Informe del estado de cultura de ciberseguridad en el entorno empresarial

2020

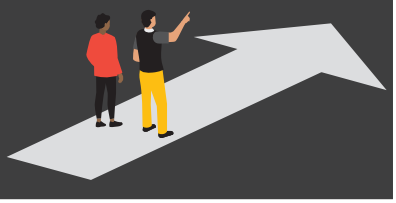
pwc

Resumen ejecutivo: Principales conclusiones del estudio

Entre los meses de Junio y Septiembre del 2020, PwC España ha realizado un estudio a 50 organizaciones en el ámbito nacional con la finalidad de conocer el estado en cultura de ciberseguridad en el entorno empresarial. El análisis realizado tiene como objetivo principal dar respuesta al paradigma actual de la cultura de ciberseguridad dentro de las organizaciones, así como buscar y proporcionar el nivel de cultura medio que existe actualmente en las organizaciones de España desde diferentes perspectivas, de tal manera que logremos tener una visión completa y significativa en base a diferentes variantes. A continuación se indican los aspectos más relevantes obtenidos del estudio.

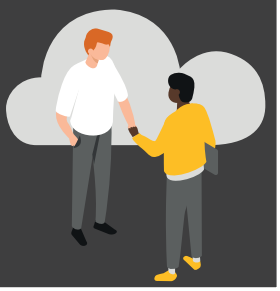
Las compañías están, de media, en un nivel de cultura inicial

El nivel de cultura de ciberseguridad en las compañías actuales es de **2,8** sobre un rango de valores de 1 a 5, lo que implica que existe un margen de mejora importante en la Cultura de Ciberseguridad actual, siendo el dominio de ***Comportamiento*** de la empresa y los empleados el de menor puntuación.



La cultura necesita empatía y motivación

El **86%** de las compañías considera que no existe una cultura de ciberseguridad en la organización o bien esta debería de mejorarse. El resultado del estudio muestra poca madurez en la cultura de ciberseguridad de las compañías actuales en España.



Las campañas de concienciación no contemplan factores motivacionales al cambio de comportamiento, estando basadas en la repetición de las buenas prácticas de seguridad como base de concienciación.

El presupuesto medio aplicado a formación y concienciación se corresponde con un 9% del presupuesto en Seguridad de la Información de la Compañía

64%

de las organizaciones considera que el presupuesto aplicado en Formación y Concienciación es escaso respecto a la importancia del área.

Sin medición no podemos lograr una cultura completamente embebida

Solo el **11%** de las compañías tienen un método de medición de la concienciación de los empleados. Este hecho hace que el nivel de gestión y seguimiento de la Cultura y la concienciación en seguridad no sea un proceso maduro ni gestionado, al igual que no permite medir la mejora asociada a los cursos y/o campañas realizadas.

Cada vez más el factor humano importa para conseguir una correcta ciberseguridad

93%

de las compañías considera que la concienciación de los empleados es una medida relevante o muy relevante, lo que significa que este ámbito de la seguridad está aumentando en importancia entre las compañías.

95%

de las compañías ya disponen, tienen planificado generar o están considerando generar un Plan de Concienciación para empleados.

Al igual que el 95% de las compañías ya han realizado, tienen planificado o están considerando realizar iniciativas de concienciación hacia la Alta Dirección.

Ante estas conclusiones, se evidencia la necesidad de mejorar de forma generalizada y relevante la cultura de ciberseguridad en el ámbito empresarial.

¿Qué metodología hemos utilizado para este estudio?

Este estudio se ha realizado sobre una muestra de 50 organizaciones de diferentes sectores, geografías, tamaños e ingresos, a fin de disponer de resultados generales que den pie a obtener conclusiones objetivas y fiables. Las fechas en las que ha transcurrido la obtención de información ha sido entre Junio y Septiembre del 2020.

Para realizar este informe donde se recoge el panorama de cultura de ciberseguridad en entornos empresariales en España se han combinado varias metodologías de recogida de datos con el fin de ofrecer una visión lo más amplia y completa posible.

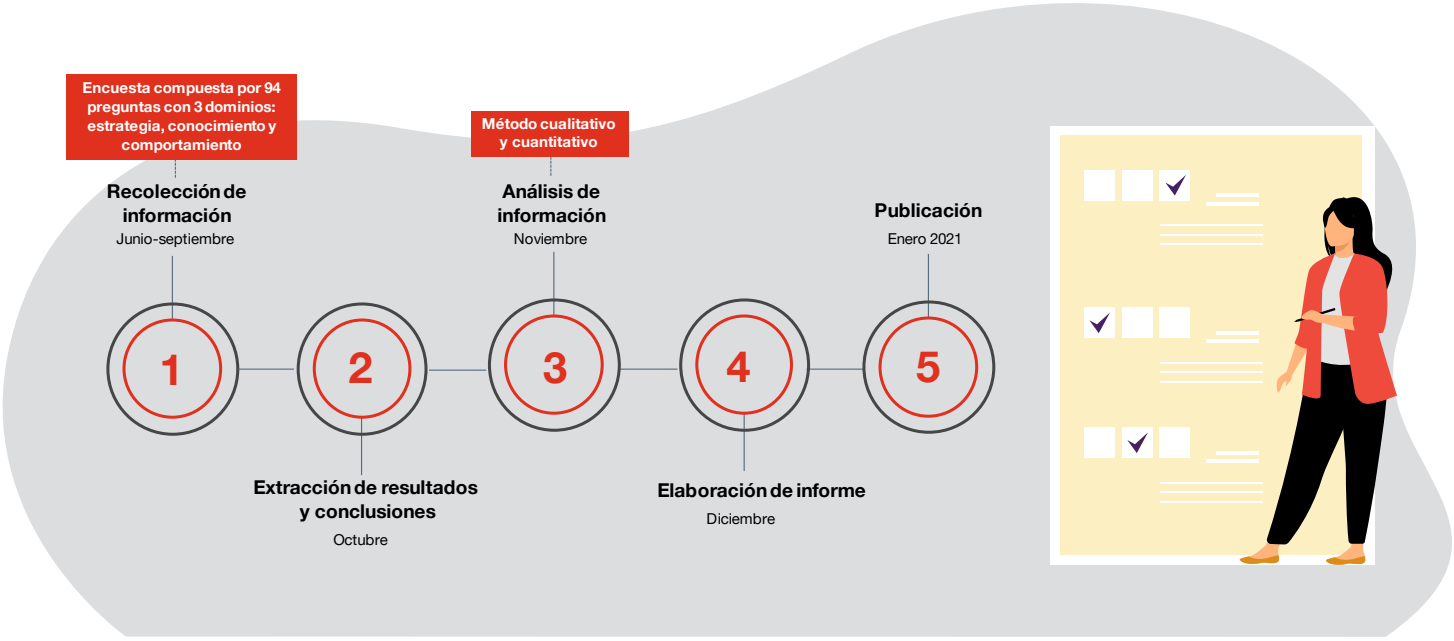
Fórmulas metodológicas utilizadas:

- **Entrevistas a expertos:** investigación cualitativa a través de entrevistas a expertos en la materia en administraciones públicas y grandes corporaciones.
- **Encuestas a responsables de seguridad:** investigación cualitativa a través de encuestas online o en remoto realizadas a responsables de la seguridad (CISOs) en empresas de todos los sectores industriales del panorama empresarial español con el fin de obtener una muestra lo más representativa posible de cada sector analizado.
- **Investigación:** análisis de fuentes secundarias sobre las cifras e indicadores básicos sobre la cultura en seguridad.

La muestra de 50 organizaciones se puede agrupar y dividir según la tabla que se muestra a continuación.

Agrupación	Divisiones
Tamaño por empleados	> 10.000 empleados
	Entre 3.000 y 10.000 empleados
	< 3.000 empleados
Tamaño por ingresos	> 5.000M€ ingresos
	Entre 2.000 y 5.000M€ ingresos
	< 2.000M ingresos
Sector	Energía
	Financiero
	Infraestructura, Logística y Manufacturing
	Retail y Consumo
	Sanidad y Farmaceutico
	Servicios, Transporte, Turismo y Juego
Geografía	Madrid
	Cataluña
	Resto del territorio

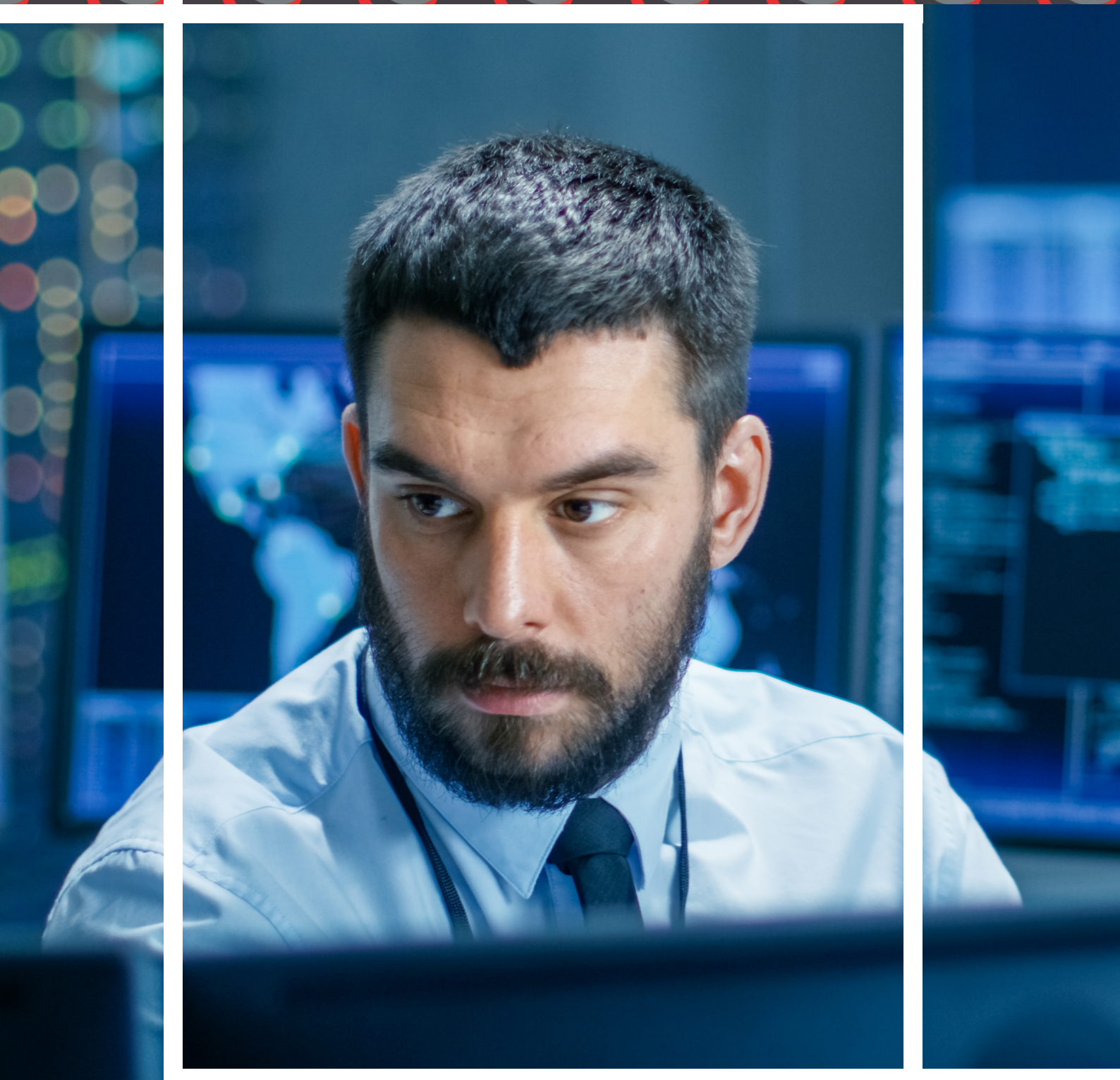
Estructura del estudio



La encuesta que da pie a este informe se compone de 94 preguntas basadas en diferentes dominios y ámbitos. El análisis exhaustivo de los resultados se ha realizado durante los meses de Noviembre y Diciembre.

Para llevar a cabo la medición del nivel actual de las organizaciones y la posterior realización de este informe, se elaboró un cuestionario cuyas preguntas estaban clasificadas en los siguientes dominios y ámbitos:

Dominio	Ámbito	
1. Estrategia	• Gobierno • Presupuesto • Estrategia en Formación	• Estrategia en Concienciación • Estrategia en Resiliencia
2. Conocimiento	• Medición de la formación • Recursos asociados a la formación • Alcance de la formación	• Formación a empleados • Formación en resiliencia
3. Comportamiento	• Medición de la concienciación • Concienciación por colectivos • Alcance de la concienciación • Motivación al cambio • Recursos disponibles • Comportamiento con clientes	• Comportamiento con accionistas • Comportamiento con proveedores • Comportamiento con familiares • Seguridad en los procesos de negocio • Medidas de seguridad
4. Perspectiva futura	• Retos • Amenazas	• Acciones a futuro



Nota: Este informe ha sido realizado por Cyber Risk Culture de PwC España a través de datos obtenidos de un cuestionario elaborado por PwC a empresas de todo el territorio nacional español. El tratamiento de los datos para generar las estimaciones y análisis ha sido anonimizado por sectores. Todos los datos del informe por tanto se basan en fuentes propias.

