Ciberseguridad

RGPD

Directiva NIS

II 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:

CNPIC

CLUB EXCELENCIA EN GESTIÓN

inmark experiencia e innovación

Tras las interesantes conclusiones obtenidas el año pasado, repetimos en 2018 la realización de este Estudio sobre "Empresas y Ciberseguridad" desde LEET Security con la colaboración del Club de Excelencia en Gestión (CEG) y Grupo Inmark. En esta ocasión, además de volver a incidir sobre algunos aspectos que tratamos en la I Edición, hemos incluido también algunas cuestiones en relación al Reglamento General de Protección de Datos (RGPD) ante su inminente aplicación.

Aunque es pronto para derivar tendencias, llaman la atención algunas respuestas recibidas en esta segunda edición. En primer lugar, destaca la reducción en el número de ataques percibidos por las organizaciones (hay que recordar que el estudio del año pasado se realizó en plena campaña del WannaCry) ya que solo un 38,1% han sido conscientes de haber sido atacadas, respecto al 55,2% del año pasado; sin embargo, el porcentaje de ocasiones en que el vector de ataque ha sido un proveedor externo se mantiene estable (16% vs. 18% en 2017). De hecho, **aunque el nivel de preocupación en ciberseguridad es inferior al de hace un año, más de la mitad consideran que el riesgo es mayor que entonces, lo que ha llevado a la mayoría de las empresas a aumentar la inversión**.

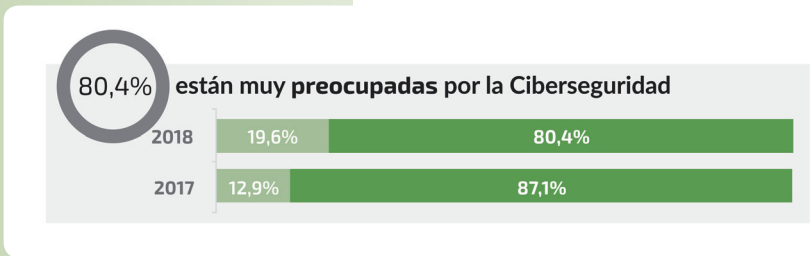
Disminuye la preocupación en ciberseguridad respecto a 2017 aunque el 50% considera que el riesgo de ciberataque es mayor y se incrementa la inversión en ciberseguridad.

En relación a la cadena de valor, hay un dato que se mantiene respecto al año pasado, pero que esperábamos se hubiera reducido significativamente: **el porcentaje de organizaciones que no evalúan a sus proveedores de servicios se mantiene en el 31% (respecto al 33% de 2017), al mismo tiempo que se reduce la utilización de certificaciones y auditorías propias como mecanismos de evaluación en favor del uso de cuestionarios**.

Finalmente, **en materia de RGPD, destaca el alto grado de preocupación**, puesto que el 71% de las organizaciones está muy preocupada, pero sin embargo, un 9,4% declara que todavía no ha puesto en marcha ningún plan de adecuación.

Actitudes ante la ciberseguridad y los ciberataques

En esta segunda edición del Estudio, siguen siendo más del 80%, las organizaciones que se declaran muy preocupadas por la ciberseguridad (en 2017, eran un 87,1%) y por ello, han aumentado la inversión en esta materia un 56,2% de las encuestadas, en línea con el 54,7% que consideran que el nivel de riesgo es mayor en 2018 (sólo un 8,5% considera que el nivel de riesgo es menor).



Este escenario favorable para la ciberseguridad, tiene más valor si consideramos que ha descendido significativamente el número de organizaciones que son conscientes de haber recibido un ataque: se han reducido en más de 17 puntos, pasando del 55,2% en 2017 a un 38,1% en 2018.

Esta circunstancia, que podría parecer contradictoria tiene sentido si consideramos el contexto en el que se realizó el estudio en 2017, justo en plena oleada de los ataques de WannaCry y NotPetya que tanto impacto tuvieron. De hecho, no es habitual que las campañas de ransomware tengan tanto efecto ya que sus promotores son conscientes de que, a mayor repercusión, menor tiempo de respuesta de las casa anti-malware y de la comunidad de seguridad, en general, por lo que cabría pensar que, en estos casos, algo se les fue de las manos.

Se mantienen los aspectos que más preocupan a las organizaciones frente a 2017. El principal: la protección de los datos de clientes (34,6%)

También llama la atención que, **frente a la reducción de los casos de ataques percibidos, se mantiene estable el porcentaje de casos en los que el vector de ataque ha incluido a proveedores de servicio** (un 15,6% respecto al 18,3% de 2017).

