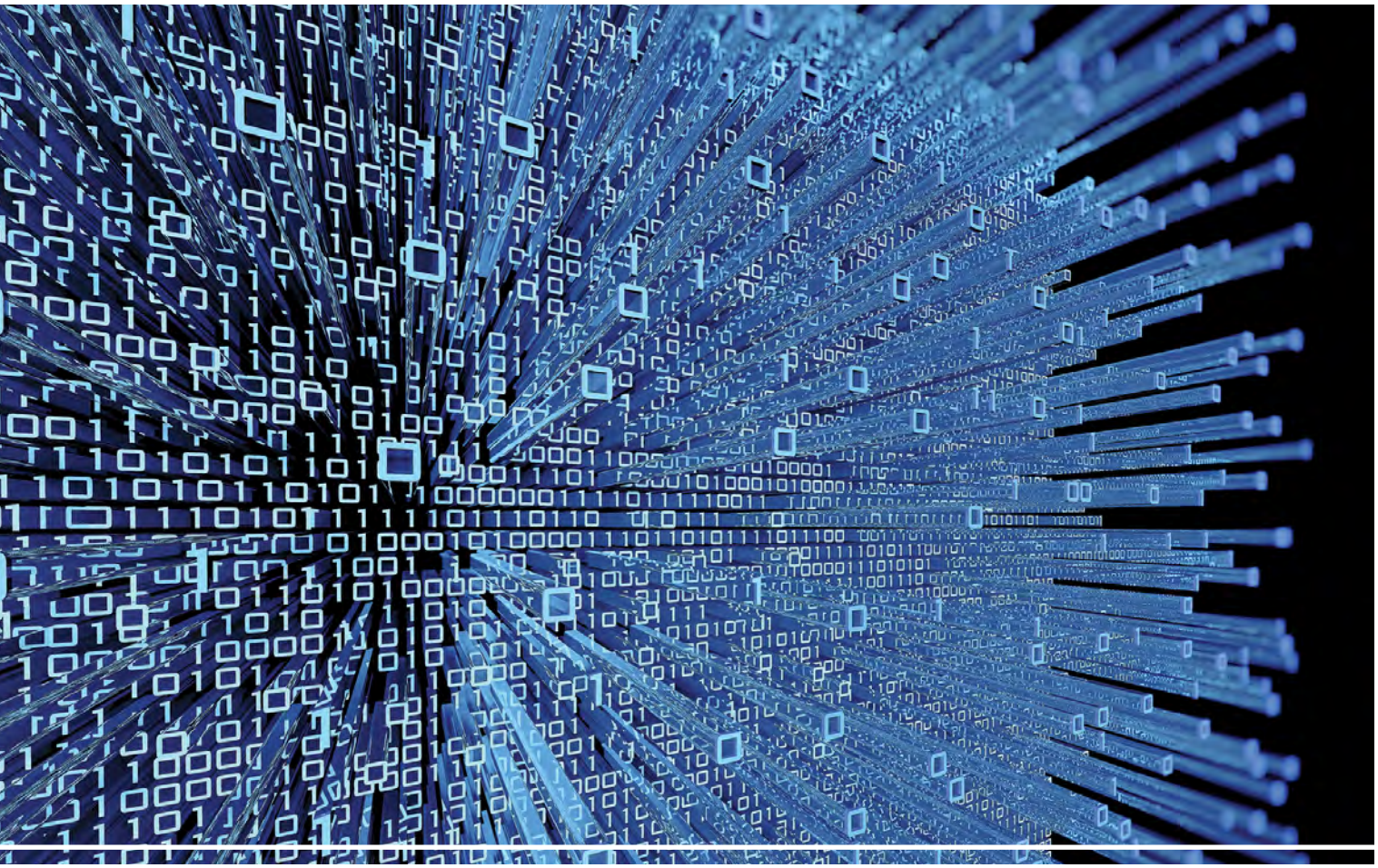
DNV·GL



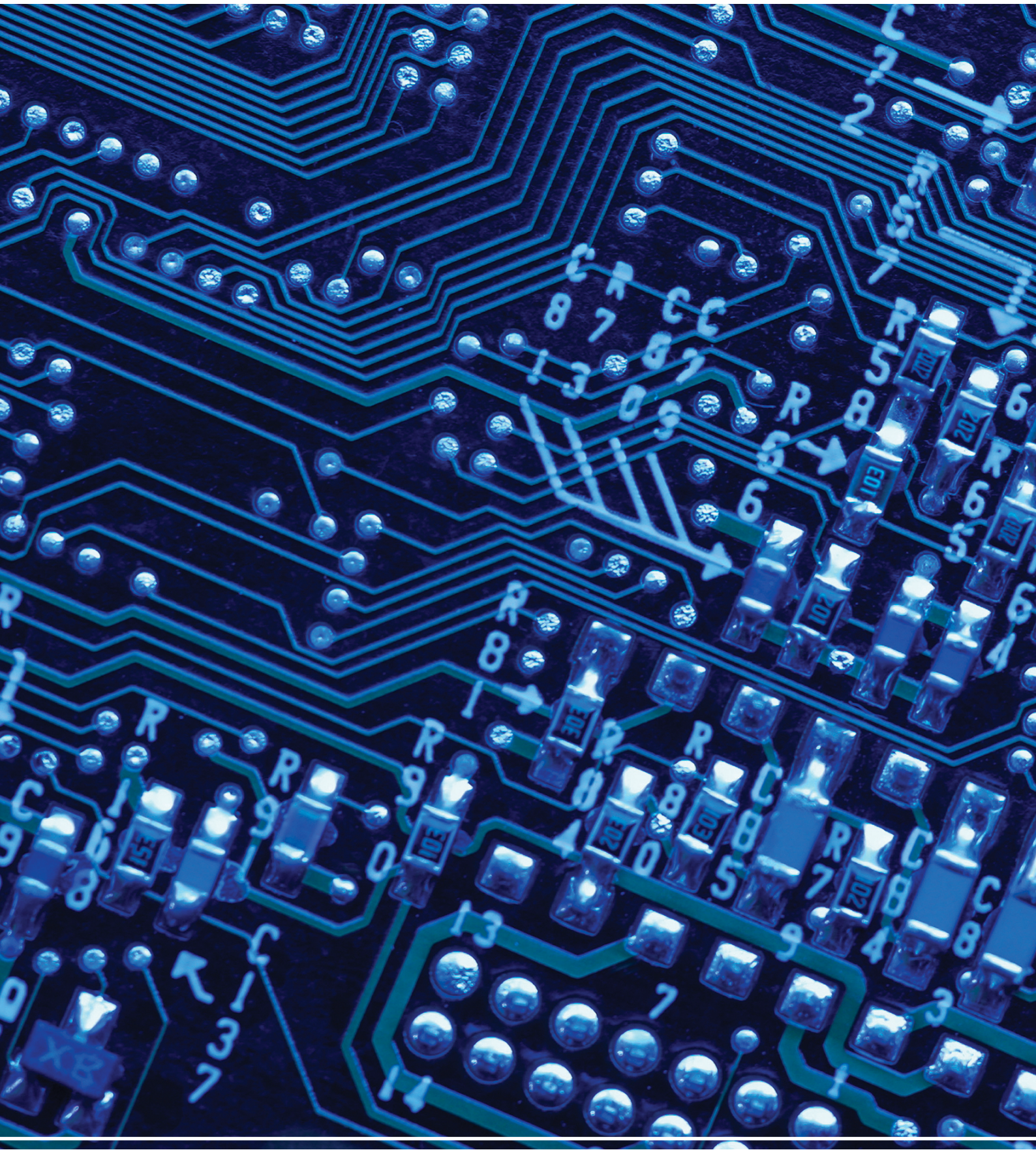
BUSINESS ASSURANCE

INFORME VIEWPOINT

¿Están seguros los datos de su empresa?

OCTUBRE 2015

SAFER, SMARTER, GREENER



CONTENIDOS

PRÓLOGO

Cada día tomamos decisiones que pueden afectar la privacidad y la seguridad de la información que manejamos, tanto online como en la vida diaria. La seguridad de la información, definida como la conservación de la confidencialidad, integridad y disponibilidad de información, es cada vez más una prioridad para las personas, y también para las empresas.

El proceso de mantener a buen recaudo los datos financieros, de personal y otros datos importantes presenta varios desafíos. ¿Comprenden las empresas las verdaderas amenazas? ¿Están haciendo lo suficiente? DNV GL – Business Assurance, líder global en certificación, ha tratado de encontrar las respuestas.

INTRODUCCIÓN

DNV GL - Business Assurance, con el apoyo del instituto internacional de investigación GFK Eurisko, ha investigado cómo manejan la seguridad de la información empresas en diferentes sectores de Europa, América del Norte, Sudamérica y Asia.

El estudio se llevó a cabo en julio de 2015 y se centró en investigar de qué forma los clientes de DNV GL - Business Assurance tratan un tema clave como es la seguridad de la información, cuáles son las iniciativas que implementan y los obstáculos que encuentran en el camino.

El estudio efectuado a casi 1200 profesionales de los sectores primario, secundario y terciario[1] destaca que existe un enfoque prioritario en el tema. La necesidad de tratar cuestiones relativas a la seguridad de la información no es algo nuevo, y las empresas están realizando esfuerzos significativos para lograrlo, a pesar de contrarse con difultades a la hora de fijar metas concretas.

Impulsados por la intención de proteger la información, la mayoría está trabajando aún en requisitos esenciales de infraestructura –que requieren altísimas inversiones y que son indispensables para evitar filtración o pérdida de información, y también para garantizar disponibilidad y acceso–, y en otras actividades de base.

En este contexto, un grupo de empresas (que a partir de ahora denominaremos "líderes") ya ha dejado atrás una actitud defensiva, optando por una gestión sistémica. Han incorporado gestión de la seguridad de la información en su práctica diaria y han sido capaces de difundir esta cultura en sus organizaciones. La protección de datos ya no es responsabilidad de una sola persona, sino uno de los objetivos clave del negocio y de todos los empleados.

[1] Primario: agricultura; secundario: fabricación; terciario: servicios, transporte.
[2] Las características de los líderes se indican en los recuadros a lo largo del informe y se resumen en la sección final Perfilando a los líderes.

