Haciendo frente al Desafío del Ciber Riesgo

20 de septiembre de 2016

Un informe de Lloyd's

LLOYD'S

Índice

Sección 1
Resumen ejecutivo

1.1 Resumen ejecutivo

Hoy en día, casi todas las empresas dependen de la tecnología digital, independientemente de su tamaño o ubicación. Aunque ayuda a las empresas a ser más eficientes, reduce sus costes y abre nuevos mercados, también las vuelve más vulnerables frente a los ciber ataques. Durante los dos últimos años, una serie de notorios incidentes informáticos, – muchos de ellos violaciones de datos que supusieron la filtración de información de clientes, sitúan a la ciber seguridad en un primer plano.

Un hecho que añade cierta urgencia es que, en 2018, la Unión Europea implantará el Reglamento General de Protección de Datos (RGPD), en el que se establecen rigurosos requisitos para cualquier empresa que gestione datos de consumidores europeos.

Lloyd's, el centro global de ciber seguros, encargó esta encuesta para descubrir lo que las empresas europeas están haciendo para abordar la cuestión de la ciber seguridad y cómo se están preparando para el RGPD.

En la encuesta participaron 346 ejecutivos senior de grandes empresas (con ingresos de 250 millones de euros o más) en toda Europa. Entre los cargos de los encuestados se incluyen los de Consejero Delegado Ejecutivo (CEO); Director Financiero (CFO); Director de Operaciones (COO); Director de Tecnologías de la Información (CIO); Director de Tecnologías (CTO); Director de Riesgos (CRO) y asesor jurídico general.

La mayoría de las grandes empresas europeas han sufrido una violación de datos en los últimos cinco años, pero no les preocupa la posibilidad de volver a sufrir otra violación de nuevo.

– El 92% de los encuestados afirmaron que sus empresas habían sufrido una violación de datos en los últimos cinco años; sin embargo, solo el 42% estaba preocupados por sufrir otra violación en el futuro.

El ciber riesgo es una cuestión que ha ganado una importancia significativa en la agenda de los consejos de administración durante el último año: ahora es el CEO y no el CIO o Director de Tecnologías de la Información quien se encarga de la estrategia de ciber seguridad.

– Actualmente son los CEOs quienes se encargan de impulsar los planes para protegerse de las violaciones de datos en la mayoría de las empresas encuestadas (54%). Por el contrario, únicamente en un 10% de las empresas son los CIOs o Directores de Tecnologías de la Información quienes se encargan de la toma de decisiones. Esto es consecuencia de una serie de notorios ciber incidentes en empresas de todo el mundo, muchos de los cuales tuvieron un importante impacto en los resultados económicos o en el precio de las acciones y, en algunos casos, llevó a que ejecutivos senior perdieran sus trabajos.

La concienciación en torno al Reglamento General de Protección de Datos Europeo (RGPD) es alta, pero la comprensión de sus implicaciones es baja, lo que podría tener graves consecuencias.

– El 97% de los encuestados han oído hablar del RGPD, pero solo el 7% dijo conocer la cuestión "en profundidad"; el 57% de ellos afirmó saber "poco" o "nada" sobre el nuevo reglamento, a pesar de las importantes consecuencias financieras y legales que implicaría un incumplimiento de sus reglas.

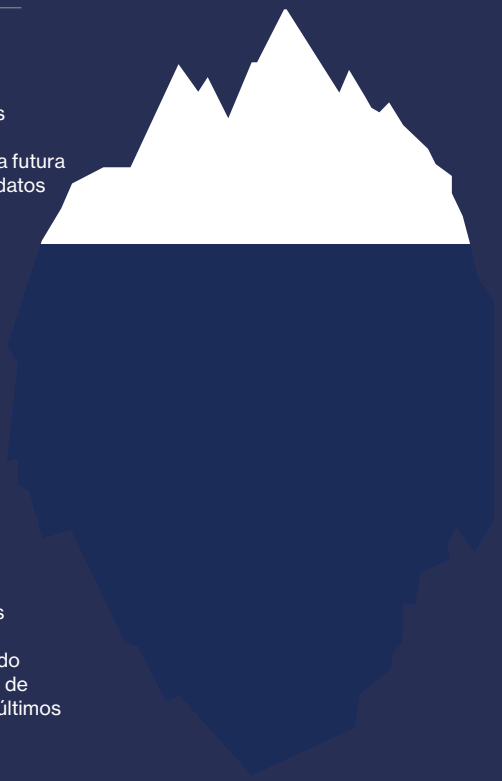
– Más de la mitad de las empresas encuestadas eran conscientes de que el RGPD podría afectarles en lo que respecta a inspecciones regulatorias (64%), sanciones económicas (58%), precio de las acciones (57%) y reputación (52%), pero solo el 13% creía que podrían perder clientes.

1.2 Conclusión

Las empresas europeas se enfrentan a un panorama del ciber riesgo en constante evolución. La implantación del RGPD centrará aún más la atención en el aspecto relativo a la seguridad de los datos de sus operaciones, ya que reguladores, accionistas y clientes lo utilizarán para responsabilizar a las empresas ante unos estándares de ciber seguridad más altos. Trabajando con socios especializados, como abogados, expertos en ciber seguridad y aseguradores, las empresas pueden comprender mejor los riesgos a los que se enfrentan y ayudar a mitigarlos, a fin de proteger sus balances.

42%

Al 42% de las empresas le preocupa una futura violación de datos



92%

El 92% de las empresas ha experimentado una violación de datos en los últimos cinco años

Cómo pueden ayudar los ciber seguros

- De acuerdo con esta encuesta, el 73% de los directivos de las empresas dispone de un conocimiento limitado sobre ciber seguros y el 50% desconoce que existen coberturas para violaciones de datos
- Los ciber seguros no solo ofrecen indemnizaciones económicas tras un ciber ataque, sino que además ofrecen asesoramiento especializado para mejorar la seguridad y soporte sobre el terreno durante el periodo de crisis
- Trabajar con suscriptores que conocen este riesgo desde el principio beneficiará a la estrategia de seguridad de la empresa. Los suscriptores pueden ayudar a las empresas a identificar riesgos y vulnerabilidades y, por consiguiente, pueden mitigar la probabilidad de que ocurra una violación de datos desde el principio
- Todo esto ayuda a proteger los balances de la empresa, así como a incrementar los estándares de ciber seguridad y mitigación de riesgos en todo el sector.