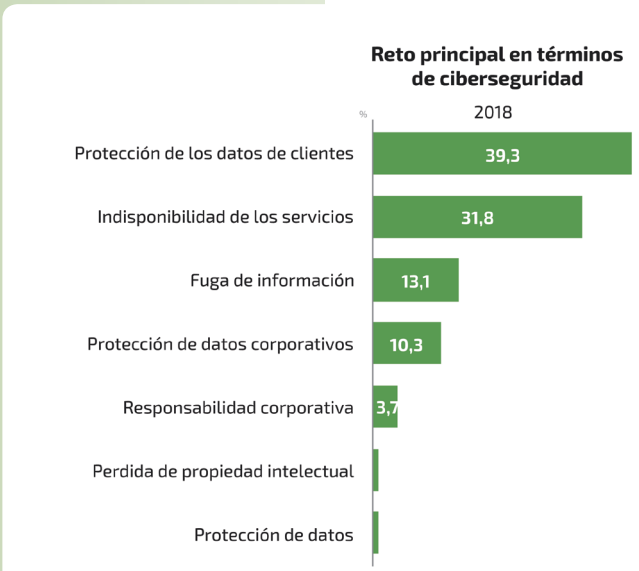
Preocupaciones

Los aspectos que más preocupan a las organizaciones se mantienen estables respecto a los resultados de 2017. De he-

cho, los tres aspectos que más menciones acumulan como primera opción son los mismos, incluso con un mayor porcentaje en todos los casos. Nos referimos a la **protección de los datos de clientes** (34,6%), **indisponibilidad de los servicios** (30,8%) **y fuga de información** (23,2%). De hecho, estos mismos elementos son reconocidos como los principales retos en materia de ciberseguridad.

Merece una mención especial la indisponibilidad de los servicios que ha pasado de ser el aspecto que acumula más menciones entre todas las personas que han respondido la encuesta (un 78,8% frente al 63,3% en 2017 cuando era el tercer aspecto más mencionado tras los otros dos enumerados más arriba).

Este incremento de la importancia del componente disponibilidad es uno de los efectos de la digitalización de los procesos productivos, puesto que la digitalización del modelo de servicios de las organizaciones conduce, necesariamente, a una mayor dependencia de los sistemas de información y, por ende, una indisponibilidad en los mismos conlleva una pérdida directa y un impacto en la cuenta de resultados de la organización. Esperamos ver en los próximos años como esta tendencia se prolonga en línea con la adopción de la digitalización (o la Industria 4.0).



Cabe destacar, no obstante, que **el principal reto para el 39,3% de los encuestados es la protección de los datos de clientes**. Este hecho pone de manifiesto que la *deperimetrización* de los entornos y el procesamiento compartido con terceros (*partners*, clientes y, cómo no, proveedores de servicio, entre otros) hace que las organizaciones tengan dificultades en llevar la protección de la información de sus clientes a todos los tratamientos que de ella se realizan. Al igual que en el caso de los incidentes, esta repuesta quizás se vea impactada por el momento de la encuesta ya que, además de estar en pleno proceso de adecuación del RGPD, se ha producido en el mismo momento en que conocíamos la filtración de datos de Facebook a Cambridge Analytics.

Responsables involucrados

En esta área se aprecia una cierta estabilidad, ya que CISO (*Chief Information Security Officer*) y CIO (*Chief Information Officer*) son los principales responsables en materia de ciberseguridad, acumulando entre ambos prácticamente un 80% de las organizaciones.

No obstante, destaca el incremento de peso de los CIOs que han pasado de un 33,1% en 2017 a un 42,2% en 2018. (es decir, han incrementado su peso en un 27,5%), mientras que los CISOs han pasado de 34,6% a un 37,3%.

Como ya exponíamos el año pasado, 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.

Es imprescindible asegurar que la ciberseguridad y la gestión de riesgo de proveedores formen parte intrínseca de los procesos de compras y aprovisionamiento de las organizaciones.

De hecho, los otros dos datos en este mismo campo son llamativos, pero por motivos distintos: que el 57,4% de los Consejos de Administración estén preocupados debemos celebrarlo, al contrario que las áreas de Compras, en las que, solo el 34,7% dicen estar preocupadas.