METODOLOGÍA Y MUESTREO

- El estudio se llevó a cabo en julio de 2015. Involucró a 1192 profesionales que trabajan en empresas de los sectores primario, secundario y terciario en diferentes industrias en Europa, América del Norte, Centroamérica, Sudamérica y Asia.
- El muestreo consiste en clientes de DNV GL y no es representativo estadísticamente de empresas a nivel mundial.
- El muestreo incluye 112 empresas definidas como líderes. La clasificación de una empresa en la categoría de líder está basada en su cumplimiento de una serie de prerrequisitos específicamente definidos por DNV GL.
- El cuestionario fue administrado utilizando la metodología CAWI (entrevistas a través de internet).

SEGURIDAD DE LA INFORMACIÓN

ATRIBUTOS PARA DEFINIR EL GRUPO DE LÍDERES

- La seguridad de la información es relevante para la estrategia comercial de la empresa.
- La empresa posee una estrategia de seguridad de la información.
- La empresa ha fijado metas mensurables sobre la seguridad de la información.
- La empresa ha invertido en iniciativas de seguridad de la información en los últimos 3 años.
- La empresa ha tomado acciones para tratar con la seguridad de la información.
- La empresa es capaz de valorar la relación costo/beneficio de las acciones tomadas.
- La empresa planea hacer inversiones mayores o iguales a las actuales en los próximos 3 años.
- La empresa ha obtenido una calificación avanzada en una valoración propia sobre la madurez de su gestión de seguridad de la información.

Europa	41%
Asia	43%
América del Norte	7%
Centroamérica/Sudamérica	6%
Otros	3%

Figura 1: Empresas en el muestreo. Desglose geográfico.

[3] La empresa ha tomado al menos una de las siguientes acciones:
Evaluación comparativa respecto de sus pares en el sector; existencia de una política de la seguridad de la información aprobada por la alta dirección; existencia de personal cualificado para gestionar la seguridad de la información dentro de la organización; implementación de un abordaj de riesgos y metodología de gestión de la seguridad de la información; definición e implementación de controles de la seguridad de la información; objetivos específicos de la seguridad de la información; existencia y evaluación de un plan comercial de continuidad (BCP) específico; existencia de un Director de Seguridad de la Información responsable de prácticas de la seguridad de la información; partes regulares a la alta dirección sobre el rendimiento de la seguridad de la información; ofrecer formación sobre la seguridad de la información a la plantilla ; invertir en acitvos y equipamiento de la seguridad de la información; invertir en seguridad física y medioambiental; gestión de mantenimiento de equipos; llevar a cabo auditorías/valoraciones sobre la seguridad de la información; divulgación de cuestiones de la seguridad de la información a las partes interesadas; otras iniciativas.

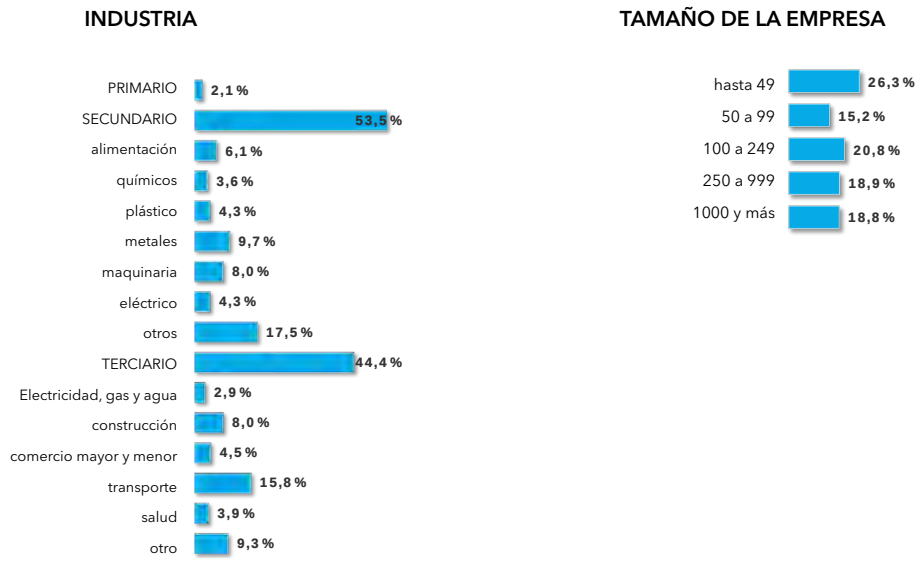


Figura 2: Empresas en el muestreo. Sectores y tamaño (número de empleados)

NOTAS PARA EL LECTOR

- En los gráficos contenidos en este informe, los círculos rojos destacan datos significativamente debajo de la media. Los círculos verdes destacan datos significativamente por encima de la media
- En los gráficos, el asterisco * indica que el muestreo es pequeño.
- Los gráficos en las figuras 3 a 10, 14 y 18 se refieren a preguntas con una sola respuesta, con respuestas sumando el 100%. Todos los demás gráficos se refieren a preguntas con múltiples respuestas.
- Excepto la figura 19, los siguientes gráficos muestran las notas obtenidas por el total de participantes, por participantes en diferentes regiones, por empresas grandes con más de 250 empleados y por líderes (ya sea de manera integral, o centrándose en algunos de estos subgrupos).

PANORAMA ACTUAL

LA IMPORTANCIA DE LA SEGURIDAD DE LA INFORMACIÓN

Desde una perspectiva personal y social

La seguridad de la información es una cuestión clave, tanto para los individuos como para la sociedad en general. Las personas entrevistadas lo ven como una preocupación en su vida diaria (76%), para su país (83%) y para la sociedad global (81%).

Esta inquietud es notable y generalizada, con algunas diferencias geográficas.

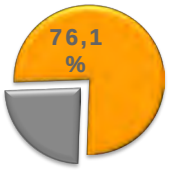
No sorprende que los europeos estén entre aquellos con baja calificación. Aunque la importancia de la seguridad de la información es reconocida también en este continente, no es una cuestión prioritaria ni para la opinión pública ni para los reguladores.

Si nos detenemos a analizar esta cuestión a nivel de países, los asiáticos (88%) y norteamericanos (86%) destacan con su inquietud por encima de la media. Además de reflejar la división digital entre las regiones del mundo, en este caso la conciencia es más alta que en otras áreas, quizás porque, recientemente, ambas regiones han sido víctimas de ataques de malware muy agresivos.

América Central y Sudamérica, en cambio, parecen preocuparse más por aspectos de seguridad de la información que pueden afectarles directamente; a nivel personal en la vida diaria (85%) o a nivel comercial en lo que respecta a la estrategia comercial total de sus empresas, como veremos en el párrafo siguiente (87%).

¿EN QUÉ MEDIDA VE A LA SEGURIDAD DE LA INFORMACIÓN COMO UNA PREOCUPACIÓN EN SU VIDA DIARIA?

Figura 3: Seguridad de la información como una preocupación en la vida diaria

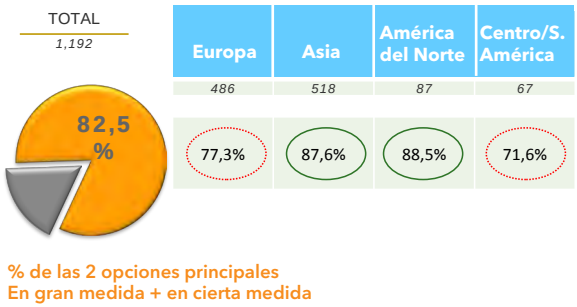


Europa	Asia	América del Norte	Centro/S. América
486	518	87	67
73,9%	77,3%	71,2%	85,1%

% de las 2 opciones principales
En gran medida + en cierta medida

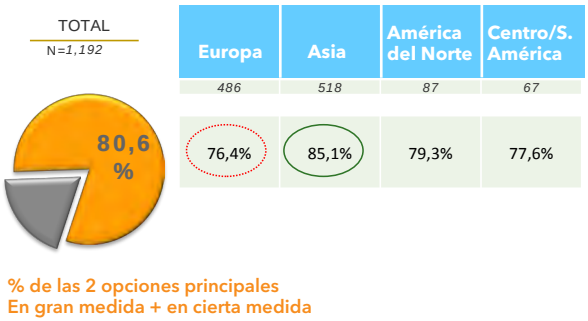
¿EN QUÉ MEDIDA VE A LA SEGURIDAD DE LA INFORMACIÓN COMO UNA PREOCUPACIÓN EN SU PAÍS?

Figura 4: Seguridad de la información como una preocupación para mi país.



¿EN QUÉ MEDIDA VE A LA SEGURIDAD DE LA INFORMACIÓN COMO UNA PREOCUPACIÓN EN LASOCIEDAD GLOBAL?

Figura 5: Seguridad de la información como una preocupación para la sociedad global.



Desde una perspectiva comercial

La seguridad de la información es también una preocupación desde una perspectiva comercial. Es relevante para las estrategias del 81% de las empresas encuestadas[4]. El porcentaje crece hasta el 85% para empresas grandes con un plantilla superior a 250 empleados.

América del Norte, y Centroamérica y Sudamérica (ambos con 87%) son los más preocupados. Sin embargo, su importancia es reconocida universalmente, y las proporciones registradas para Europa (80%) y Asia (79%) están dentro de la media.

Los LÍDERES consideran que las cuestiones de seguridad de la información son relevantes para sus estrategias comerciales.

[4] Entre los aspectos investigados en los últimos estudios Viewpoint –gestión del agua, gestión de la energía, etc.–, la seguridad de la información registró uno de los porcentajes más altos en términos de relevancia para las estrategias comerciales. .

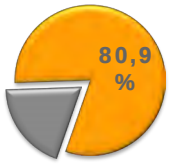
La necesidad de lidiar con cuestiones de seguridad de la información no constituye una sorpresa. Las empresas están, de algún modo, familiarizadas con el tema. En una escala del 1 al 5 (desde "principiante" a "vanguardia") que mide la madurez en la gestión de seguridad de la información, el 40% calificó a sus empresas como "avanzadas" (niveles 4 y 5).

Este porcentaje crece hasta el 55%en América del Norte. A pesar de registrar porcentajes significativos en términos de conciencia, Asia está por debajo de la media en niveles de confianza. Entienden que aún deben trabajar para mantener esta cuestión bajo control.

El tamaño es también un factor: las empresas grandes tienen marcas por encima de la media.