Visite www.lloyds.com/cyber

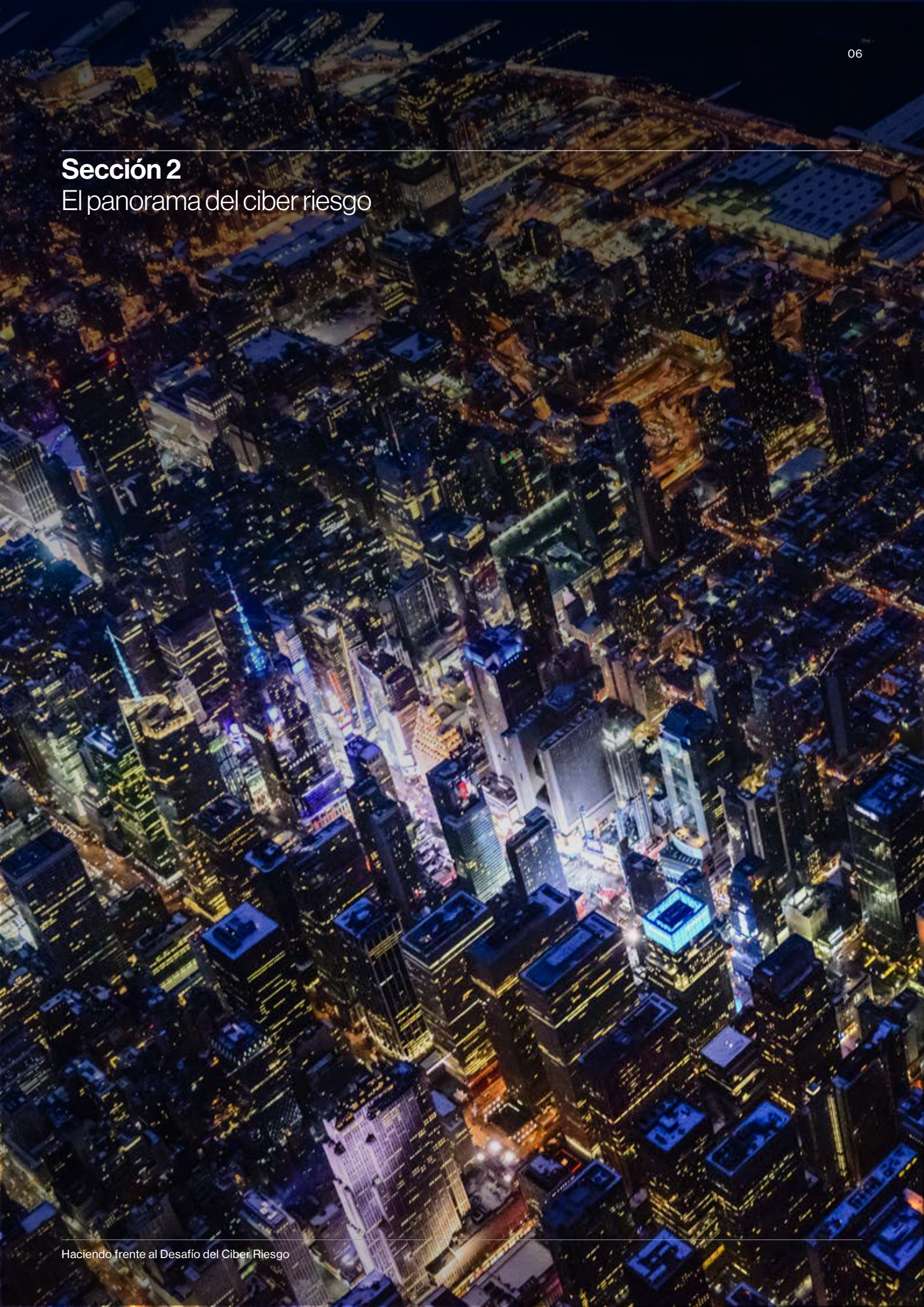
97%

El 97% de las empresas ha oído hablar de la nueva regulación de la UE (RGPD)

57%

El 57% de las empresas sabe poco o nada sobre la nueva regulación de la UE (RGPD)

Sección 2
El panorama del ciber riesgo



2.1 Aumento de los ciber riesgos

Hoy en día, casi todas las empresas dependen de la tecnología digital, independientemente de su tamaño o ubicación. Minoristas, empresas de servicios financieros y marcas de bienes de consumo utilizan actualmente tecnologías digitales para dirigir sus empresas, monitorizar el inventario, diseñar productos, comunicar y almacenar la información del cliente.

Pero, aunque las tecnologías digitales ayudan a las empresas a ser más eficientes, reducir sus costes y desarrollar nuevos mercados, también las vuelve más vulnerables a los ciber ataques.

Por ello, la ciber seguridad se ha convertido en una cuestión de gran importancia para las empresas. Hoy en día, el ciber riesgo se sitúa al nivel de riesgos ya consolidados como los daños materiales, el terrorismo y los desastres naturales; constituye una amenaza que toda empresa debe evaluar, mitigar y gestionar.

El aumento de la concienciación en torno a los ciber riesgos entre las empresas se ha visto impulsado por algunos notorios incidentes en todo el mundo durante los últimos años. El ciber ataque reciente más destacado en Reino Unido fue contra el proveedor de telecomunicaciones TalkTalk en otoño de 2015. En otras partes de Europa, ha habido ataques contra la cadena de televisión francesa TV5 Monde, el sistema de control aéreo de Suecia, empresas petrolíferas y de energía noruegas y una planta siderúrgica alemana, entre otros. En E.E. U.U., una serie de ciber incidentes han llenado los titulares desde 2014, entre ellos los ataques a Sony, Target, Home Depot y Experian.

Consecuentemente, el mercado de Lloyd's, que fue pionero en la emisión de la primera póliza de ciber seguro hace 10 años, ha visto como el mercado de los ciber seguros crecía rápidamente. Actualmente, hay 65 aseguradores en el mercado de Lloyd's que ofrecen ciber seguros, con una capacidad combinada de 300 millones de libras. Su negocio representa un cuarto del mercado global de ciber seguros, lo que convierte a Lloyd's en el centro global de este tipo de seguros.

En este informe, basado en una encuesta a 346 ejecutivos senior de grandes empresas en toda Europa, se analiza la forma en la que los directivos de las empresas están abordando el desafío de la ciber seguridad, así como las medidas que están adoptando para garantizar que sus organizaciones están bien preparadas en caso de un ciber ataque.

Asimismo, en el informe, también se investiga el nivel de preparación de las empresas europeas para la implementación del Reglamento General de Protección de Datos (RGPD), que entrará en vigor en 2018. Este nuevo reglamento endurecerá considerablemente las normas y responsabilidades existentes que rigen la forma en la que las empresas procesan y salvaguardan la información de los consumidores. Además, introduce una serie de requisitos para las empresas que sufren una violación de datos, incluyendo la obligación de informar sobre la misma en 72 horas o hacer frente a importantes multas.

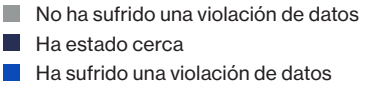
Este informe se centra en un solo tipo de ciber incidente: la violación de datos. Ello se debe a que la protección de la información confidencial, en especial los registros financieros o los historiales médicos de los clientes, está considerada como una prioridad en la mayoría de las empresas. Los datos son su principal activo digital y, por consiguiente, el objetivo de la mayoría de los ciber ataques.

2.2 Violación de datos

¿Cuál es la importancia de una violación de datos para las empresas europeas hoy en día? Para cuantificar la escala del problema, se preguntó a los encuestados si habían sufrido alguna violación de datos en su organización.

El 92% de los encuestados afirmó que su empresa había sufrido una violación de datos en los últimos cinco años; mientras que un 3% afirmó "haber estado cerca". Sólo el 5% negó haber sufrido una violación de datos o afirmó no tener conocimiento de haberla sufrido.

¿Cuál de las siguientes opciones describe mejor la experiencia de una violación de datos en tu empresa en los últimos cinco años?



Total

Reino Unido

Francia

Alemania

Italia

España

Países Bajos

Noruega

Suecia

Dinamarca

Base: Total de encuestados (346): Reino Unido (100) Francia (31) Alemania (34) Italia (30) España (30) Países Bajos (31) Noruega (30) Dinamarca (30)

2.3 Amenazas internas y externas

Las violaciones de datos pueden estar causadas por varios métodos de ciber ataque, algunos de ellos muy sofisticados y maliciosos y otros relativamente inofensivos o accidentales. En la encuesta se preguntaba cuál de las amenazas preocupaba más a las empresas.

