Grant Thornton

Seguridad informática

Consultoría

Riesgo

Ciberseguridad: protegiendo el valor de los datos

2018

Índice:

Sección	Page
Resumen ejecutivo: el epicentro de la seguridad informática	03
¿Está protegiendo los datos que no debería?	07
Las joyas de la corona: ¿Qué? ¿Por qué?	10
Obstáculos para el éxito	15
El camino a seguir: tres pasos para un mejor conocimiento de los datos	17

Resumen ejecutivo

El epicentro de la seguridad informática

En la actualidad, los altos directivos se enfrentan a una amplia gama de riesgos complejos, interconectados y que evolucionan rápidamente. Pocos de ellos son tan críticos y desconocidos como el riesgo de un ciberataque.

Uno de los principales desafíos reside en la naturaleza inmaterial de este tipo de amenaza. Los datos son muy diferentes de los bienes materiales tradicionales, que se pueden definir con claridad y cubrir con un seguro empresarial al uso. La mayoría de las veces, la posibilidad de sufrir un ciberataque se considera un problema informático y no un asunto que afecte al conjunto de la empresa. Sin embargo, una infracción grave de la seguridad puede tener consecuencias catastróficas: socava la confianza del cliente, provoca un aumento de atención por parte de los reguladores, altera las actividades del negocio y causa perjuicios financieros a largo plazo.

Hemos llevado a cabo un estudio con una cuestión en mente: ¿qué hacen hoy en día los directivos para asegurarse de que sus empresas puedan prever y superar el riesgo de ciberataque?

Pretendíamos ir más allá de la jerga, del lenguaje técnico y de los artículos alarmistas de los medios de comunicación y definir un enfoque práctico para los directivos actuales que les permita ver el ciberataque como una amenaza más gestionable. En concreto, queríamos centrarnos en el riesgo que sufren los datos, porque eso es, en última instancia, lo que las empresas intentan proteger de los hackers.

"Creemos que las empresas no pueden realizar una gestión eficaz del riesgo de ciberataque si no tienen una visión clara de los datos de los que disponen", afirma Paul Jacobs, responsable mundial de seguridad informática en Grant Thornton. "Puede que sean los datos de su servidor de correo electrónico, la información financiera, los datos de clientes, los procesos patentados o sus secretos comerciales". "Sólo cuando llegan a comprender la importancia de estos datos y dónde se encuentran almacenados —lo que se conoce en algunas esferas como categorización o clasificación— pueden aplicar mecanismos de protección a prueba de piratas informáticos allí donde más lo necesitan".

Para entender el nivel de madurez de las empresas en este ámbito, encuestamos a un total de 2.900 altos directivos a través del International Business Report (IBR) de Grant Thornton.[1] También entrevistamos a 12 expertos —de la red de Grant Thornton, así como del ámbito académico y empresarial— en seguridad informática y gestión de datos.

"La mayoría de las organizaciones creen que no van a sufrir un ataque a su seguridad informática. Aproximadamente el 20% considera que serán víctimas de un ataque pronto y por eso han realizado inversiones en sofisticados sistemas de seguridad informática. Probablemente en torno al 30% está bastante bien preparado. El resto se encuentra en un punto intermedio o considera que no serán el objetivo de estos ciberataques."

Luis Pastor, Socio de Consultoría Tecnológica e Innovación de Grant Thornton

1. Estudio de Grant Thornton realizado en el 1T de 2018. La metodología completa se recoge al final del

Principales conclusiones

Qué saben, dicen y hacen las empresas con sus datos críticos

Muchas empresas desconocen los datos de los que disponen

Todas las empresas generan una cantidad de datos impresionante cada día. La forma más fácil y económica de almacenar toda esta información consiste en adoptar el modelo "vertedero", es decir, guardarlo todo y mover a la nube la mayor cantidad posible de datos. Sin embargo, observamos que muchas de ellas lo hacen sin ni siquiera mantener un registro de lo que tienen.

Nuestro estudio sugiere que casi dos tercios empresas (65 %) toman medidas para conocer sus datos; pero, sin embargo, desconocen en gran medida la cantidad de datos de que se trata, qué hace con ellos y las consecuencias que podría tener el hecho de que su seguridad se viese comprometida. Por tanto, si desconocen esta información básica, ¿cómo pueden asegurarse de que están convenientemente protegidos?

La mayoría de los procesos de gestión de riesgos presentan una brecha en materia de datos

Una de cada tres organizaciones (36 %) no asigna un perfil de riesgo a sus datos. Esto resulta sorprendente si tenemos en cuenta lo que se podría perder si la seguridad de sus datos se viese comprometida. Es posible que esto se deba en parte a que, a pesar de que los altos directivos reconocen que existe un riesgo de ciberataque, todavía no hacen lo suficiente por promover acciones para mitigarlo.

Otra explicación es que anteriormente la gestión del riesgo se centraba en gran medida en un número limitado de riesgos que podían cubrirse con una póliza de seguro. Como resultado de ello, los equipos de gestión de riesgos tradicionales no disponen de la experiencia necesaria para predecir, gestionar y valorar amenazas inmateriales como las infracciones de seguridad. Esto debe cambiar en el panorama actual.

Muchas empresas "quieren proteger todo y no protegen nada"

Tres de cada cuatro empresas encuestas por nuestro IBR (78 %) establecen una base de protección informática sin determinar medidas concretas para defender sus datos más preciados. En el peor de los casos, esto quiere decir que aplican cortafuegos de elevados costes para proteger datos de escaso valor, mientras que su información más crítica —aquella necesaria para que la empresa realice su actividad básica— está más expuesta de lo que debería.

30%

de empresas considera que, probablemente, estén bien preparadas

50%

se encuentra en una situación intermedia o considera que nunca sufrirán un ciberataque

20%

considera que sufrirá un ataque en breve y ha invertido en sofisticados sistemas de seguridad informática en previsión de ello

Para conocer los datos de los que se dispone es necesario alcanzar un equilibrio entre pensamiento lateral y vertical

A la mayoría de las organizaciones les resultaría prácticamente imposible valorar y clasificar todas las hojas de datos, correos electrónicos archivados o ficheros de datos que generan cada día. Por otra parte, se trata de un proceso que no puede ser automatizado por completo: para entender el riesgo y el valor de los datos es necesario aplicar el criterio humano.

Para conseguirlo también se necesita imaginación: ser capaz de pensar como un pirata informático sin escrúpulos y oportunista e identificar aquellos datos que afectarían a la actividad de la empresa en caso de verse comprometidos. Sin embargo, en la medida de lo posible, también es necesario compensar el razonamiento cualitativo con un análisis cuantitativo. ¿Cuáles serían las consecuencias financieras de una infracción grave de la seguridad? ¿Estas repercusiones serían siempre las mismas? ¿Qué probabilidad estadística existe de que esto ocurra?