¿EN QUÉ MEDIDA ES LA SEGURIDAD DE LA INFORMACIÓN RELEVANTE PARA LA ESTRATEGIA COMERCIAL DE SU EMPRESA?

Figura 6: Relevancia de la seguridad de la información para estrategias comerciales.

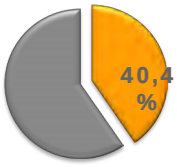


TOTAL	Europa	Asia	América del Norte	Centro/S. América	Empresas grandes	Líderes
1,192	486	518	87	67	433	112
80,9 %	80,2%	78,9%	87,3%	86,6%	83,6%	100,0%

% de las 2 opciones principales
En gran medida + en cierta medida

¿DÓNDE POSICIONARÍA A SU EMPRESA, EN UNA ESCALA DE 5 PUNTOS DE MADUREZ EN SEGURIDAD DE LA INFORMACIÓN? (1=PRINCIPIANTE, 5=LÍDER)

Figura 7: Escala de madurez en gestión de seguridad de la información.



TOTAL	Europa	Asia	América del Norte	Centro/S. América	Empresas grandes
N=1,192	486	518	87	67	433
40,4 %	45,1%	33,0%	55,1%	43,3%	48,3%

% punto 4-5

PROTECCIÓN DE DATOS PERSONALES

La Unión Europea publicará probablemente un nuevo Reglamento para regular la protección de datos a comienzos de 2016. Este Reglamento exigirá el cumplimiento de sus requisitos dentro de los dos años, y reemplazará todas las demás leyes nacionales relacionadas.

Para muchos países, el Reglamento exigirá agregar o cambiar algunas de las prácticas actualmente en conformidad con las leyes nacionales. Se prestará la debida atención a las medidas de protección de datos locales existentes que, probablemente, aún sean aplicables. En cualquier caso, todas las organizaciones tendrán dos o tres años para completar la transición al nuevo Reglamento.

Algunos requisitos que podemos esperar del futuro Reglamento (a confirmar hasta que sea aprobado y emitido):

- Modelo organizacional basado en principios de responsabilidad;
- Función de Delegado de Protección de Datos (DPO);
- Gestión de información facilitada a los titulares de los datos, incluyendo su consentimiento;
- Gestión de proveedores y subcontratistas, incluyendo requisitos contractuales;
- Evaluación de riesgo de la intimidad y evaluación de impacto sobre la intimidad (PIA)
- Informes periódicos acerca de la implementación de medidas de seguridad de la intimidad;
- Códigos éticos para algunos tratamientos.

No todos los requisitos serán aplicables a todas las empresas en todos los países de la UE. Por ejemplo, la función de DPO era una regla obligatoria en los borradores iniciales del Reglamento, pero es opcional en los borradores de mediados de 2015. Por ende, las organizaciones deberán esperar a la versión final del Reglamento.

Se deberán considerar las medidas de otras autoridades (por ejemplo, la autoridad europea de protección de datos, si es que se crea) que han publicado y continuarán publicando directrices relevantes.

Es probable que el futuro Reglamento promueva programas de certificación para demostrar una buena gestión de la privacidad. Hasta el momento, ISO/IEC JTC1 SC27 ha publicado un marco para la gestión de privacidad (ISO/IEC 29100), una guía para la privacidad en la informática en la nube (ISO/IEC 27018), y un modelo para la evaluación de la capacidad en privacidad (ISO/IEC 29190). Probablemente, un futuro programa de certificación esté basado en los requisitos de ISO/IEC 29190.

GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

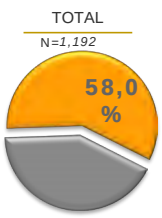
Las empresa globales gestionan activamente los aspectos de seguridad de la información. Sin embargo, por el 58% que adopta una estrategia específica, solo el 27% fija metas mensurables. Los porcentajes en empresas grandes están por encima de la media: para estrategias, el porcentaje llega al 71%; sin embargo, en lo que respecta a metas, el aumento es solo el 36%. Aunque el compromiso es generalizado, no es fácil medir aspectos relacionados con la seguridad de la información, especialmente si se trata de cuantificar el coste de la filtración o pérdida de información.

Con tasas por encima de la media para estrategia (70%) y metas (33%), América del Norte destaca por su enfoque avanzado. Por el contrario, en Asia menos que 1 empresa de cada 2 dice adoptar una estrategia de seguridad de la información; una vez más, no creen dominar aún las herramientas adecuadas para lidiar con esta cuestión.

Los LÍDERES preparan estrategias de seguridad de la información y fijan también objetivos específicos mensurables.

¿TIENE SU EMPRESA UNA ESTRATEGIA DE SEGURIDAD DE LA INFORMACIÓN?

Figura 8: Adopción de estrategias de seguridad de la información

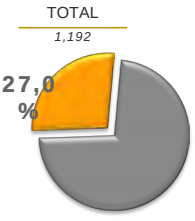


Europa	Asia	América del Norte	Centro/S. América	Empresas grandes	Líderes
486	518	87	67	433	112
63,6%	49,8%	70,1%	61,2%	70,7%	100,0%

% Sí

¿TIENE SU EMPRESA METAS MENSURABLES EN SEGURIDAD DE LA INFORMACIÓN?

Figura 9: Metas en seguridad de la información



Europa	Asia	América del Norte	Centro/S. América	Empresas grandes	Líderes
486	518	87	67	433	112
27,0%	26,3%	33,3%	23,9%	35,8%	100,0%

% Sí

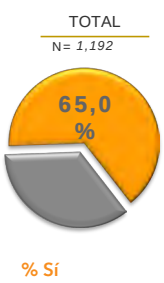
INICIATIVAS CLAVE EMPRENDIDAS

Las empresas están haciendo esfuerzos significativos para garantizar la seguridad de la información. 65% de las empresas, y 73% de las empresas grandes, invirtieron en iniciativas específicas en los últimos 3 años.

Los LÍDERES invirtieron en iniciativas de seguridad de la información en los últimos 3 años.

¿HA INVERTIDO SU EMPRESA EN INICIATIVAS DE SEGURIDAD DE LA INFORMACIÓN EN LOS ÚLTIMOS 3 AÑOS?

Figura 10: Inversiones en iniciativas en seguridad de la información en los últimos 3 años



Europa	Asia	América del Norte	Centro/S. América	Empresas grandes	Líderes
486	518	87	67	433	112
68,9%	60,6%	66,7%	70,1%	73,2%	100,0%

Sin embargo, al agrupar las acciones de seguridad de la información en 3 categorías de madurez incrementales –esenciales, básicas y avanzadas–, resulta que las empresas se centran en su mayor parte en requisitos esenciales y acciones en la categoría básica.

Las iniciativas esenciales son aquellas de las que no podemos prescindir para alcanzar un nivel mínimo de seguridad de la información, como inversiones en activos y equipamiento de seguridad de la información (41%) o en seguridad física y medioambiental (32%). Son de carácter tecnológico y generalmente exigen grandes inversiones.

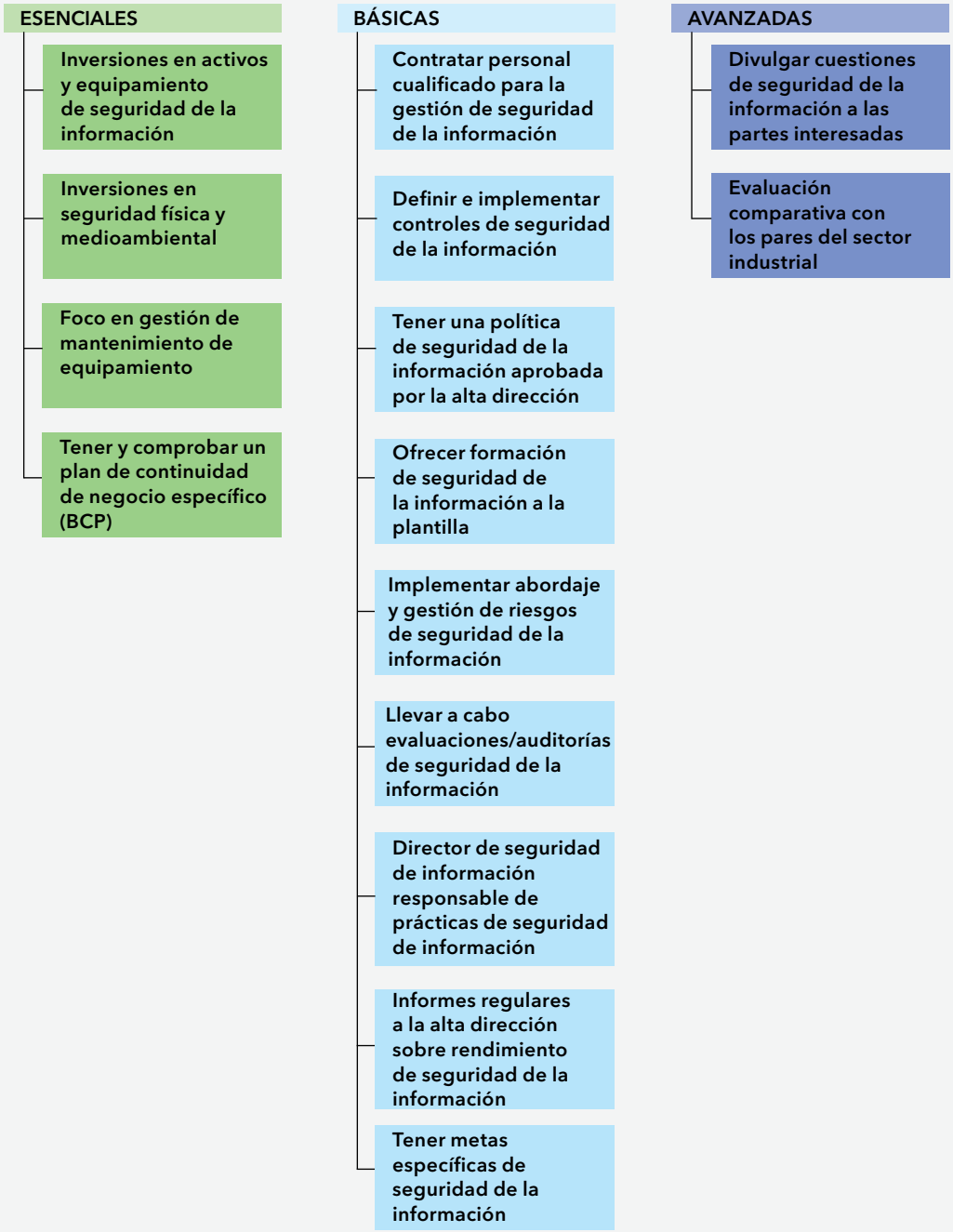
Las iniciativas básicas representan ir un paso más allá: se centran en la plantilla o en el desarrollo de un sistema de gestión, y exigen niveles medios de inversiones. Las más comunes son la contratación de personal dedicado a la gestión de seguridad de la información (40%) y controles de seguridad de la información (35%). Las empresas todavía están centrándose en protección y defensa, en lugar de crear un enfoque de gestión sistemático.