Las ciber amenazas se clasificaron como “internas” o “externas”. Las amenazas internas son las que habitualmente se originan dentro de la propia empresa ya sea por un error humano, como puede ser la pérdida o el robo de información o equipo, o por un empleado deshonesto que filtra información confidencial intencionadamente. Las amenazas externas tienden a proceder de tecnologías más avanzadas e incluyen técnicas como el hackeo, phishing, ransomware y malware (ver el glosario abajo).

En la encuesta se descubrió que la mayoría de las empresas estaban más preocupadas por las amenazas externas que por las internas. Las amenazas internas que más preocupaban a las empresas procedían de tecnologías menos avanzadas, de las cuales un 42% de los encuestados señalaba la pérdida de documentos físicos como la principal preocupación. El mismo porcentaje también incluyó como una amenaza principal la del trabajador que divulga información intencionadamente.

La amenaza externa número uno es el hackeo. La mitad de las empresas encuestadas (51%) afirmó que estaban preocupadas por la posibilidad de ser hackeadas para obtener beneficios económicos, en comparación con el 46% que estaba preocupado por ser hackeado por razones políticas. El 41% incluyó el hackeo por parte de la competencia como una amenaza importante.

No resulta sorprendente que el hackeo sea la amenaza número uno, dadas las recientes y notorias violaciones de datos. TalkTalk, Sony y Home Depot, por nombrar solo a tres, han sido víctimas de ciber ataques recientemente. Aunque la verdadera motivación de este tipo de incidentes a menudo no queda clara, los ataques de esta naturaleza pueden utilizarse para robar información de clientes que puede venderse al mejor postor.

También puede haber motivos políticos, en especial en el caso de empresas que operan en industrias geopolíticamente sensibles, como las dedicadas a la energía o los recursos naturales. Cada vez con más frecuencia, grupos clandestinos de hackers con objetivos políticos específicos atacan organizaciones individuales. Aunque los niveles de espionaje empresarial son difíciles de medir con precisión, el hecho de que el hackeo por parte de la competencia esté en el tercer puesto de la lista sugiere que es considerado como una amenaza seria por los directivos de las empresas.

Glosario de ciber amenazas

- Hacking – buscar y explotar vulnerabilidades en un sistema o red informática, normalmente para obtener beneficios económicos.
- Phishing – tratar de obtener información confidencial haciéndose pasar por una persona u organización de confianza en un correo electrónico.
- Whaling – un ataque de phishing que implica hacerse pasar por un alto ejecutivo, a menudo el CEO.
- Malware – (del inglés «malicious software») es un programa informático utilizado para alterar las operaciones informáticas, recopilar información confidencial u obtener acceso a sistemas informáticos privados.
- Ransomware – un tipo de malware que afecta negativamente a un ordenador y exige un rescate para restaurarlo.

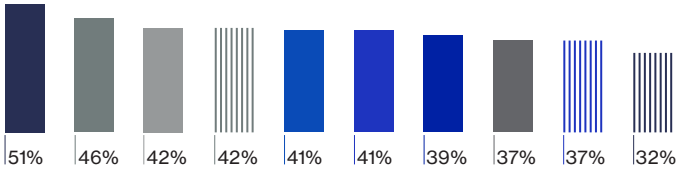
51%

Al 51% le preocupa la posibilidad de sufrir un hackeo para obtener beneficios económicos

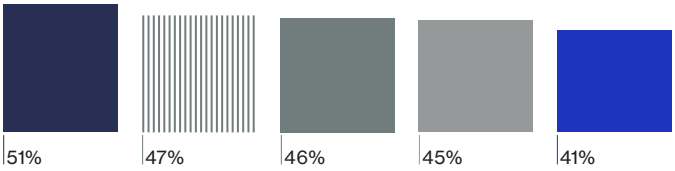
2.3 Amenazas internas y externas

- Hackeo – para obtener beneficios económicos
- Hackeo – por parte de la competencia
- Hackeo – por motivaciones políticas
- Error humano/divulgación involuntaria
- Phishing
- Equipo perdido, descartado o robado
- Ransomware
- Malware
- Pérdida física de papel o dispositivos no electrónicos
- Trabajador que filtra información intencionadamente

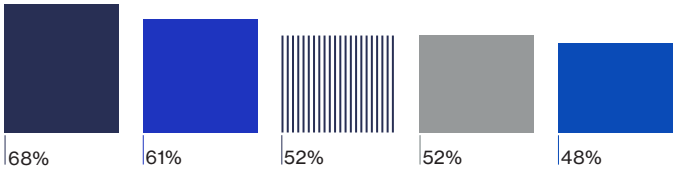
Total



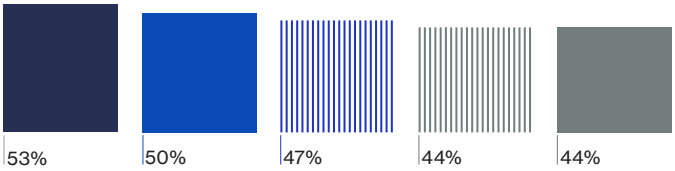
Reino Unido



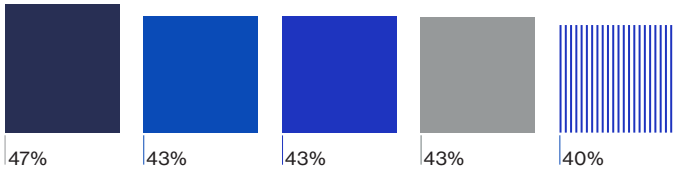
Francia



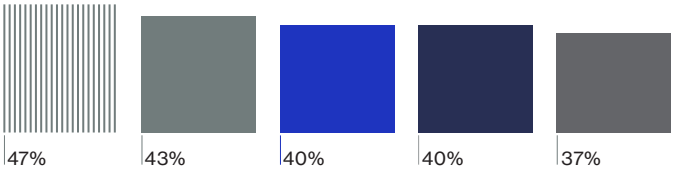
Alemania



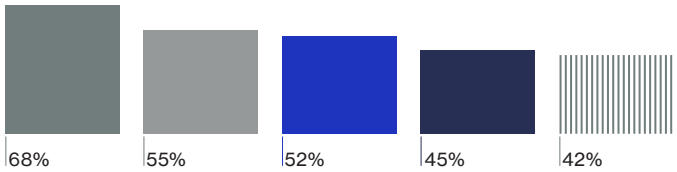
Italia



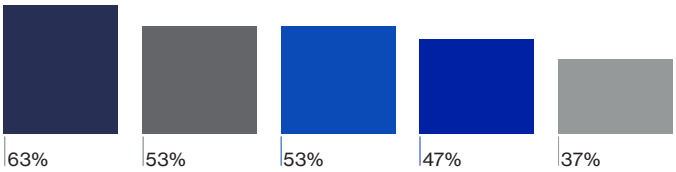
España



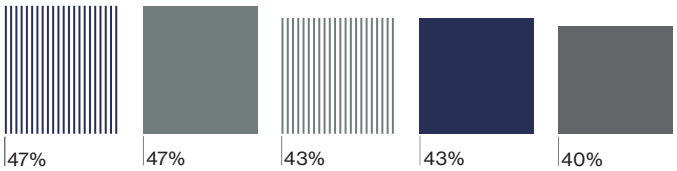
Países Bajos



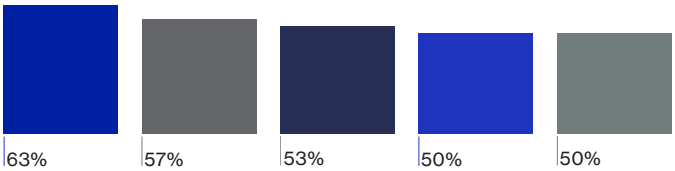
Noruega



Suecia



Dinamarca



Base: Total de encuestados (346): Reino Unido (100) Francia (31) Alemania (34) Italia (30) España (30) Países Bajos (31) Noruega (30) Dinamarca (30)

2.4 Una falsa sensación de ciber seguridad

Aunque el 92% de las empresas ha sufrido una violación de datos en los últimos cinco años, tan solo el 42% de los encuestados demuestran preocupación en lo que respecta a sufrir una futura violación de datos.

