (intrusiones de software malicioso, robo de información de carácter personal o confidencial, denegación de acceso a servicios, etc.) cuyo impacto en la empresa, en caso de producirse algún incidente, puede ser elevado.

En este contexto, resulta ciertamente oportuno identificar los riesgos y amenazas contra la ciberseguridad y los sistemas de información de la empresa, y gestionarlos adecuadamente. Una gestión que ha de ser planteada con un carácter de largo plazo, teniendo además presente que una cobertura del 100% no es

iStock/Thinkstock.

alcanzable, condicionado ello en gran medida por el carácter extraordinariamente cambiante del entorno tecnológico (aunque tampoco sería eficiente, en términos de coste).

¿Conoce tu empresa el alcance de los ciberriesgos a los que está expuesta?

Algunas estimaciones apuntan a que los ataques con-

tra la ciberseguridad pueden ocasionar en las empresas españolas pérdidas superiores a los 13.000 millones de euros anuales[1].

Más allá del impacto económico, que puede ser cuantioso e incluso poner en jaque la viabilidad del negocio, las consecuencias de los ciberataques pueden ser también dramáticas para la empresa en términos de reputación e imagen de marca. Las empresas están expuestas por tanto a pérdidas en sus capacidades operativas, a la falta de acceso a información relevante propia, a daños en el valor de la marca, etc.

Lejos de ser un fenómeno atípico, los ciberataques o la proliferación de ciberamenazas han venido incrementándose. El número de incidentes y amenazas gestionados en España por el Instituto Nacional de Ciberseguridad (Incibe) relativos tanto a ciudadanos como empresas, ha pasado de los 14.715 incidentes registrados en 2014 hasta los 45.689 en 2015. Los ataques más frecuentes acaecidos durante el año pasado se refieren al cibercrimen y la fuga de información. Asimismo, fueron publicados 134 avisos de vulnerabilidades en ciberseguridad dentro de la industria española, que han afectado a todos los sectores considerados estratégicos, aunque ha sido el energético el más impactado, de acuerdo con los datos de Incibe.

En cuanto al grado de criticidad de esos avisos, los que tienen la consideración de «alta» y «crítica» (máxima criticidad) representan dos tercios del total. Estos avisos ponen en relieve la inseguridad de la información almacenada o manejada; y se manifiesta en avisos ligados a credenciales embebidas en los dispositivos y falta de cifrado o de autenticación, entre otros.

Gestionar los ciberriesgos es clave

La gestión de los ciberriesgos pasa por entender y priorizar los activos físicos y la información más relevante para la empresa. Es preciso evaluar las amenazas y debilidades que resulten singulares para la propia empresa (el sector al que pertenece también condiciona la tipología y exposición a posibles incidentes) y alinear estas con los bienes prioritarios para la organización.

La Cámara de Comercio Internacional (CCI) destaca que un 35% de los incidentes que afectan a la seguridad de la información son consecuencia de errores humanos. Y del 65% restante, más de la mitad responderían a ataques intencionados evitables si los recursos humanos hubiesen utilizado la información bajo estándares de mayor seguridad. Por tanto, la sensibilización y concienciación del personal de la empresa resulta fundamental.

Las empresas han de ser proactivas en este campo de la ciberseguridad e implementar medidas preventivas que promuevan el desarrollo de capacidades organizativas eficaces para la gestión de los riesgos que atentan contra dicha ciberseguridad. En este sentido, es importante analizar los riesgos a los que está expuesta la empresa y poner especial atención en aquellos activos que han de estar más protegidos. También se apela al liderazgo para una óptima toma de decisiones e implementación de las mejores prácticas en materia de seguridad de la información, así como al establecimiento de procedimientos, dentro de la empresa, para hacer frente a potenciales ciberataques, mediante una eficaz detección y respuesta a los mismos. La empresa ha de estar preparada para activar un protocolo de respuesta y evitar la improvisación. Pero también aprovechará las oportunidades de aprendizaje que afloren al ejecutar la respuesta al ciberataque y con ello corregir los mecanismos de respuesta diseñados, en un proceso que se retroalimenta de cara a ajustarse a las mejores prácticas en la gestión de riesgos.