Son relativamente raras las iniciativas avanzadas. Incluye actividades como la divulgación de cuestiones de seguridad de la información a las partes interesadas (12%) o evaluación comparativa con los pares (8%), cosas que normalmente no exigen grandes inversiones. En lo que respecta a seguridad de la información, cuando se ponen en marcha las acciones esenciales, se gasta menos a medida que se avanza.

América del Norte es la más activa, con porcentajes por encima de la media para todas las categorías de iniciativas. Lo mismo se cumple para caso de las empresas grandes.

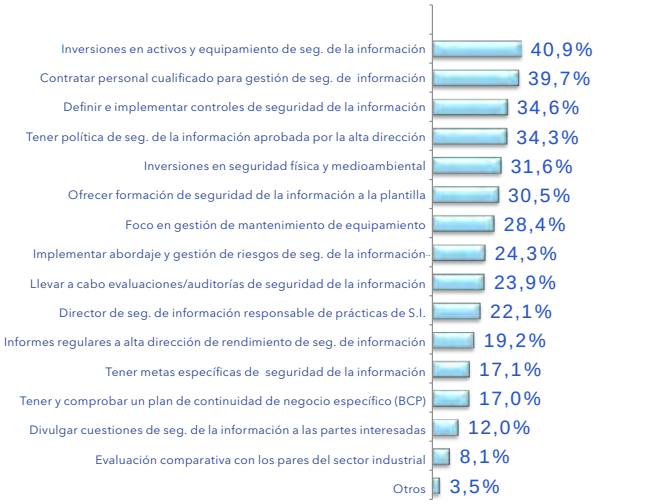
ACCIONES DE SEGURIDAD DE LA INFORMACIÓN AGRUPADAS SEGÚN 3 CATEGORÍAS DE MADUREZ INCREMENTALES: ESENCIAL, BÁSICA Y AVANZADA

Figura 11



¿CUÁLES DE LAS SIGUIENTES INICIATIVAS DE SEGURIDAD DE LA INFORMACIÓN HA TOMADO SU EMPRESA? (Respuestas múltiples)

Figura 12: iniciativas de seguridad de la información tomadas por las empresas



Europa	Asia	América Norte	Centro/S América	Large comp.	Líderes
486	518	87	67	433	112
45,5%	33,2%	48,3%	53,7%	46,4%	79,5%
39,7%	35,9%	54,0%	49,3%	52,7%	80,4%
33,7%	30,5%	49,4%	46,3%	45,5%	77,7%
39,5%	27,8%	40,2%	35,8%	49,2%	82,1%
34,4%	25,3%	43,7%	43,3%	41,6%	60,7%
29,6%	32,8%	32,2%	20,9%	43,9%	69,6%
31,1%	25,1%	33,3%	28,4%	33,9%	58,0%
26,5%	22,0%	27,6%	19,4%	35,1%	70,5%
26,1%	19,7%	29,9%	28,4%	35,6%	70,5%
20,6%	22,8%	29,9%	19,4%	32,8%	63,4%
18,7%	19,3%	26,4%	11,9%	28,2%	60,7%
19,3%	12,9%	21,8%	23,9%	24,0%	62,5%
17,7%	16,2%	21,8%	13,4%	27,3%	50,0%
10,5%	10,6%	20,7%	19,4%	17,8%	42,0%
6,8%	7,5%	11,5%	13,4%	11,5%	23,2%
3,3%	4,1%	4,6%	1,5%	3,7%	3,6%

Los LÍDERES registran porcentajes más altos en todas las acciones, tanto en iniciativas esenciales como básicas o avanzadas.

Tienden a un enfoque sistemático. Los LÍDERES no se centran solo en los requisitos esenciales, sino que son capaces de invertir en acciones más sofisticadas, además de en actividades de auditoría (71%), implementación de una metodología de abordaje y gestión del riesgo (71%) y formación de la plantilla (70%). También registran porcentajes significativos la fijación de metas específicas de seguridad de la información (63%) e informar regularmente a la alta dirección sobre el rendimiento de seguridad de la información (61%)

Aunque su porcentaje es el triple de la media, los LÍDERES también obtienen bajos porcentajes en la implementación de acciones avanzadas. Menos de 1 de cada 2 divulga cuestiones de seguridad de la información a las partes interesadas y solo el 23% ejecuta evaluaciones comparativas con los pares.

ISO 27001:2013 SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (ISMS)

Durante los años 90 del siglo pasado, se desarrolló una norma británica (BS7799) para documentar y diagramar los requisitos de un sistema de gestión de seguridad de la información. Esta norma tenía dos partes, los requisitos y las mejores prácticas en el campo de la seguridad de la información.

A partir de esta norma BS7799, el comité de ISO desarrolló la norma ISO/IEC 27001:2005 y el código de prácticas ISO/IEC 27002:2005 para controles de seguridad de la información. Desde ese momento, esta norma* fue adoptada por la mayoría de los organismos de certificación mundiales, y hoy el número de certificaciones aumenta en un 7% anual, según la la encuesta de ISO 2014.

De acuerdo a esa encuesta, se emitieron unas 24000 certificaciones válidas en todo el mundo, con algunas peculiaridades. Japón, como innovador en tecnología digital, se destaca históricamente como uno de los países más avanzados en el sector de seguridad de la información, y el Reino Unido también aparece de manera prominente (con el crecimiento más importante en términos absolutos).

¿Qué significa que una empresa obtenga una certificación? La certificación de sistemas de gestión es la actividad que determina que una empresa cumple los requisitos de una norma dada. Para obtener la certificación ISO/IEC 27001 (ISMS), la empresa será auditada por un auditor líder o un equipo de auditores para determinar este cumplimiento, y solo entonces, al demostrar el cumplimiento, se emitirá la certificación.

Son varios los desafíos a los que se enfrentan las empresas u organizaciones al implementar un sistema de gestión de seguridad de la información, según ISO/IEC 27001.

El análisis de las bases de datos de DNV GL (descripción detallada de datos de auditoría provenientes de actividades de auditoría recientes en todo el mundo) muestra que la mayoría de conclusiones y no conformidades de las que se da parte están relacionadas con la siguientes cláusulas ISO/IEC 27001:

6.2 Objetivos de seguridad de la información
9.2 Auditorías internas
9.3 Revisión por la dirección
A17 Gestión de continuidad de negocio

6.2 Objetivos de seguridad de la información
La empresa establecerá objetivos mensu-

**Cada 7-8 años se actualizan y revisan las normas ISO, y hace dos años se publicó la norma ISO/IEC 27001:2013 revisada, con un enfoque de requisitos diferente. Esta nueva norma concuerda ahora con ISO 9001 (Gestión de Calidad) e ISO 14001 (Gestión Medioambiental), y contiene una estructura de alto nivel con requisitos comunes y un anexo con 114 controles distribuidos en 14 capítulos.*

rables en funciones y niveles relevantes, de acuerdo la política de seguridad de la información y el análisis de riesgos. Estos objetivos serán comunicados, y se definirá la planificación para alcanzar estos objetivos.

- *Al analizar las conclusiones, es evidente que la mayoría de las empresas encuentran dificultades al definir y monitorizar objetivos mensurables de ISMS: para las empresas es una ardua lucha definir objetivos que se correspondan con sus objetivos, riesgos y continuidad de negocio.*

9.2 Auditorías internas

Todo sistema de gestión exige planificar, ejecutar y dar parte de las auditorías internas para determinar la implementación eficaz del ISMS.

- *La mayoría de las conclusiones de auditoría tienen que ver con falta de planificación y de experiencia en ISMS, y falta de competencias en el equipo auditor interno de la empresa. Estos equipos auditores necesitan conocimiento específico de seguridad de la información.*

9.3 Revisión por la dirección

La alta dirección revisará el ISMS a intervalos planificados para garantizar su idoneidad, aptitud y eficacia continuas. Al valorar y debatir sobre una serie definida de temas, la organización decidirá si el ISMS necesita mejoras o cambios, o si es acorde con la organización, su política y su análisis de riesgos.

- *La mayoría de conclusiones de auditoría se refieren a temas que no aparecen en el análisis del ISMS. A menudo en la documentación faltan datos de política, abordaje de riesgos, resultados de auditorías y seguimiento de los objetivos.*

A17 Gestión de continuidad de negocio

Los requisitos para la seguridad de la información (C-Continuidad I-Integridad D-Disponibilidad) deben estar incluidos en la gestión de continuidad de negocio de la organización. Se desarrollarán hipótesis de crisis y desastres y se establecerá y ejecutará un plan de pruebas para garantizar la continuidad de negocio durante situaciones adversas.

- Las conclusiones de auditoría relacionadas con este tema son generalmente la falta de hipótesis apropiadas de crisis y desastres y un plan de pruebas de BCP documentado y monitorizado. Los simulacros de evacuación y las actividades de recuperación después de los desastres a menudo se posponen o no realizadas en absoluto.

Se pueden obtener mejoras significativas en las áreas de objetivos, auditorías, revisión y gestión de la continuidad; esto es lo que emerge claramente tanto de los resultados de esta encuesta de Viewpoint como del análisis de las conclusiones de auditoría más comunes registradas durante nuestras auditorías de certificación en todo el mundo. Las empresas están todavía centrándose en infraestructuras, y sus metas son principalmente la protección y la defensa. Necesitan trabajar aún con miras a construir un enfoque sistemático de gestión de seguridad de la información.

PRINCIPALES RAZONES PARA EMPRENDER INICIATIVAS DE SEGURIDAD DE LA INFORMACIÓN

La protección de información es el principal impulsor para que las empresa emprendan iniciativas de seguridad. Salvaguardar los activos de la empresa (45%) y reducir las pérdidas (31%) están entre las principales razones. Las políticas internas (40%) y el cumplimiento con leyes y normativas (39%) también juegan un papel significativo.