92%

El 92% ha sufrido una violación de datos

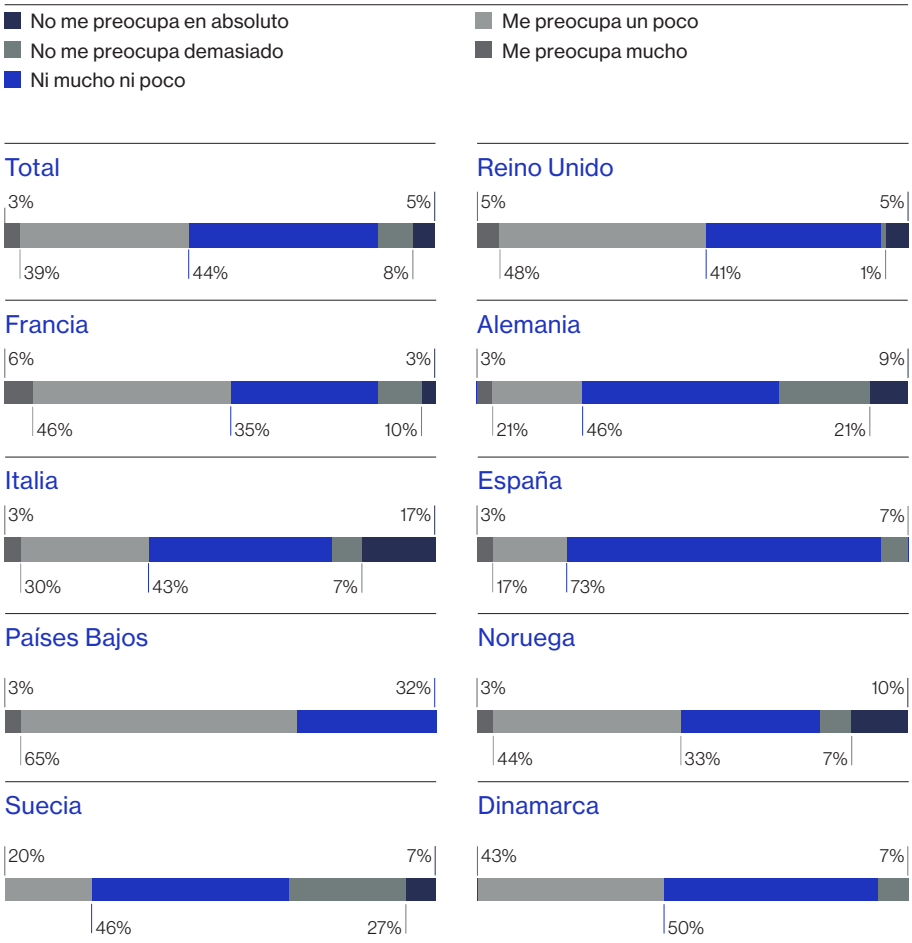
42%

Al 42% le preocupa la posibilidad de sufrir una futura violación de datos

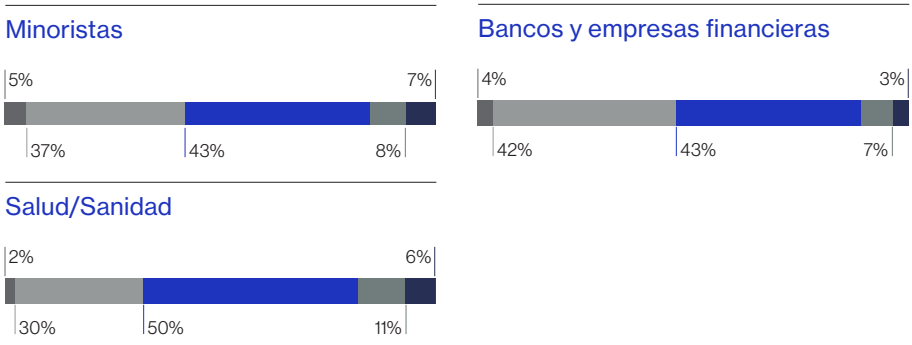
Los resultados difieren ligeramente de un sector a otro. Las empresas de servicios financieros eran más proclives a preocuparse por una violación de datos (46%), algo comprensible dado el volumen de información confidencial que tienen sobre sus clientes. Las empresas del sector sanitario estaban menos preocupadas (32%), algo que resulta sorprendente dado que los historiales médicos son más valiosos y, como tal, son cada vez más codiciados por los hackers.

Estos resultados muestran que, o las empresas confían en las medidas de ciber seguridad que han adoptado o están satisfechas con su resiliencia a los ciber ataques. Independientemente de la respuesta, el hecho es que la tecnología usada en los ciber ataques evoluciona constantemente, haciendo casi imposible para las empresas el estar 100% seguras. A menos que las empresas se tomen la ciber seguridad en serio, serán vulnerables a los ciber ataques en el futuro.

Piense en su empresa: en una escala del 1 al 5, donde 1 es “no me preocupa en absoluto” y 5 es “me preocupa mucho”, ¿cuánto le preocupa que su empresa pueda sufrir una violación de datos?



Base: Total de encuestados (346): Reino Unido (100) Francia (31) Alemania (34) Italia (30) España (30) Países Bajos (31) Noruega (30) Dinamarca (30)



Base: Total de encuestados (346): Minoristas (109) Bancos y empresas financieras (95) Salud/Sanidad (90)

Sección 3
Preparación y respuesta

3.1 Fallar en la preparación...

Tal y como se ha debatido en el capítulo anterior, un 92% de las empresas ha sufrido una violación de datos en los últimos cinco años. También se preguntaba a los encuestados cómo de preparados se sentían si dicho incidente sucediera de nuevo. Se preguntó a las empresas cómo describirían su nivel de preparación para una violación de datos en base a tres criterios:

1. Elaborar una respuesta a la crisis: p. ej. comunicando la noticia a los clientes y actualizando los sistemas de TI.
2. Gestionar el daño a la reputación: p. ej. a través de relaciones públicas, publicidad y otras actividades de marketing.
3. Implicaciones regulatorias: p. ej. cooperando con una investigación o respondiendo a cambios regulatorios.

93%

El 93% de las empresas estaría "preparada" o "muy preparada" para elaborar una respuesta a una crisis.

89%

El 89% afirmaron lo mismo sobre la gestión del daño a la reputación.

87%

El 87% sobre la gestión de las implicaciones regulatorias.

La mayoría de las empresas dispondrán de procesos y procedimientos para los ciber incidentes; pero no es lo mismo que estar completamente preparado. Muchas empresas se centran en desarrollar un plan de respuesta que establezca lo que deberán hacer en caso de una violación de datos; aun así, existe una serie de medidas, aquellas que cubren el antes y el después de la violación de datos, que deben adoptarse si una organización quiere estar totalmente preparada.

Las empresas deberían asegurarse de que sus sistemas se ponen a prueba de forma rigurosa y que han sido validados de forma externa antes de estar satisfechas con su nivel de preparación. Incluso entonces, es fundamental permanecer constantemente alerta y actualizar sus planes periódicamente a medida que surgen nuevas amenazas.