Índice de contenido

Introducción a la cultura de ciberseguridad

Qué es la cultura en ciberseguridad

De acuerdo con instituciones de referencia en el ámbito de la ciberseguridad como ENISA, la cultura de la seguridad de las organizaciones se refiere a los conocimientos, hábitos, percepciones, actitudes, normas y valores de las personas en relación con la seguridad cibernética y la forma en que se manifiestan en el comportamiento de las personas con las tecnologías de la información.

Hasta ahora las empresas y organizaciones habían dirigido sus acciones y esfuerzos a la concienciación en seguridad. En PwC España consideramos que la concienciación se ha quedado atrás en cuanto las necesidades de seguridad que reclama la realidad actual de riesgos y amenazas.

Nuestros años de experiencia en el sector nos ha hecho comprender la complejidad de nuestro trabajo, años en los que hemos ido adaptando, reinventando y mejorando nuestros enfoques y metodologías para estar a la vanguardia de la concienciación. Es por ello por lo que creemos que las empresas deben repensar la manera en la que se integra la seguridad desde el punto de vista humano y apostar por la creación, desarrollo e integración de una cultura de ciberseguridad.

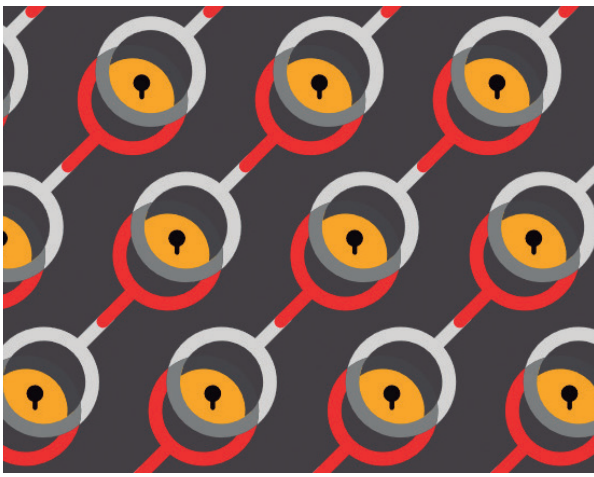
Concienciación

- Acciones de concienciación aisladas.
- Inexistencia de estrategia y metodología.
- Enfoque basado en hacer *compliance*.
- No se realiza seguimiento.
- No aporta pruebas enpíricas de la evolución.
- Sin resultados demostrables.
- Bajo impacto.

Cultura de seguridad

- Generación de un plan de transformación cultural.
- Metodología y estrategia constrastadas.
- Aproximación multidiciplinar.
- Enfoque integral a largo plazo.
- Seguimiento constante.
- Proporciona datos empíricos.
- Se mide el impacto y la evolución.
- Resultados demostrables.

1



La ciberseguridad se compone de tecnología, procesos y personas. Estos tres pilares son interdependientes. Es decir, las tecnologías no pueden proteger a las organizaciones si no se integran y utilizan correctamente o si los empleados no conocen los procesos. Las medidas técnicas de seguridad cibernética deben funcionar en armonía con los procesos empresariales y las personas.

Es por ello por lo que las personas son una pieza clave de la estrategia de ciberseguridad. En este contexto, el desarrollo de una cultura de ciberseguridad es esencial para reducir los riesgos y ciberamenazas.

La necesidad de una cultura de ciberseguridad

El desarrollo e integración de una cultura de ciberseguridad dentro de la propia cultura de las organizaciones responde, sobre todo, a la necesidad de poner a los seres humanos en el eje central de las estrategias de seguridad. Actualmente alrededor del 95 % de los ciberataques que sufren las empresas tienen su origen en el factor humano, ya sea por desconocimiento o error. “Una cadena es tan fuerte como su eslabón más débil” y actualmente las personas son el eslabón más débil de la cadena de seguridad de las empresas.

Lo que trata la cultura de ciberseguridad es que las personas se conviertan en cortafuegos humanos contra los ciberataques y los riesgos y amenazas de seguridad del día a día.

Hay múltiples factores que impulsan el surgimiento de una cultura de ciberseguridad como una necesidad dentro de las organizaciones. Esta necesidad refleja por sí misma la aceptación de que el comportamiento de una organización depende de las creencias, valores y acciones compartidas por sus empleados, y en esto se incluyen los comportamientos y actitudes de estos hacia la ciberseguridad.

Se ha venido observando que los esfuerzos realizados en las organizaciones a través de campañas de concienciación esporádicas no ofrecen, per se, suficiente protección contra los ciberataques que están en constante evolución. El propósito de la capacitación o concienciación realizadas como acciones aisladas se basan en la “esperanza” de que las personas cambien su comportamiento de seguridad. Esta hipótesis sin embargo no se basa en pruebas empíricas ni en una estrategia fundamentada por una metodología.

Cambiar los comportamientos de las personas de una organización es un trabajo difícil, y a veces las organizaciones buscan respuestas sencillas y no científicas a cuestiones complejas. Instituciones como SANS, NIST o ENISA vienen avisando de este desacierto y proponiendo que se realice un enfoque desde las ciencias sociales. Para tener más éxito con sus iniciativas, las empresas deben construir una cultura organizacional en el que todos los empleados se comprometen unos con otros como participantes iguales.

Introducción al informe de cultura de ciberseguridad

Cyber Risk Culture, ¿Quiénes somos?

Cyber Risk Culture (CRC) es una línea perteneciente al departamento de Business Security Solutions (BSS), dedicada a la formación, concienciación y resiliencia en seguridad de la información y riesgos tecnológicos que tiene a las personas como eje central de la estrategia de seguridad. Para ello, contamos con un equipo multidisciplinar que tiene como objetivo formar, concienciar y aumentar la resiliencia de empresas y usuarios a través de estrategias innovadoras.

CRC se divide en tres grandes áreas que en su conjunto dan una respuesta 360º a las necesidades y demandas del sector: Be Prepared, Be Aware y Be Resilient.

Motivación y ámbito del estudio

La digitalización de la sociedad ha implicado consecuencias a nivel de seguridad a las que se enfrentan diariamente todas las empresas. En la estrategia contra las amenazas de seguridad las personas son una pieza clave.

Be <Prepared>

Centrados en la **educación y formación de los usuarios a nivel técnico** con una plataforma propia, un amplio catálogo de cursos y un *pool* de expertos para la tutorización e impartición de sesiones.

- *Webinars* y *workshops*
- Carreras formativas
- Diplomas de especialización
- Máster
- Medición del conocimiento en seguridad y riesgo tecnológico

Be <Aware>

Especializados en **cultura, cambio de comportamiento y transformación**. Mediante la concienciación, con un enfoque metodológico e iniciativas de *design thinking*, ayudamos a las organizaciones a alcanzar su objetivo de seguridad.

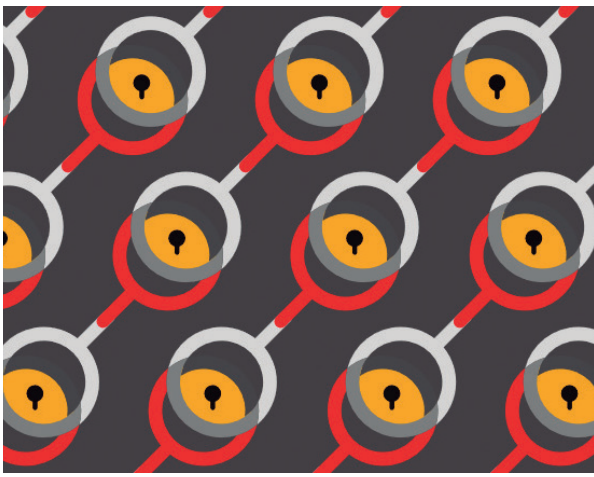
- Generación de planes de concienciación
- Medición del nivel de concienciación
- Diseño de todo tipo de campañas de concienciación
- Simulaciones de *phishing*
- Talleres de concienciación
- Gestión integral de eventos de concienciación

Be <Resilient>

Expertos y analistas especializados en **mejorar la capacidad de resilencia de las empresas con ejercicios y entornos de entrenamiento** que guian a las organizaciones a aprender y gestionar diferentes incidentes.

- Ciberejercicios
- *Tabletops*
- *Wargaming*

2



Es importante saber que, la mayoría de las brechas de seguridad en las organizaciones son resultado de un error humano y, en muchos casos, se debe a la falta de concienciación y formación en ciberseguridad. Esto, a su vez, viene motivado por la falta de visibilidad que tiene la capa ejecutiva sobre la cultura en seguridad de su empresa y la comprensión de la necesidad de incluir la madurez en ciberseguridad como una pieza clave de la estrategia ejecutiva de la empresa a nivel global.

La mayoría de las violaciones de datos dentro de las organizaciones son el resultado de acciones de los empleados, bien por desconocimiento o falta de cultura. Y aunque las políticas de ciberseguridad son comunes entre las organizaciones en el panorama actual, los empleados suelen verlas como pautas en lugar de normas básicas y esenciales que deben cumplir en el día a día. De manera similar, las tecnologías no pueden proteger a las organizaciones si se integran y utilizan incorrectamente. En este contexto, el desarrollo de una cultura de ciberseguridad logra un cambio de mentalidad, fomenta la concienciación de seguridad y la percepción del riesgo, así como mantiene una cultura organizacional cercana, en lugar de intentar coaccionar un comportamiento seguro.

Una cultura de ciberseguridad en las empresas ayuda a hacer entender que las recomendaciones de seguridad de la información son una parte integral del trabajo, los hábitos y la conducta de los empleados, incorporándolas en sus acciones diarias. Adoptar el enfoque correcto para la seguridad de la información permite que una cultura de ciberseguridad se desarrolle naturalmente a partir de los comportamientos y actitudes de los empleados, y como parte de la cultura organizacional más amplia de una empresa. La cultura de ciberseguridad puede ser moldeada, adaptada y transformada de acuerdo las propias realidades, cultura y valores de cada empresa.

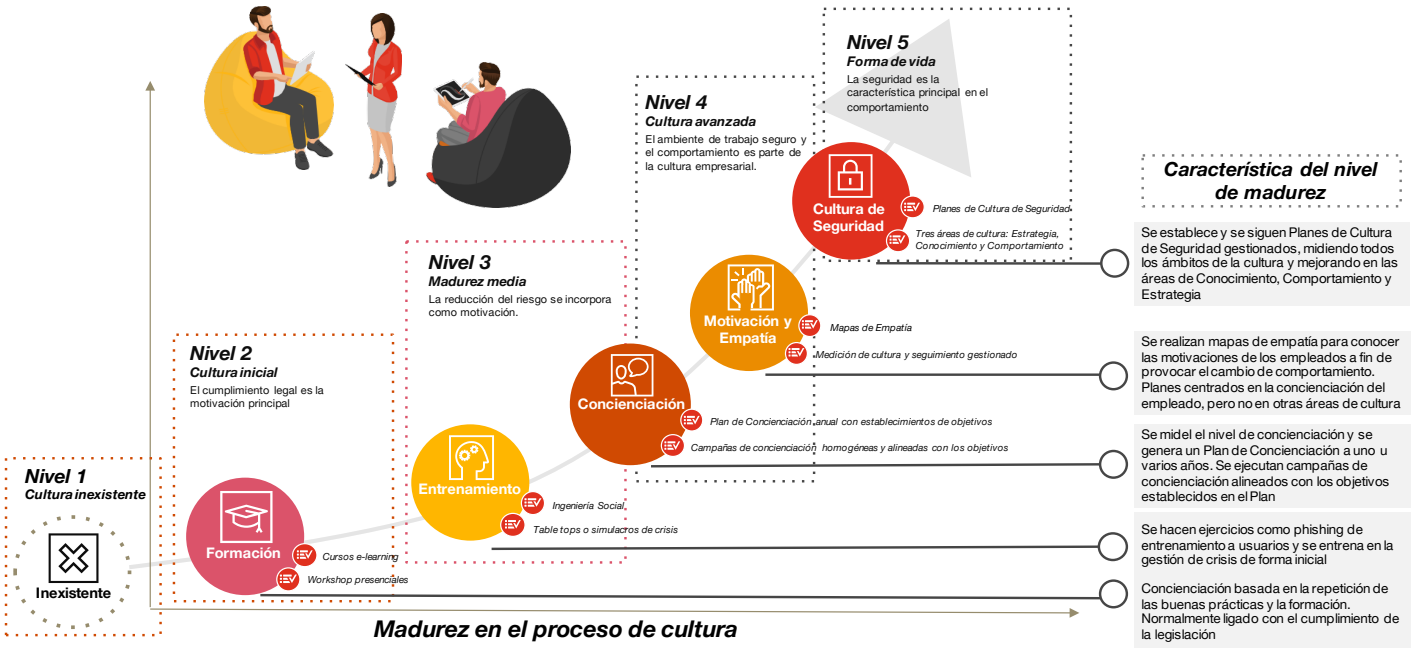
Sin embargo, los entornos empresariales cambian constantemente, por lo que las organizaciones deben mantener y adaptar activamente su cultura de ciberseguridad en respuesta a las nuevas tecnologías y amenazas, así como a sus objetivos, procesos y estructuras cambiantes. Una cultura de ciberseguridad implementada de forma adecuada da forma al pensamiento de seguridad de todo el personal (incluido el equipo de seguridad), mejorando la resiliencia contra todas las amenazas cibernéticas, especialmente cuando tienen su origen a través de la ingeniería social.