La ventaja competitiva/reputación de marca alcanza el 28%: las empresa son conscientes de que la pérdida de información puede afectar su posicionamiento.

La presión externa –ya sea de los clientes (14%) o de otras partes interesadas (13%)– no es un factor.

Las cifras son más altas, pero el ranking de razones principales de los LÍDERES es el mismo. Salvaguardar los activos de la empresa (80%), políticas internas (80%) y el cumplimiento con leyes y normativas (79%) encabezan la lista.

Sin embargo, sus motivaciones son ganar ventaja competitiva/reputación de marca (64%), las presiones de las partes interesadas (25%) y los clientes (22%) en una proporción muy por encima de la media. Además, recomendaciones de auditorías y la necesidad de divulgar el rendimiento de seguridad de la información juegan un papel relevante para 1 de cada 4.

¿CUÁLES SON LAS RAZONES QUE LLEVARON A SU EMPRESA A EMPRENDER INICIATIVAS DE SEGURIDAD DE LA INFORMACIÓN? (MÚLTIPLES RESPUESTAS)

Figura 13: Razones que llevan a las empresas a emprender iniciativas de seguridad de la información

	TOTAL	Europa	Asia	América Norte	Centro/S. América	Empresas grandes	Líderes
	N=1,192	486	518	87	67	433	112
Salvaguardar los activos de la empresa	44,7%	46,3%	39,8%	55,2%	53,7%	54,0%	79,5%
Política interna	39,8%	42,4%	35,1%	44,8%	50,7%	51,5%	79,5%
Cumplimiento de leyes y normativas	39,1%	46,1%	34,4%	36,8%	29,9%	48,5%	78,6%
Reducir pérdidas de información y costes asociados	30,6%	26,3%	35,3%	24,1%	32,8%	36,3%	63,4%
Ventaja competitiva/reputación de marca	27,7%	26,5%	29,2%	19,5%	35,8%	37,6%	64,3%
Recomendación de clientes	13,7%	14,4%	15,3%	9,2%	7,5%	16,2%	22,3%
Preocupación/presión de partes interesadas	12,8%	9,7%	15,3%	13,8%	11,9%	19,6%	25,0%
Recomendación en una auditoría de seg. de información	9,0%	9,9%	8,7%	6,9%	9,0%	11,5%	25,0%
Necesidad de divulgar rendimiento de seg. de información	8,6%	9,7%	8,5%	6,9%	6,0%	10,9%	25,0%
Incentivos/reembolsos fiscales	1,5%	1,2%	1,9%	1,1%	1,5%	1,6%	1,8%
Otros	3,4%	3,9%	2,9%	3,4%	6,0%	3,9%	3,6%

CONTINUIDAD DE NEGOCIO Y SEGURIDAD DE LA INFORMACIÓN

Un resumen de ISO 22301 para la gestión de continuidad de negocio.

La primera norma para la gestión de continuidad de negocio se publicó como BS 25999 en 2006. Desde ese momento, se movió hacia el panorama internacional en 2012, con la publicación de ISO 22301:2012 – Seguridad de la Sociedad – Sistemas de gestión de la continuidad del negocio. Esta especificación es reseñable por dos motivos: en primer lugar, situó a la continuidad de negocio en el espacio global, y en segundo lugar, marcó el camino con la nueva Estructura de Alto Nivel para normas ISO.

Estructura ISO 22301:2012

1. Alcance
2. Referencias Normativas
3. Términos y Definiciones
4. Contexto de la organización
5. Liderazgo
6. Planificación
7. Soporte
8. Operación
9. Evaluación del rendimiento
10. Mejora

La estructura da soporte a organizaciones de todos los tamaños y en todos los sectores para evaluar y controlar disrupciones que pueden afectar su negocio. La ISO 22301 adopta un enfoque BCM* de 6 elementos, para representar la operación continua del programa de continuidad de negocio dentro de la organización.

Los seis elementos son:
Gestión del Programa de Continuidad de Negocio
Integrar Competencia y Conciencia
Comprender la Organización
Seleccionar Opciones de Continuidad de Negocio
Desarrollar e Implementar una Respuesta de Continuidad de Negocio
Ejercicios y Pruebas

Estos elementos son necesarios para controlar de manera eficaz los riesgos de continuidad y garantizar que todo requisito de seguridad de la información relevante sea identificado y gestionado durante una disrupción. Se espera que se tengan en cuenta los principios claves de seguridad de la información —confidencialidad y disponibilidad— al planificar respuestas de continuidad; esto significa que los equipos operativos deben considerar qué información se protegerá y qué información deberá estar disponible durante una situación de desastre.

La continuidad en la protección de datos se exige formalmente en el Anexo A de la norma ISO/IEC 27001 para seguridad de la información; por esta razón las dos normas encajan tan bien. La norma de sistemas de gestión de seguridad de la información ISO/IEC 27001, mediante los controles definidos en el Anexo A17, destaca en qué parte del plan de continuidad de negocio debería la organización garantizar que se cumplen los requisitos de seguridad. La norma de continuidad de negocio ISO 22301, mediante la evaluación operacional de impactos y riesgos comerciales, tiene en cuenta esos requisitos, para que los planes de emergencia y continuidad no solo ofrezcan una operación de negocio continua, sino que también garanticen que está segura en los niveles apropiados.

**BCM es una sigla para Gestión de Continuidad de Negocio. BC significa Continuidad de Negocio.*

PRINCIPALES BENEFICIOS

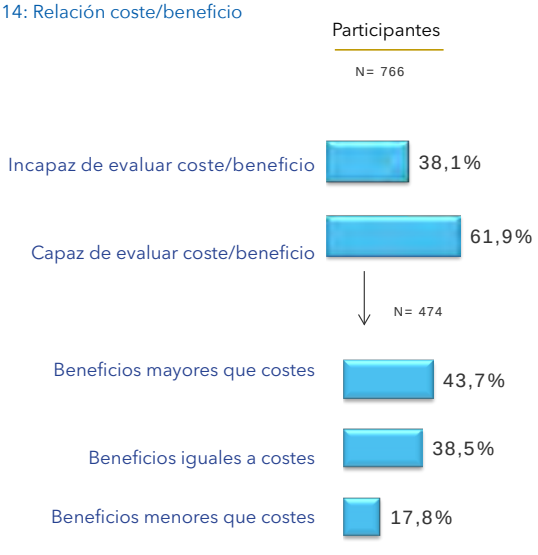
Cerca del 40% de empresas no saben responder a la pregunta sobre la relación coste/beneficio de las acciones emprendidas (también aparecen dificultades en la medición para fijar objetivos). Aunque con porcentajes menores, las empresa grandes experimentan las mismas dificultades.

Sin embargo, dentro de las que sí pudieron responder, aquellas que creen que los beneficios son mayores que los costes son mayoría (44%). La proporción crece a 1 de cada 2 para Centroamérica y Sudamérica, y para las empresas grandes.

Para el 60% de los LÍDERES, los beneficios son mayores que los costes.

¿CÓMO VALORA LA RELACIÓN COSTE/BENEFICIO PARA LAS ACCIONES EMPRENDIDAS POR SU EMPRESA?

Figura 14: Relación coste/beneficio



	Europa	Asia	América Norte		Empresas grandes	Líderes
	331	*311*	*58*	*47*	*314*	*112*
Incapaz de evaluar coste/beneficio	36,0%	43,4%	34,5%	25,5%	43,9%	0%
Capaz de evaluar coste/beneficio	64,0%	56,4%	65,5%	74,5%	56,1%	100%
	N= 212	N= 176	N= 38*	N= 35*	N= 176	N= 112
Beneficios mayores que costes	44,3%	38,7%	47,5%	51,4%	48,9	59,8%
Beneficios iguales a costes	40,1%	39,2%	28,9%	42,8%	31,7	28,6
Beneficios menores que costes	15,6%	22,1%	23,6%	5,8%	19,4	11,6

Reducir las pérdidas relacionadas con la seguridad de la información es visto como el beneficio más común (35%). Esto concuerda con el feedback que mostraba que proteger los activos de la empresa es el principal impulsor para emprender acciones.

La protección de información puede sonar como "un asunto interno", pero en realidad tiene muchas repercusiones externas. Las empresa también se benefician en términos de cumplimientos con leyes y normativas (32%) y en ventaja competitiva/ reputación de marca (23%). Las relaciones se refuerzan también: 23% habla de una mejora en las relaciones con clientes; y un 16%, en relación con otras partes interesadas.

La tendencia es más pronunciada entre empresas grandes, que registran porcentajes por encima de la media en casi todos los puntos mencionados.

Los LÍDERES ganaron mucho más que los demás, tanto en términos de benficios externos como internos, obteniendo al menos el doble de la media en ambos casos.

¿QUÉ BENEFICIOS OBTUVO SU EMPRESA GRACIAS A LAS ACCIONES EMPRENDIDAS? (Respuestas múltiples)

Figura 15: Beneficios derivados de inciciativas de seguridad de la información.

	Europa	Asia	América Norte	Centro/S. América	Empresas grandes < 250 emp.	Líderes
	486	518	87	67	433	112
Pérdidas por filtración de seg. de información reducidas	27,0%	42,1%	34,5%	44,8%	44,3%	73,2%
Lograr cumplimiento de leyes y normativas	37,4%	26,6%	33,3%	26,9%	38,8%	71,4%
Ventaja competitiva/ aumento reputación de marca	22,0%	25,1%	19,5%	22,4%	31,4%	65,2%
Mejor relación con clientes	21,2%	23,9%	25,3%	20,9%	26,3%	47,3%
Mejor relación con partes interesadas	13,6%	15,8%	20,7%	25,4%	22,4%	42,0%
Ahorros financieros	10,7%	7,1%	14,9%	13,4%	11,8%	31,3%
Otros beneficios	9,5%	5,2%	18,4%	11,9%	10,4%	17,0%
Sin beneficios	2,7%	1,7%	2,3%	1,5%	1,4%	0,0%
No sabe	8,2%	3,9%	9,2%	7,5%	7,9%	0,0%

OBSTÁCULOS PRINCIPALES

Los factores que impiden que las empresas progresen en seguridad de la información tienen que ver con restricciones económicas o con plantilla. El alto coste de implementación y mantenimiento (33%), y otras prioridades (31%) encabezan la lista. Le siguen la falta de plantilla competente (23%) y de conciencia de la dirección (19%).