3.2 ¿Quién asume la responsabilidad?

Hubo un tiempo en el que la seguridad de los datos era responsabilidad única del departamento de TI. Hoy en día, la importancia de la seguridad de los datos es tal que ha escalado muchos puestos en la lista de prioridades de los directivos.

Este cambio se ha producido significativamente rápido. El año pasado (2015), una encuesta de Marsh mostró que solo el 17% de las empresas europeas incluían el ciber riesgo dentro de sus cinco principales riesgos corporativos, mientras que el 25% ni siquiera lo tenía en su registro de riesgos. Casi dos tercios de las empresas (65%) afirmaron que sus departamentos de TI eran los principales responsables de los ciber riesgos en sus organizaciones, mientras que el 11% afirmaron que era responsabilidad del consejo de administración.

La encuesta de Lloyd's, llevada a cabo nueve meses más tarde, descubrió que los consejos de administración de las empresas europeas estaban adoptando ahora enfoques mucho más prácticos, en un intento de hacer frente a los ciber riesgos.

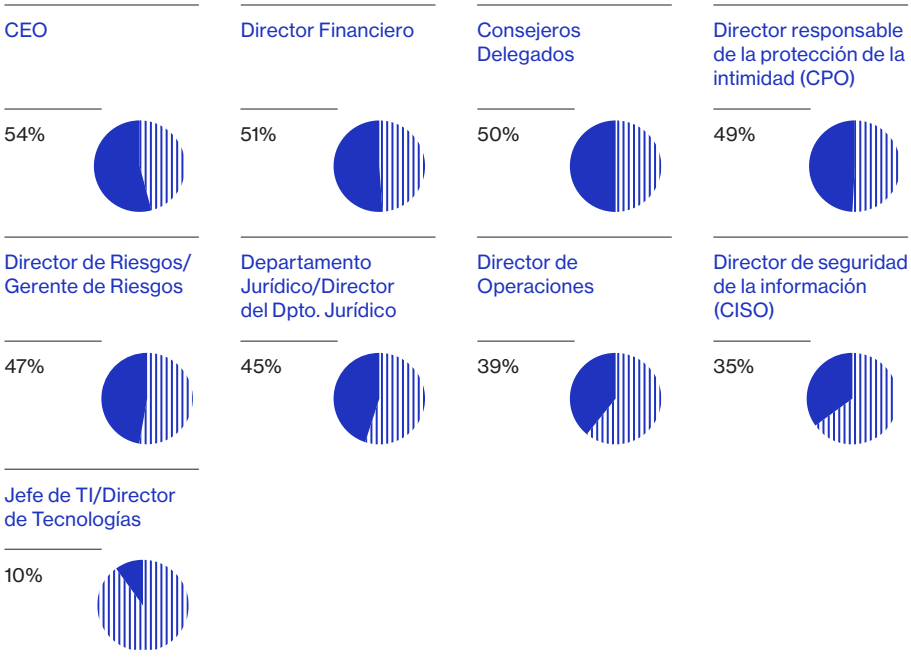
Se preguntó a los encuestados quién era el responsable en sus empresas de tomar las decisiones de protección y planificación relativas a una violación de la seguridad de datos. La mayoría de los encuestados (54%) afirmaron que era el CEO. Aquellos ejecutivos para quienes los ciber riesgos son parte de su día a día se situaban mucho más abajo en la lista: solo el 35% afirmó que el Director de Seguridad de la Información era quien se encargaba de esta cuestión y solo el 10% nombró al Director de Tecnologías de la Información (CIO) o al Director de Tecnologías (CTO). En el 96% de los casos, se nombraba a un representante del consejo de administración como el promotor.

Es probable que la reciente sucesión de violaciones de datos ampliamente publicitadas, así como sus consecuencias, desplome del precio de las acciones, costes, demandas, haya provocado que los CEOs desarrollen rigurosas estrategias en materia de ciber seguridad. Los accionistas esperan que el CEO asuma la responsabilidad de la ciber seguridad y haga todo lo que esté en su mano para mitigar los riesgos que, en última instancia, tendrán un impacto en el rendimiento financiero de la empresa.

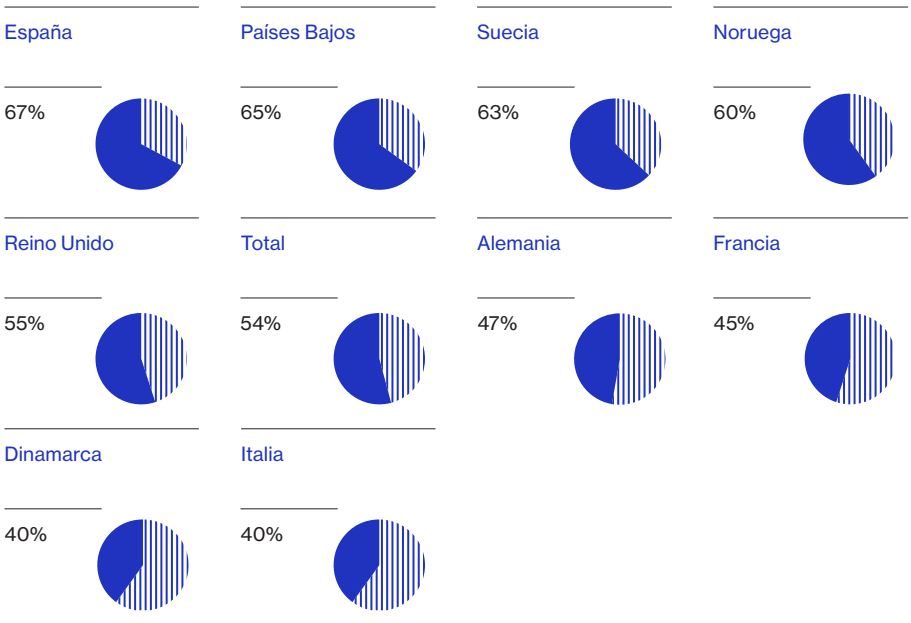
Los CEOs también tienen una razón clara para tomarse este asunto en serio, ya que sus puestos de trabajo están vinculados a las consecuencias de las violaciones de la ciber seguridad. Los CEOs de la minorista estadounidense Target y de la empresa aeroespacial austriaca FACC perdieron sus puestos de trabajo por razones vinculadas a ciber incidentes.

Es alentador ver que, tal y como muestra esta encuesta, cada vez más CEOs están tomándose en serio los ciber riesgos. Los próximos cambios en la regulación europea situarán en un primer plano esta cuestión en todas las empresas en Europa.

¿Quién es el responsable en su empresa de tomar la decisión sobre la protección y planificación relativas a una violación de la seguridad de datos?