Por ello, hemos elaborado este informe a partir de un estudio previo, con el objetivo de conocer el panorama actual del sector empresarial español en materia de seguridad y, también con el objetivo de concienciar sobre la importancia de ésta.

Framework de cultura en ciberseguridad

La metodología empleada tanto para la generación del informe como para la medición del nivel de cultura de ciberseguridad de cada una de las empresas participantes se ha basado en el *framework* y proceso de madurez en cultura de ciberseguridad de PwC España. Este *framework* logra posicionar a las organizaciones en 5 niveles de cultura y ayuda a marcar objetivos claves y concretos para poder avanzar de nivel con iniciativas y acciones que involucren tanto el área de conocimiento, como el de comportamiento y estrategia. El *framework* utilizado por PwC España mide el nivel de cultura en un rango de 1 a 5, siendo 1 el menor de los niveles de cultura y 5 el mayor.

Gráfico 1 **Proceso de madurez en cultura de seguridad**



Los cinco niveles incluidos dentro del *framework* son:

1 Nivel Cultura inexistente

No existe una cultura en ciberseguridad dentro de la empresa. Los empleados no son conscientes de que son objetivo de ciberataques ni de que sus acciones tienen un impacto directo en la seguridad de la organización. Son potenciales víctimas de fraudes cibernéticos y representan un vector de entrada real de ciberataques. No conocen ni entienden las políticas de seguridad de la organización.

2 Nivel Cultura inicial

Existe una cierta cultura de ciberseguridad donde se ha realizado un primer acercamiento a la concienciación. Se han realizado acciones aisladas de formación y concienciación, pero el programa está diseñado principalmente para cumplir con los requisitos específicos de cumplimiento o auditoría. La capacitación se limita a una base anual o ad hoc. Los empleados no están seguros de las políticas de seguridad de la organización y/o su papel en la protección de los activos de información de su organización.

3 Nivel Cultura en desarrollo

Hay un plan y una estrategia de concienciación y capacitación en seguridad en los que se identifican grupos y temáticas específicas. La organización sabe identificar los temas con mayor necesidad e impacto para el objetivo de seguridad y se centra en estos elementos clave. El programa de formación va más allá de la formación anual e incluye refuerzo a lo largo de año. El contenido se comunica, o al menos se pretende comunicar, de una manera atractiva y positiva que fomenta el cambio de comportamiento en el trabajo y en el hogar. Como resultado, la gente entiende y sigue las políticas de seguridad de la organización y reconoce, previene y reporta activamente los incidentes de seguridad.

4 Nivel Cultura avanzada

El programa cuenta con los procesos, recursos y apoyo de la Alta Dirección necesarios para un ciclo de vida a largo plazo, incluyendo (como mínimo) una revisión y actualización anual del programa. Como resultado, el programa es una parte establecida de la cultura de la organización y es actual y atractivo. El programa ha ido más allá de cambiar el comportamiento y está cambiando las creencias, actitudes y percepciones de seguridad de las personas.

5 Nivel Forma de vida

El programa tiene un marco robusto de métricas alineado con la misión de la organización de hacer seguimiento del progreso y medir el impacto. Como resultado, el programa está mejorando continuamente y es capaz de demostrar el retorno de la inversión. Esta etapa no implica que las métricas no sean parte de cada etapa (que lo son). Esta etapa refuerza que, para tener un programa verdaderamente maduro, se deben tener métricas para demostrar el éxito.

Esta etapa del programa tampoco significa que la organización esté exenta de los riesgos y amenazas que comportan la seguridad y el componente humano, sino que es consciente del mismo y trabaja de forma activa y proactiva en reducir estos riesgos a través de un plan estratégico que es considerado vital en la organización. Es decir, se trabaja la seguridad de la empresa desde el punto de vista humano de forma constante teniendo en cuenta todas las consideraciones anteriores para hacer de la seguridad su forma de vida.

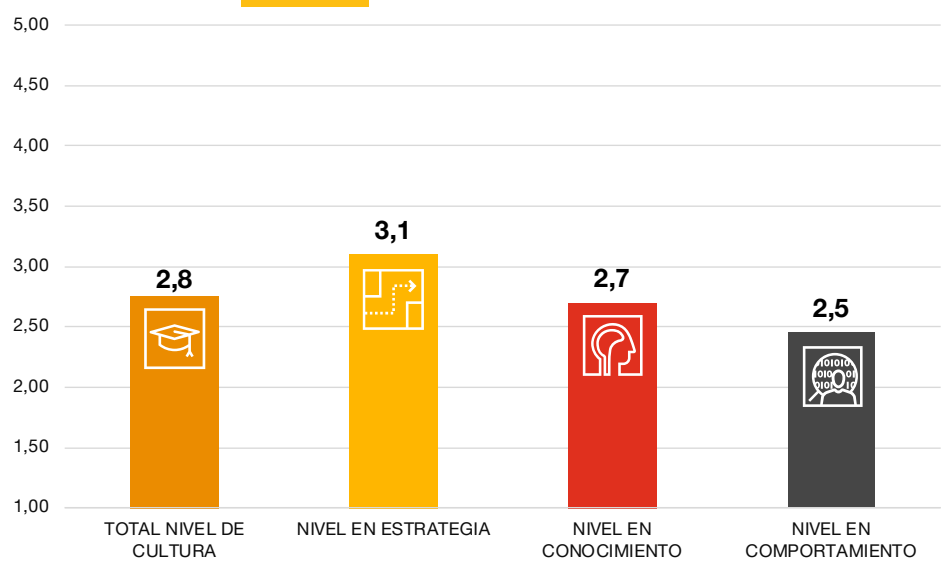
Resultados del estudio: La cultura de ciberseguridad en el ámbito nacional

Resultados generales del estudio de cultura de ciberseguridad

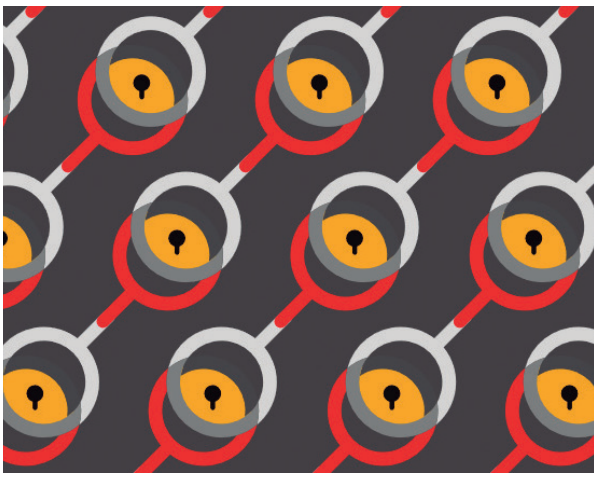
Las tecnologías de seguridad sólo pueden ser efectivas si los empleados tienen el conocimiento, las habilidades, la comprensión y la aceptación necesarias para usarlas. Lograr esta cultura de ciberseguridad requiere un cambio tanto en el conocimiento como en el comportamiento de los empleados. Este cambio tan solo puede conseguirse mediante la educación y la capacitación. Sin embargo, lo que hemos podido observar de las organizaciones entrevistada para el presente estudio, es que a pesar de que las compañías son cada vez más conscientes de la necesidad de formar a sus empleados y establecer una estrategia de concienciación para asimilar un nivel de cultura óptimo, esto no se ve reflejado en el comportamiento de las personas.

En este sentido, encontramos clave que el comportamiento y la concienciación de las personas se considere un aspecto relevante en las empresas, siendo el aspecto que más se debe mejorar para aumentar el nivel de cultura de las organizaciones.

Gráfico 2 **Nivel de Cultura de Seguridad**



3



De los resultados obtenidos, el **nivel de cultura de ciberseguridad de media en las compañías de España se sitúa en un 2,8 sobre un rango de valores de 1 a 5** (ver gráfico 2).

Es decir, se encontraría bajo nuestra propia denominación y clasificación en un nivel inicial de cultura. Esto significa que el sector empresarial español está en proceso de tomar conciencia de la necesidad de establecer un plan de cultura, capacitación y concienciación en ciberseguridad, a pesar de que de forma generalizada:

- No existe un plan estratégico de cultura y las iniciativas de concienciación se despliegan al azar.
- El programa de concienciación cuenta con un apoyo limitado por parte la organización, dando lugar en la mayoría de los casos a que la Alta Dirección invierta los recursos mínimos para cumplir con la normativa.
- La concienciación en seguridad no ocupa un lugar destacado en la estrategia de la organización.
- De forma generalizada, no existe una persona nombrada responsable de la ejecución y desarrollo de los planes de cultura y concienciación.
- Se realizan formaciones de ciberseguridad, pero de forma aislada sin un refuerzo constante ni un alcance generalizado.
- Hay poca participación de otros departamentos, como el de recursos humanos, comunicación o formación.

Todo ello quiere decir, que actualmente el panorama de cultura en ciberseguridad que nos encontramos a nivel empresarial en España está inmaduro con un alto margen de mejora.

Comparativa detallada por ámbitos de los dominios

Si pasamos a realizar una breve comparativa de los ámbitos analizados, podemos destacar dos grandes hallazgos generales a la totalidad de ámbitos:

1) Entre las fortalezas de las compañías se sitúan la incorporación de medidas de seguridad ligadas con la seguridad de los recursos humanos, así como la realización de entrenamientos en gestión de crisis y resiliencia.

2) En contrapartida, entre los aspectos más débiles comunes en la mayoría de los encuestados encontramos:

    a. La no incorporación de motivaciones al cambio de conducta en las campañas de concienciación.
    b. La falta de visibilidad de la seguridad hacia los clientes.
    c. La ausencia en la incorporación de los familiares de los empleados en las campañas de concienciación.

En este último punto, hemos podido encontrar ciertas reticencias y limitaciones por parte de las compañías. Este se debe en parte a la propia cultura de empresa de cada compañía, así como a su nivel de madurez en concienciación en ciberseguridad (ver gráfico 3). No obstante, incorporar a los familiares en las campañas de concienciación tiene un efecto muy positivo a fin de mejorar la seguridad en el ámbito personal, siendo también esta una de las motivaciones al cambio más usuales. También entra en consideración que incorporar a los familiares en las iniciativas de concienciación tiene una correlación directa con la responsabilidad social corporativa.

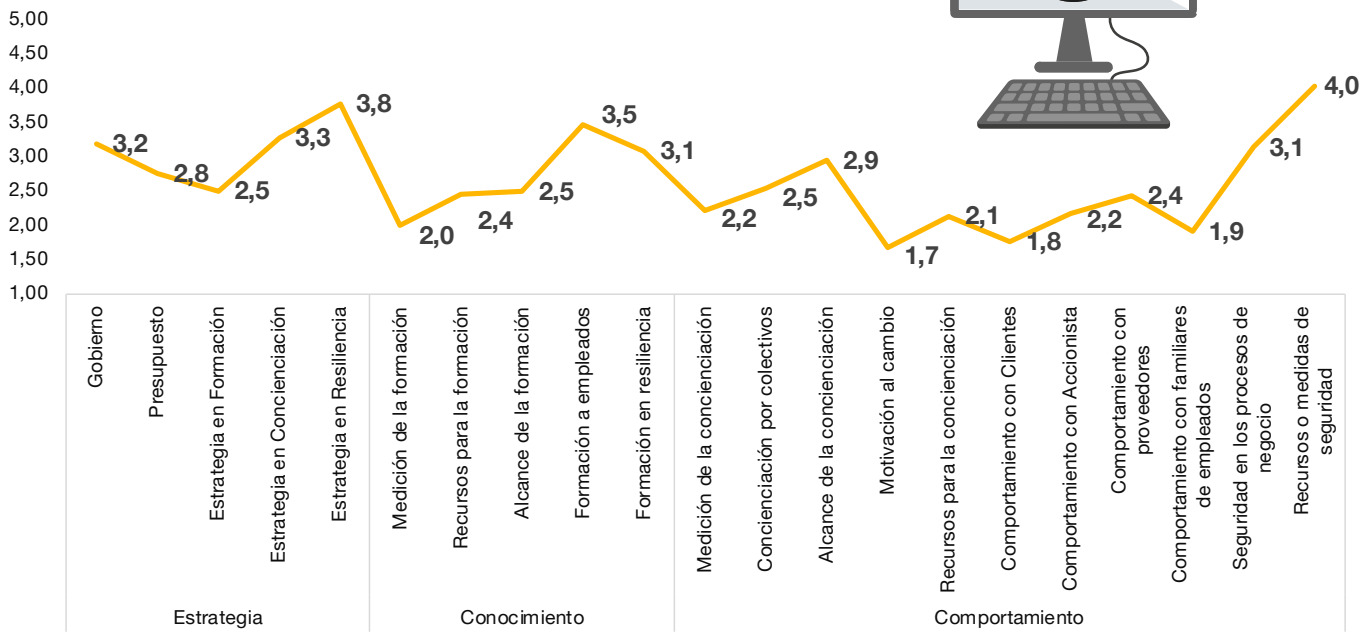
Por otro lado, se ha podido observar que no existe de forma generalizada una estrategia o políticas de formación y capacitación formalizadas que permitan aumentar las competencias de las personas con responsabilidad en seguridad. Esto puede ser un problema ya que cada vez es más importante que los perfiles que operan la seguridad y están encargados de ella estén formados no sólo en la parte técnica si no también adquiriendo la conciencia correcta para los riesgos que se pueden encontrar dentro de sus roles y responsabilidades. Por lo que el desarrollo de procesos que garanticen que las personas implicadas en este ámbito consigan la formación y concienciación adecuada es imprescindible para tener una securización correcta en el factor humano responsable de la seguridad.