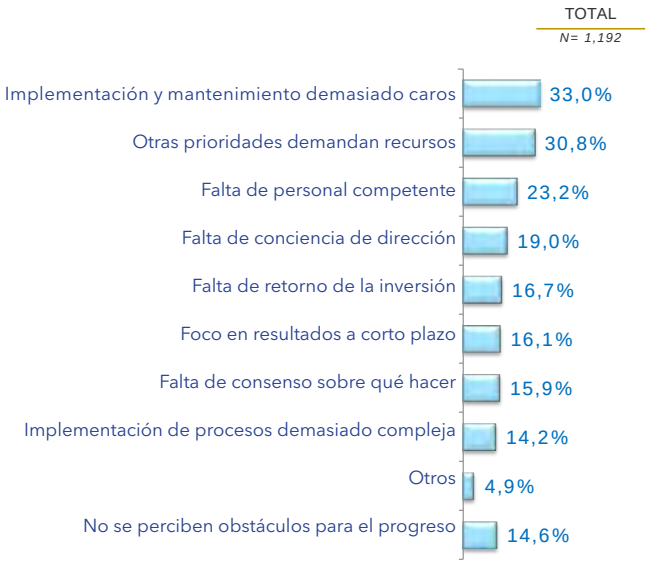
Hace no muchos años, la gestión de seguridad de la información se consideraba una competencia de especialistas; hoy en día existe una necesidad clara de que se transforma en una habilidad transversal en la organización.

La falta de competencia es significativa sobre todo en Asia (33%), mientras que para Europa (16%) Y América del Norte (10%) es un obstáculo menor.

Los LÍDERES gestionan los obstáculos mejor que el resto. La mayoría de los factores puntúan por debajo de la media, excepto la conciencia de la dirección, a la que consideran una barrera importante.

¿QUÉ FACTORES IMPIDEN QUE SU EMPRESA PROGRESE EN SEGURIDAD DE LA INFORMACIÓN? (Respuestas múltiples)

Figura 16: Obstáculos para progresar en gestión de seguridad de la información.



	TOTAL	Europa	Asia	América del Norte	Centro/S. América	Empresas grandes	Líderes
	N= 1,192	*486*	*518*	*87*	*67*	*433*	*112*
Implementación y mantenimiento demasiado caros	33,0%	22,2%	45,9%	18,4%	38,8%	27,5%	26,8%
Otras prioridades demandan recursos	30,8%	40,3%	17,4%	44,8%	46,3%	29,3%	5,4%
Falta de personal competente	23,2%	15,6%	33,4%	10,3%	20,9%	19,9%	12,5%
Falta de conciencia de dirección	19,0%	18,3%	18,1%	17,2%	28,4%	20,6%	26,8%
Falta de retorno de la inversión	16,7%	13,2%	22,2%	12,6%	7,5%	11,1%	6,3%
Foco en resultados a corto plazo	16,1%	13,6%	18,5%	17,2%	13,4%	17,6%	12,5%
Falta de consenso sobre qué hacer	15,9%	11,1%	20,3%	12,6%	20,9%	13,2%	6,3%
Implementación de procesos demasiado compleja	14,2%	10,1%	20,3%	6,9%	9,0%	16,2%	15,2%
Otros	4,9%	6,4%	4,2%	2,3%	4,5%	5,1%	9,8%
No se perciben obstáculos para el progreso	14,6%	19,5%	8,5%	18,4%	14,9%	15,0%	33,0%

ACCIONES PARA AUMENTAR LA CONCIENCIA

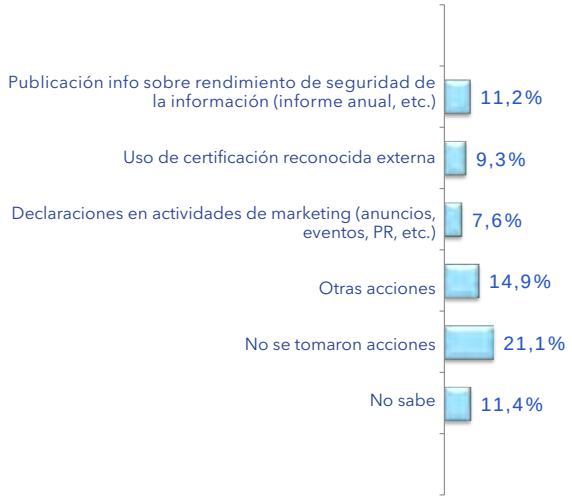
Las empresas no están haciendo mucho para aumentar la conciencia de lo que hacen para asegurar su información. Solo 1 de cada 10 empresas publicó información en sus informes corporativos u otros documentos oficiales. El 9% usó una certificación reconocida externamente y aún menos (el 8%) hizo declaraciones en actividades de marketing. 1 de cada 5 no emprendió ninguna acción. La proporción crece a casi 1 de cada 3 en Europa y Centroamérica/Sudamérica.

La precaución en la comunicación puede deberse sobre todo al miedo de ataques derivados de la exposición, pero también a la falta de presión externa para mostrar las medidas de protección tomadas.

Los LÍDERES registran porcentajes muy por encima de la media para todo tipo de actividades orientadas a aumentar conciencia. Entienden que es necesario comunicar las acciones tomadas.

EN LOS ÚLTIMOS 3 AÑOS, ¿HA TOMADO ALGUNA DE LAS ACCIONES SIGUIENTES PARA AUMENTAR CONCIENCIA SOBRE LO QUE HACE SU EMPRESA EN SEGURIDAD DE LA INFORMACIÓN?
(Respuestas múltiples)

Figura 17: Acciones para aumentar concien-cia.



	TOTAL	Europa	Asia	América del Norte	Centro/S. América	Empresas grandes	Líderes
	N= 1,192	486	518	87	67	433	112
Publicación info sobre rendimiento de seguridad de la información (informe anual, etc.)	11,2%	10,5%	12,0%	9,2%	14,9%	15,5%	37,5%
Uso de certificación reconocida externa	9,3%	10,7%	9,8%	2,3%	6,0%	11,8%	29,5%
Declaraciones en actividades de marketing (anuncios, eventos, PR, etc.)	7,6%	5,6%	10,4%	5,7%	4,5%	9,9%	17,9%
Otras acciones	14,9%	13,2%	18,0%	8,0%	13,4%	20,8%	34,8%
No se tomaron acciones	21,1%	27,8%	13,3%	24,1%	32,8%	15,9%	20,5%
No sabe	11,4%	10,7%	10,8%	20,7%	9,0%	15,5%	4,5%


Smart Home
Room Lighting
Off
On
Alarm system
Disarmed
1 2 3
4 5 6
7 8 9
* 0 #
Video Security
cam 1
cam 2
cam 3
Room Temperature
-
+
Living room
Bedroom

PRINCIPALES TENDENCIAS EN IT

La industria IT está atravesando importantes cambios, permitiendo a las organizaciones – incluso a las pequeñas – alcanzar horizontes que no podrían haber imaginado hace pocos años. Las tendencias emergentes son muchas, pero las más importantes son Big Data, la Informática en la Nube y la Internet de las Cosas (IoT). Todas ellas se basan en conceptos de compartir información, construir redes y crear conexiones. Las especificidades y aplicaciones pueden ser muchas, pero todas tienen los mismos cimientos: la capacidad de proteger información, para evitar filtraciones, intrusiones y usos indebidos.

BIG DATA

El término "Big Data" se oye cada vez más en todos los sectores de negocio, y se usa para describir varias operaciones caracterizadas por la disponibilidad de una cantidad de datos demasiado grande para ser procesada mediante los sistemas de software y bases de datos convencionales.

Las soluciones Big Data sacan partido de técnicas, herramientas tecnológicas e integraciones avanzadas que permiten comparaciones complejas, un análisis de datos más eficaz y minucioso y una maximización de los resultados. Cuando las organizaciones no tienen en marcha soluciones Big Data, hay una enorme cantidad de información que ni siquiera se monitoriza, y tampoco se pueden identificar patrones de datos extensos.

INFORMÁTICA EN LA NUBE

La Informática en la Nube responde a una de las necesidades más apremiantes de nuestros tiempos: la necesidad de manejar grandes cantidades de datos desde distintas ubicaciones y a través de varios dispositivos. Ya no es obligatorio ir a la oficina o depender de almacenamiento físico. Los usuarios y empresas pueden almacenar y procesar sus datos en centros de datos y acceder a ellos mediante varias herramientas gracias a una interfaz de internet.

INTERNET DE LAS COSAS (IoT)

La Internet de las Cosas es la tendencia aglutinadora. Se basa en comunicación máquina-a-máquina, saca partido de la informática en la nube y de redes de recolección de datos. El concepto informático de IoT describe un futuro donde los objetos físicos cotidianos estarán conectados a internet y serán capaces de identificarse ante otros dispositivos. IoT no está limitada a una industria o aplicación específicas: el universo de dispositivos conectados a la red se está volviendo omnipresente en cada área del negocio y en muchos aspectos de la vida de la comunidad. Los campos de aplicación incluyen procesos de producción, logística y eficiencia energética, control remoto y protección medioambiental.

Para sacar el mayor partido a estas nuevas tecnologías, es fundamental otorgar un valor económico a la información. Ser capaces de calcular los costes financieros relacionados con cualquier pérdida o daño a nuestra información estimulará el desarrollo de procesos de seguridad. Esto ayudará a evitar el almacenamiento de datos antiguos o innecesarios, un elemento que no puede soslayarse, especialmente en entornos de informática en la nube. Es altamente recomendable, en el uso de soluciones de informática en la nube, prestar atención tanto a las cargas de trabajo de servidores como a la encriptación.

Big Data en sí misma será de ayuda para mejorar la capacidad de responder a amenazas. Un enfoque analítico e inteligente al enorme volumen de datos en amenazas externas permitirá una respuesta más adecuada, a veces incluso automatizada, útil también para manejar la revolución que trae IoT. Con la llegada de IoT, las empresas tendrán que lidiar con un gran número de dispositivos inteligentes interconectados dentro de su entorno con los consumidores. Todo esto acarreará problemas específicos de seguridad. Por esta razón, la seguridad de la información debe convertirse en parte integral del proceso de diseño de las propias soluciones de IoT, con directores de IT aconsejando y guiando a los diseñadores en el campo de privacidad y ciberseguridad.

