BARÓMETRO ciberseguridadTIC

Estado de Ciberseguridad en España 2024

SECURE IT by LKS Next

Introducción

Dada la creciente sofisticación de los ataques y las estrictas regulaciones, la ciberseguridad ha pasado a ser una prioridad estratégica para empresas de todos los tamaños y sectores.

Este estudio tiene como objetivo ofrecer una visión sobre las prácticas, tecnologías y preocupaciones actuales de las empresas en relación con la ciberseguridad. A través de una serie de preguntas enfocadas en la adopción de tecnologías de seguridad, la preparación frente a amenazas y el cumplimiento de normativas, buscamos entender cómo las organizaciones están enfrentando los riesgos y se preparan para los desafíos futuros.

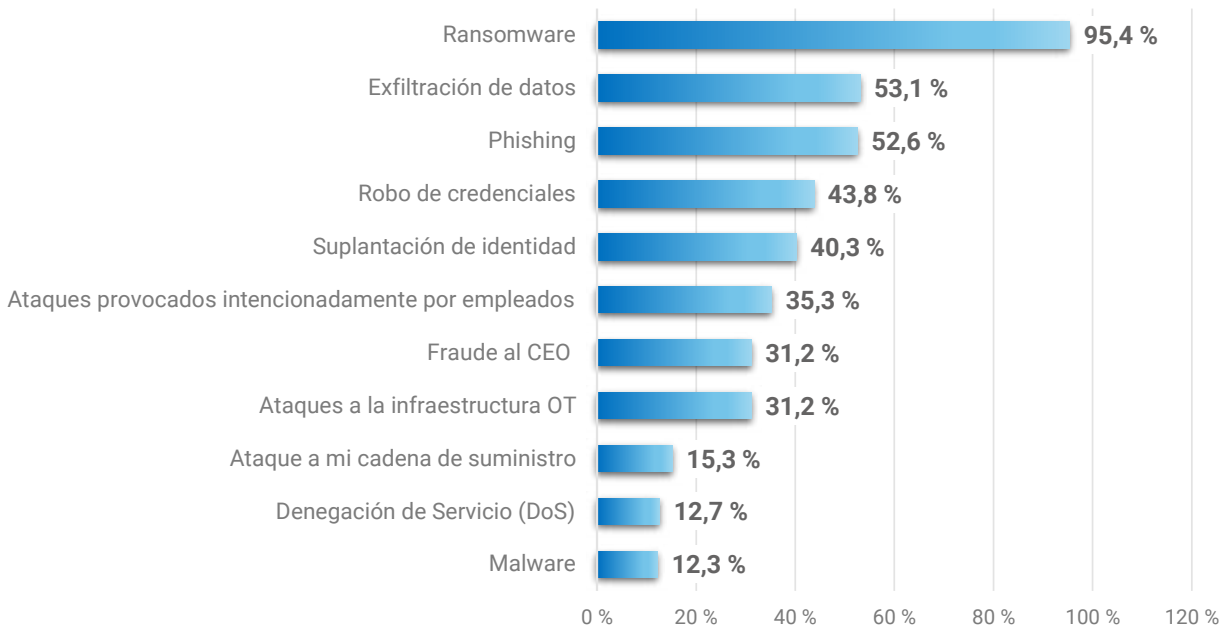
Los resultados de la encuesta reflejan que las empresas son cada vez más conscientes de la importancia de la seguridad, al tiempo que revelan áreas en las que aún hay margen de mejora. En primer lugar, la implementación de tecnologías clave, como la protección de endpoints o la seguridad en la nube, así como el uso de soluciones avanzadas ocupa un lugar destacado en las estrategias de defensa. Sin embargo, también se observa que, aunque muchas empresas reconocen la necesidad de cumplir con normativas y estándares internacionales de seguridad, como la Directiva NIS2 y la Ley de Ciberresiliencia (CRA), aún persiste cierta incertidumbre y falta de acción en cuanto a su implementación efectiva.

Otro hallazgo relevante es la creciente preocupación por los ataques dirigidos a personas, como el phishing, el robo de credenciales y el fraude al CEO, lo que destaca la necesidad de fortalecer la formación y concienciación en toda la organización. Si bien la mayoría de las empresas están adoptando medidas preventivas, se observa que hay un fuerte enfoque en la ciberseguridad externa, sin descuidar las amenazas internas, como los ataques intencionados por empleados.

Las empresas son cada vez más conscientes de la importancia de la ciberseguridad

Este informe proporciona una imagen clara de las tendencias actuales en ciberseguridad, las tecnologías implementadas y las principales amenazas que preocupan a las empresas. También subraya la importancia de tomar medidas proactivas, tanto en términos de tecnología como de formación y cumplimiento, para garantizar la resiliencia en un mundo cada vez más digitalizado y vulnerable.

¿Qué tipo de ataque te preocupa más?