Estas pautas vienen recogidas en la Guía de seguridad ICC para los negocios que acaba de publicar la Cámara de Comercio Internacional, que orientarán el abordaje de los desafíos de la seguridad de la información y la gestión de riesgos para mejorar el entorno de ciberseguridad empresarial. A continuación

se analizan los principios y acciones básicas que pueden seguir las empresas.

¿Cómo actuar ante los riesgos de ciberseguridad?

El tipo de negocio de la empresa, su tamaño, el grado de interconexión de que goce, el nivel de riesgos al que esté expuesta, o las exigencias regulatorias son algunos de los condicionantes del enfoque sobre la seguridad de la información que ha de adoptar la empresa. Sin embargo, pueden definirse una serie de principios básicos de actuación que dan soporte a la implementación de buenas prácticas y que serían aplicables a cualquier tipo de empresa, con independencia de su dimensión o del sector de actividad al que pertenezca. En la Guía de seguridad ICC para los negocios se hace alusión a seis principios fundamentales.

El primero de los principios se refiere a una **focalización en la información** (vs la tecnología) en un contexto en que la cuestión de la seguridad de la información involucra a toda la organización y no sólo al área de tecnologías de la información: desde el equipo de profesionales, los productos / servicios y procesos, las instalaciones, hasta las políticas, procedimientos, tecnologías, sistemas y la propia información. La empresa ha de velar por proteger la información considerada de mayor valor y los sistemas cuya pérdida de confidencialidad, disponibilidad o integridad conllevaría un fuerte perjuicio para la compañía.

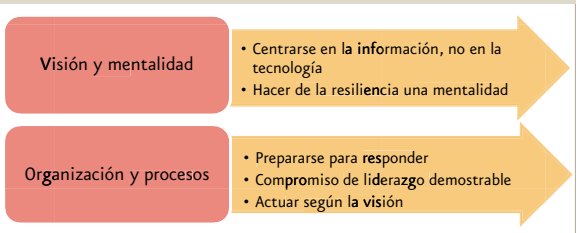
Un segundo principio aboga por una **mentalidad resiliente** frente al riesgo de pérdida o menoscabo de información, teniendo en cuenta que la velocidad con la que aparecen nuevas amenazas a la ciberseguridad es mucho mayor que la de adaptación de los marcos regulatorios. De ahí la importancia de que la empresa analice periódicamente, mediante auditorías internas y/o externas, sus vulnerabilidades y el nivel de protección frente a tales amenazas. La dirección de la empresa debe involucrarse tanto en la identificación de los problemas como en velar recurrentemente por la existencia de un entorno adecuado en el que todo el equipo sea consciente de la importancia de gestionar los riesgos que inciden en la ciberseguridad. La mentalidad resiliente se hará así patente en toda incorporación de nuevos dispositivos e innovaciones en procesos, que vendrán acompañadas de la adopción de las oportunas medidas de seguridad.

El tercer principio apela a la **preparación para responder**, en tanto que la empresa ha de contar con un plan de respuesta frente a incidentes que atenten contra la ciberseguridad, para que su impacto en la organización sea el menor posible. En dicho plan se identificará cuándo se requiere la intervención de terceros (tanto especialistas en ciberseguridad, como policía u otros) y se contemplará la estrategia de comunicación a implementar en la respuesta a una incidencia.