El personal es el eslabón más débil

La gestión de datos conlleva su tiempo y para que sea eficaz debe formar parte del día a día de su empresa. Esto supone la designación de responsables de esta actividad para el conjunto de la empresa, así como responsables individuales de los activos de datos.

Sin embargo, muchos empleados se ven obligados a asumir la responsabilidad de los datos encima de sus tareas diarias, por lo que tratan de eludir esta carga extra. En el peor de los casos, se trata de una elusión pasiva —en la que los empleados asignan a los datos la categoría de bajo riesgo con el único fin de evitarse el problema de protegerlos frente a los piratas informáticos—.

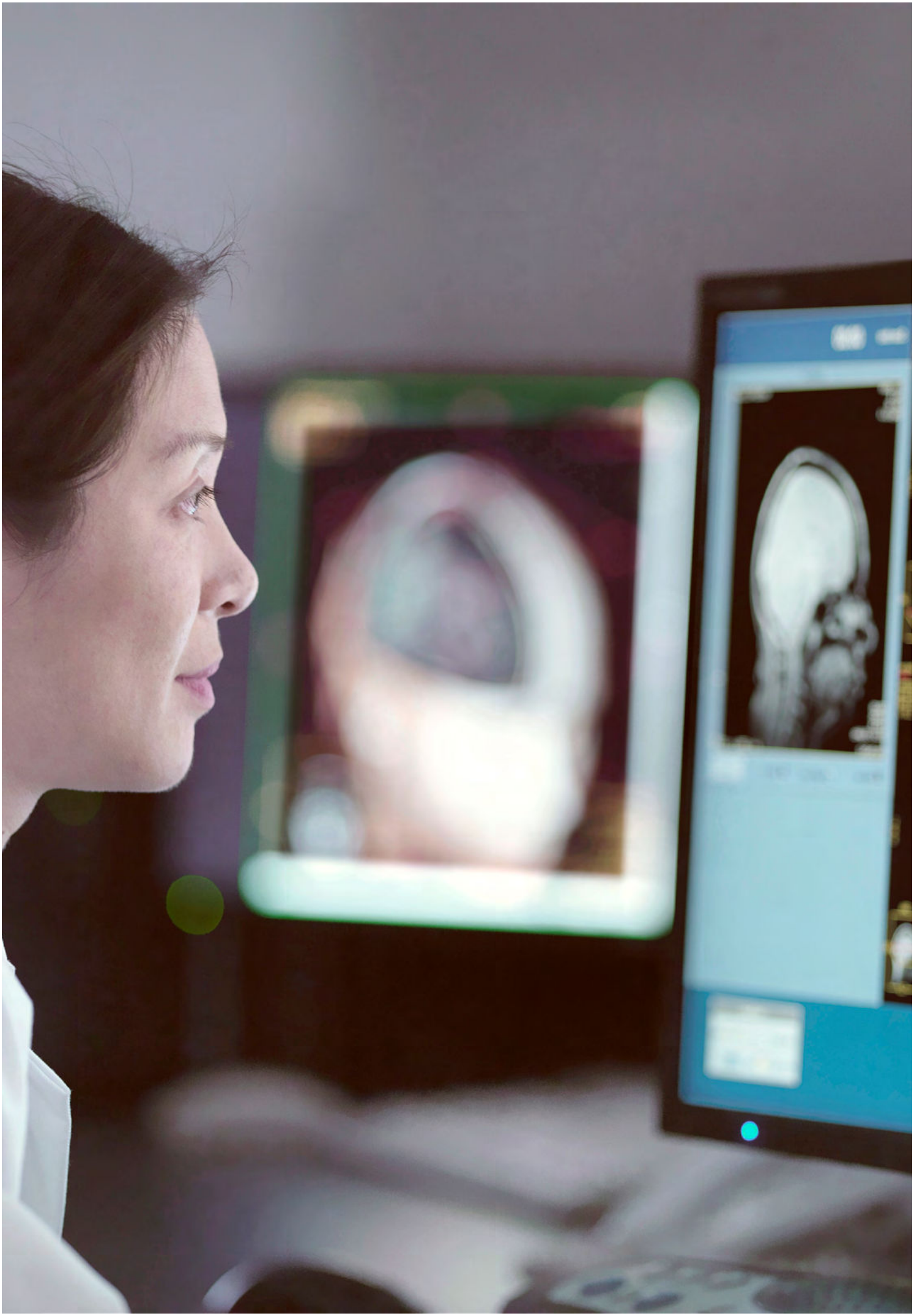
La gestión eficaz del riesgo informático requiere que las empresas prevean esta reacción de los empleados y tomen medidas para evitarlo.

La gestión eficaz del riesgo de los datos se basa en tres principios

En primer lugar, la seguridad de los datos debe considerarse un riesgo constante para el conjunto de la empresa, debe estar gestionada por los altos directivos e implementada por los empleados a nivel operativo. En segundo lugar, el conocimiento de los datos se debe basar en proyectos diseñados al efecto, con un equipo multidisciplinar que determine las principales amenazas en materia de datos que afronta la empresa. Por último, toda implicación —ya se trate de las comunicaciones de los altos directivos o de la formación— se debe centrar en el plano humano y no técnico.

Una infracción grave de la seguridad puede tener consecuencias catastróficas:

- socava la confianza del cliente
- provoca un mayor control regulatorio
- altera las operaciones
- causa perjuicios financieros a largo plazo



¿Está protegiendo los datos que no debería?

En la actualidad, la calidad de una empresa depende de sus datos. Cuanto mejor sea la información de la que dispone, sean registros de clientes o datos de los empleados, documentación sobre procesos o gastos diarios, mejor será su capacidad de planificación, toma de decisiones y gestión de las operaciones.

Todo lo que es importante representa una fuente de riesgo. Si la seguridad de los datos sensibles se ve comprometida, su reputación podría verse perjudicada, podría sufrir pérdidas económicas, fuertes sanciones (véase el recuadro "Reglamento general de protección de datos de la UE"), alteraciones de sus actividades y generar preocupación entre sus clientes. Este es el motivo por el que el riesgo para la seguridad de la información ocupa ahora un lugar prioritario en las agendas de los consejos de administración y se sitúa entre los principales riesgos identificados por las aseguradoras de todo el mundo[2] y por el Informe de riesgos globales del Foro Económico Mundial.[3]

Sin embargo, nuestra encuesta internacional, en la que han participado un total de 2.900 empresas, sugiere que muchas de ellas no disponen de una idea clara de los datos que mantienen o de su importancia general. Menos de dos de cada tres (65 %) están tomando medidas para tener un conocimiento claro de los datos de los que disponen y sólo aproximadamente la mitad (56 %) asigna un perfil de riesgo a su información.

Protecciones mal asignadas

Nuestras conclusiones plantean una pregunta sencilla: si las organizaciones desconocen la información de la que disponen o su importancia, ¿están perdiendo tiempo y dinero protegiendo información de escaso valor, mientras que sus activos de datos más críticos se encuentran expuestos a riesgos?