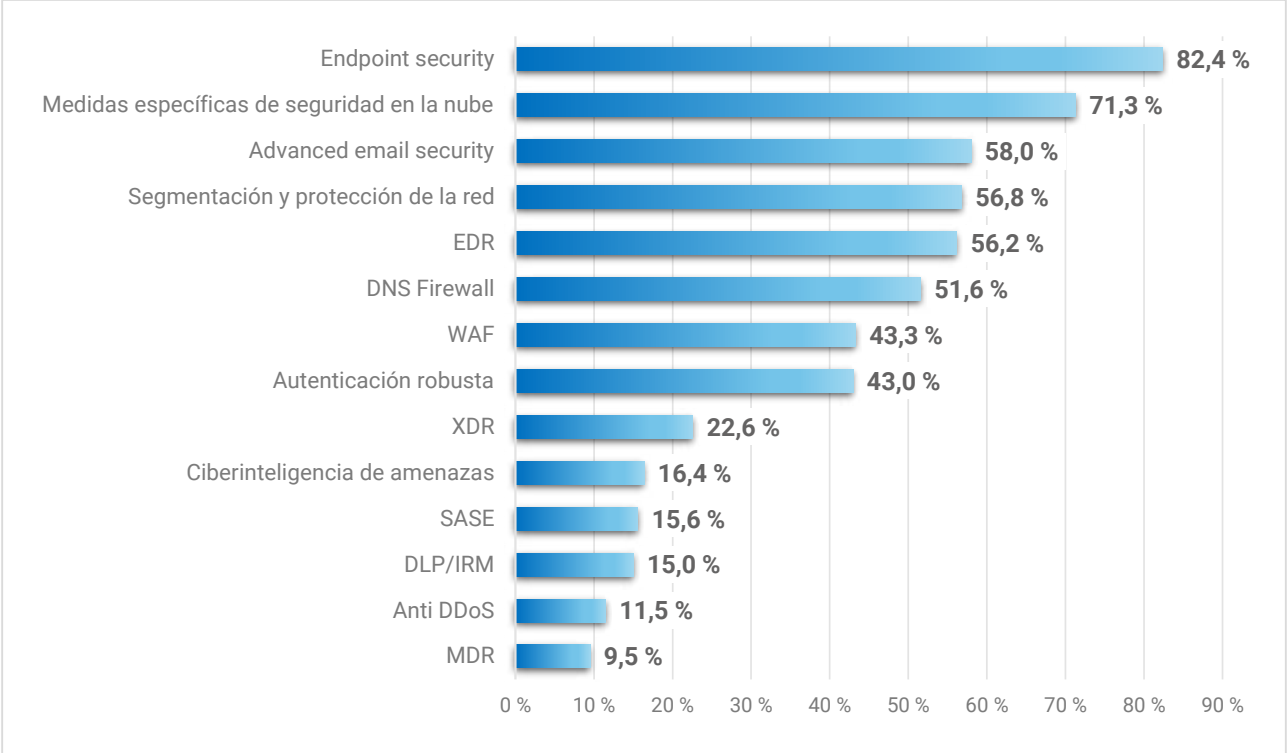
La encuesta revela que el ransomware destaca como la amenaza más significativa, identificada por el 95,4 % de los encuestados. Este tipo de ataque representa un grave riesgo debido a la pérdida de datos, los costos financieros y la interrupción de las operaciones normales de las empresas.

Además del ransomware, los ataques que explotan la ingeniería social, como el phishing (52,6 %) y la exfiltración de datos (53,1 %), son también una gran preocupación. Estos ataques se basan en engañar a los usuarios para obtener acceso a sistemas o información confidencial. La suplantación de identidad (40,3 %) y el robo de credenciales (43,8 %) siguen de cerca, lo que subraya el creciente enfoque de los ciberdelincuentes en obtener acceso a las cuentas de los empleados y usuarios.

Otras amenazas significativas incluyen los ataques internos, provocados intencionadamente por empleados (35,3 %), los fraudes al CEO (31,2 %) y los ataques a la infraestructura OT (31,2 %). Estos últimos resultan especialmente preocupantes debido a las posibles interrupciones operativas y riesgos de seguridad.

Finalmente, los ataques a la cadena de suministro (15,3 %) reflejan la creciente complejidad de las redes empresariales y la necesidad de asegurar a todos los actores involucrados.

¿Qué tipo de tecnologías tienes implantadas en tu empresa?