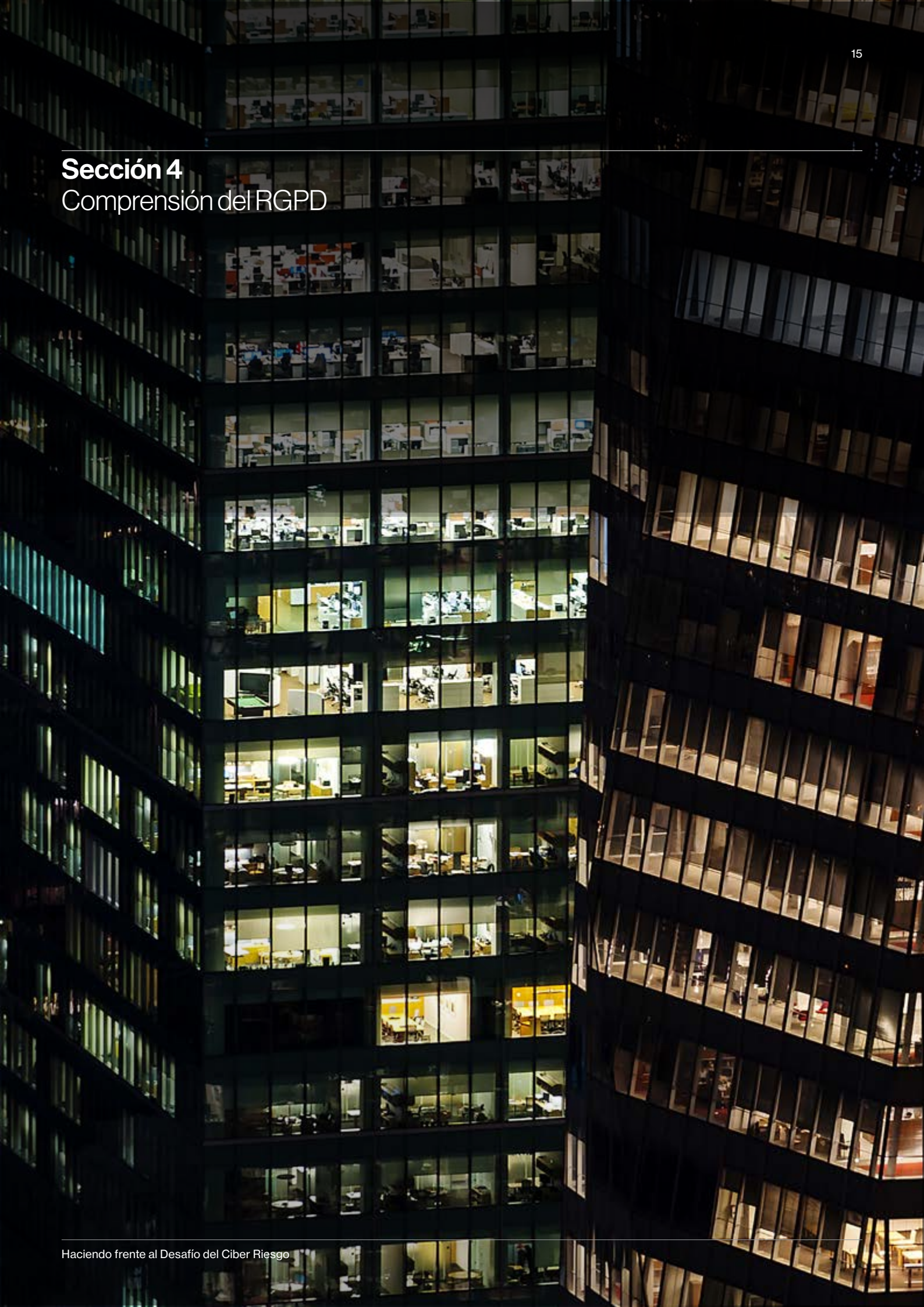


CEO



Base: Total de encuestados (346)

Sección 4
Comprensión del RGPD



4.1 Una nueva era de ciber regulación

La implementación del Reglamento General de Protección de Datos (RGPD) en 2018 transformará la ciber regulación en Europa. También tiene repercusiones significativas para las empresas de todo el mundo, muchas de las cuales no son del todo comprendidas por las propias empresas.

El RGPD plasma los derechos fundamentales de privacidad de los consumidores, como el "derecho a ser olvidado" y el derecho a oponerse a actividades de elaboración de perfiles, derechos que las empresas tendrán que respetar.

Significativamente el RGPD no se aplica únicamente a las empresas de los Estados miembros de la UE. Cualquier empresa que ofrezca bienes y servicios a ciudadanos europeos o que monitorice su comportamiento, también tendrá que cumplir con esta regulación. Ello significa que muchas empresas de los Estados Unidos y de Asia, por ejemplo, entrarán dentro del alcance jurisdiccional del RGPD.

Claramente, el RGPD no puede ignorarse. En esta encuesta, se preguntó a los encuestados sobre la preparación que están realizando para su implementación, que tendrá lugar en menos de dos años.

¿Qué es el RGPD?

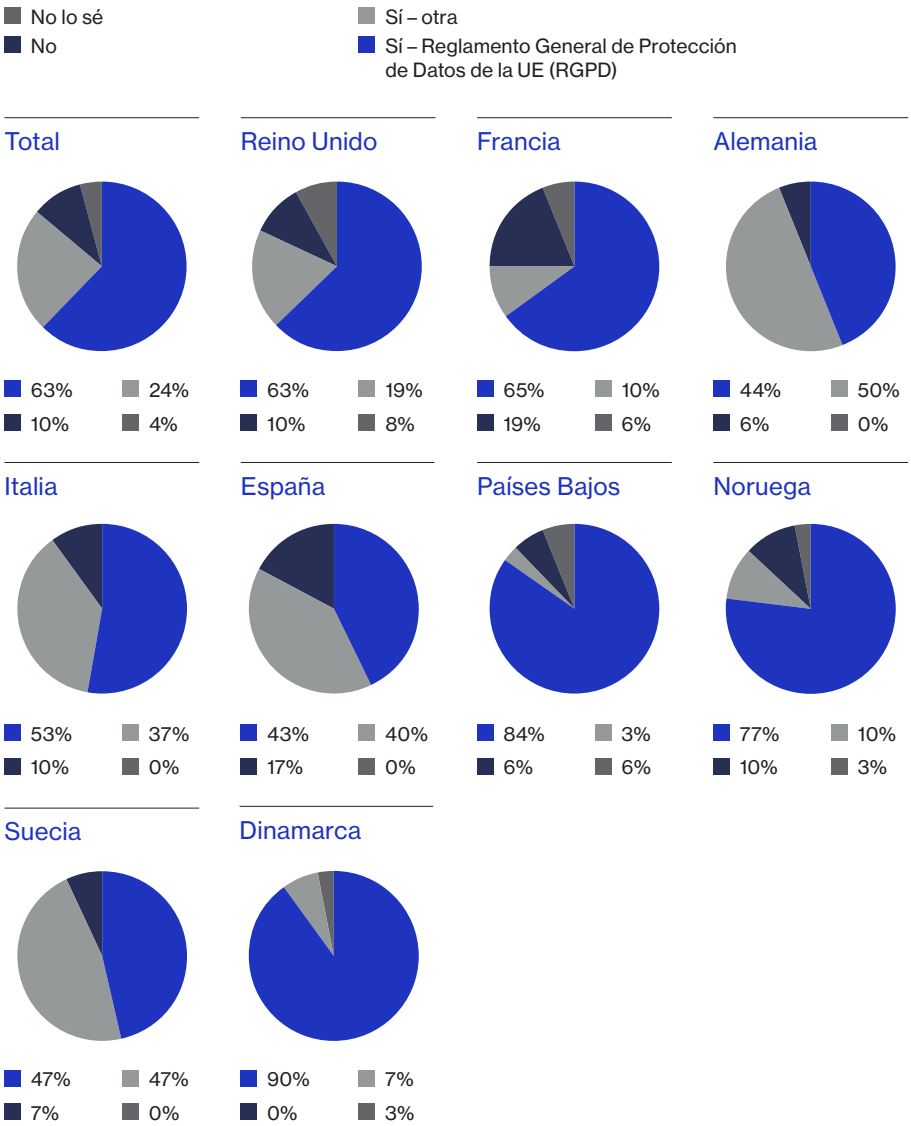
- El Reglamento General de Protección de Datos (RGPD) es una normativa europea que armoniza las diversas legislaciones en materia de protección de datos en Europa y actualiza la legislación de la UE con las posibilidades tecnológicas de la era del Big Data.
- En especial, obliga a las empresas a informar de las violaciones de seguridad a sus reguladores dentro de las siguientes 72 horas y a los ciudadanos afectados sin retrasos injustificados.
- Castiga con multas de hasta el 4% de la facturación mundial anual o 20 millones de euros, la cantidad que sea mayor, a las empresas que sufran violaciones de datos. Las personas físicas también pueden reclamar indemnizaciones a las organizaciones por las pérdidas económicas o el estrés sufrido.
- Entrará en vigor el 25 de mayo de 2018 en todos los Estados miembros de la UE, pero afectará a todas aquellas empresas que operen con ciudadanos europeos, independientemente de donde tenga la sede la empresa.