Dado que, como hemos visto, los proveedores tienen un peso importante en el tratamiento de la información de cualquier organización, **se hace imprescindible asegurar que la ciberseguridad y la gestión de riesgo de proveedores** (más conocidos por sus siglas en inglés, VRM – *Vendor Risk Management*) **forma parte intrínseca de los procesos de compras y aprovisionamiento de las organizaciones**.

La seguridad de la cadena de valor

Las respuestas recibidas nos permiten ver ligeramente la evolución que los procesos de VRM van teniendo en las organizaciones. En cuanto al tipo de proveedores que existen vemos que el balance existente en 2017 se ha roto y ahora los proveedores no-conectados son mayoría respecto a los proveedores conectados:

- Se ha reducido en un 17,4% el porcentaje de organizaciones en las que los proveedores se conectan a sus sistemas (pasando de un 47,6% en 2017 a un 39,3% en 2018) aunque todavía existen estas conexiones en 4 de cada 10 organizaciones.
- Por el contrario, ha aumentado ligeramente el porcentaje –un 7,4%– de organizaciones con información gestionada en sistemas de terceros. En 2018 son un 49,5% de las encuestadas respecto al 46,1% del año previo.

El porcentaje de organizaciones que no realizan ningún tipo de revisión a sus proveedores permanece prácticamente igual que en 2017 (un 31,3% respecto a un 33,7%).

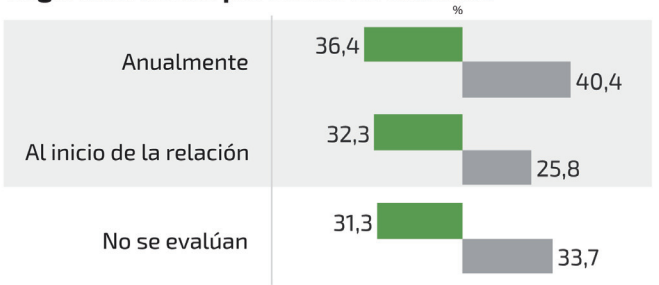
Por tanto, **las organizaciones no deberían olvidar incluir en sus procesos de supervisión de proveedores a aquellos que gestionan información de la organización en sus propios sistemas** ya que, probablemente, el volumen de información gestionado por éstos sea mayor que el de los proveedores que sí están conectados y que eran en los que, tradicionalmente se había enfocado esta supervisión.

De hecho, un 31,4% de los encuestados reconoce que exclusivamente evalúan a los proveedores tecnológicos y que sólo un 40,0% extiende dicha evaluación a todos sus proveedores. Esta supervisión "limitada" es más evidente si consideramos que un 28,6% de los encuestados nos indican que sólo supervisan a los proveedores que consideran críticos.

Aunque la estratificación de proveedores en función del riesgo del servicio es una buena práctica en cualquier proceso de VRM, no es menos cierto que eso no significa que debamos asumir el

riesgo de no realizar ningún tipo de supervisión, sino aplicar en cada caso los requisitos y el mecanismo de supervisión más adecuado al nivel de criticidad del servicio prestado.

Momento en el que evalúan los niveles de seguridad de sus proveedores externos



Para nosotros la conclusión más importante del Estudio es lo que los encuestados nos han dicho en relación a la supervisión de los terceros que tratan sus datos puesto que vemos que la situación respecto al año pasado no ha mejorado, sino que, a nuestro juicio, supone que las **organizaciones están asumiendo un mayor riesgo por la seguridad en su cadena de valor** ya que:

- Ha habido un desplazamiento de las organizaciones que hacían revisiones anuales de sus proveedores (un 4% menos) hacia las que las realizan únicamente al inicio de la relación (un 6,5% más) lo que supone un entorno de control mucho más relajado.
- Por otro lado el porcentaje de organizaciones que no realizan ningún tipo de revisión permanece prácticamente igual, ya que solo se ha reducido en 2,4 puntos: un 31,3% en 2018 respecto al 33,7% del año previo.

Y no sólo ésto sino que, cuando realizan esta gestión, crecen en importancia los mecanismos utilizados para la supervisión del riesgo de terceros que menos garantías ofrecen:

- Los cuestionarios son utilizados por más organizaciones, casi 5 de cada 10 (frente a los 4 del año 2017).
- Tanto las auditorías / certificaciones de terceros como las propias se reducen (en 6,1 puntos las primeras y en 7,5 las segundas).