Sin embargo, el punto que queremos resaltar como un **hecho preocupante es que la medición del estado y del nivel tanto de formación técnica como de concienciación en ciberseguridad de la compañía se contempla de forma muy limitada o casi inexistente.**

Las métricas desempeñan un papel crucial en el cambio de cultura y la seguridad de la información, ya que ayudan a evaluar el estado actual de la compañía y el nivel objetivo deseado de forma realista y progresiva. Nos ayudan a gestionar el proceso y el progreso. Ofrecen retroalimentación útil a la compañía y a la gerencia, y pueden afirmar la efectividad de las medidas de seguridad implementadas y de las iniciativas de cultura de ciberseguridad que se lleven a cabo.

Las buenas métricas deben ser cuantificables, repetibles y comparables para permitir información precisa. También deben poder obtenerse fácilmente, ser relevantes y ofrecer información útil para mejorar la cultura. Un ejemplo de ello sería la realización de simulaciones de ataques de ingeniería social de forma periódica o la realización de una encuesta de ciberseguridad que mida los comportamientos de los empleados en las diferentes áreas de seguridad.

Gráfico 3 **Detalle del nivel de cultura de seguridad**

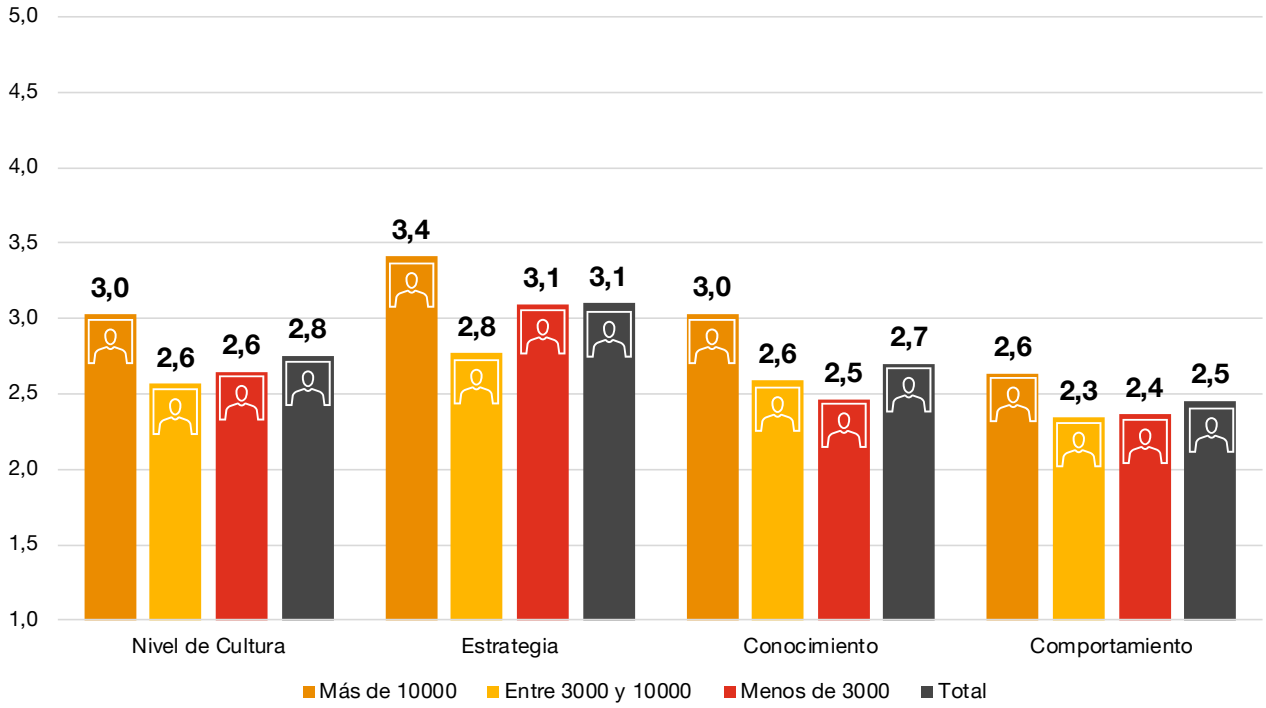


Comparativa por número de empleados

Se puede observar a partir del siguiente gráfico, que las compañías con más de 10.000 empleados tienen un nivel de cultura superior a empresas con un menor número de empleados.

Esto se debe principalmente, a que empresas con un alto número de empleados se traduce en más recursos, así como un mayor grado de exposición a los riesgos y amenazas derivados del factor humano en ciberseguridad. Por tanto, la necesidad es mayor y el proceso de toma de conciencia más acelerado

Gráfico 4 **Nivel de Cultura según número de empleados**



Comparativa por sectores

Es igualmente interesante realizar un análisis comparativo por sectores. En este sentido, hemos podido comprobar que no existe una clara diferenciación respecto a la concienciación por sectores.

Las principales conclusiones son:

- El sector de la energía se muestra muy estable en todos los dominios, lo que implica que los esfuerzos en cultura están distribuidos de forma homogénea.
- El sector financiero, teniendo un nivel de madurez en ciberseguridad más elevado que el resto, no dispone de un nivel de cultura en seguridad diferenciado. Se diferencia en la parte estratégica, si bien los dominios de Conocimiento y Comportamiento están por debajo de la media.
- Los sectores de Infraestructuras, Logística y Manufacturing, así como Servicios, Transporte, Turismo y Juego, tienen unos niveles parecidos al sector financiero. Se nota un desequilibrio entre la parte estratégica y el resto de los dominios, lo que implica una posible falta de implantación de las políticas o estrategias definidas.
- Retail y Consumo, junto con Sanidad y Farmacéutico tienen unos niveles similares en Cultura. Tienen áreas de mejora respecto a otros sectores, destacando el dominio de Comportamiento dónde tienen los niveles más bajos del estudio.

Gráfico 5 **Nivel de Cultura por sector**

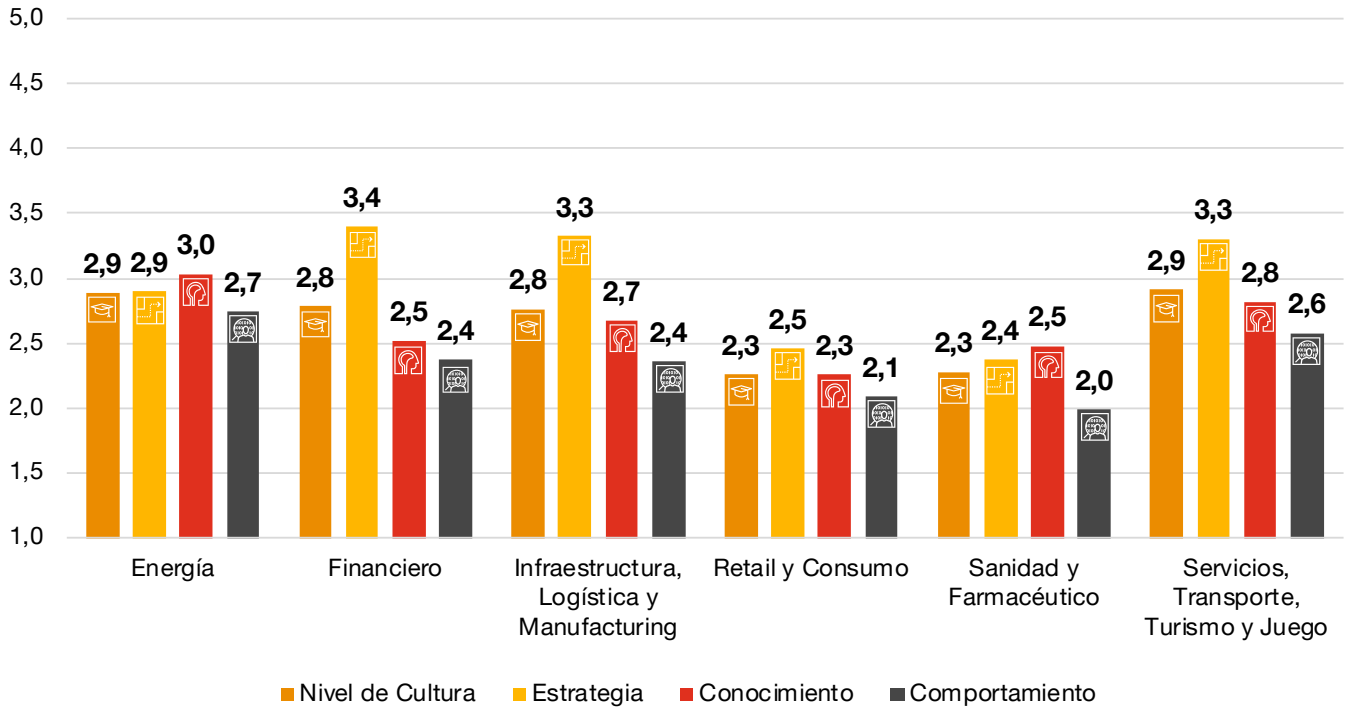
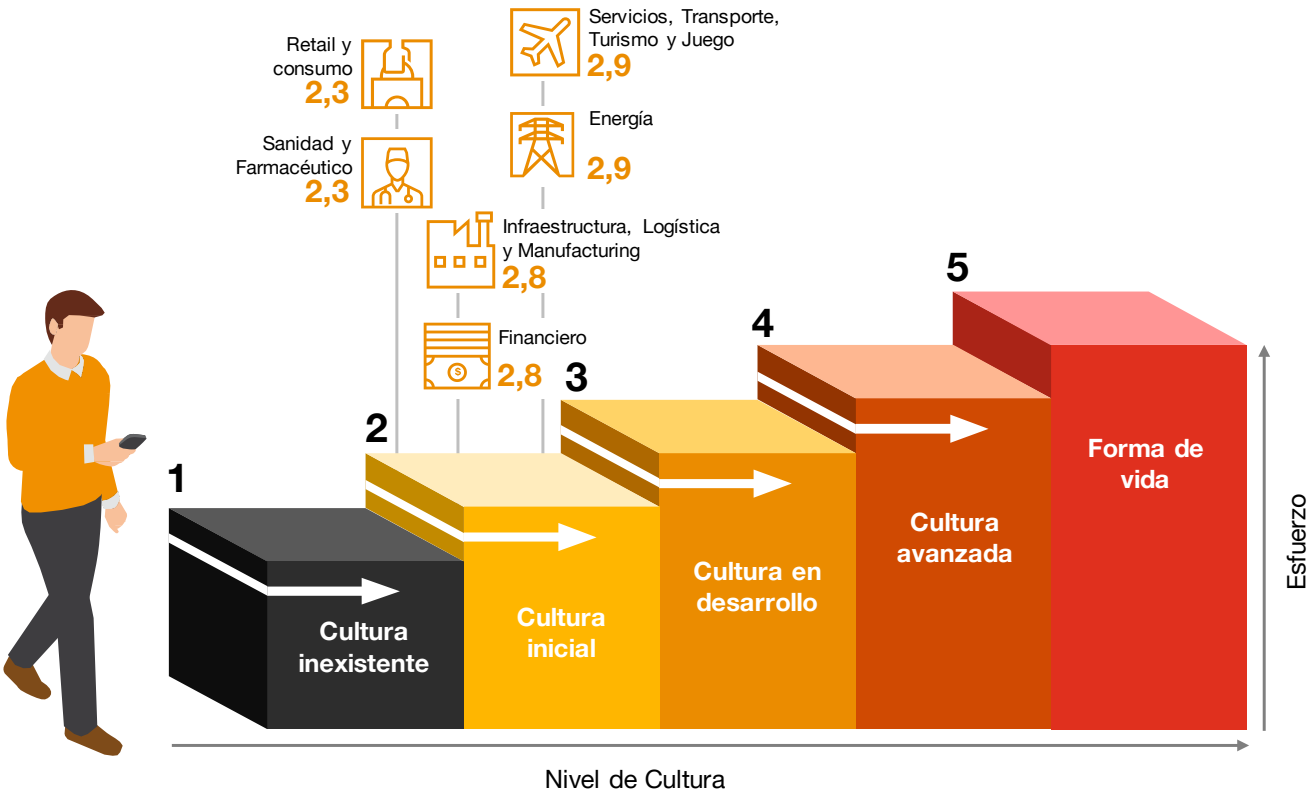