4.2 Concienciación y comprensión

Dada la importancia del RGPD, el hecho de que se anunciara públicamente por primera vez en 2012 y su inminente implementación, era de esperar que las empresas tuvieran ya implementados sus planes. La encuesta descubrió un panorama bastante más heterogéneo.

Se descubrió que la mayoría de las empresas están al tanto del RGPD. Cuando se les preguntaba si conocían alguna nueva regulación que pudiera afectar al panorama de la protección de datos, el 63% mencionó al RGPD. Otro 24% citaba otras regulaciones, lo que podría incluir cambios en la protección de datos a nivel nacional.

¿Está al tanto de alguna nueva regulación o cambios en la regulación sobre protección de datos?



Base: Total de encuestados (346): Reino Unido (100) Francia (31) Alemania (34) Italia (30) España (30) Países Bajos (31) Noruega (30) Dinamarca (30)

4.2 Concienciación y comprensión

Cuando se les preguntaba directamente sobre el RGPD, un total del 97% de las empresas afirmó haber oído hablar de él. Sin embargo, esa cifra enmascara un nivel mucho más bajo de conocimiento en profundidad. Tan solo el 7% de los encuestados afirmó conocer "en profundidad" el RGPD, mientras que más de la mitad (57%) admitió conocer "poco" o "nada" sobre él. Dada la importancia que tiene el RGPD para las empresas, ello revela una sorprendente falta de conocimiento.

97%

El 97% de los encuestados han oído hablar del RGPD

57%

El 57% admitió que conocía "poco" o "nada" sobre el RGPD

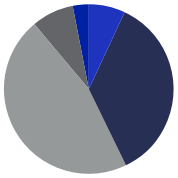
Las reglas del RGPD incluyen, por ejemplo, las posibles e importantes multas económicas que podrán imponerse a las empresas que incurran en el incumplimiento del mismo (hasta un 4% de los ingresos globales). También establece estándares más altos de transparencia en lo que concierne a la forma en la que se usa la información de los clientes, la seguridad de los sistemas que la protegen y la rapidez con la que los clientes deben ser informados sobre una violación de datos. Ninguno de estos requisitos son fáciles de cumplir; llevará tiempo, inversiones y esfuerzo.

Este hallazgo sugiere que las empresas deben hacer más para comprender la forma en la que las reglas del RGPD afectarán a su organización, así como saber cuáles son sus responsabilidades.

¿Cuánto sabe sobre el Reglamento General de Protección de Datos de la Unión Europea (RGPD)?

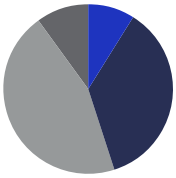
- Conozco en profundidad el RGPD de la UE
- He oído hablar del RGPD de la UE pero no conozco muchos detalles
- No he oído hablar del RGPD de la UE y no sé nada sobre él
- Dispongo de un conocimiento práctico del RGPD de la UE
- He oído hablar del RGPD de la UE pero no conozco muchos detalles

Total



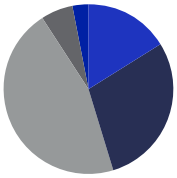
7% 36% 46% 8% 3%

Reino Unido



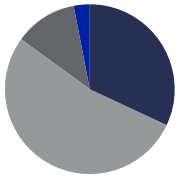
9% 36% 45% 10% 0%

Francia



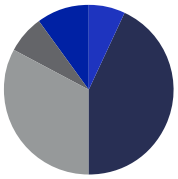
16% 29% 45% 6% 3%

Alemania



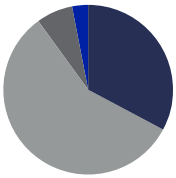
0% 32% 53% 12% 3%

Italia



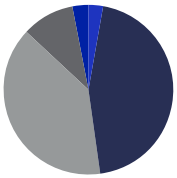
7% 43% 33% 7% 10%

España



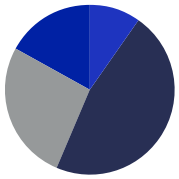
0% 33% 57% 7% 3%

Países Bajos



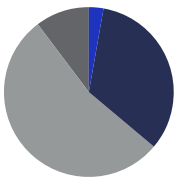
3% 45% 39% 10% 3%

Noruega



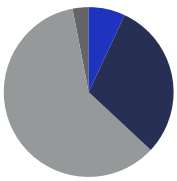
10% 47% 27% 0% 17%

Suecia



3% 33% 53% 10% 0%

Dinamarca



7% 30% 60% 3% 0%

Base: Total de encuestados (346): Reino Unido (100) Francia (31) Alemania (34) Italia (30) España (30) Países Bajos (31) Noruega (30) Dinamarca (30)

4.3 Identificar las repercusiones para las empresas

Aunque la mayoría de los directivos de las empresas admitieron saber poco sobre el RGPD, el 66% afirmó que conocía las implicaciones del RGPD si su empresa sufría una violación de datos.

Cuando se profundizaba en este tema, los encuestados se centraban en dos áreas principales: el impacto regulatorio y el financiero. La investigación regulatoria se encontraba en los primeros puestos de la lista, citada por un 64% de las empresas como la repercusión más probable. Las siguientes eran las multas o sanciones económicas (58%) y el impacto en los beneficios o el precio de las acciones (57%). Tan solo el 13% estaba preocupado por la pérdida de clientes.