Casi con total seguridad la respuesta es afirmativa. Cuatro de cada cinco encuestados (78 %) admiten que suelen asignar sus medidas de protección de manera uniforme entre todos sus datos.

Solo el 22 % restante señala que establece protecciones especiales para su información más crítica.

El responsable de tecnologías de un banco internacional, entrevistado para este informe, alerta del peligro de la ausencia de asignación de controles específicos a los datos de más alto riesgo. "Veo datos críticos colgados en SharePoint", afirma refiriéndose a la plataforma web de almacenamiento de archivos. "Son muchas las empresas que dan acceso a datos críticos en plataformas colaborativas".

La regla del 80/20 de los datos

En nuestra opinión, el principio de Pareto resulta aplicable al riesgo de la información; es decir, que el 20 % de los datos de la empresa comporta el 80 % del riesgo. Para Tom Fulkner, responsable de producción de TI en CMC Markets, la proporción es todavía más extrema. "Existe una capa superior muy reducida de datos, tal vez un 5% del total, que deben ser exactos y protegidos al más alto nivel, dado que no se pueden perder", afirma. "A continuación está una cantidad significativa de datos que deben ser precisos y estar convenientemente protegidos".

Hay una célebre frase que dice: "quien quiere proteger todo, no protege nada". Resulta prácticamente imposible proteger todos los sistemas frente a los piratas informáticos. Por lo tanto, ¿por qué no centrarse en la reducida cantidad de datos cuya seguridad resulta absolutamente esencial?

2. http://www.agcs.allianz.com/assets/PDFs/Reports/AllianzRiskBarometer2016.pdf https://www2.chubb.com/TR-TR/_Assets/documents/20150707_EMERGING_RISK_BAROMETER_FINAL_PUBLISHED.pdf
3. http://www3.weforum.org/docs/GRR17_Report_web.pdf

"Si comprar cortafuegos, IPS y dispositivos IDS de última generación te va a costar un dinero, pero el impacto económico de un ataque a tu seguridad va a ser inferior a ese dinero, entonces es posible que algunas organizaciones prefieran asumir el riesgo y no invertir en dispositivos de seguridad tan caros, o instalar un sistema de seguridad menos sofisticado", señala John Kan, responsable de información en A*STAR en Singapur.

Teniendo esto en cuenta, estamos totalmente convencidos de que las empresas deben aplicar un programa estructurado para valorar y conocer sus activos de datos, utilizando un proceso de categorización o clasificación. De este modo, podrán identificar sus "joyas de la corona" y establecer un sistema de seguridad eficaz al respecto.

"El primer paso es reconocer que sus activos de datos no tienen todos el mismo valor, y el segundo paso es admitir que es probable que su seguridad se pueda ver comprometida. En ese caso, debemos centrarnos en proteger los activos más valiosos."

Antonio García-Lozano, Socio Director de Management, Risk & IT Consulting de Grant Thornton

Reglamento general de protección de datos de la UE Implicaciones a escala mundial

En 2018, una infracción de la seguridad conllevará un coste más directo y tendrá consecuencias económicas más graves. A partir del mes de mayo de 2018, el Reglamento general de protección de datos de la UE (en adelante, GDPR) impondrá a las empresas una sanción de hasta el 5 % de su facturación mundial por la pérdida de datos de sus clientes. Cabe esperar que otras jurisdicciones de todo el mundo apliquen normativas similares una vez que el GDPR haya entrado en vigor.

Para poner en contexto este cambio de normativa, sirva de ejemplo el reciente ciberataque contra Tesco Bank en el Reino Unido, que afectó a las cuentas de 9.000 clientes, y por el que el banco tuvo que reembolsar un total de 2,8 millones de €. Si esta infracción de la seguridad se hubiese producido después de la entrada en vigor del GDPR, al banco se le habría impuesto una sanción de 2.200 millones de €.

Las joyas de la corona: ¿Qué? ¿Por qué?

En un mundo digital resulta extremadamente difícil realizar un seguimiento de todos los datos que una organización genera y recopila cada día.

IBM calcula que el 90 % de todos los datos del mundo se han producido en los dos últimos años [4]. Otros estudios indican que en 2020 viviremos en un planeta que contendrá 40 zettabytes de datos [5] —que según nuestros cálculos representaría material de lectura suficiente para cubrir 50 millones de vidas humanas—.

Por tanto, ¿cómo puede identificar sus joyas de la corona y sus datos más sensibles entre todos esos bytes? ¿Cuáles son los datos de alto, bajo y medio riesgo? ¿Y en qué amenazas —desde agentes patrocinados por un estado, por un lado, hasta adolescentes descontentos, por el otro, pasando por delincuentes, empleados descontentos y "hackertivistas"— debería concentrar su defensa?

Confidencialidad, integridad, disponibilidad

En primer lugar, es poco realista intentar clasificar todas las hojas de datos, correos electrónicos archivados o ficheros de datos de los que dispone su organización. Y este proceso no se puede automatizar por completo: existen herramientas que facilitan la gestión de datos, pero siempre se requiere el criterio humano en algún punto. Por último, tendrá que asegurarse de que sus altos directivos y el personal de riesgo valoren de forma activa los diferentes tipos de datos de los que disponen —de este modo, podrán aislar los activos que requieren una atención más detenida—.

"Hemos desarrollado cuestionarios para que nuestros empleados puedan tomar esa decisión por sí solos", señalar el responsable de tecnología de un banco internacional "Es subjetivo. Al final y al cabo, es una persona quien ha de tomar una decisión".

En la siguiente parte de este informe, recomendamos métodos prácticos para garantizar que sus empleados participen en esta actividad. Pero, ¿qué datos deberían identificar como críticos?

Muchas organizaciones adoptan un modelo dinámico que evalúa los datos en función de la confidencialidad, integridad y disponibilidad (CIA, por sus siglas en inglés) y que puede ser adaptado para reflejar los cambios en la importancia o relevancia de los datos con el paso del tiempo.

"La documentación sobre la estrategia del consejo es confidencial hasta el momento en que se hace pública y debe ser protegida", afirma Manu Sharma de Grant Thornton (Reino Unido), para explicar el planteamiento CIA. "Con respecto a la integridad, la información puede estar a disposición del público pero ha de ser precisa —el precio de la acción en la Bolsa de Nueva York es un buen ejemplo—. La disponibilidad se refiere al hecho de si las personas que necesitan los datos pueden acceder a ellos y utilizarlos, como pueda ser las listas de marketing".

4. https://www-01.ibm.com/software/data/bigdata/what-is-big-data.html
5. https://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm

En la mente de un hacker

Otra forma de identificar los riesgos asociados a sus datos más críticos consiste en pensar como un hacker y, a continuación, analizar los daños más graves que podrían causar.

"El actual entorno de seguridad de la información evoluciona de forma constante, y cada día surgen nuevas amenazas y vulnerabilidades", afirma Vishal Chawla de Grant Thornton (EE. UU.). "Los directivos tendrán que estar dispuestos a ponerse en la piel de los ciberdelincuentes, entender las amenazas que suponen estos grupos y elaborar estrategias proactivas para proteger sus intereses comerciales".