PANORAMA FUTURO

INVERSIONES FUTURAS

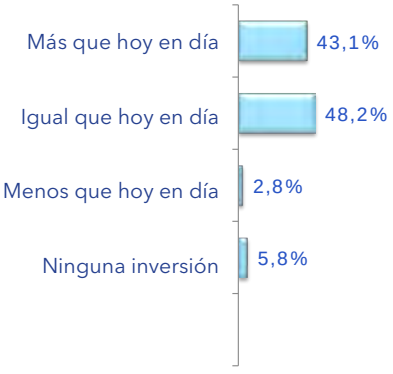
Entre los participantes, la mayoría de las empresas planean mantener o incluso aumentar las inversiones en seguridad de la información en los próximos 3 años. 43% pretende invertir más que hoy en día, y el porcentaje aumenta al 49% para estadounidenses.

Los datos de aquellas que invertirán menos que hoy en día o no invertirán son insignificantes. Todos entienden que se trata de una cuestión clave.

Aunque ya han abordado cuestiones de sguridad de la información, los LÍDERES también mantendrán y aumentarán inversiones en el futuro.

¿INVERTIRÁ SU EMPRESA EN SEGURIDAD DE LA INFORMACIÓN EN LOS PRÓXIMOS 3 AÑOS?

Figura 18: Inversiones futuras



	Europa	Asia	América del Norte	Centro/S. América	Empresas grandes	Líderes
	306	294	49*	45*	250	112
Más que hoy en día	41,8%	41,5%	49,0%	48,9%	38,6%	42,0%
Igual que hoy en día	46,8%	51,0%	45,0%	51,1%	56,2%	58,0%
Menos que hoy en día	4,9%	1,1%	4,1%	0,0%	3,4%	0,0%
Ninguna inversión	6,5%	6,5%	2,0%	0,0%	1,8%	0,0%

INICIATIVAS FUTURAS

En el futuro, el equilibrio irá de las acciones esenciales y básicas a las básicas y avanzadas. Las empresas adoptarán un sistema de gestión de seguridad de la información, en lugar de centrarse en requisitos de infraestructura esenciales.

Entre las iniciativas que registran aumentos en el futuro, la formación de plantilla registra el crecimiento más significativo (+13% al 44%). Al mismo tiempo, hay una disminución en el establecimiento de directores de seguridad de la información (-7% to 15%) y en personal especializado para gestionar la seguridad de la información dentro de la organización (-9% to 31%). Las empresas perciben la gestión de la seguridad de la información cada vez más como una actitud a ser instaurada en la organización, en lugar de ser la responsabilidad de una sola persona o equipo.

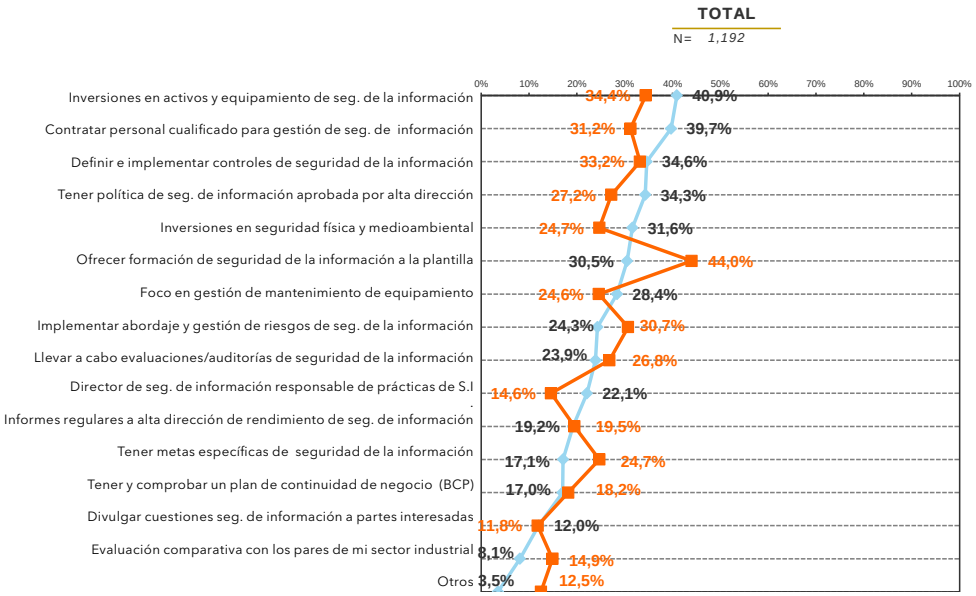
La implementación de un abordaje de riesgos de seguridad de la información y una metodología de gestión ha experimentado un crecimiento notable (+6% to 31%) similar al de fijar metas de seguridad de la información (+8% to 25%), marcando una tendencia hacia un enfoque más sistemático.

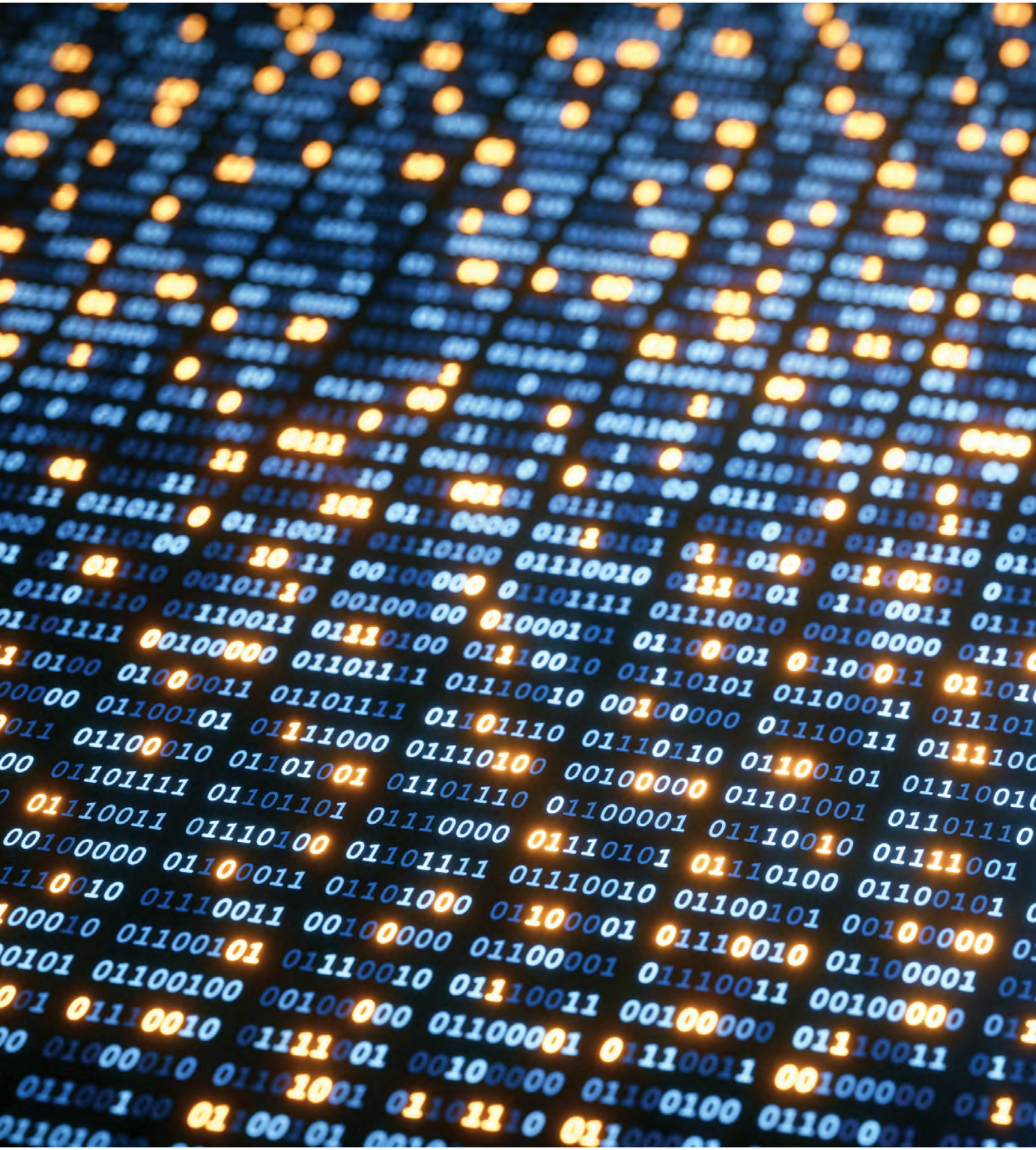
Además, crecen también las acciones más sofisticadas, como la ejecución de auditorías/valoraciones (+3% to 27%) y evaluación comparativa con los pares (+7% to 15%).

Los LÍDERES ya han resuelto las necesidades esenciales y básicas. En el futuro se centrarán en iniciativas mucho más avanzadas, como la evaluación comparativa (+6% to 31%). El foco en formación sigue primero en la lista.

¿CUÁLES DE LAS SIGUIENTES INICIATIVAS DE SEGURIDAD DE LA INFORMACIÓN HA TOMADO SU EMPRESA?
¿CUÁLES DE LAS SIGUIENTES INICIATIVAS DE SEGURIDAD DE LA INFORMACIÓN TOMARÁ PROBABLEMENTE SU EMPRESA DE AQUÍ A 3 AÑOS?