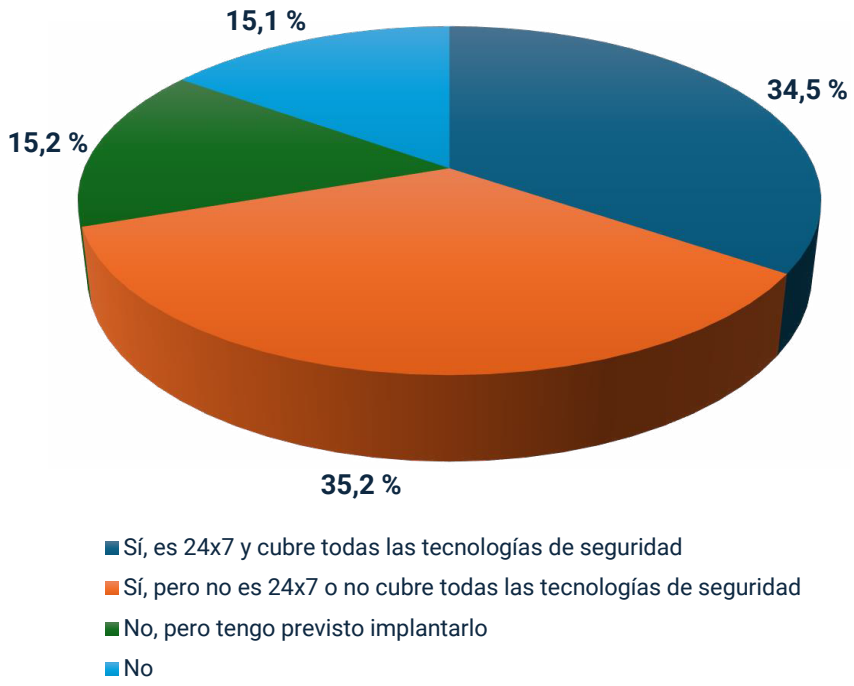
La mayoría de las empresas han adoptado medidas de seguridad de endpoints (82,4 %), convirtiéndolas en la primera línea de defensa. Además, el creciente uso de servicios en la nube ha llevado a un aumento en las medidas de seguridad en la nube (71,3 %).

Para detectar y prevenir amenazas de manera proactiva, muchas organizaciones utilizan EDR (56,2 %), segmentación de redes (56,8 %) y protección avanzada del correo electrónico (58 %). Asimismo, tecnologías más avanzadas como XDR (22,6 %) y ciberinteligencia de amenazas (16,4 %) están siendo implementadas para una detección y respuesta más rápida ante incidentes.

Para proteger las aplicaciones web y las comunicaciones en línea, las empresas están adoptando DNS Firewall (51,6 %) y WAF (43,3 %). Además, se observa un creciente interés en la autenticación robusta (43 %) y SASE (15,6 %).

Aunque con una adopción más baja, tecnologías como DLP/IRM (15 %) y Anti DDoS (11,5 %) siguen siendo relevantes para la protección de datos y la mitigación de ataques DDoS.

¿Cuentas con un Centro de Operaciones de Seguridad que gestione las tecnologías anteriores?