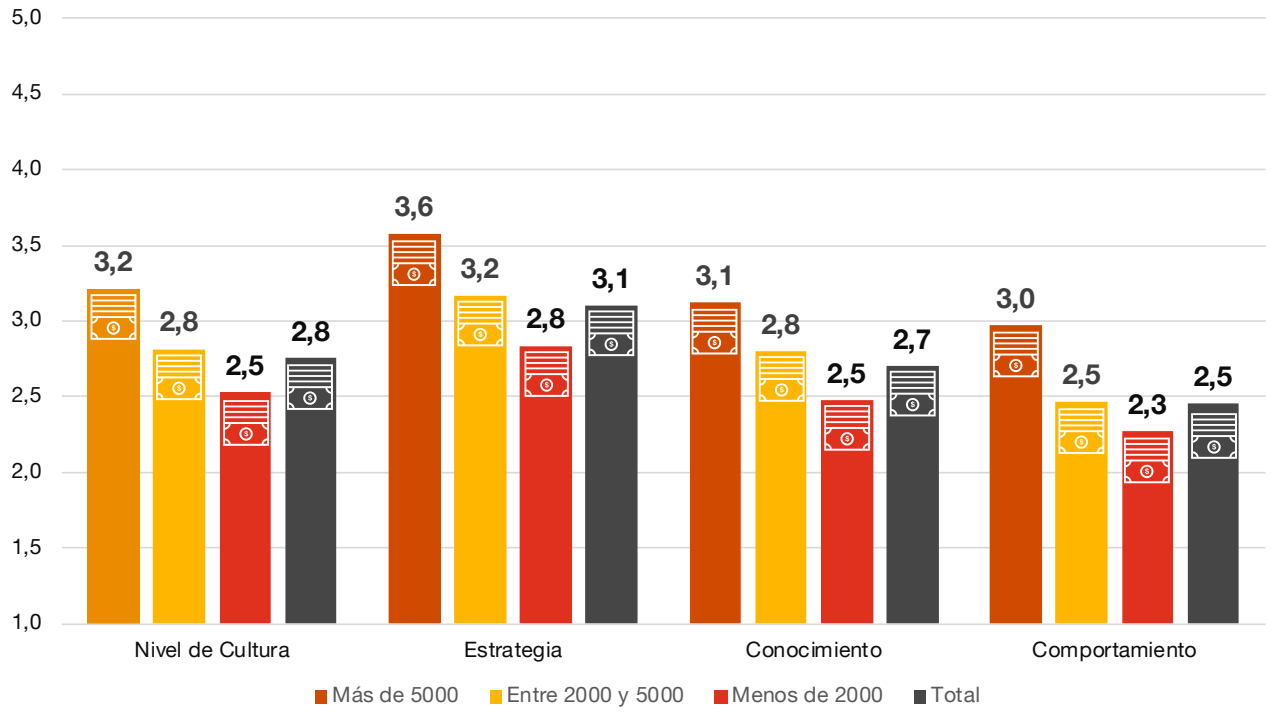
Gráfico 6 **Nivel de Cultura por sector**

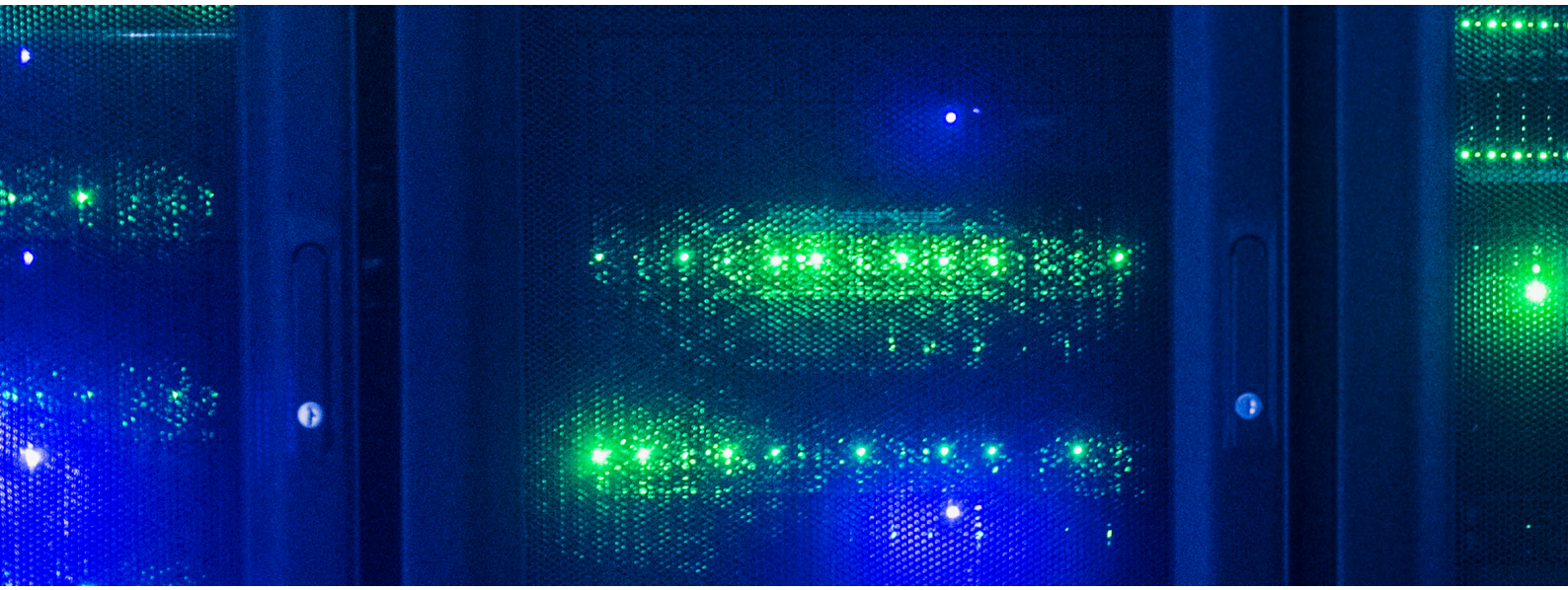


Comparativa por cuantía de ingresos de la organización

En la comparativa entre compañías según la cuantía de ingresos (más de 5.000 millones de euros, entre 5.000 y 2.000 millones de euros y menos de 2.000 millones) se puede observar una clara distinción en el nivel de madurez en cultura de ciberseguridad. Esta correlación es directa prácticamente en todos los ámbitos de los dominios. La conclusión es que las compañías más grandes a nivel de ingresos, tanto por el control del cumplimiento de la legislación, los estándares en los que se certifican así como por los procesos internos seguramente más estrictos, provocan que exista un mayor nivel de cultura de ciberseguridad que en las empresas más pequeñas respecto a ingresos.

Gráfico 7 **Nivel de cultura de seguridad según ingresos**

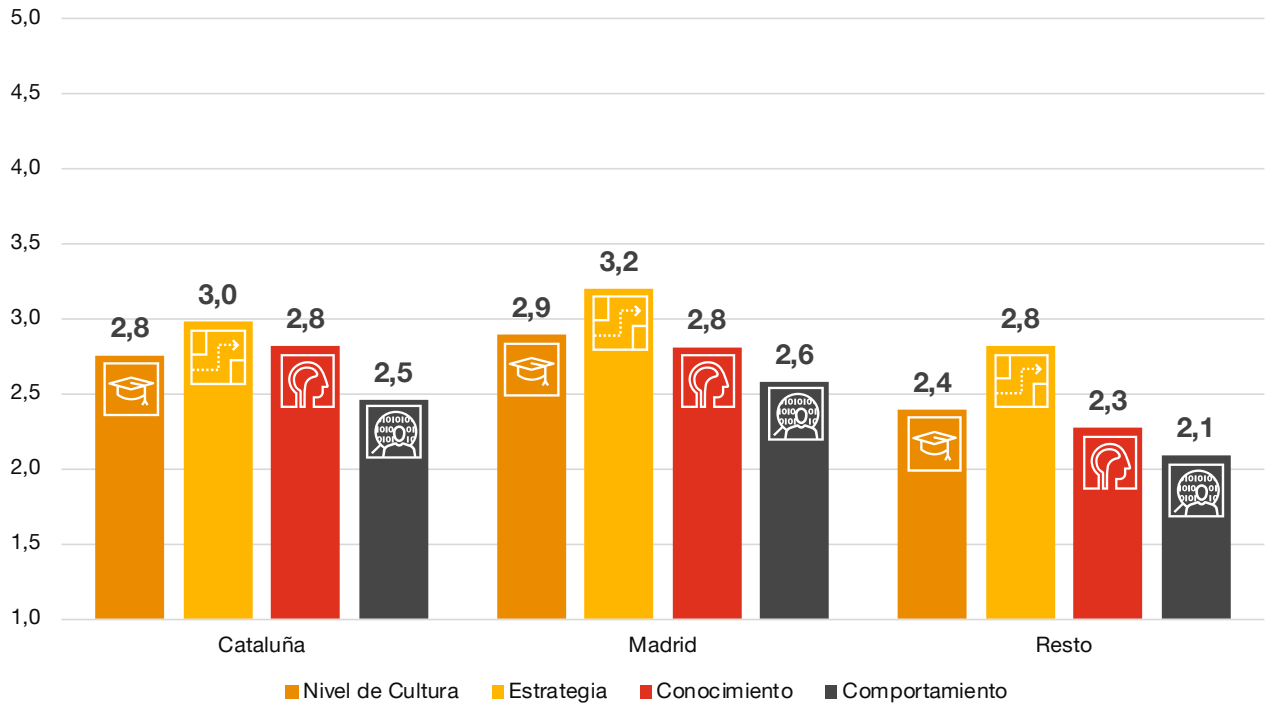




Comparativa por geografía

Los resultados que desprende el estudio cuando miramos las organizaciones según su localización resaltan que las compañías ubicadas tanto en Cataluña como en Madrid disponen de un nivel de cultura en ciberseguridad mayor que el resto de compañías. Posiblemente derivado también del tamaño de dichas compañías encuestadas, se puede reflejar un salto relevante en dicha valoración. El porcentaje de compañías que han compuesto la muestra se corresponde con un 53% de compañías ubicadas en Madrid, un 25% de compañías ubicadas en Cataluña y un 22% de compañías ubicadas en el resto del territorio.

Gráfico 8 **Nivel de cultura de seguridad según geografía**



Resultados detallados por dominio

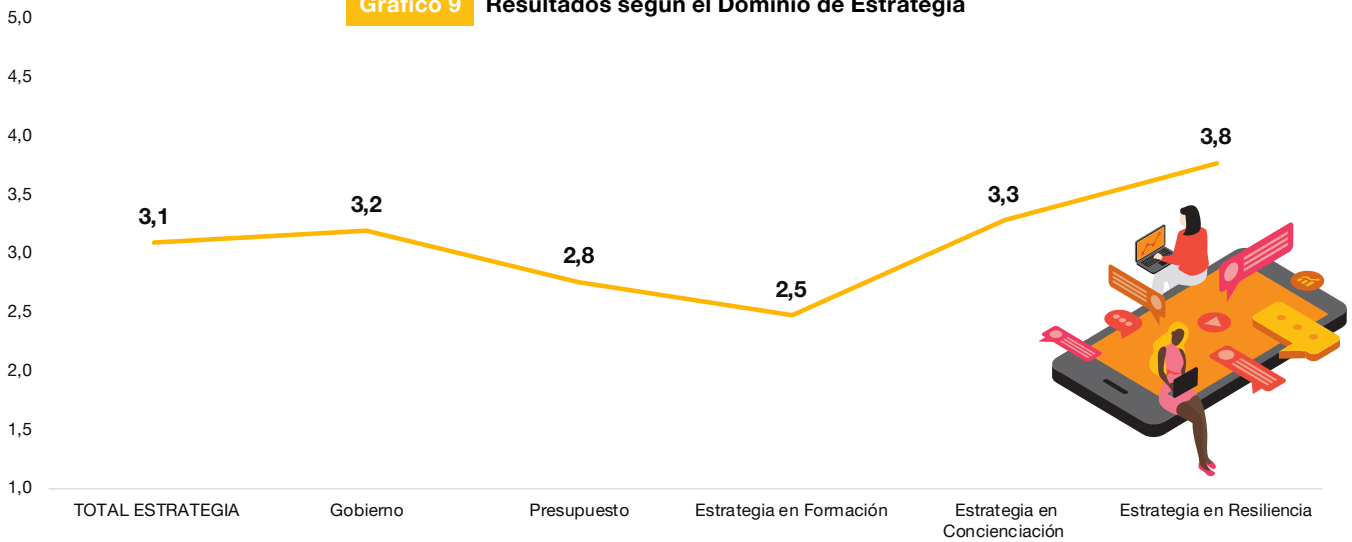
Estrategia

El dominio de **Estrategia** engloba los conceptos de apoyo a la cultura de seguridad de la Dirección, así como la madurez en la gestión de los procesos de formación, concienciación y resiliencia.

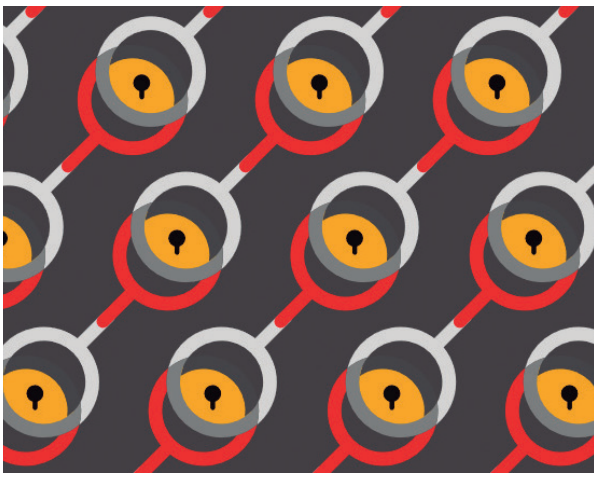
En el análisis del dominio de estrategia en los diferentes sectores, se ha podido observar que los planes de resiliencia es el ámbito más maduro de todos los evaluados (ver gráfico 9). El disponer de una estrategia de recuperación y gestión de crisis es un ámbito abordado de forma generalizada.

Por otro lado, el ámbito de estrategia en formación y capacitación de los empleados es el ámbito menos maduro en las organizaciones. Este hecho queda agravado según los ingresos de las compañías. A menor número de ingresos, la valoración de la estrategia en formación y capacitación disminuye materialmente.