Figura 19: Iniciativas de seguridad de la información en el futuro versus hoy en día





BIG DATA & SEGURIDAD DE LA INFORMACIÓN

Big data es uno de los temas más ampliamente debatidos en la economía global digitalizada de hoy en día. "¿Qué es big data"? es una de las preguntas más comunes que planea sobre la comunidad de negocios. No hay consenso sobre la definición de big data: tiene varias definiciones, basadas en diferentes perspectivas. IBL, la organización líder en big data y análisis, la define de la siguiente forma: "Cada día creamos 2.5 trillones de bytes de datos, tanto que el 90% de los datos mundiales hoy se ha creado solamente en los últimos dos años. Estos datos vienen de todas partes: sensores utilizados para recoger información sobre el clima, entradas en redes sociales, imágenes y vídeos digitales, registros de transacciones de compra y señales de GPS de teléfonos móviles, por nombrar solo algunos. Estos datos son big data"*. Big data se está convirtiendo en un tema candente, porque los elementos comunes de datos están en todas partes, en todas las industrias, en cada país, en cada organización y, finalmente, con cada usuario personal de internet y dispositivos móviles. La capacidad de almacenar, agregar y combinar datos y luego usar los resultados para ejecutar análisis profundos ya se ha generalizado. Big data ha creado diversas aplicaciones en diversas industrias, como el aprendizaje con máquinas, optimización de redes, búsqueda semántica y muchas otras. Por ejemplo, uno de los mayores cambios impulsados por datos es la aparición de datos de ubicación en tiempo real, lo cual ha creado una serie completamente nueva de servicios basados en la localización, desde sistemas de navegación a fijación de precios de inmuebles, y seguros de accidentes basados en dónde y cómo conduce la gente sus coches.

Los líderes visionarios ya están comenzando a construir las capacidades de big data de sus organizaciones. **

Aunque el gran volumen de datos crea diversas oportunidades y aplicaciones, también plantea preguntas sobre la privacidad individual, la seguridad de la información y demás. El riesgo social más evidente que se nos presenta es la violación a la intimidad. Además, big data y las tecnologías se están volviendo cada vez más intrusivas, y demasiado complejas como para que el ciudadano de a pie las entienda. Hoy en día, el consumidor promedio ni tiene idea de la huella que crea con cada click en internet, ni comprende cuan seguros son los datos que ofrece. Este enorme volumen de información personal sin duda creará un conflicto entre intimidad y conveniencia.

El aumento exponencial en los datos y sus usos plantea varias preguntas interesantes, por ejemplo: ¿Cómo puede la sociedad protegerse del abuso de estos datos? ¿Qué sistemas regulatorios y de cumplimiento tenemos que poner en marcha para estas actividades? ¿Quién está facultado para garantizar a las organizaciones y a la sociedad que sus datos e información se gestionan de manera adecuada? ¿Qué medidas tenemos para controlar las intrusiones? Y la pregunta más importante: ¿Cómo definimos las prácticas legítimas en este campo, sobre todo si las actividades y consecuencias de big data son tan innovadoras? La innovación en este ámbito está creciendo a la velocidad del rayo, y definir un protocolo legal o de seguridad en un entorno tan cambiante no es fácil. Big data, del mismo modo que crea oportunidades, plantea desafíos formidables a gobiernos e industrias sobre la definición de regulaciones normativas para el tratamiento de datos.

* *http://www-01.ibm.com/software/data/bigdata/what-is-big-data.html*

** *Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., & Byers, A. H. (2011). Big data: The next frontier for innovation, competition, and productivity.*

NUESTRA CONCLUSIÓN

Vivimos en la era digital. La tecnología está cambiando nuestras vidas, pero ciertamente plantea nuevos desafíos y nuevos riesgos que no estamos acostumbrados a manejar. Hablaremos de algunos de ellos para comprender el alcance de la cuestión.

Los objetos de la era digital –desde smartphones y dispositivos de oficina hasta los sistemas de producción industrial– no están diseñados aún para ser seguros y protegerse de ataques cibernéticos. Además, el delito informático se está convirtiendo en una de las actividades más rentables para los delincuentes y, lamentablemente, mientras escribimos esto es probable que haya terroristas internacionales buscando nuevos modos de eludir las defensas de la seguridad de la información.

El panorama no es nada alentador, pero ser consciente de los riesgos es el primer paso para mitigarlos. Las empresas comienzan a entenderlo y a levantar sus barreras. Ahora comprenden que incluso una planta embotelladora puede acabar en la mira de los delincuentes. Un ataque que interrumpa los procesos de producción no solo derivará en una gran pérdida, sino que expone a la empresa a nuevas formas de chantaje. Peor: una filtración por motivos de espionaje industrial puede anular cualquier ventaja competitiva y borrar del mapa enormes inversiones.

Además del sabotaje criminal, cualquier pérdida de información puede afectar a la facturación, ya que los procesos de producción se basan cada vez más en la información .

Las empresas deben reevaluar sus organizaciones teniendo muy presentes estos nuevos desafíos, empezando por la base: su infraestructura y cultura. Para esto existen los sistemas de gestión en general, y los sistemas de gestión de seguridad de la información en particular: para ayudar a las empresas a lograrlo.

De hecho, la seguridad de la información puede ser definida, gestionada y monitorizada usando varias normas, entre las cuales la norma internacional ISO 27001:2013 es la más usada en todo el mundo. El número de empresas que usa esta norma y que trabaja para obtener una certificación externa está creciendo aproximadamente un 7% anual.

Los elementos básicos para implementar un sistema de gestión de seguridad de la información (ISMS) de acuerdo a los requisitos de ISO 27001:2013 pueden ser resumidos en 10 pasos fáciles de seguir:

Paso 1: Estudiar los requisitos de la norma ISO 27001:2013 y las guías, reglas y regulaciones asociadas aplicables a su organización

Paso 2: Obtener compromiso, soporte, presupuesto y aprobación de la alta dirección para la puesta en marcha de un proyectos de ISMS.

Paso 3: Definir las políticas, objetivos, funciones, responsabilidades y alcance (ubicaciones, procesos, activos) de seguridad para el ISMS.

Paso 4: Definir y documentar la metodología de abordaje de riesgos, que se centra en la Confidencialidad, Integridad y Disponibilidad (CID) de la información de la empresa. La metodología debe fijar la meta de identificar criterios y niveles de aceptación, evaluación de riesgos y posibles acciones de mitigación.

Paso 5: Identificar, analizar y evaluar las amenazas relevantes y el posible impacto para su organización de los incidentes y crisis de seguridad de la información, evaluar los niveles de riesgo y definir el nivel aceptable para los riesgos definidos.

Paso 6: Definir las acciones de mitigación de riesgos en el plan de tratamiento de riesgos, y objetivos acordes con los criterios de aceptación, los posibles requisitos de normas y regulaciones y los contratos de clientes.

Paso 7: Crear el plan final de implementación del ISMS, incluidos los formularios y modelos aplicables, el plan de tratamiento de riesgos, la implementación de controles seleccionados del ISMS, sesiones para concientizar a la plantilla y acciones para la implementación.

Paso 8: Formar a la plantilla y asignar activos, sistemas,procesos y actividades para garantizar el funcionamiento adecuado del ISMS dentro del alcance definido.

Paso 9: Planificar y ejecutar auditorías internas, acciones de revisión por la dirección y acciones de mejora para determinar el cumplimiento de los requisitos e identificar mejoras posibles en el sistema.

Paso 10: Iniciar la certificación externa y considerar una auditoría básica (abordaje preliminar) para obtener feedback sobre el estado del ISMS y para transmitir confianza a los empleados de la organización acerca de la implementación y cumplimiento de los requisitos.

Una certificación representa un pasaporte importante para el mercado. Un empujón definitivo, sobre todo para las nuevas oportunidades de negocio. Las empresas pueden demostrar su compromiso con la seguridad de la información y que han adoptado todas las medidas necesarias para garantizar la integridad de sus datos y sistemas.

ISO 27001:2013 es, de hecho, una herramienta excelente para que las empresas refuercen la seguridad de la información y reduzcan el posible riesgo de fraude, pérdida de información y divulgación. También contribuye a la difusión de cultura de seguridad de la información dentro de la propia organización.

La seguridad de la información hoy en día ya no es responsabilidad de un solo individuo o un equipo en particular, sino de todos los niveles de dirección. Al implementar un sistema de gestión de seguridad de la información acorde con la serie de normas ISO 27000, la organización completa está mejor equipada para gestionar todos los riesgos relacionados y para sacar el máximo provecho, en términos de reducción de filtraciones y pérdidas y en términos de mejora de las primas de seguros de responsabilidad civil. Además, la adopción de un sistema de gestión de seguridad de la información es la mejor estructura con la que puede contarse para trabajar hacia una mejora continua.

PERFILANDO A LOS LÍDERES

Los LÍDERES están un paso por delante en la gestión de seguridad de la información. Adoptan estrategias de seguridad de la información, fijando metas concretas a pesar de las dificultades de medición en un área como esta.

Sus inversiones en seguridad de la información son significativas. Aunque todavía deben trabajar en algunos de los aspectos más avanzados, no se centran solo en los requisitos esenciales –fundamentales para la protección de datos–, sino que también están dispuestos a invertir en acciones más sofisticadas, como actividades de auditoría, implementación de abordajes y metodología de gestión del riesgo y formación de la plantilla.

Los LÍDERES ya están pasando de una actitud defensiva a una proactiva y sistemática. Han sido capaces de incorporar la gestión de seguridad de la información en sus prtácticas cotidianas, y de difundir esa cultura en sus organizaciones.

De este modo, los LÍDERES obtienen beneficios significativo, no solo en términos de reducción de pérdidas, sino también con respecto a ventajas externas, como margen competitivo y la mejora de relaciones con los clientes y partes interesadas.

SEGURIDAD DE LA INFORMACIÓN: EL ENFOQUE DEL LÍDER

01 Los LÍDERES consideran las cuestiones de seguridad de la información en sus estrategias de negocio.

02 Los LÍDERES fijan metas de seguridad de la información.

03 Los LÍDERES invierten considerablemente para lograr seguridad de la información.

04 Además de implementar iniciativas centradas en requisitos esenciales, los LÍDERES también toman acciones más sofisticadas, como actividades de auditoría, implementación de abordajes y metodología de gestión del riesgo y formación de la plantilla.

05 El enfoque de los LÍDERES no es solo defensivo, sino sistemático.

06 La protección de datos no es la única razón que motiva a los LÍDERES a emprender iniciativas de seguridad de la información. La posibilidad de obtener margen competitivo/reputación de marca y la presión de las partes interesadas los motiva.

07 Los LÍDERES se benifician mucho más que otros de las iniciativas de seguridad de la información.

08 Los LÍDERES superan los obstáculos de seguridad de la información mejor que el resto.

09 Los LÍDERES comunican lo que hacen para lograr seguridad de la información.

10 Los LÍDERES planean mantener y aumentar sus inversiones en seguridad de la información en el futuro.


CONFIDENTIAL
SECURITY

www.dnv.com