¿Qué conversaciones de correo electrónico podría filtrar un antiguo empleado para comprometer a sus antiguos jefes? ¿Qué propiedad intelectual y secretos comerciales podrían interesar a una potencia extranjera? ¿Y cómo podría utilizar sus datos un ciberdelincuente para intentar extorsionar a su empresa? Estas son solo algunas de las preguntas que tiene que plantearse.

Las empresas del sector de la logística podrían enfrentarse a una amenaza casi existencial si los piratas informáticos recopilasen o manipulasen sus datos. El Dr. Ayman Omar, profesor adjunto de la Kogod School of Business, tiene experiencia en el ámbito de las cadenas de suministro y conoce los riesgos. "Si alguien hace un envío de un artículo de alto valor, se podría acceder a los datos de distribución de la mercancía y lanzar un ataque contra la entrega física de ese artículo", señala. "Hemos visto casos en los que se persigue al mensajero, se le saca de la carretera y se obliga a la empresa a pagar un rescate para evitar retrasos en la entrega de ese artículo".

Un hospital de los Estados Unidos nos sirve como ejemplo de cómo los hackers pueden comprometer los datos que necesita una organización para realizar sus actividades básicas. Los ciberdelincuentes podrían, por ejemplo, modificar los historiales médicos de sus pacientes y cambiar sus grupos sanguíneos, para posteriormente exigir un pago a cambio de devolver los historiales a su estado original. Si el hospital no cumple sus exigencias, a los pacientes se les podría administrar una medicación incorrecta. Esto es mucho más grave que si al hospital le hubiesen robados los datos de las tarjetas de crédito de los pacientes.

Incluso los archivos de datos aparentemente más insignificantes se pueden utilizar para causar graves daños, tal y como explica Ross Anderson, profesor de ingeniería de seguridad en el Laboratorio de Informática de la Universidad de Cambridge: "Una empresa a la que asesoraba creía que si sus datos se veían comprometidos, lo peor que les podría pasar era que se les impondría una sanción. Yo les pregunté: "¿qué pasaría si todos sus correos electrónicos, con todas las críticas que ustedes hacen habitualmente y demás contenidos similares, acabasen en WikiLeaks o Pastebin?". "Los directivos se quedaron blancos y la seguridad informática. pasó a ocupar el primer puesto de su registro de riesgos".

> "Los directivos tienen que estar dispuestos a ponerse en la piel de los ciberdelincuentes, entender las amenazas que suponen estos grupos y elaborar estrategias proactivas para proteger sus intereses comerciales"
>
> **Vishal Chawla,** Grant Thornton, EE. UU.

Amenazas reales: ¿cuáles son los datos críticos a proteger por sectores?

A continuación señalamos algunas de las amenazas por sectores, con la colaboración de expertos sectoriales de Grant Thornton.

Salud

- Recopilación de historiales de pacientes para hacer chantajes o pedir rescates
- Alteración de los datos de las instalaciones (control del aire acondicionado del hospital) para pedir un rescate
- Robo o recopilación de datos de entregas y almacenamiento de fármacos

"Todas las organizaciones sanitarias deberían analizar de manera crítica la forma en que sus departamentos de TI aportan valor y evitar que se limiten a tareas rutinarias." Hay que empezar por conocer y priorizar los datos desde un punto de vista clínico y comercial.

En el sector sanitario, si falla o se infringe la seguridad de un sistema crítico puede morir gente. El departamento de TI debe centrarse particularmente en educar a los usuarios finales acerca de la constante necesidad de gestionar la seguridad, que no es un evento aislado sino más bien un estado mental.

Anne McGeorge, Grant Thornton (EE. UU.)

Servicios financieros

- Robo o recopilación de historiales de clientes para cometer un fraude o pedir un rescate
- Robo de datos comerciales que provoca una parálisis operativa
- Introducción de algoritmos para paralizar/alterar la operativa bursátil automatizada

"Los servicios financieros internacionales se enfrentan a una "cibertormenta" perfecta. La dependencia de la tecnología digital es cada vez mayor y los delincuentes cada vez se concentran más en los sistemas basados en esta tecnología, tal y como demuestran los recientes incidentes con los códigos SWIFT y el aumento de la preocupación por los sistemas de pago. Además de incrementar la atención prestada por los reguladores a la gestión de riesgos informáticos, estos problemas suponen un verdadero quebradero de cabeza para muchas empresas.

Las organizaciones de servicios financieros deberían centrarse en primer lugar en crear un sólido programa de ciberseguridad basado en los riesgos. Esto ayudará a lograr objetivos estratégicos, al tiempo que se cumplan los requisitos regulatorios. Por último, esto permite acelerar la innovación en este ámbito y centrarse de lleno en la ciberseguridad".

Mike Harris, Grant Thornton (Irlanda)

Energía y recursos naturales

- Corrupción de los datos SIG que registran la ubicación del gas o la electricidad en la red
- Recopilación/captura de datos de seguridad y ubicación de un pozo de petróleo para pedir un rescate

"La noción de un mundo plenamente conectado en el que todos los sistemas y las personas están vinculados y en el que se puede acceder online a todos los sistemas resulta extremadamente peligroso. Pensemos en las presas o en las centrales nucleares —los piratas informáticos han demostrado que pueden infringir los niveles de seguridad más elevados—. Estas infraestructuras críticas, entre otras, son blancos fáciles para grupos de piratas informáticos dispuestos a causar estragos".

Michiel Jonker,Grant Thornton (Sudáfrica)

Sector Público

- Robo de datos esenciales para la prestación de servicios de urgencia
- Alteración/manipulación de datos económicos y comerciales por parte de agentes extranjeros
- Robo de secretos de Estado

Productos de consumo

- Robo de información sobre procesos de fabricación
- Alteración o robo de documentación de transporte o de la cadena de suministro
- Robo de datos de propiedad intelectual el+D

Sector inmobiliario y Construcción

- Alteración/robo de especificaciones de materiales de construcción para pedir un rescate
- Alteración/robo de documentación de transporte o de la cadena de suministro
- Introducción de defectos intrínsecos en proyectos de construcción para provocar debilidades estructurales en el futuro

"El volumen de datos sensibles que almacenan,gestionan y procesan los organismos públicos es muy superior al de algunas de las empresas más importantes del mundo.

Un único organismo público también puede necesitar asegurar diversos tipos de información de alto valor, incluidos datos de identificación personal, historiales sanitarios, patentes y secretos comerciales e información bancaria.

Teniendo todo esto en cuenta, y dados los limitados recursos para invertir en herramientas y conocimientos informáticos, los organismos deben abandonar el actual enfoque administrativo (basado en meras listas de comprobación) y adoptar un modelo de control continuo basados en prioridades de riesgos".

Scott King, Grant Thornton (EE. UU.)