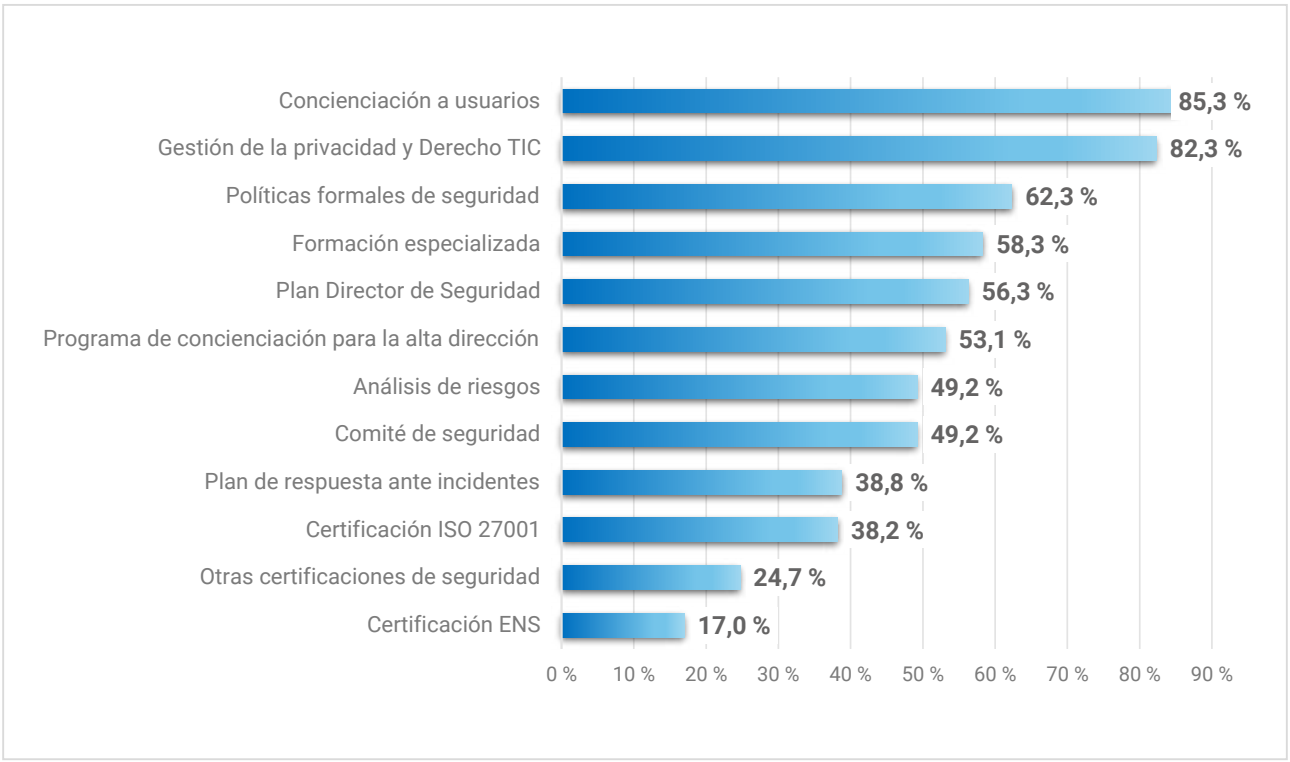


Los resultados de la encuesta muestran una adopción variada de los Centros de Operaciones de Seguridad (SOC). Un 34,5 % de las organizaciones cuentan con un SOC que opera las 24 horas del día, los 7 días de la semana, y cubre todas las tecnologías de seguridad, lo que indica un alto compromiso con la seguridad. Sin embargo, un 35,2 % tiene un SOC con limitaciones en cuanto a horario o cobertura, sugiriendo que, aunque hay una estructura de seguridad en marcha, no está completamente optimizada.

Un 15,2 % de las empresas planea implementar un SOC en el futuro, lo que refleja una creciente conciencia sobre la importancia de estos centros especializados. Por otro lado, un 15,1% no cuenta con un SOC, lo que indica que aún dependen de otros métodos de gestión de seguridad.

En resumen, los resultados de la encuesta realizada muestran que aunque un porcentaje significativo de empresas (alrededor del 70 %) ya dispone de un SOC o tiene planes de implementar uno, hay áreas de oportunidad en cuanto a la cobertura y la disponibilidad de estos centros, lo que podría mejorar la capacidad de respuesta ante incidentes y amenazas.

Acciones implementadas para el gobierno de la ciberseguridad



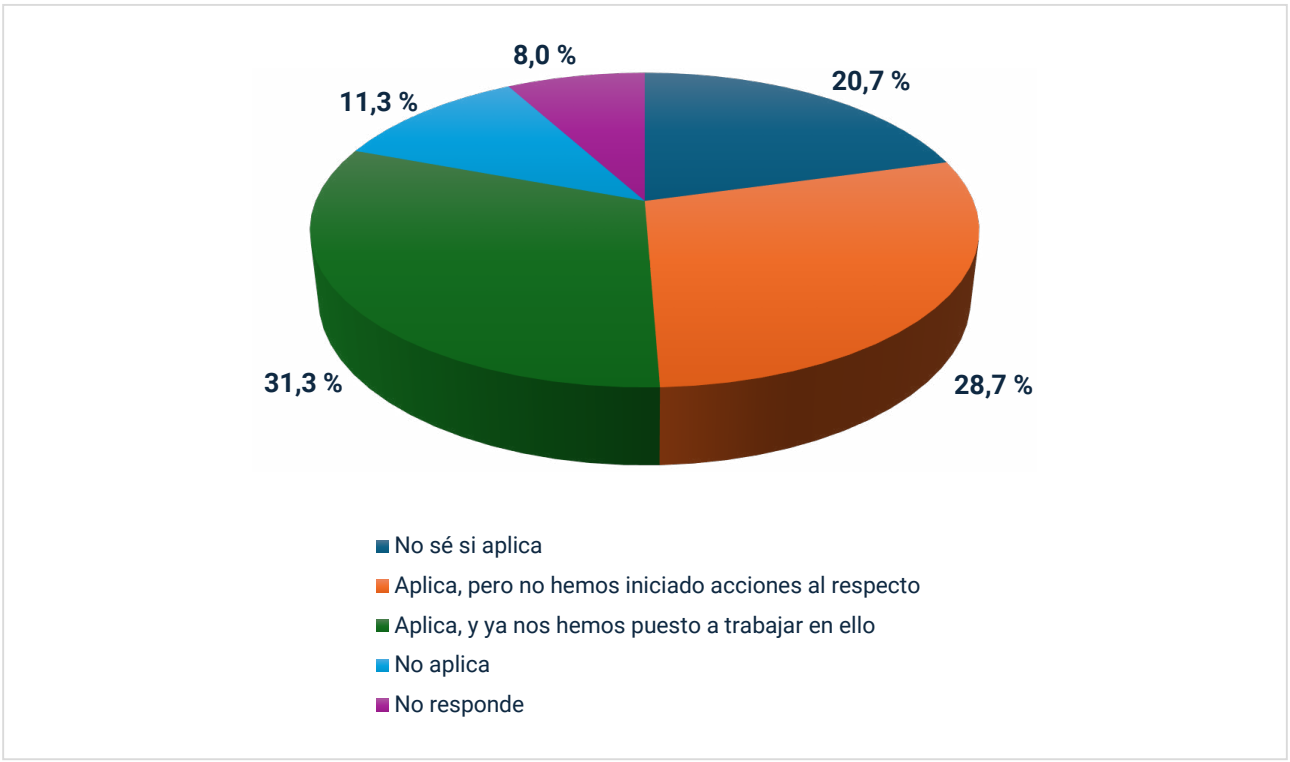
Los resultados muestran un fuerte enfoque de las organizaciones en fortalecer el gobierno de la ciberseguridad. Destaca la importancia que se le da a la concienciación y formación de los usuarios (85,3 %) y a la gestión de la privacidad y el cumplimiento normativo (82,3 %). Estas dos áreas son las más comúnmente implementadas, reflejando un creciente compromiso con la protección de datos y la prevención de incidentes.