Por tanto, **ante las dificultades evidentes que supone gestionar el riesgo de múltiples terceros, las organizaciones cada vez supervisan dicho riesgo con menos asiduidad y con mecanismos de menores garantías** (aunque más baratos).

Este hecho, que hasta ahora podía considerarse como una buena práctica, cobra una nueva dimensión con la entrada en vigor del RGPD, ya que el principio de responsabilidad del mismo obliga a

mostrar una debida diligencia en la vigilancia de los encargados de tratamiento que, sin duda, va más allá de incluir las medidas de seguridad en un contrato con un clausulado estándar, sino que nos obliga a una supervisión mucho más cercana y continuada. Todo ello con la complicación añadida de que las medidas de seguridad requeridas para cada tratamiento ya no son "estándar", sino que cada organización establecerá las medidas que considere adecuadas en función del riesgo y, por tanto, los proveedores deberán adecuarse a cada caso concreto, sin disponer de criterios definidos en la legislación.

Reglamento General de Protección Datos

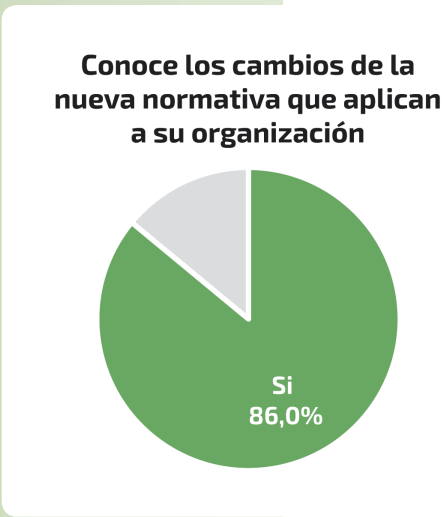
***LEET Security** acaba de lanzar **EQualify**, una herramienta de auto-evaluación online que facilita a proveedores y usuarios conocer el nivel de seguridad de un servicio de manera más flexible a la vez que exhaustivo. Además de poder mapear los requisitos específicos del responsable del tratamiento, la herramienta incluye un mapeo con el **RGPD** para poder evaluar la adecuación del proveedor al nuevo Reglamento.*

Una de las novedades de esta segunda edición del Estudio son las preguntas relacionadas con el RGPD. La motivación de las mismas era tener una visión más objetiva de la situación de las organizaciones en relación a la entrada en vigor del Reglamento el 25 de mayo de 2018 y contrastar el nivel de actividad de las organizaciones en esta materia.

El primer aspecto que nos gustaría destacar es el grado de concienciación existente, ya que prácticamente **9 de cada 10 organizaciones indican conocer los cambios de la normativa que le aplican**, lo que es un dato muy elevado por el que nos debemos felicitar. A raíz de este conocimiento, un 70,9% de organizaciones han indicado estar muy preocupadas por dicha aplicación. En nuestra opinión se trata de una situación muy razonable, ya que el RGPD incluye algunos cambios sobre nuestra anterior regulación de gran calado (especialmente, en relación al consentimiento de los afectados y los principios de responsabilidad –*accountability*– y privacidad por diseño y por defecto) que van a modificar la aproximación que

las organizaciones realizaban al cumplimiento de esta normativa, obligándoles a diseñar procesos mucho más continuos e integrados con la operativa de negocio.

En relación al nivel de adecuación a un mes vista de la completa aplicación del RGDP, vemos que no dista mucho de la que debe ser en toda Europa: **sólo un 12,3% de las organizaciones han finalizado su proceso de adaptación y un 76,4% se encuentran trabajando en ello**. No podemos dejar de indicar que un 11,3% de las organizaciones encuestadas, o no han planificado ninguna acción o tienen un plan previsto pero todavía no han empezado a trabajar.



Finalmente, preguntadas por quién ha asumido la responsabilidad de esta materia en la organización, la respuesta mayoritaria ha sido el departamento jurídico (30,2%), aunque llama la atención que haya sido el propio CEO en un 16,7% quien la haya asumido –de hecho, nos parece la idea más acertada debido al amplio impacto en la operativa que hemos mencionado anteriormente.

Es indiscutible el impacto que este tipo de regulaciones tienen sobre el mercado, puesto que un 69,4% de las organizaciones han contado con el apoyo de consultores en el proceso de adaptación y un 37,5% se han apoyado en despachos de abogados; vemos de nuevo, el efecto *driver* que las regulaciones tienen en el desarrollo de una demanda que, de otra manera, habría tardado mucho más en desarrollarse o quizás nunca se hubiera desarrollado.