Viajes, turismo y ocio

- Robo/alteración de pasaportes o visados de turistas para cometer un fraude
- Robo o recopilación de datos esenciales para los sistemas de transporte público
- Alteración/recopilación de datos de seguimiento o control del tráfico

Tecnología, medios de comunicación y telecomunicaciones

- Ataque sobre los historiales de los clientes
- Alteración de redes de comunicaciones críticas
- Robo de propiedad intelectual

"Debido a que la tecnología representa el epicentro de las vidas de empresas y consumidores, las empresas tecnológicas son claros objetivos de los ataques informáticos. Estas afrontan el doble desafío de proteger sus activos corporativos y consolidar los productos e infraestructuras que representan la piedra angular para el comercio electrónico y las redes sociales. La gran cantidad de valor que generan y aportan los datos debe estar protegida en todo momento".

Steven Perkins, Grant Thornton (EE. UU.)

Equilibrio entre evaluación cualitativa y cuantitativa

Es fundamental realizar una valoración cualitativa coherente de los datos, pero no se debe pasar por alto la evaluación cuantitativa. Esto significa estimar el impacto financiero de una infracción de seguridad y calcular su probabilidad.

El Dr. Ayman Omar, profesor adjunto de Kogod School Business, considera que muchas empresas hacen demasiado hincapié en los análisis subjetivos. "Se le pide a los altos directivos que puntúen en una escala de cero a cinco lo que opinan acerca de los riesgos de la empresa", afirma. "La realidad es que esto es parecido a no hacer nada". No se están cuantificando las probabilidades de que el riesgo se materialice ni su impacto en dólares. Si se dice que el impacto es "tres", ¿eso qué significa?".

Añade que, para realizar una valoración cuantitativa del impacto y la probabilidad, es necesario analizar la tasa de incidencia dentro de la organización y en otros actores del sector.

Lista de comprobación:

Posibles "joyas de la corona" en términos de datos

- ☐ Datos de investigación y desarrollo
- ☐ Datos regulados: datos sanitarios, datos de operaciones financieras
- ☐ Datos de tarjetas de crédito y otros datos sobre pagos
- ☐ Procesos patentados
- ☐ Datos del servidor de correo electrónico que contienen el tráfico de correo del equipo directivo
- ☐ Secretos comerciales
- ☐ Datos de identificación personal
- ☐ Propiedad intelectual
- ☐ Información financiera

Obstáculos para el éxito

Una proporción relativamente elevada de organizaciones no conoce los datos de los que dispone o no consigue gestionar los riesgos asociados. Apenas dos de cada tres (65%) trata de tener un conocimiento claro de los datos de los que disponen y solo la mitad (56 %) asigna un perfil de riesgo a este activo empresarial tan crítico.

Sin embargo, la gestión de los datos no resulta sencilla y no se puede tomar a la ligera. Para intentar conocer los datos de los que disponen, las empresas deben superar varios desafíos.

1. Riesgos tradicionales y amenazas emergentes: falta conexión

En muchas empresas se ha creado el departamento de riesgos para controlar, valorar y mitigar una lista definida de riesgos empresariales que se pueden proteger mediante pólizas de seguros. Estos equipos tradicionales suelen disponer de escasa experiencia en la gestión de riesgos inmateriales que evolucionan rápidamente.

Como resultado de ello, es posible que las infracciones de la seguridad e infiltraciones por parte de los piratas informáticos no estén tan arraigadas en su estrategia de mitigación de riesgos como otras amenazas. Esto podría explicar por qué un número relativamente reducido de empresas de todo el mundo asigna un perfil de riesgo a sus datos.

"La dimensión cibernética es bastante reciente y nunca ha formado parte de la clasificación de riesgos establecida", afirma el responsable de tecnología de un banco internacional. "La clasificación tradicional de los riesgos nunca ha tenido en cuenta los escenarios cibernéticos, los modelos de amenazas cibernéticas ni los ciberataques". Hasta hace poco no se invertía dinero en tener un sólido grupo de expertos en la materia".

2. Elusión pasiva: los responsables de los datos no quiere más carga de trabajo en su día a día

Como sucede con toda iniciativa interna basada en procesos, es probable que las organizaciones se enfrenten a la oposición de unos empleados a los que ya se les exige lo suficiente y que están muy ocupados con sus tareas diarias. No es de sorprender que algunos intenten eludir sus nuevas responsabilidades.

Uno de los directivos entrevistados para este informe está de acuerdo en que muchos empleados dan prioridad a su propio trabajo. "Lo que observamos es que los datos están por todas partes", señala. "El personal ha tomado datos exportados y los ha guardado en su red local y los ha enviado por correo electrónico a otros trabajadores —solamente para realizar su trabajo—".

Más preocupante resulta el hecho de que uno de los directivos con los que hemos hablamos en las entrevistas cualitativas realizadas para este Informe descubrió que algunos de sus empleados clasificaban sus datos de forma errónea deliberadamente. "Solíamos dejar que los responsables del servicio asignasen una categoría a los datos, pero descubrimos que el 70% les asignaba una clasificación inferior a la correspondiente para evitar la aplicación de controles", señala. "Por ese motivo creamos un grupo con el objetivo de validar las respuestas antes de introducirlas en el sistema".

Es difícil dar con el equilibrio adecuado. Si se asigna un nivel de seguridad muy alto y se aplican unos controles sumamente rígidos, se corre el riesgo de generar un ambiente de trabajo desagradable que suponga un gran desgaste. Sin embargo, con una implementación demasiado flexible, se obtiene una "elusión pasiva" en la que los empleados ignoran las directrices, o asignan baja prioridad a los datos para no complicarse la vida.

3. El personal adecuado (o directivo) se encuentra al margen

Si no se mantiene un control al más alto nivel, es probable que cualquier iniciativa de datos con alcance al conjunto de la empresa esté abocada al fracaso. No es solo que los directivos deben asumir sus responsabilidades en esta materia y dar al programa la importancia que se merece, sino que además deben conseguir que quienes evalúen los datos conozcan claramente su importancia estratégica. Aparte de los altos directivos, puede que se tenga que implicar a profesionales de todos los ámbitos de la organización.

En opinión del Dr. Ayman Omar, “deben participar los departamentos de operaciones, marketing y finanzas, además de TI”. “El empleado de TI preguntará qué tipo de impacto podemos esperar si se produce un ataque”. “Operaciones hablará de los retrasos en la producción, lo que podría conllevar un aumento del inventario de seguridad. Y alguien del equipo de finanzas dirá que el inventario de seguridad se carga el margen de beneficios”.

Parte del problema reside en que el esfuerzo de las últimas décadas por intercambiar conocimientos entre las unidades funcionales hace que resulte más difícil calcular el impacto total de una infracción de la seguridad. “El conocimiento se debe obtener a partir de diferentes unidades y diferentes áreas funcionales”, afirma Omar.

