Ciberseguridad

Estudio "Empresas y Ciberseguridad"

La otra cara de la digitalización: ¿es segura nuestra cadena de valor?

LEET SECURITY

ICT Services Rating Agency

Con la colaboración de:

CLUB EXCELENCIA EN GESTIÓN

inmark 40 aniversario

El proceso de digitalización global ha dibujado un nuevo escenario para las organizaciones marcado por una necesaria protección de la información como principal activo. En este nuevo entorno tecnológico, la ciberseguridad se convierte en un valor clave dentro de las compañías y en una garantía de confianza frente a clientes, proveedores y colaboradores.

Un 87% de los directivos está preocupado por la ciberseguridad de su empresa.

Pero, ¿en qué momento se encuentran las empresas españolas? ¿Son conscientes de los riesgos de la digitalización? ¿Cómo influye la externalización de servicios en la seguridad de sus propios procesos de negocio?

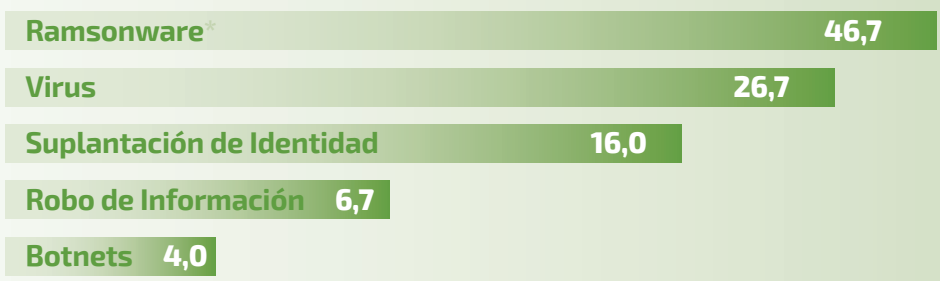
Para profundizar en estos aspectos, LEET Security, con la colaboración del Club de la Excelencia en Gestión (CEG) e Inmark, ha realizado el estudio "Empresas y Ciberseguridad" entre directivos de las principales empresas españolas. Sus resultados ponen de manifiesto que **las organizaciones deben marcarse como reto la protección de la seguridad de la cadena de valor, e incorporar unos procesos de supervisión y calificación de proveedores que les permitan conocer el nivel de protección que su información tiene cuando es gestionada por terceros**.

Actitudes ante la ciberseguridad y los ciberataques

Un 87% de los directivos está preocupado por la ciberseguridad de sus empresas. Y no es para menos, ya que cerca del 60% de estas compañías afirma ser consciente de haber sufrido un ciberataque.

A pesar de ello, todavía 1 de cada 4 organizaciones, considera muy alto el riesgo de sufrir un ciberataque, lo que significa que, es necesario reforzar las medidas para minimizar el riesgo de una posible brecha en

TIPOS DE CIBERATAQUE



la seguridad de sus sistemas.

La detección de los ataques es uno de los aspectos más relevantes actualmente, puesto que una identificación temprana es un elemento fundamental para la minimización del impacto de los ciberataques. De hecho, los elevados tiempos de detección de fugas de información es uno de los más importantes caballos de batalla de la ciberseguridad actualmente.

En cuanto al tipo de ciberataque recibido, en la mayoría de los casos (46,7%) fue un ransomware -programa malintencionado que restringe el acceso a archivos y pide un rescate por eliminar la restricción-, seguido de virus; la suplantación de identidad; el robo de información y el botnets.

Es también reseñable que, del 58,9% de empresas que reconocen haber sido víctimas de un ciberataque, **un 18,3% declara que el ataque ha utilizado como vector a un proveedor de la organización**. Una cifra que, aunque menor que la detectada por otros estudios, pone de manifiesto la necesidad de controlar los niveles de ciberseguridad de toda la cadena de valor.

CONSECUENCIAS DE UN CIBERATAQUE QUE MÁS LE PREOCUPAN

Preocupaciones

El estudio "Empresas y ciberseguridad" constata que los principales drivers para la toma de decisiones en el ámbito de la ciberseguridad son el económico y el legal.

Obviamente, los impactos económicos derivados de la indisponibilidad de los servicios junto con las potenciales sanciones, son los aspectos más considerados por los directivos. En este último punto, debemos recordar la especial relevancia que la protección de datos personales de los clientes tendrá en un futuro próximo, con la introducción del nuevo Reglamento Europeo de Protección de Datos en mayo de 2018.

En el capítulo de principales preocupaciones en términos de ciberseguridad, llama la atención el poco peso dado al robo de propiedad intelectual frente a las fugas de información o la protección de datos corporativa. No obstante, si consideramos el escaso papel de España

en el número de patentes a nivel mundial, podemos entender por qué no es un elemento básico en la toma de decisiones.