64% investigación regulatoria

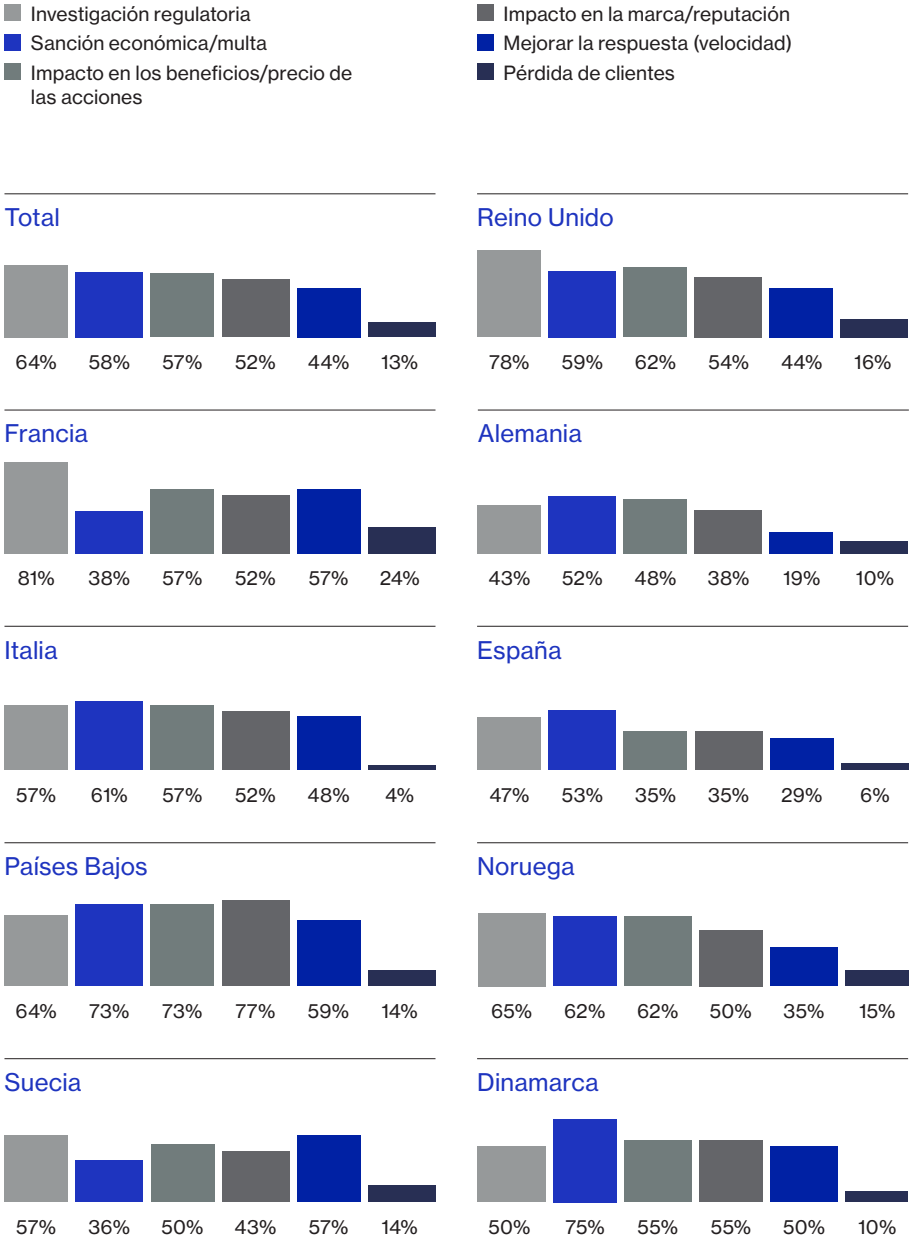
58% sanción económica/ multa

57% impacto en los beneficios/precio de las acciones

13% pérdida de clientes

La encuesta muestra que las grandes empresas europeas están más preocupadas por las repercusiones económicas que la regulación del RGPD podría tener en caso de una violación de datos. El ciber ataque contra TalkTalk, por ejemplo, le costó a la empresa cerca de 60 millones de libras y llevó a un desplome del precio de las acciones del 10% el día en el que se informó del incidente. Al amparo de la regulación del RGPD, es probable que el impacto económico de una violación de datos sea aún mayor.

Teniendo en cuenta los procesos actuales de seguridad de la información en su empresa, ¿cuáles serán las repercusiones que cree más probables que el RGPD tenga en su empresa?



Base: Total de encuestados (227): Reino Unido (63) Francia (21) Alemania (21) Italia (23) España (17) Países Bajos (22) Noruega (26) Dinamarca (20)

Sección 5
Conclusión

5.1 Conclusión

El ciber riesgo es el riesgo más complejo, actual y crítico al que las empresas se enfrentan actualmente: es una cuestión de cuándo y no de si una empresa es víctima de un ciber ataque.

Los ciber incidentes tienen el potencial de provocar una interrupción del negocio, sanciones económicas, una inspección del regulador y daños a la reputación. Todas ellas son amenazas serias a los ingresos, precio de las acciones e, incluso, la supervivencia de una empresa. En esta coyuntura, puede que resulte difícil para los directivos de las empresas saber lo que pueden hacer para proteger a sus organizaciones.

Los resultados de esta encuesta muestran que, aunque muchas empresas parecen confiar en su nivel de preparación para el RGPD, la comprensión de sus repercusiones es baja. Y los últimos ejemplos de violaciones de datos sugieren que las empresas no están tan preparadas contra los ciber ataques como ellas piensan.

Quedando aún 18 meses para que el RGPD entre en vigor, las empresas todavía disponen de tiempo para hacer que sus procesos y sistemas cumplan el RGPD. Mientras tanto, es fundamental que las empresas sigan revisando su estrategia en materia de ciber riesgos, así como su comprensión de la amenaza. Las ciber amenazas no van a desaparecer y, a medida que pase el tiempo, se volverán más complejas. Es casi imposible estar protegido al 100% de los ciber ataques.

A continuación, incluimos tres pasos que los directivos de las empresas deberían tener en cuenta para proteger sus organizaciones:

1 Identificar los riesgos específicos a los que hacer frente.

Definir la forma más probable en la que un ciber incidente podría producirse en su organización. Crear planes específicos para mitigarlos. ¿Cuáles son los casos improbables que no ha tenido en cuenta? Sus planes de respuesta deben ponerse a prueba y actualizarse de forma regular. Pida a asesores externos que los auditen. Trabajen de forma conjunta en hipótesis y simulaciones. Asegúrese de que está preparando para lo que hay que hacer antes y después de una violación de datos, no sólo sobre cómo ponerse en contacto con los clientes afectados.

2 Fomentar la concienciación sobre los ciber riesgos y la regulación dentro de su organización.

Muchos de los ciber incidentes empiezan con un error humano, desde la filtración accidental al phishing. La concienciación en torno a estos problemas es una cuestión cultural y debe proceder de las esferas más altas de la empresa. Asegúrese de que todo el mundo está formado y conoce, por ejemplo, lo que la regulación del RGPD les exige.

3 Nunca deje de aprender

La tecnología digital sigue evolucionando al igual que las ciber amenazas que la acompañan. Desarrolle una cultura de “aprendizaje continuo” en la que se comparta la información sobre los ciber riesgos. Comprenda que es imposible el 100% en lo que a la ciber seguridad respecta. Lo que hace que los esfuerzos para mitigar un incidente, como los ciber seguros, sean aún más fundamentales.

5.2 Cómo pueden ayudar los ciber seguros

1 De acuerdo a esta encuesta, el 73% de los directivos de las empresas dispone de un conocimiento limitado sobre ciber seguros y el 50% no sabe que hay disponible coberturas para violaciones de datos.

2 Los ciber seguros no solo ofrecen indemnizaciones económicas tras un ataque sino que, además, ofrecen asesoramiento especializado para mejorar la seguridad y soporte sobre el terreno durante el periodo de crisis.

3 Aunque las pólizas de seguros para ciber riesgos pueden ser diferentes, normalmente cubren el coste de las labores legales y forenses para identificar cómo ha sucedido la violación de datos y quién es el responsable, así como los costes de notificación a los clientes e interrupción del negocio.

4 Trabajar con suscriptores que conocen este riesgo desde el principio beneficiará a la estrategia de seguridad de la empresa. Los suscriptores pueden ayudar a las empresas a identificar los riesgos y las vulnerabilidades y, por consiguiente, mitigar la probabilidad de que ocurra una violación desde el principio.

5 Todo esto ayuda a proteger los balances de la empresa, así como a incrementar los estándares de ciber seguridad y mitigación de riesgos en todo el sector.

Hay disponibles informes sobre hechos destacados de los siguientes países: Alemania, Dinamarca, España, Francia, Italia, Noruega, Países Bajos, Reino Unido y Suecia.

Para más información y para contactar con un corredor de Lloyd's especializado en ciber Riesgos, visite www.lloyds.com/cyber