Además de estas áreas, otras iniciativas también están siendo adoptadas significativamente, como el Plan Director de Seguridad (56,3 %) y la formación especializada (58,3 %), lo que demuestra un esfuerzo por construir una cultura de seguridad sólida.

Asimismo, un porcentaje considerable de empresas cuenta con un comité de seguridad (49,2 %) y realiza análisis de riesgos (46,3 %), lo que indica un enfoque proactivo y estructurado para la gestión de riesgos. También se han implementado planes de respuesta ante incidentes (38,8 %) y políticas formales de seguridad (62,3 %), reforzando la preparación ante posibles incidentes.

En lo que respecta a las certificaciones, la ISO 27001 (38,2 %) y la ENS (17 %) son las más comunes.

¿Sabes si la Directiva NIS2 aplica a tu empresa?



Un 20,7 % de las organizaciones encuestadas no sabe si la directiva les aplica, lo que indica una falta de claridad sobre los alcances de la normativa. Esto subraya la necesidad de mejorar la comunicación y educación sobre la ciberseguridad, especialmente en lo que respecta a las regulaciones europeas.

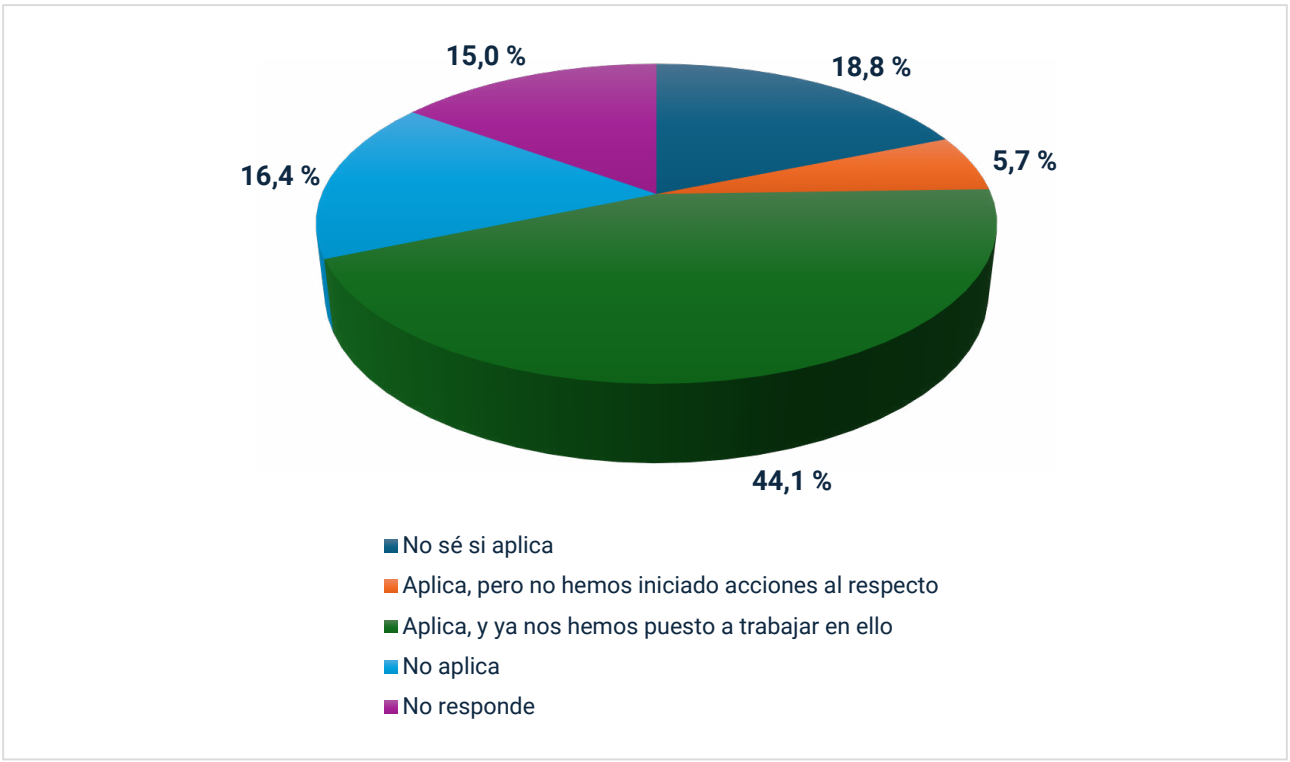
A pesar de conocer la aplicabilidad de la directiva, el 28,7% aún no ha actuado, posiblemente por falta de recursos u otras prioridades.