4. Falta de coherencia en la aplicación

A pesar de la existencia de guías como el modelo CIA (mencionado en el tercer apartado) y las proporcionadas por el Instituto de Normas y Tecnología (NIST) estadounidense y otros organismos públicos, a las grandes organizaciones les resulta difícil conseguir que su personal tenga una idea coherente sobre los datos. El hecho de que el riesgo asignado a un conjunto de datos puede cambiar con el paso del tiempo en función de su relevancia no hace sino agravar este problema.

“Tenemos procedimientos de control que ofrecen orientaciones sobre lo que es información confidencial”, afirma uno de los directivos entrevistados. “Sin embargo, no resulta posible crear una lista que abarque todos los conjuntos de datos. Algunos han tenido dificultades para decidir qué se debe incluir”.

5. Subestimando la amenaza

Algunas organizaciones consideran que la principal amenaza de un ciberataque es la pérdida de datos de los clientes y el deterioro de su reputación a consecuencia de la mala prensa generada. Sin embargo, en algunos casos el resultado no ha sido tan perjudicial como se pensaba, y esto ha provocado que algunos subestimen los perjuicios que podría causar un ataque informático.

Según Chris Hankin, director del Institute for Security Science and Technology del Imperial College London, Sony es un claro ejemplo. “Los ataques sufridos por Sony tuvieron un efecto a corto plazo sobre el valor de sus acciones y su base de clientes”, explica. “La gente asumió muy rápidamente el hecho de que se habían perdido sus datos. Esto no les apartó de Sony; seguían valorando bien a la empresa y a lo que hacían”.

Hankin reconoce que el deterioro de la reputación podría haber resultado fatal para una organización como la suya. “La universidad estaría muerta si los estudiantes dejasen de venir. Las bases de datos de estudiantes son parte de nuestras joyas de la corona. Si se corriese la voz de que no las cuidamos como se debe, si perdiésemos grandes cantidades de expedientes, los estudiantes dejarían de confiar en nosotros y de solicitar plaza, y no podríamos funcionar como universidad”.

Un ataque puede ser algo positivo

Algunos de los entrevistados afirmaron que una infracción puede ser una experiencia positiva porque puede alertar a los directivos de la gravedad del problema —y poner de relieve las deficiencias—.

“En las organizaciones que han sido víctimas de ciberataques, observamos que, posteriormente, han asignado la financiación necesaria para desarrollar sistemas más seguros y aplicar programas de sensibilización en materia de seguridad”, señala Kan de A*STAR.

David Pollino, vicepresidente y responsable de seguridad adjunto del Bank of the West en Estados Unidos, considera que un incidente de escasa importancia puede tener consecuencias positivas.

“Se puede tener un buen nivel de preparación, pero hasta que no se sufre una catástrofe, uno no sabe si todo va a funcionar a la perfección”, afirma. “Siempre hay un margen de mejora”.

Nuestra experiencia confirma esta idea de que en ocasiones es necesaria una infracción menor para que el consejo demuestre un mayor interés, lo que a su vez garantiza un planteamiento más estructurado en materia de seguridad. “El control es positivo”, señala Mike Harris de Grant Thornton (Irlanda). “Cuando el consejo se implica, se consigue disciplina y una gestión estructurada de los proyectos. El problema de algunos proyectos de seguridad es que son una cuestión secundaria para los profesionales de TI y se dedican a ellos cuando les sobra tiempo. Esto cambia cuando el consejo demuestra un gran interés”.

El camino a seguir: Tres pasos para conocer mejor los datos que hay en su empresa

Las empresas necesitan conocer mejor los datos de los que disponen, aunque para ello se enfrentan a numerosos obstáculos y desafíos. En el presente documento perfilamos nuestras recomendaciones para ayudar a las organizaciones a reconocer la importancia de sus datos, y en última instancia a adoptar un planteamiento más maduro en materia de gestión del riesgo de la información.

1 PASO 1: Asignar responsabilidades: para todo el sistema y para datos concretos

La seguridad de la información se debe entender como un componente de la gestión de riesgos aplicado de forma coherente al conjunto de la organización. Esto supone la designación de un responsable para el conjunto del sistema —por lo general, el director financiero, en caso de que no haya un responsable de seguridad de la información—, así como de un responsable "directo" en el plano operativo. **Significa aceptar que sus datos constituyen un activo estratégico cuyo riesgo debe ser clasificado e incorporado al registro de riesgos.**

"El director financiero, más que cualquier otro alto directivo, dirige los esfuerzos en materia de seguridad", señala Johnny Lee de Grant Thornton (EE. UU.). "Por lo general, los directores financieros son lo que contratan los seguros de protección y quienes más interactúan con otros directivos sobre el riesgo de la empresa".

David Pollino de Bank of the West considera que, en el ámbito operativo, el depositario de los datos debe ser el responsable de su aplicación técnica. "Ellos tienen que dictar los requisitos y asegurarse de que todo funcione correctamente", afirma. "También están mejor preparados para decir cuando se precisa protección de nivel uno, de nivel dos o de nivel tres".

Una de las ventajas de asignar la responsabilidad del día a día, en opinión de Andrew Harbison de Grant Thornton (Irlanda), es que los responsables de los datos son conscientes de que ellos serán los culpables si se produce una infracción de seguridad. "El personal responde mejor a la elusión del riesgo personal que a las amenazas directas", afirma. "Si se explica que algo se está haciendo para proteger tanto a los empleados como a la empresa y que serán culpables si le han asignado una prioridad baja para quitarse el trabajo de encima, harán lo que se les pide para no ser personalmente culpables de ello".

2 PASO 2: Integrar la gestión del riesgo en el día a día

Disponer de un responsable de la gestión del riesgo de la información para el conjunto de la empresa hace que resulte más sencillo integrar desde un principio la evaluación o categorización de los datos en los proyectos.

"Es necesario contar con un responsable de seguridad específico", considera Nick Oldham, abogado especialista en privacidad y seguridad de datos del bufete internacional King & Spalding. "La seguridad y la privacidad suelen ser un componente que las empresas añaden al final, y esto genera problemas más adelante".

El responsable de tecnología de un banco internacional también defiende que la seguridad de los datos debe integrarse en una etapa anterior. "Lo que defendemos es una mayor integración en el ciclo de desarrollo", afirma. "Desarrollamos modelos de amenazas y revisiones del diseño en los que basar las evaluaciones realizadas y en último término hacemos una prueba de evaluación de un ciberataque simulado por un 'red team'".

Implicación de los distintos departamentos

La seguridad específica (o "por diseño") se compone de varias partes. Una consiste en garantizar que participen una serie de departamentos en el proceso de establecimiento de políticas y evaluación —no solo los responsables individuales de los datos—.

"Para las evaluaciones de riesgos y el análisis del impacto de los ciberataques, es necesario que participe toda la organización —y no solo el departamento de TI—", señala Kan de A*STAR. "Se necesita un equipo multidisciplinar compuesto por diversos departamentos, divisiones y unidades de negocio para formular la planificación del escenario y las evaluaciones de impacto de estos incidentes".