El cuarto principio habla de **demostrar un compromiso de liderazgo**, de forma que el equipo directivo de la empresa participe activamente en la supervisión de las políticas de gestión de riesgos asociados a la ciberseguridad, asegurándose una correcta asignación de recursos financieros y humanos para la protección frente a dichos riesgos, así como la creación de una función, dentro de la empresa, de seguridad de la información. El equipo directivo, junto con el Consejo de Administración de la empresa y los auditores, han de recibir un informe, al menos una vez al año, sobre la eficacia e idoneidad de las medidas de seguridad de la información existentes. La información sobre este desempeño servirá para adoptar las oportunas decisiones en materia de seguridad. Nuevamente, se hace hincapié en la necesidad de concienciar a todo el equipo sobre la relevancia de la seguridad de la información.

El quinto y último principio propone **actuar de acuerdo con la visión propia**, confeccionando distintas políticas de seguridad de la información, como soporte que oriente las acciones de seguridad e incremente la concienciación sobre la misma dentro

PRINCIPIOS FUNDAMENTALES PARA LA CIBERSEGURIDAD EN LA EMPRESA



Fuente: *Afi, a partir de Guía de seguridad ICC para los negocios.*

de la empresa. Dichas políticas determinarán una serie de procedimientos operativos, teniendo en cuenta la configuración de la cadena de valor y el flujo de información entre distintos agentes externos y las relaciones de interdependencia existentes, ya que la falta de protección de uno de esos agentes no deja de ser una fuente de riesgo para la empresa. De ahí la conveniencia de que los proveedores de la empresa también implementen estos principios de seguridad de la información.

¡Actúa! Algunas acciones básicas

Además de los cinco principios enunciados, en la guía de la Cámara de Comercio Internacional se incluye media docena de acciones que podría poner en práctica cualquier empresa, sea pyme o grande, para mitigar los ciberriesgos.

Hacer una copia de seguridad de la información, así como validar su contenido y los procesos de prueba de recuperación de dicha información, y en caso de utilizar servicios en la nube (uso de un proveedor de servicios externo para el almacenamiento, procesado y gestión de datos en Internet) verificar que se realizan los *back-ups* para recuperar la información, es una de la prácticas esenciales.

También se han de actualizar los sistemas de tecnologías de la información, mediante parches de seguridad y actualizaciones de *firmware*, para reducir su grado de vulnerabilidad frente a posibles ciberataques. En este sentido, se recomienda la utilización de servicios automatizados para actualizaciones de aplicaciones *antimalware*, herramientas de filtrado web y otras relativas al sistema de seguridad.

Es igualmente importante invertir en la concienciación y capacitación de los RR. HH. de la empresa sobre los ciberriesgos y los aspectos de ciberseguridad, dotándose de una cultura organizativa de gestión relativos a la seguridad de la información. Esto resulta clave para que todo el personal de la empresa tenga claro cuáles son sus responsabilidades y cuente con las habilidades necesarias para ejercerlas. En caso contrario, podrían representar incluso fuentes de riesgo.

La empresa ha de poder controlar su entorno de información, de tal forma que en caso de incidencia sobre la seguridad de la información, los sistemas y procesos existentes emitan la oportuna alerta. Para ello, existen distintas soluciones tecnológicas, como los sistemas de prevención y detección de intrusiones y de gestión de incidentes de seguridad; pero también es necesario realizar un seguimiento permanente y analizar la información que captan esos sistemas.

Por otra parte, para reducir los ciberataques o incidentes de seguridad de la información es importante desarrollar una defensa en varias capas, combinando distintas técnicas (protección proactiva contra *malware*, antivirus, filtrado web, cortafuegos, etc.) y con la posibilidad de recurrir al seguro de ciberriesgo.

Para completar la media docena de acciones básicas que la empresa puede poner en marcha para hacer frente a los ciberriesgos, habría que incluir la preparación previa para cuando la brecha se produzca, de cara a minimizar el perjuicio potencial en caso de acontecer la incidencia. Ello pasa asimismo por contar con un plan para la rápida toma de decisiones y la coordinación de acciones para controlar los posibles incidentes ::

[1] García Cuesta, J. «Ciberseguridad, en defensa de la información». El Exportador. Sept. 2015.