El 31,3% de las organizaciones ha tomado la iniciativa de alinear sus prácticas de seguridad con los requisitos de la NIS2, lo que indica una actitud proactiva ante la ciberseguridad.

Un 11,3 % considera que la directiva no les aplica, lo que podría indicar que no operan en sectores críticos. Sin embargo, este porcentaje relativamente bajo sugiere que la mayoría de las empresas, especialmente en sectores clave, reconocen la relevancia de la NIS2.

Finalmente, un 8 % no respondió a la pregunta, lo que podría reflejar una falta de información o interés en el tema.

¿Aplica el Reglamento de Resiliencia Operativa Digital (DORA) a tu organización?



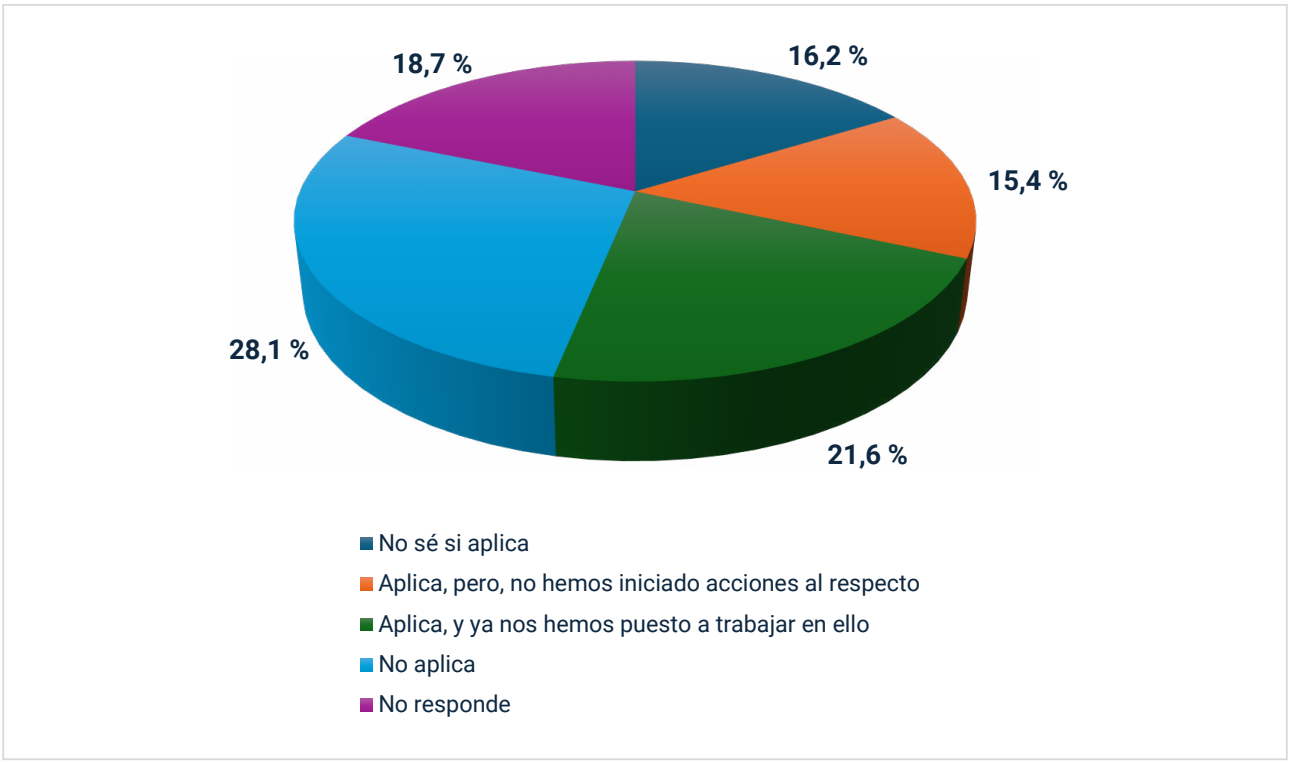
Un 18,8 % de los encuestados no sabe si el reglamento les aplica, lo que señala una necesidad de mejorar la comunicación y la formación sobre DORA.