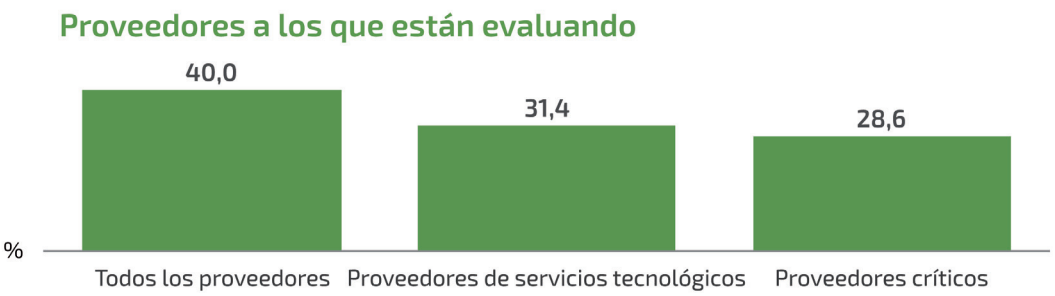
La calificación de ciberseguridad

La otra novedad del Estudio en 2018 es la inclusión de algunas preguntas relacionadas con la utilización de calificaciones de seguridad por las organizaciones. **LEET Security** como pionera de la aplicación de este mecanismo en el sector de la ciberseguridad lleva realizando esfuerzos para su utilización desde su fundación en 2010, pero especialmente desde su salida al mercado en 2015.

Tras este tiempo, vemos que un 30,3% de las organizaciones encuestadas nos indican que están utilizando ya este mecanismo de calificación de seguridad de una u otra forma. En concreto, **el uso mayoritario** (un 66,7% de las que la usan) **es la evaluación del nivel de ciberseguridad de la organización**.

Otras finalidades típicas como la demostración de cumplimiento con el RGPD, la utilización como herramienta de información a la Dirección y para informar a terceros (socios, reguladores u otros) se mueven entre el 20 y el 40%.

Finalmente, en cuanto a los sistemas utilizados y aunque somos conscientes del amplio camino que nos queda por recorrer, vemos que **LEET Security** es el sistema mayoritario, siendo usado por un 55,6% de los encuestados, mientras que otros sistemas basados en la calificación de las medidas desde fuera suponen un 29,6%.



Dado el escenario de riesgo existente y la importancia de la cadena de valor en el aseguramiento de un nivel de ciberseguridad adecuado (ya sea para satisfacer los requisitos de negocio o para dar cumplimiento a una legislación: RGPD) sigue siendo imprescindible que las organizaciones desarrollen procesos de gestión de riesgo de dichos terceros. Dado que la utilización de medios propios supone un esfuerzo que, como hemos visto no es fácil mantener en el tiempo, la calificación aporta un mecanismo eficiente para el desarrollo de dichos programas puesto que reduce el número de procesos de *assurance* (la calificación se realiza una vez pero se puede utilizar con todos los usuarios del servicio sustituyendo a los procesos *ad hoc* que revisan criterios personalizados) a la vez que incorpora mecanismos de supervisión para evitar que deban ser implementados por cada organización de manera independiente.

Como exponíamos en el Estudio del año pasado, esta supervisión de riesgos de terceros, antes era necesaria en el sector financiero, pero con la aplicación del RGPD es ya obligatoria en cualquier servicio que suponga el tratamiento de datos de carácter personal.

Ante esta situación, cada organización tiene que tomar la decisión de si desarrollar un esquema de evaluación personalizado a medida o si se beneficia de las economías de escala y de todas las ventajas de la estandarización en la evaluación del nivel de seguridad de los servicios que aporta la calificación. Evidentemente, existirán casos dónde los requisitos específicos y el tamaño de la organización conllevarán el desarrollo de un programa personalizado, pero para el resto de los casos la calificación es la solución más eficiente y eficaz con la que contamos.

FICHA TÉCNICA: **Base muestral: 110 empresas ubicadas en territorio español. Trabajo de campo entre el 9 de abril y el 10 de mayo de 2018. Error muestral máximo en los datos del ±9,67% trabajando en un entorno de confianza del 95,5%**

Ciberseguridad

RGPD

Directiva NIS

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: +34 915 798 187

info@leetsecurity.com

LEET SECURITY
ICT Services Rating Agency

Este documento ha sido descargado de la web del Club Excelencia en Gestión: www.clubexcelencia.org