Responsables involucrados

Las organizaciones encuestadas señalan que la responsabilidad principal en materia de ciberseguridad se deposita, bien en el CISO (Chief Information Security Officer), o bien en el CIO (Chief Information Officer), aunque es grato comprobar como **casi el 70% de la Dirección General se involucra en esta materia**.

PRINCIPALES PREOCUPACIONES EN TÉRMINOS DE SEGURIDAD

Dado que la ciberseguridad tiene un alto componente técnico no es de extrañar el alto peso de las áreas técnicas como responsables en esta materia. No obstante, es importante señalar que las mejores prácticas recomendarían que la responsabilidad en materia de seguridad no recayeran en aquella persona que también es responsable de la gestión de los sistemas de información de la organización y que, en cualquier caso, el responsable de seguridad no dependiera del área técnica. Por dos motivos: primero, por evitar potenciales conflictos de intereses y, segundo, y no menos importante, porque la ciberseguridad no son solo medidas técnicas y requieren de la involucración de toda la organización: asesoría jurídica, gestión del personal, compras, etc.

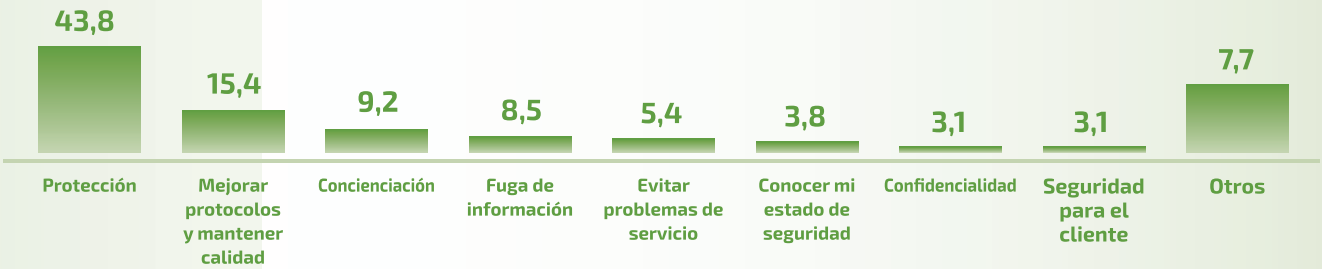
La seguridad de la cadena de valor

Sin lugar a dudas, la protección de la información y los sistemas ha sido revelada como la principal preocupación en materia de ciberseguridad, identificada como tal por un 43,8% de los encuestados.

Sin embargo, **aunque la protección es un factor esencial, como pone de manifiesto cualquier marco de ciberseguridad, no se puede considerar el único elemento, sino que debe de ir acompañado por mecanismos de detección temprana, respuesta rápida y apalancamiento en el incidente**. Es decir, por lo que se denomina una seguridad ágil que es fundamental para mejorar el nivel de resiliencia

en la organización puesto que no existen fortalezas inexpugnables en materia de ciberseguridad. Es por tanto esencial que la organización se preparare para responder cuando sufre el ciberataque.

¿CUÁL ES EL RETO PRINCIPAL EN MATERIA DE CIBERSEGURIDAD DE SU ORGANIZACIÓN?



Cadena de Valor

La subcontratación de servicios en terceros no es, en absoluto, una tendencia reciente. Sin embargo, los necesarios procesos de digitalización en organizaciones de todo tipo y tamaño está incrementando el nivel de dependencia de dichos terceros, especialmente cuando sus colaboraciones son esenciales para hacer posibles nuevos modelos de negocio.

Por tanto, **las organizaciones afrontan un escenario en el que su dependencia de terceros aumenta tanto en número como en importancia**. Es decir, la digitalización conlleva la necesidad de ampliar la gestión de riesgos a toda esa tecnología y, como consecuencia, a todos los terceros que incorporamos a nuestros procesos productivos.

Es relevante destacar que esto incluye, tanto a proveedores que se conectan a nuestros sistemas para proporcionarnos servicios "tecnológicos" (hosting, mantenimientos o administración de sistemas, aplicaciones, bases de datos, help desk, etc.) como a proveedores no-conectados, es decir, proveedores que nos prestan algún tipo de servicio sin conectarse a nuestro sistema pero gestionando nuestra información en sus propios sistemas (consultoras, gestorías, abogados, etc.).

En este aspecto, lo primero que llama la atención en este apartado del estudio es que en casi la mitad de las compañías, los proveedores se conectan a la red interna y prácticamente el mismo porcentaje almacena o gestiona información de la organización (47,6% frente a un

46,1%). Es decir, los proveedores conectados (aquellos que se conectan a nuestros sistemas de información) son, estadísticamente, igual de numerosos que los proveedores no-conectados (aquellos que gestionan nuestra información en sus propios sistemas de información).

Por tanto, la primera conclusión que debemos obtener es que, cuando nos pongamos a asegurar el nivel de protección de nuestros proveedores **debemos prestar igual atención a los proveedores conectados que a los no-conectados**.