Gráfico 9 **Resultados según el Dominio de Estrategia**



4

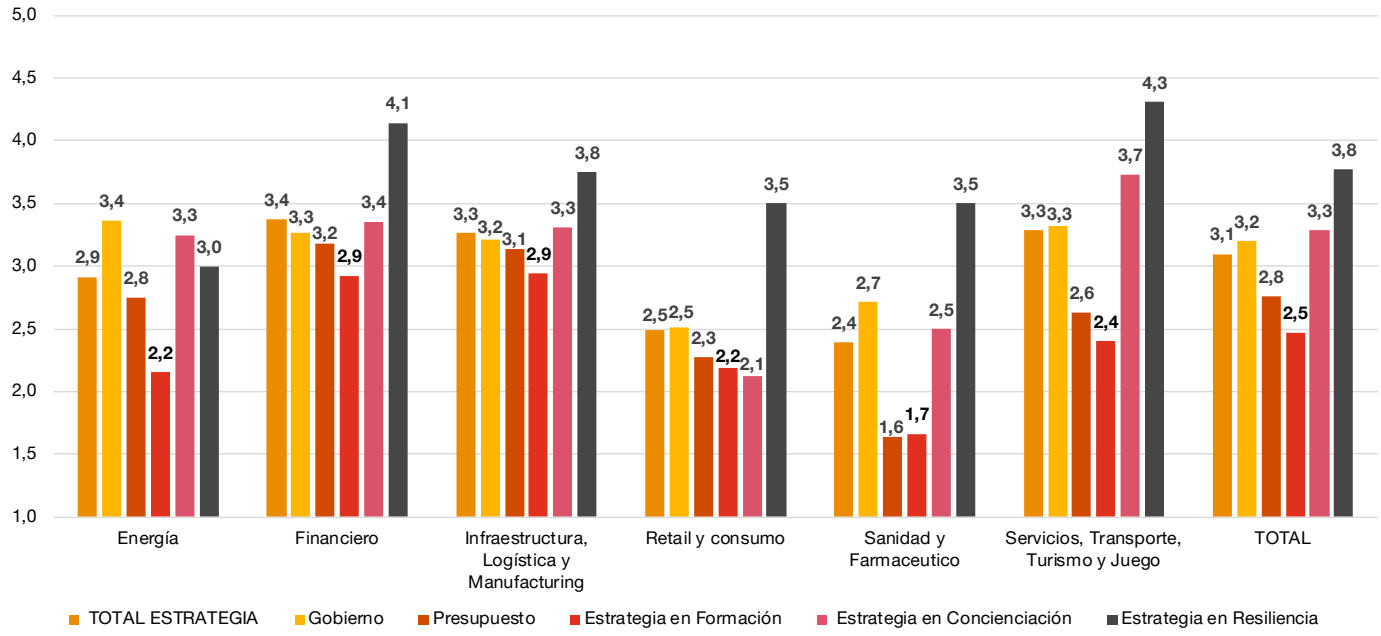


Datos destacados

- El **42%** de las organizaciones ya dispone de un rol o un comité ligado a la formación y la capacitación en seguridad de las compañías, mientras que el **48%** de las organizaciones tiene un rol o un comité ligado a la concienciación en seguridad.
- El **66%** de las organizaciones dispone de un rol o un comité ligado con la gestión de crisis en la compañía.
- Para el **25%** de las organizaciones la seguridad de la información se trata de un tema recurrente en los Comités de Dirección, mientras que para el **57%** es un tema que se trata de forma discrecional.
- El **60%** sin embargo no considera la seguridad como uno de sus valores, o bien no lo refleja claramente en sus políticas o prácticas generales.
- El **86%** de las compañías no publicita o envía comunicados a sus clientes relativos a la seguridad de sus datos o de la organización.
- El **80%** de las organizaciones no reporta el estado de la cultura en seguridad la Dirección, o lo hace de forma puntual. La cultura todavía no se considera un indicador del estado de la seguridad en las organizaciones.
- El **48%** de las organizaciones ya disponen de planes de formación en Ciberseguridad formalizados, si bien, el **72%** no considera dentro de dicho plan las funciones actuales y futuras que tendrán los empleados afectados, ni las preferencias de los empleados.
- El **52%** de las organizaciones disponen de planes de concienciación, aunque solo el **30%** de estas miden su cumplimiento. De igual forma que el **9%** de las organizaciones no han realizado ningún tipo de acción de concienciación todavía.
- El **66%** de las organizaciones tienen una estrategia formalizada de gestión de crisis, mientras que un **14%** adicional disponen de dicha estrategia aunque esta no esté formalizada.
- El **41%** de las organizaciones no dispone o no actualiza el Plan de Continuidad de Negocio.

Si pasamos a realizar una comparativa del dominio de estrategia por sectores, los resultados obtenidos serían los que se muestran en el siguiente gráfico.

Gráfico 10 **Comparativa para el dominio Estrategia según sector**



Como se puede observar, el sector financiero es el que más resalta en el dominio de Estrategia, destacando la valoración en la estrategia de Resiliencia y con un valor bastante homogéneo para el resto de los ámbitos.

Por otro lado, el ámbito con menor puntuación es la Estrategia en Formación, que desprende que las compañías no hacen esfuerzos en establecer planes de capacitación formales, ni rutas formativas para aumentar las competencias de sus empleados especializados.

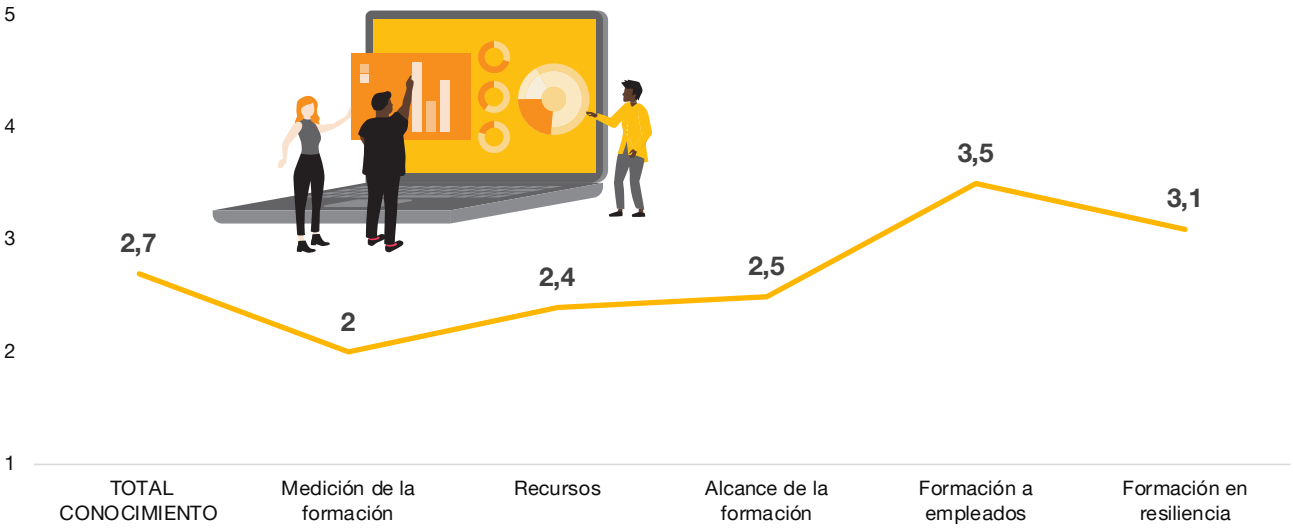
Cabe mencionar que, de las entrevistas realizadas, la estrategia en resiliencia es el valor que más preocupa a todas las organizaciones independientemente del sector al que pertenezcan.

Conocimiento

El dominio de **Conocimiento** engloba las acciones que realiza una organización para formar a sus empleados, considerando tanto la capacitación de sus equipos técnicos como la formación general al resto de empleados. Los recursos que la organización pone a disposición de la formación es un aspecto relevante del estudio en este dominio.

De este dominio hemos podido concluir que en general, las compañías ofrecen formación en ciberseguridad a los empleados, así como realiza ejercicios de simulación de ataques de ingeniería social, especialmente *phishing*. Sin embargo, casi ninguna de las compañías realiza ciberejercicios para entrenar y conocer sus capacidades de ciberseguridad. En este punto, es crítico el dato obtenido en empresas de menos de 3.000 empleados, donde actualmente no existe capacidad de respuesta ante incidentes o análisis forense.

Gráfico 11 **Resultados detallados para el dominio de Conocimiento**

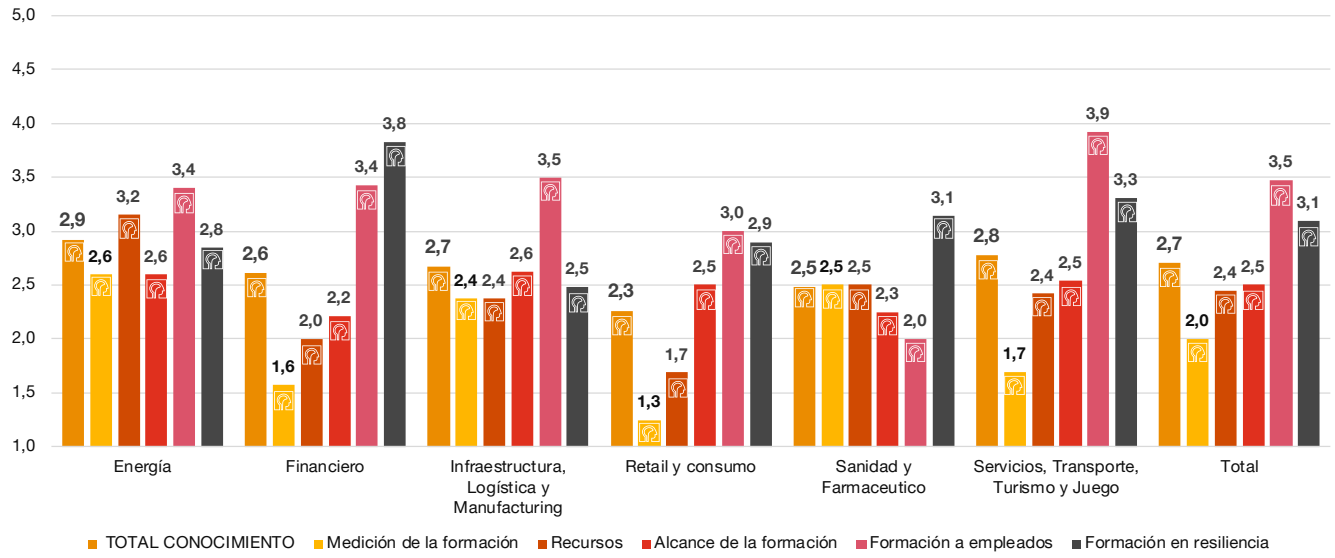


Datos destacados

- Solo el **9%** de las organizaciones disponen de un procedimiento para medir el conocimiento de los profesionales de ciberseguridad, lo que dificulta el establecimiento de planes de formación adecuados a la organización y sus diferentes colectivos.
- Aunque se ofrece formación a empleados especialistas el porcentaje de personas que reciben dicha formación sobre el total de personas es menor del **50%**. Es una cifra escasa si se quiere mantener actualizados los conocimientos de dichos expertos.
- Tan solo el **30%** de las organizaciones ofrece iniciativas periódicas de formación en ciberseguridad a los empleados, el **50%** ofrece iniciativas de manera discrecional, mientras que el **20%** de las organizaciones no ofrecen ninguna o casi ninguna sesión o contenidos de formación en seguridad a los empleados.
- El **48%** de las organizaciones hace ejercicios de entrenamiento de ingeniería social como puede ser el phishing de forma periódica. Mientras que el **43%** del grupo restante hace ejercicios de entrenamiento de forma discrecional. Aunque este es un buen dato que refleja un entrenamiento generalizado, si no se encuentra respaldado por iniciativas de concienciación y formación enmarcados dentro de un plan, estos ejercicios podrían resultar poco eficaces.
- Alrededor del **50%** de las organizaciones no dan formación técnica en respuesta ante incidentes ni realizan ciberejercicios, lo que puede provocar reacciones técnicas poco eficaces ante incidentes sufridos.