La destrucción por norma

La destrucción responsable de los datos reduce las probabilidades de infracción de seguridad. "Se puede disponer de una política sobre registros de operaciones y presentaciones de ventas, en la que se especifique el tiempo que se deben conservar", afirma David Pollino de Bank of the West. "A continuación, se deben tomar medidas para deshacerse de los datos. La información que se mantiene en correos electrónicos o la que no se archiva debería filtrarse y eliminarse de forma automática".

Sunil Chand de Grant Thornton (Canadá) considera que la destrucción de datos debe ser parte clave de cualquier norma de manipulación de datos. "La utilidad de sus datos vendrá dictada por las necesidades de la empresa, la legislación, la normativa y si la empresa tiene algún litigio", señala. "El mejor planteamiento es muy sencillo: disponer de una política de destrucción de datos con controles automáticos o manuales integrados que se ejecute por norma a menos que se vaya a necesitar la información en el futuro".

3 PASO 3: Comunicación "humana" y formación

"Para que sus empleados entiendan mejor la realidad de las amenazas informáticas es necesario que se impliquen a nivel humano y evitar la jerga especializada". "Hay que crear equipos de TI capaces de cerrar la brecha de comunicación que existe entre los usuarios de la empresa y las herramientas técnicas, utilizando para ello términos no especializados".

Ross Anderson, de la Universidad de Cambridge, apunta que, para conseguir una comunicación eficaz, es necesario contar historias que toquen la fibra sensible. "Las empresas no deberían hablar tanto sobre datos", afirma. "Deberían hablar sobre lo que puede ir mal en términos humanos. El cerebro está optimizado para contar historias y cuando uno comienza a hablar sobre categorías de datos, la gente desconecta".

Nick Oldham, de King & Spalding, está de acuerdo y sugiere que las empresas adapten sus mensajes para orientarlos a las preocupaciones y prioridades personales de los individuos. “Es necesario que la comunicación sea fluida desde el consejo hasta el equipo técnico”, señala. “Que los mensajes se transmitan de forma que el equipo legal pueda aplicarlos en términos judiciales y los directivos puedan entenderlos en términos empresariales”.

Formación continua

“Si una empresa tiene que depender de que Mike, del equipo de nóminas, haga clic en el enlace correspondiente, entonces la organización está abocada al fracaso”, señala Chris Brok, profesor adjunto de la Universidad de Houston. “Los hackers son muy sofisticados. Esperar que el personal de la organización sea más hábil que los delincuentes es como esperar que los ciudadanos de a pie sean más hábiles que los ladrones de coches”.

La formación desempeña un papel fundamental para sensibilizar y aumentar la resiliencia entre los empleados, y también ayuda a conseguir las relaciones humanas de las que habla Kan —en particular, a que los empleados se familiaricen con el riesgo de los datos—.

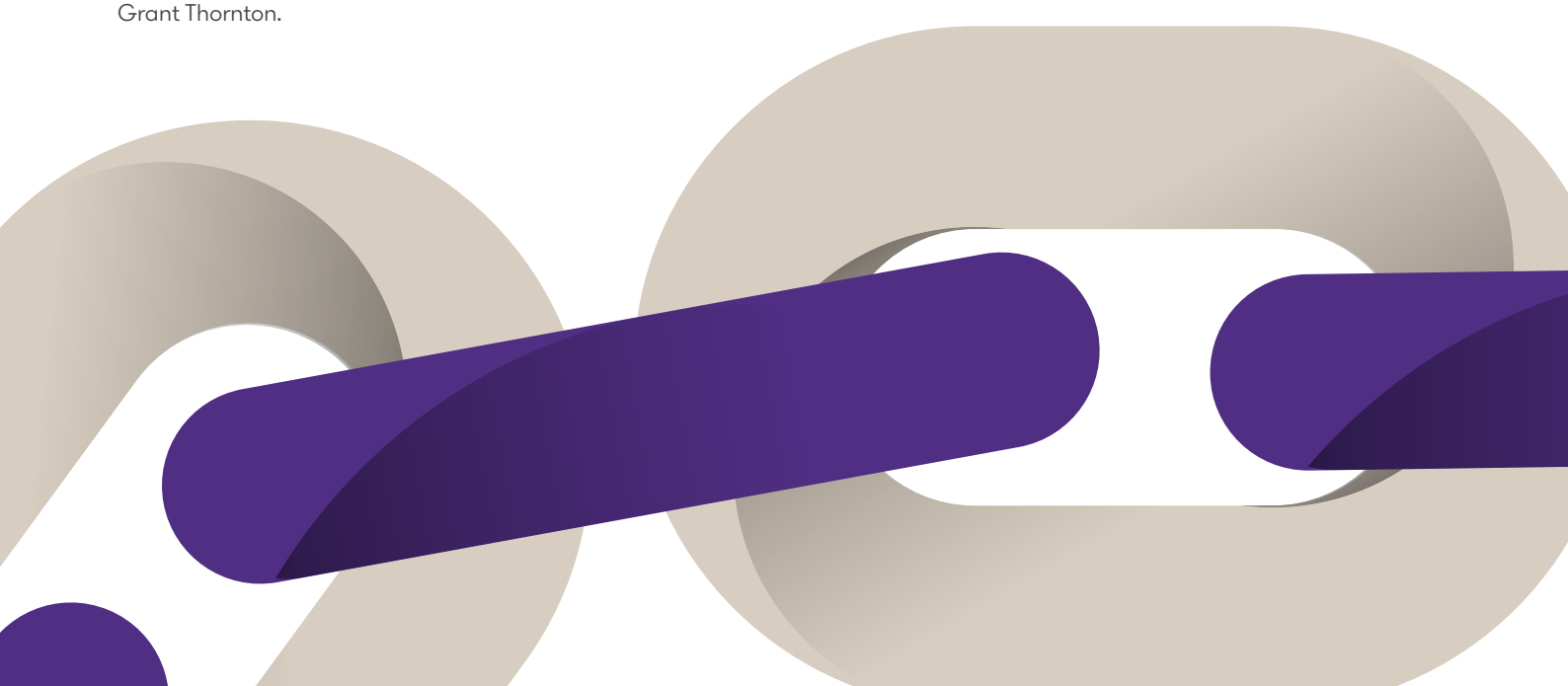
“Cualquier hacker le podrá decir que el eslabón más débil de un sistema son las personas”, advierte Andrew Harbison de Grant Thornton.

“Es necesario centrarse en la formación, formación y más formación. En una organización en la que trabajé tenían una clasificación por colores (verde, amarillo y rojo) para los datos. Pero llegó un momento en que todo era rojo, y tuvieron que introducir el morado para los casos todavía más graves que el rojo. Si eso ocurre, hay que sentar a los empleados y explicarles cómo clasificar correctamente los datos”.