El 16% de los proveedores que se conectan a la red interna de una organización lo hace sin pasar ninguna verificación de seguridad.

El segundo aspecto que llama la atención es que son más las organizaciones que evalúan los niveles de seguridad de sus proveedores durante toda la vida del servicio (un 40,4%) que las que lo hacen solo al principio (un 25,8%) o no lo hacen nunca (un 33,7%), aunque **siguen siendo una minoría (6 de cada 10 solo lo hacen al principio o no lo hacen nunca)**. Esto supone que el 16% de los proveedores que se conectan a la red interna de una organización lo hace sin pasar ninguna verificación de seguridad.

En tercer lugar, vemos que actualmente no hay ningún mecanismo para verificar la seguridad de los proveedores que prevalezca sobre el resto: cuestionarios de seguridad, auditorías de seguridad propias y certificaciones o auditorías de terceros son usados por igual.

Este planteamiento implica que hay un gran espacio para la mejora puesto que los cuestionarios, por ejemplo, deberían estar reservados a servicios de muy poco riesgo que, en ningún caso, serían el 42,4% del total. Y, por otra parte, **que el 47,5% de las empresas esté empleando recursos propios para revisar la seguridad de sus proveedores, realizando tareas repetitivas y redundantes (todas las auditorías que se realizan a proveedores presentan un solape superior al 75-80%) es un uso muy poco eficiente de los recursos propios**.

El 77,5% de las empresas valoraría positivamente un sistema que le permitiera conocer el nivel de seguridad de los sistemas de sus proveedores

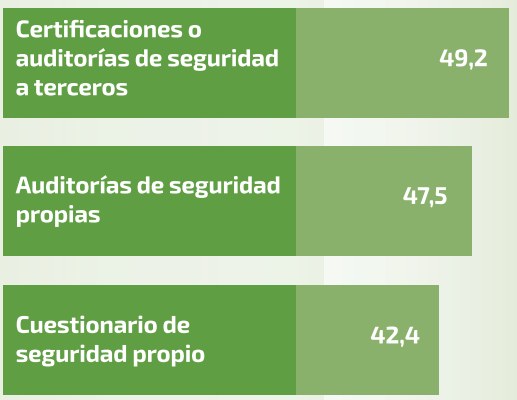
Evaluaciones fiables, garantía de ciberseguridad

Como consecuencia de lo anterior, es lógico que **el 77,5% de las empresas valore favorablemente disponer de un sistema que les in-**

forme del nivel de seguridad de los proveedores, puesto que evita la dedicación de recursos propios a una actividad que no aporta valor a la actividad del negocio, sino que reduce la rentabilidad de la subcontratación de servicios.

Una calificación de ciberseguridad que ofrece un alto nivel de garantía, siempre que se realice conforme a estándares como la UNE71381, como es el caso del Sello LEET Security. Este sello, además, no encarece la transacción, y hace el proceso de cumplimiento más eficiente, puesto que permite reutilizar los trabajos para todos los usuarios del servicio. Es decir, la utilización de una calificación de seguridad supondría un potencial ahorro de costes por el traslado a precio de la reducción de costes operativos de proveedores en la prestación del servicio calificado, con la consiguiente eficiencia en la entidad usuaria que no solo se ahorraría el coste de la auditoría propia, sino que además, tendría un servicio más barato que el actual.

¿CÓMO EVALÚA LOS NIVELES DE SEGURIDAD DE SUS PROVEEDORES EXTERNOS?



La conclusión, por tanto, es que las empresas deben incorporar a sus procesos de gestión de proveedores mecanismos que les permitan supervisar su nivel de seguridad de la manera más eficiente posible. Dado que los mecanismos que se apoyan en terceros son los más recomendables (al ofrecer mayores niveles de garantía), esto supone incorporar una mezcla de auditorías y calificaciones en los procesos de supervisión que permitan conocer el nivel de protección que la información propia de la compañía tiene cuando es gestionada por estos terceros.

Este requisito que, hoy por hoy, es necesario desde un punto de vista de gestión de riesgos empresarial, es obligatorio ya en algunos sectores como el financiero, y lo será, en breve, cuando el nuevo Reglamento de Protección de Datos Europeo entre en vigor, por tanto, mejor no dejarlo para el último momento y comenzar cuanto antes a gestionar el riesgo de los proveedores como si fuera propio.

FICHA TÉCNICA: Base muestral: 150 empresas ubicadas en territorio español. Trabajo de campo: entre el 1 y el 22 de marzo de 2017. Error muestral máximo en los datos del ±8,25%, trabajando en un entorno de confianza del 95,5%.

La calificación LEET Security es la única metodología independiente reconocida por organismos de seguridad que permite cualificar de forma objetiva, eficaz y permanente el nivel de ciberseguridad en las empresas y sus proveedores.

Pº de la Castellana, 153 - 28046 - Madrid
Tel: +34 915798 187

info@leetsecurity.com

LEET SECURITY
ICT Services
Rating Agency