En cuanto a la comparativa por sectores, los resultados serían los siguientes:

Gráfico 12 **Comparativa para el dominio de Conocimiento según sector**

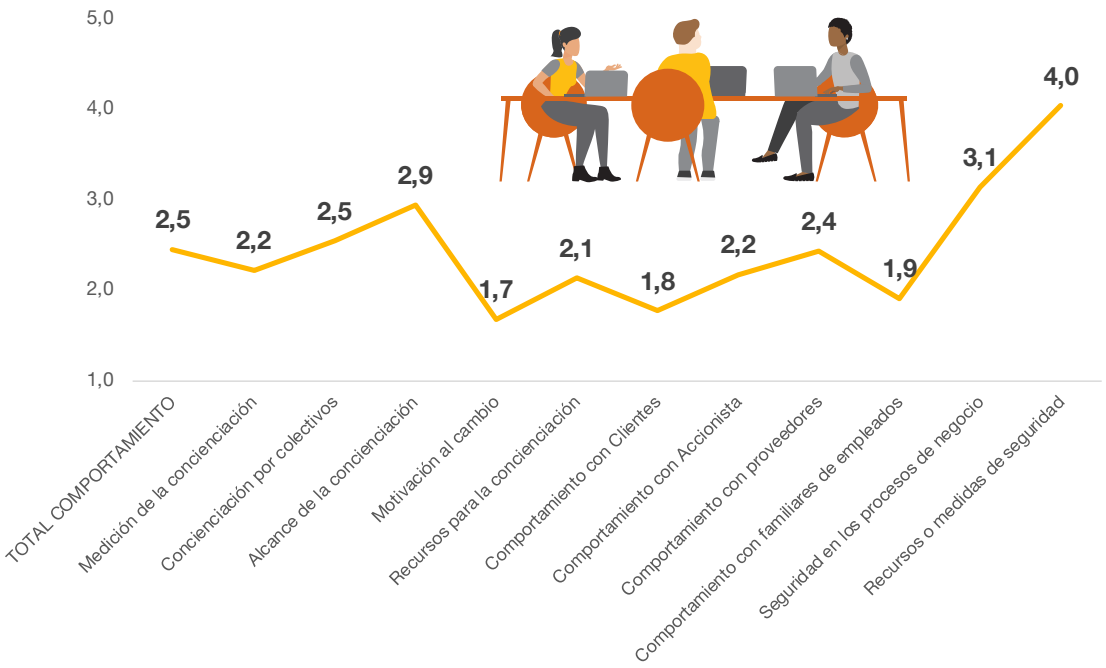


Comportamiento

El dominio de **Comportamiento** engloba los aspectos relacionados con el comportamiento de la organización sobre actores externos, como clientes, accionistas o proveedores, engloba factores de comportamiento de los empleados respecto a la seguridad de los activos y engloba las medidas de seguridad implantadas en la organización ligadas con la seguridad de los recursos humanos.

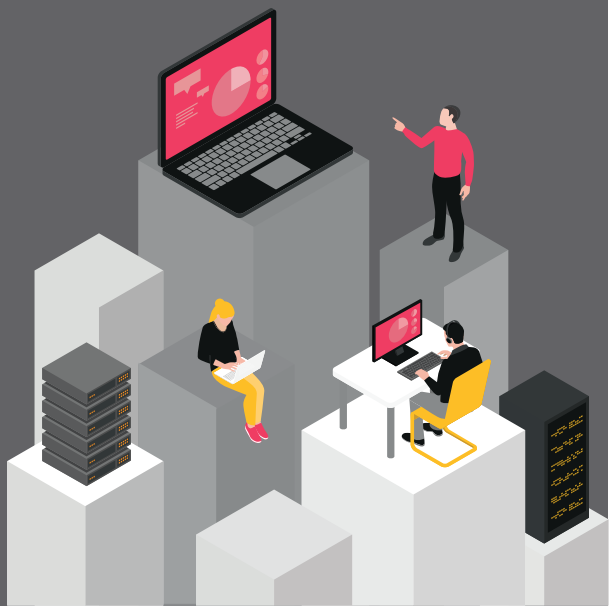
En general, dentro del dominio de Comportamiento podemos concluir que las organizaciones no tienen en cuenta las motivaciones de los empleados o riesgos específicos por perfiles para lograr un cambio de comportamiento completo dentro de la organización. A su vez, la gran mayoría de organizaciones no tienen a los clientes en mente en tema de concienciación y no comunican ni realizan ninguna acción para llegar a este gran colectivo.

Gráfico 13 **Comparativa para el dominio de Comportamiento**



Datos destacados

- El **84%** de las organizaciones no es capaz de medir, o no puede medir de forma homogénea, el nivel de concienciación de los empleados. La medición principalmente se realiza mediante resultados de las pruebas de ingeniería social única y exclusivamente. Esto quiere decir que las mediciones obtenidas son parciales y poco realistas.
- El **70%** tampoco miden el éxito de las campañas de concienciación que realizan.
- El **61%** de las compañías no establecen colectivos para concienciar, o bien no diferencian las campañas según dichos destinatarios.
- El **77%** de las compañías sólo conciencian a los usuarios que tienen un puesto de usuario. El resto no se incluyen en el alcance y difusión de las campañas.
- El **45%** de las compañías tienen un alcance en la concienciación menor al **75%** de los empleados.
- El **77%** de las compañías hacen menos de 10 iniciativas al año de concienciación a los empleados. Este hecho no ayuda a realizar una concienciación continuada, constante o con la periodicidad necesaria para aumentar su efectividad.
- El **73%** de las compañías no incorporan información de las motivaciones al cambio de los empleados dentro de las campañas de concienciación que realizan.
- Sólo el **18%** de las organizaciones considera a los clientes como colectivo a concienciar, y ninguna compañía incorpora la seguridad de la información como parte de la publicidad que puedan hacer hacia sus clientes.
- El **70%** de las compañías no lanzan avisos sobre alertas de seguridad o incidentes a sus clientes.
- El **84%** de las organizaciones no hacen ningún tipo de acción de concienciación a sus accionistas o propietarios.
- El **70%** de las compañías ya reporta indicadores de seguridad a la Alta Dirección, y el 11% de estos lo reportan a sus accionistas. Este es un buen dato ya que indica que la Dirección recibe, de forma generalizada, información sobre el estado de la seguridad en la organización.
- El **70%** de las compañías no incorpora a los proveedores en el entrenamiento de resiliencia y concienciación, lo que puede provocar brechas de seguridad.
- El **59%** de las compañías no exige a los proveedores ni formación ni concienciación a los empleados.
- El **77%** de las compañías no incorpora a los familiares de los empleados dentro de las campañas de concienciación. Incluir a familiares incorpora una motivación personal en la puesta en práctica de las recomendaciones.
- Sólo el **7%** de las compañías priorizan la seguridad antes que la producción o el negocio.
- Sólo el **18%** de las compañías incorporan “siempre” al departamento de seguridad en la implementación de proyectos. Lo que significa que estamos lejos todavía de “seguridad en el diseño”.
- Sólo el **23%** de las compañías incorpora al departamento de seguridad en los proyectos estratégicos desde el arranque.
- El **64%** de las compañías dispone de un proceso de auditoría de seguridad significativo con resultados relevantes para la organización.
- Existe por lo general un alto grado de cumplimiento respecto a las medidas de seguridad como son disponer de sitios para mantener conversaciones confidenciales, destructoras de papel, políticas de mesas limpias, etc.
- El **84%** de las compañías han puesto un mecanismo de reporte de incidentes fácil o cómodo para que el empleado pueda utilizarlo en caso de sospecha. Este es un dato interesante, ya que nos indica que la madurez en cuanto a ataques de ingeniería social en las empresas es alta. Esto se debe principalmente a que el *phishing* en sus diferentes tipologías y canales es la principal amenaza de ciberseguridad de las empresas de todo el mundo, cuya intensidad y sofisticación no deja de aumentar.

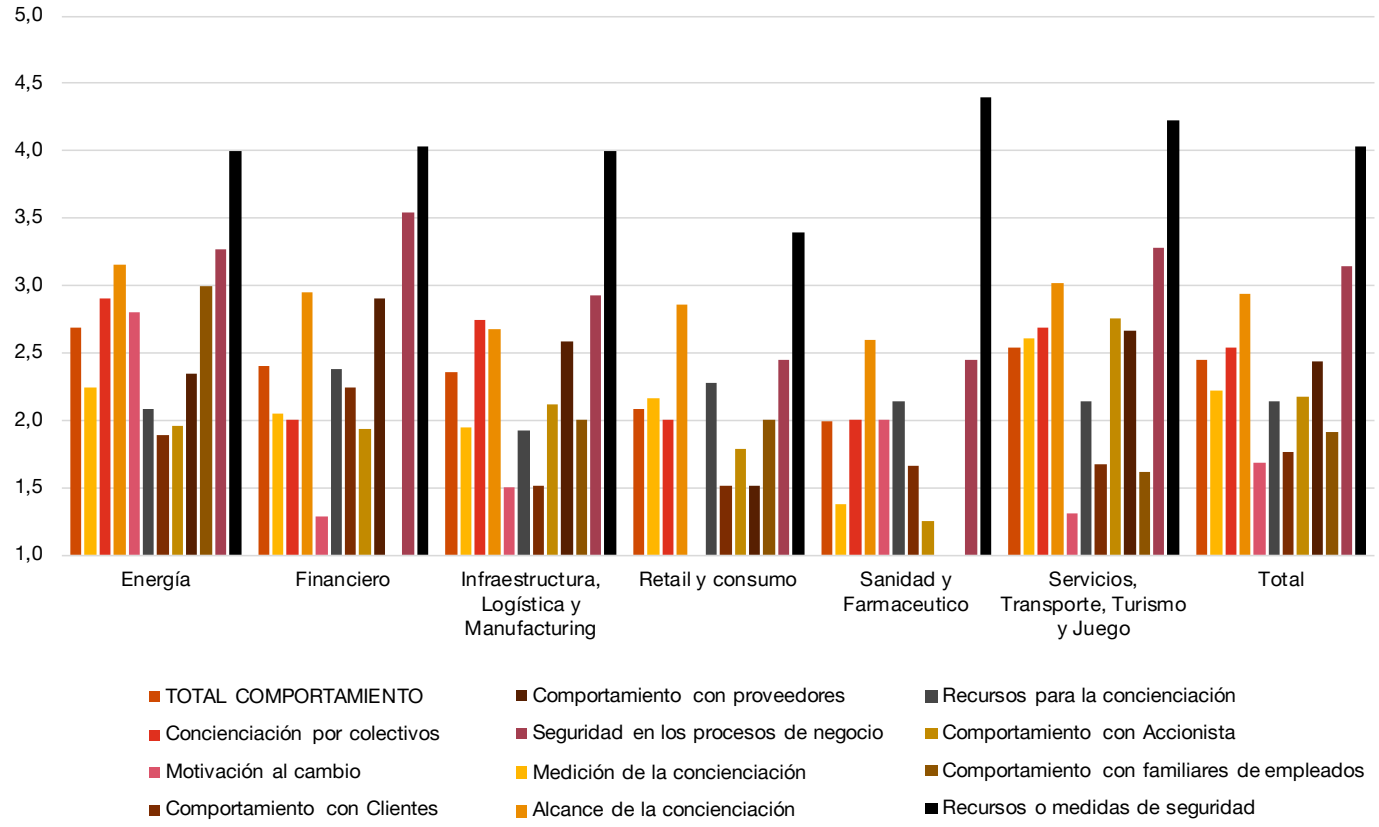


Los resultados obtenidos en este dominio por sectores se recogen en el gráfico 14.

Desde el punto de vista de sectores, el sector de Sanidad y Farmaceútico se desmarca con el mejor resultado respecto a los recursos y medidas que pone para mejorar la seguridad ligada a los empleados, sin embargo, es el sector que menor puntuación respecto a Comportamiento en seguridad.

Tener en cuenta la motivación que mueve al cambio de comportamiento en los empleados es uno de los valores con peor puntuación a nivel general, excepto en el sector energético, que lo tiene en consideración a la hora de generar las campañas de concienciación.

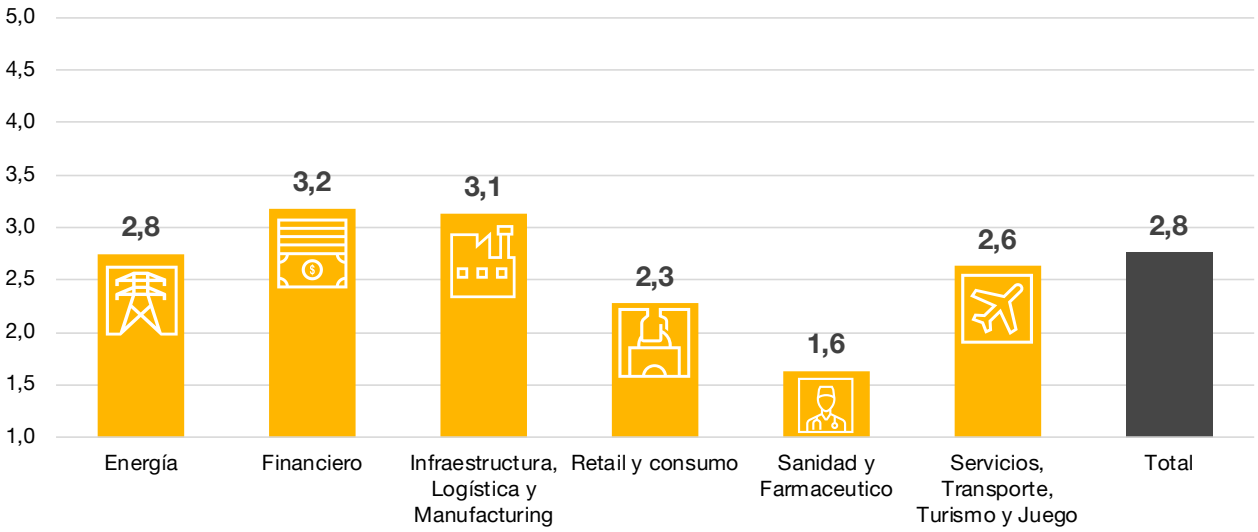
Gráfico 14 **Comparativa para el dominio de Comportamiento según sector**



Resultados relevantes en el ámbito de presupuesto

Este ámbito analiza la existencia de partidas presupuestarias diferenciadas para dinamizar iniciativas que aumenten la cultura de ciberseguridad.