A pesar de que un 5,7 % reconoce que DORA les aplica, aún no han iniciado acciones para cumplirla. Esto sugiere que, aunque existe conciencia, la implementación de medidas concretas se ha retrasado, posiblemente debido a falta de recursos o priorización.

Por otro lado, un 44,1 % indica estar trabajando activamente en el cumplimiento de DORA, lo que es una señal positiva. Estas organizaciones demuestran un alto nivel de preparación y proactividad para enfrentar los desafíos de la resiliencia operativa digital.

Un 16,4 % considera que DORA no les aplica, y un 15 % no respondió a la pregunta.

¿Sabes si la Ley de Ciberresiliencia (CRA) aplica a tu empresa?



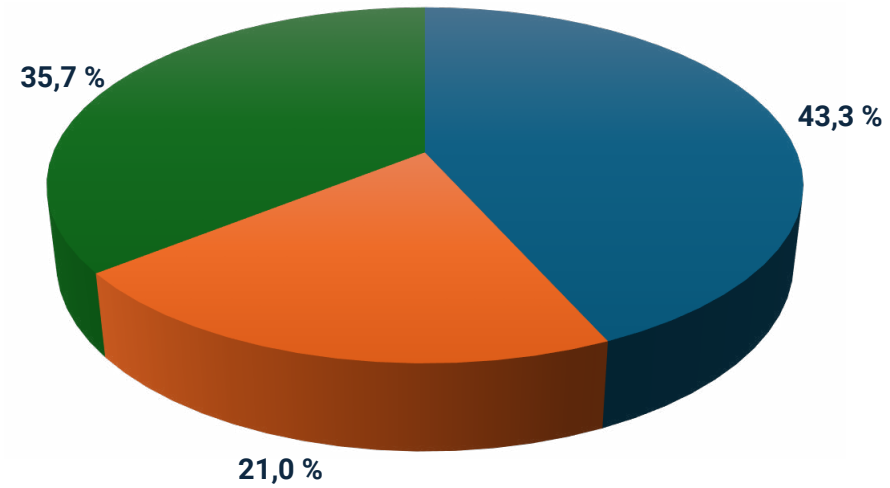
Un 16,2 % de los encuestados no está seguro de si la ley aplica a su empresa, lo que indica una falta de claridad sobre los alcances de la normativa. Esto subraya la necesidad de mejorar la comunicación y la educación sobre la ciberseguridad, especialmente en lo que respecta a esta nueva ley.

Aunque el 15,4 % sabe que la ley les afecta, la falta de acciones concretas sugiere que esta no es una prioridad para ellos.

Por otro lado, un 21,6 % afirma estar trabajando activamente en el cumplimiento de la CRA, lo que es una señal positiva.

El 28,1 % cree que la normativa no les resulta aplicable. Por otro lado, un 18,7 % optó por no responder a la pregunta, lo que subraya la necesidad de mejorar la comunicación y formación sobre las implicaciones de la ley para garantizar una mayor claridad y cumplimiento en el sector.

¿Cómo crees que impacta la situación geopolítica en la ciberseguridad de tu empresa?



Los resultados de esta encuesta reflejan la diversidad de percepciones que existen en torno al impacto de la situación geopolítica en la ciberseguridad de las empresas.

Por un lado, más del 43 % de los encuestados considera que su actividad empresarial las coloca en el foco de los ciberdelincuentes, lo que sugiere una creciente conciencia de los riesgos, posiblemente ligados a la digitalización y la exposición en línea. Sin embargo, un 35,7 % de los participantes no ve una conexión directa entre la situación geopolítica y los desafíos de ciberseguridad, lo que podría señalar una falta de percepción de amenaza inmediata en ciertos sectores.

Mientras tanto, un 21% considera que los conflictos internacionales, como los de Rusia y Ucrania o Israel y Palestina, representan una amenaza generalizada. Este porcentaje refleja el reconocimiento de los impactos indirectos que los conflictos pueden tener sobre la seguridad global, aunque no todos los encuestados lo perciban como algo que afecta a su entorno empresarial de manera directa.