Sin embargo, la formación también tiene sus límites. “Si los empleados no son buenos en seguridad informática y no consigue incentivarlos, el problema nunca desaparece”, afirma Bronk. “Es necesario encontrar algún tipo de solución técnica que elimine todos los factores de riesgo posibles. Podría ser un sistema basado en los clientes para el correo electrónico que nos avise cuando “alguien ha hecho clic sobre el enlace de “contraseña olvidada” de un correo nuestro. Veamos desde dónde se ha hecho ese clic, demos la señal de alerta y analicemos los datos”.

Más allá del miedo

Las ventajas de conocer mejor los datos de los que se dispone van mucho más allá de la seguridad informática. Anderson afirma que las empresas pueden animar a sus empleados a que conozcan mejor sus datos apuntando al valor añadido que esto les puede aportar. “Si hay algo que he aprendido en los últimos 15 años”, señala, “es que la ciberseguridad se basa en la economía”.



Conclusiones

Somos conscientes de que el riesgo de ciberataque se irá intensificando a medida que vayan apareciendo nuevas tecnologías, y la mayoría de las organizaciones aceptan que necesitan mejorar su gestión de esta amenaza.

El riesgo de ciberataque se debe afrontar a través de un planteamiento de mejora continua y estamos convencidos de que esto no resulta posible a menos que se disponga de una imagen clara y fiable de los datos de los que dispone.

Para ello, es necesario considerar los datos como un activo empresarial crítico —aunque nuestro estudio sugiere que muchas organizaciones no los perciben como tal—. No hacen lo suficiente para conocer los datos de los que disponen ni para protegerlos. Incluso cuando toman medidas para mejorar la protección de sus datos, suelen utilizar herramientas y planteamientos tradicionales que resultan insuficientes para medir, gestionar y valorar los riesgos inmateriales.

Sin embargo, tal y como hemos señalado en el informe, no cabe duda de que se puede adoptar un planteamiento práctico y eficaz. En primer lugar, las organizaciones deben aceptar que la cantidad de datos de los que disponen es demasiado abultada —y demasiado importante— como para no tenerla en cuenta.

Además, deben ser pragmáticas. Si da por sentado que alguien, en algún momento, encontrará la manera de acceder a sus sistemas, seguramente haga todo lo posible por garantizar que sus datos más valiosos se mantengan a salvo.

En última instancia, esto supone entender cuáles son sus joyas de la corona —dependiendo de su sector, su perfil de riesgo y sus objetivos comerciales— y asignar controles específicos al respecto. No se trata de una actividad sencilla, ni siquiera limitada, pero resulta una parte indispensable de la gestión de riesgos en la era digital.

“En el plazo de cinco años, la infraestructura informática de la que disponemos se utilizará para orquestar ciberataques que ni siquiera podemos llegar a imaginar”

Luis Pastor, Socio de Consultoría Tecnológica e Innovación de Grant Thornton

Póngase en contacto con nosotros

Ayudamos a nuestros clientes a prepararse para las amenazas de seguridad informática, a conseguir una protección continuada, a reaccionar de forma eficaz ante posibles ataques y a impulsar el cambio para mejorar su capacidad en la materia.

Si desea mejorar la gestión de la información y minimizar el riesgo de ciberataque, póngase en contacto con uno de nuestros equipos de especialistas:

Luis Pastor
Socio de Consultoría Tecnológica e Innovación
E Luis.Pastor@es.gt.com
T+34 91 576 39 99

Jaime Morales
Supervisor de Consultoría Tecnológica e Innovación
E Jaime.Morales@es.gt.com
T+34 91 576 39 99

Para obtener más información sobre nuestros servicios de ciber-resiliencia, visite GrantThornton.es

Metodología de estudio del IBR

El informe International Business Report (IBR) de Grant Thornton ofrece información de valor sobre las opiniones y expectativas de más de 10 000 empresas de 36 economías cada año. Los cuestionarios se traducen a los idiomas locales y cada país participante tiene la opción de introducir una serie de preguntas específicas para su país además del cuestionario general. El trabajo de campo se realiza con una periodicidad trimestral, principalmente por teléfono. En el IBR participan tanto sociedades cotizadas como empresas privadas.

Los datos para este informe se han obtenido de entrevistas realizadas a más de 2.900 directores generales, consejeros delegados, presidentes u otros altos directivos entre enero y marzo de 2018.

Reconocimientos

Además de realizar el estudio cualitativo anterior, trabajamos con Longitude para realizar entrevistas completas a especialistas en ciberseguridad de la red de Grant Thornton, así como a líderes empresariales externos y miembros del consejo a comienzos de 2017.

Queremos dar las gracias a las siguientes personas por habernos dedicado su tiempo y por su aportación a este informe:

- Ross Anderson, profesor de seguridad , Computer Laboratory, Universidad de Cambridge
- Chris Bronk, profesor adjunto, Universidad de Houston
- Tom Faulkner, responsable de producción de TI, CMC Markets
- Chris Hankin, director del Institute for Security Science and Technology, Imperial College London
- John Kan, responsable de información, A*STAR
- Nick Oldham, abogado especialista en privacidad y seguridad de datos, King & Spalding
- Ayman Omar, profesor adjunto e investigador del Kogod Cybersecurity Governance Center, Kogod School of Business, American University
- David Pollino, vicepresidente y responsable de seguridad adjunto, Bank of the West
- El responsable de TI de una sociedad de gestión de inversiones que ha preferido mantener su anonimato
- El responsable de tecnología de un banco internacional que ha preferido mantener su anonimato

Acerca de Grant Thornton

Grant Thornton es una de las organizaciones de firmas independientes de auditoría, fiscalidad y consultoría más importantes del mundo. Estas firmas ayudan a las organizaciones dinámicas a aprovechar su potencial de crecimiento, ofreciéndoles un asesoramiento de alto valor añadido y orientado al futuro.

Nuestros equipos de profesionales proactivos, dirigidos por socios implicados y accesibles, utilizan sus análisis, experiencia y conocimientos para entender los complejos asuntos que afectan a las empresas cotizadas y privadas, así como a los clientes del sector público, para ayudarles a encontrar soluciones. Más de 50.000 empleados de Grant Thornton distribuidos en más de 135 países se esfuerzan por marcar la diferencia en beneficio de nuestros clientes, nuestros compañeros y las comunidades en las que vivimos y trabajamos.

Grant Thornton

An instinct for growth™

grantthornton.global

© 2018 Grant Thornton International Ltd. Todos los derechos reservados.

«Grant Thornton» se refiere a la marca bajo la que las firmas asociadas de Grant Thornton suministran servicios de aseguramiento, tributarios y consultoría a sus clientes y/o a una o más firmas asociadas, según lo que dicte el contexto. Grant Thornton International Ltd (GTIL) y sus firmas asociadas no constituyen una asociación internacional. GTIL y cada una de las firmas asociadas constituyen una persona jurídica independiente. Los servicios son prestados por las firmas asociadas. GTIL no suministra servicios a clientes. GTIL y sus firmas asociadas no son agentes, ni asumen obligación ni responsabilidad alguna con respecto a los actos u omisiones de las demás.