Gráfico 15 **Medición ámbito de Presupuesto**



Datos destacados

- El presupuesto medio aplicado a formación y concienciación se corresponde con un **9%** del presupuesto en Seguridad de la Información de la Compañía.
- El **90%** de las compañías declara que ha crecido el presupuesto en seguridad en los últimos años.
- El **50%** de las compañías no dispone de presupuesto específico para formación en seguridad.
- Un **75%** de las compañías sí dispone de presupuesto específico o diferenciado para concienciación en seguridad.
- El **60%** de las compañías ha incrementado el presupuesto en formación y concienciación en los últimos años.
- El **64%** de la compañía considera que el presupuesto aplicado en formación y concienciación es escaso para la importancia de dicho ámbito en la seguridad de la compañía.
- El sector financiero, junto con los sectores conjuntos de infraestructura, logística y Manufacturing, destacan en los aspectos medidos en el ámbito de "Presupuesto" al disponer de forma más generalizada de un presupuesto específico en formación y en concienciación, y haberse producido un aumento material del presupuesto en los años anteriores.

Perspectiva de futuro

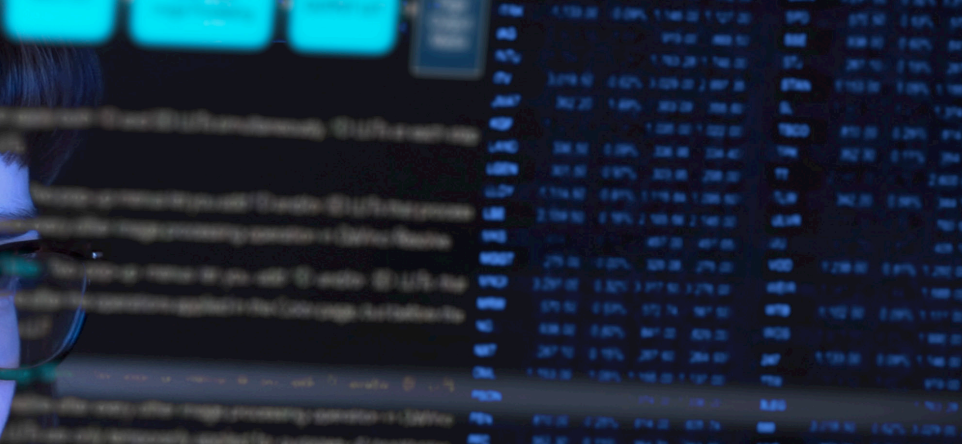
En la sección de perspectiva futura se abordan preguntas ligadas con la opinión, sentimiento o intención de cada una de las organizaciones encuestadas. A continuación, se muestran los resultados más relevantes sobre dichas cuestiones.

Estrategia

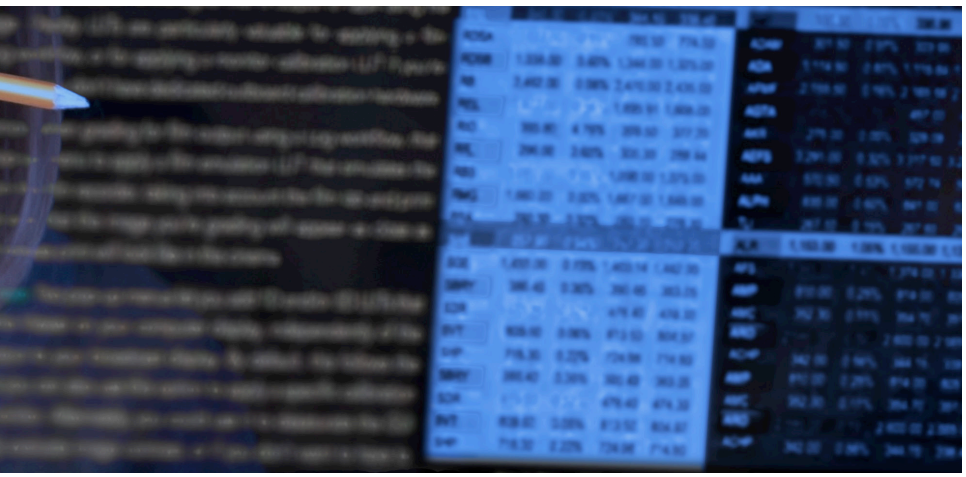
- El **86%** de las compañías considera que no existe una cultura de ciberseguridad en la organización o bien esta debería de mejorarse.
- La reducción del presupuesto, la diminución del apoyo de la Alta Dirección y la mala imagen del departamento de seguridad son las principales amenazas que consideran las empresas que pueden dificultar la cultura de ciberseguridad en la organización.
- El **36%** de las compañías considera que el presupuesto es muy reducido. El **32%** considera que es recomendable mejorar, mientras que el **32%** considera que dispone de un presupuesto adecuado.
- El **50%** de las compañías creen que la crisis del coronavirus ha influido positivamente en aumentar la cultura de ciberseguridad, mientras que sólo el **4%** de las compañías que ha influido negativamente en la cultura.
- Sólo el **12%** de las compañías han realizado entrenamiento en gestión de crisis para los comités oportunos. Sin embargo, el **70%** de las compañías tiene planificado o está considerando realizar entrenamiento de gestión de crisis a la Alta Dirección.

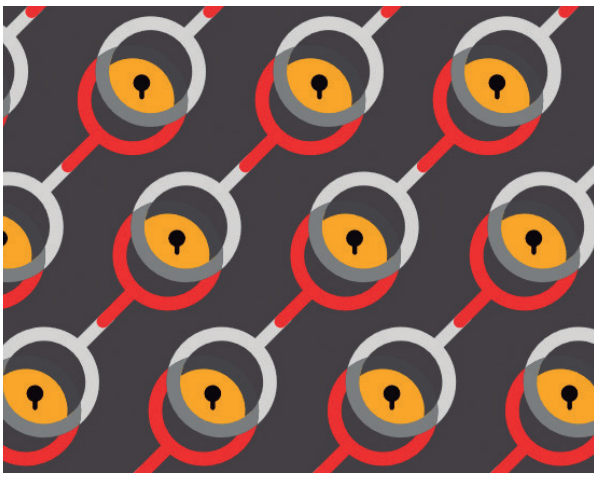
Conocimiento

- El **55%** de las compañías creen que es necesario disponer de un rol ligado con la formación y la concienciación dentro de la Compañía. De igual forma, el **41%** de las compañías ya disponen o están considerando disponer de una persona con un rol ligado directamente a la formación y la concienciación.
- El **32%** de las compañías tienen un plan de formación actualmente, el **41%** lo tienen planificado o lo están considerando, y sólo el **27%** de las compañías no han considerado tener un plan de formación.
- Sólo el **14%** de las compañías disponen de métodos de medición del conocimiento de los especialistas en seguridad. Y el **61%** de las compañías tiene planificado o está considerando establecer métodos de medición del conocimiento en seguridad de los especialistas.
- El **23%** de las compañías ya están haciendo entrenamiento de respuesta ante incidentes para los equipos técnicos de respuesta.



5





Comportamientos

- El **93%** de las compañías considera que la concienciación de los empleados es una medida relevante o muy relevante.
- El **55%** de las compañías consideran que se infravalora la importancia de la concienciación en seguridad.
- El **61%** de las compañías ya tienen o está planificado tener un Plan de Concienciación en seguridad para los empleados. Solo el **5%** restante no considera relevante tener un plan de concienciación.
- Sólo el **11%** de las compañías tienen un método de medición de la concienciación.
- Sólo el **27%** de las compañías ya han realizado iniciativas de concienciación a la Alta Dirección, mientras que **68%** tiene planificado o está considerando realizar iniciativas de concienciación a la Alta Dirección.
- El **48%** de las compañías ya está realizando entrenamiento de detección de fraude y amenazas a los empleados.

Conclusiones y percepciones

La cultura de ciberseguridad en las compañías debe involucrar a todos dentro de la organización, y debe de considerar actores externos a esta. Cada miembro es responsable de sus prácticas, y es importante que esto se fomente a través de un refuerzo positivo. Las personas deben de disponer de las herramientas y la capacitación adecuadas para cumplir con las políticas y tomar decisiones seguras en su día a día. La cultura de ciberseguridad por tanto debe integrarse en las tareas diarias de las personas.

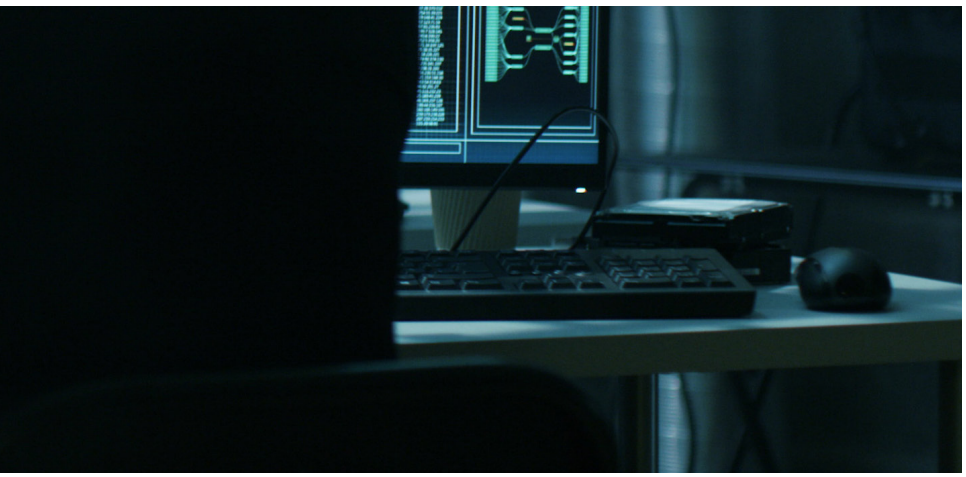
Se necesita capacitación, conciencia, promoción y medición constantes para construir una cultura de ciberseguridad sólida. El compromiso con los empleados garantizará su participación en la construcción de defensas sólidas contra el delito cibernético. Idealmente, las actividades de formación, sensibilización y concienciación deberían ser variadas y abarcar desde campañas de ingeniería social hasta eventos, formación para toda la familia o campañas para un riesgo específico, por nombrar algunos ejemplos que se presentaron en las entrevistas. La formación y la concienciación inclusivas y constante ayudarán a solidificar una cultura de ciberseguridad adecuada.

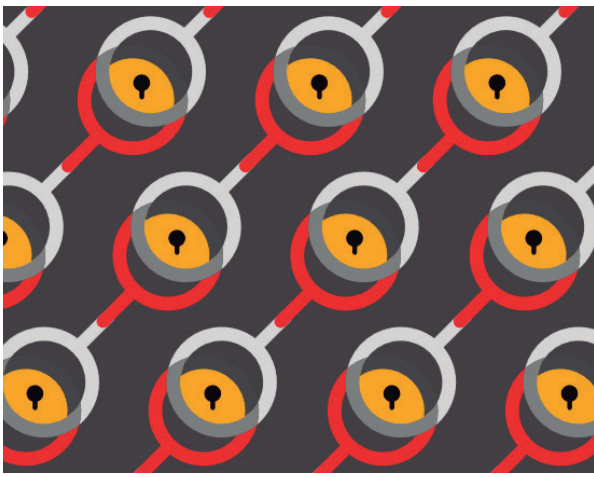
Lo que ha quedado patente, es que el ingreso económico de las compañías está relacionado con la cultura de ciberseguridad de forma directa. Cuanto mayor es el ingreso económico de las compañías, mejor puntuación se ha obtenido en cultura de ciberseguridad, tanto para el dominio de Estrategia, como para los dominios de Conocimiento y Comportamiento.

En el ámbito de la resiliencia y gestión de crisis las compañías tienen un nivel de cultura más elevada que el resto de los ámbitos, demostrando que la preocupación en la gestión de crisis y los incidentes de seguridad es un ámbito prioritario en todos los sectores.

Sin embargo, lo que se ha podido observar es que el presupuesto medio aplicado a formación y concienciación se corresponde, de media, solo con un 9% del presupuesto en Seguridad de la Información de la compañía. Esto quiere decir que el camino por recorrer hacia la obtención de una cultura de ciberseguridad óptima y deseada en las organizaciones es largo.

6





Lo que más preocupa es que las compañías actuales no disponen de métodos de medición de la cultura, así como tampoco realizan medición de la formación y capacitación, lo que impide establecer procesos gestionados que permitan medir la mejora asociada a las campañas realizadas y los cursos de formación y capacitación que se ofrece a los empleados. Por otro lado, las campañas de concienciación no contemplan factores motivacionales al cambio de comportamiento, estando basadas en la repetición de las buenas prácticas de seguridad como base de concienciación. Esto responde con una madurez baja en cultura, ya que al no tener en cuenta las motivaciones de los empleados al cambio y entender la importancia de valorar ese factor humano en la concienciación, el impacto de las iniciativas de concienciación queda muy reducido en su eficacia.

Esto lo podemos observar de forma general en que las compañías invierten en medidas de seguridad para que el empleado pueda mantener la seguridad de la información (destructoras de papel, políticas de mesas limpias, espacios para mantener conversaciones confidenciales,…). Es decir, cada vez tiene más presente la necesidad de invertir en garantizar la seguridad de los activos, pero estas medidas no son eficaces por una falta de conciencia de los empleados, de seguimiento del uso o de madurez en la gestión del cumplimiento de la normativa.

© 2021 PricewaterhouseCoopers Asesores de Negocios, S.L.. Todos los derechos reservados. “PwC” se refiere a PricewaterhouseCoopers Asesores de Negocios, S.L., firma miembro de PricewaterhouseCoopers International Limited; cada una de las cuales es una entidad legal separada e independiente.