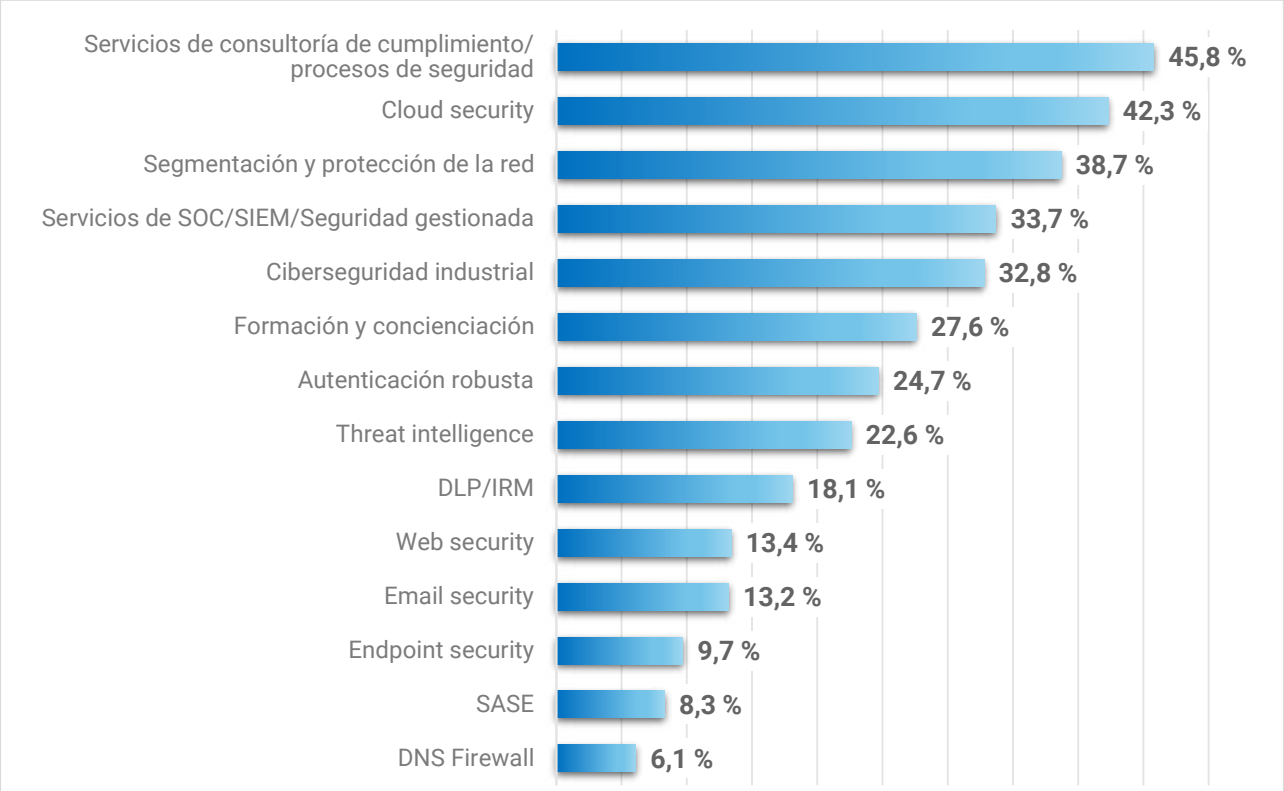
¿Haces uso en tu empresa de herramientas de IA Generativa?

Los resultados de la encuesta revelan una adopción notable de herramientas de IA Generativa en las empresas, aunque con diferentes enfoques respecto a su implementación y gestión. Un 22,6 % de los encuestados asegura que su empresa no solo utiliza herramientas de IA Generativa, sino que también controla activamente su uso y seguridad, lo que indica una alta preocupación por la gestión responsable y segura de estas tecnologías. Sin embargo, un porcentaje más alto, el 32,7 %, reconoce usar estas herramientas pero sin medidas específicas de control, lo que sugiere que la adopción está ocurriendo rápidamente, pero la seguridad y regulación aún no están completamente implementadas en muchas organizaciones.

Un 21,5 % de los encuestados indica que no están usando IA Generativa en este momento, pero tienen planes de implantarla. Mientras tanto, el 14,4 % de las empresas no utilizan estas herramientas y no tienen planes inmediatos de hacerlo.

Finalmente, un 8,8 % de los encuestados optó por la opción de "No sabe/no contesta", lo que podría reflejar falta de conocimiento sobre las herramientas de IA Generativa o incertidumbre sobre su implementación dentro de la empresa.

¿Cuáles son los siguientes proyectos que tienes previstos?



Los datos muestran un énfasis especial en la protección de datos en la nube y el cumplimiento normativo. El proyecto más destacado es la consultoría de cumplimiento y procesos de seguridad (45,8 %), lo que subraya la importancia de alinear las estrategias de seguridad con las regulaciones vigentes. Esto refleja una creciente conciencia sobre los riesgos legales y la necesidad de proteger los datos de manera adecuada.

A continuación, se priorizan proyectos relacionados con la seguridad en la nube (42,3 %) y la segmentación y protección de la red (38,7 %). También se observa una creciente preocupación por la ciberseguridad industrial (32,8 %), lo que demuestra un enfoque más integral que incluye la protección de sistemas críticos.

Proyectos como la autenticación robusta (24.7 %) y la inteligencia de amenazas (22,6 %) muestran un enfoque en la prevención y detección de amenazas. Asimismo, la protección de datos (DLP/IRM, 18,1 %) y la seguridad del correo electrónico y web (13,2 % y 13,4 %, respectivamente) siguen siendo prioridades.

Por último, aunque con menor prioridad, proyectos como endpoint security (9,7 %) y DNS firewall (6,1 %) también se consideran parte de la estrategia general.