Estado de CIBERSEGURIDAD en España

Elaborado por:

itRESEARCH

Para:

Secure&IT by LKS Next

www.secureit.es

Estado de ciberseguridad en España

Secure&IT by LKS
www.secureit.es

Este documento busca conocer la situación de las empresas a la hora de hacer frente a los ciberataques y ciberamenazas, cada vez más numerosas y más sofisticados, así como la importancia de las labores de formación y concienciación, o qué tipo de amenazas preocupan más.

Ahora más que nunca, la ciberseguridad es esencial para nuestro futuro; después de todo, es vital para proteger todo aquello en lo que confiamos hoy. Sin embargo, a raíz de las migraciones masivas a la nube y la transformación digital, muchas organizaciones aún no han alcanzado la cima de sus operaciones de seguridad debido a algunos desafíos clave, como un panorama de amenazas en constante evolución y una creciente complejidad de los entornos híbridos y de múltiples nubes.

IT Digital Security, en colaboración con Secure&IT, ha realizado una encuesta entre profesionales españoles durante los meses de junio a septiembre de 2022 para conocer qué tipo de amenaza preocupa más a las empresas, qué aspecto se valora más a la hora de trabajar en una empresa, qué tecnologías se tienen implementadas o cuáles son las tendencias de inversión en ciberseguridad.

Por otra parte, existe una preocupación generalizada de que la fuerza laboral aún no está preparada para hacer frente a las ciberamenazas con éxito debido a la falta de experiencia en ciberseguridad y TI a nivel local. Los planes de formación y conciención, ¿interesan a las empresas? ¿tienen planes de inversión?

El objetivo de este estudio es conocer la situación de las empresas a la hora de hacer frente a los ciberataques y ciberamenazas, cada vez más numerosas y más sofisticados, así como la importancia de las labores de formación y concienciación, o qué tipo de amenazas preocupan más.

Secure&IT by LKS
www.secureit.es

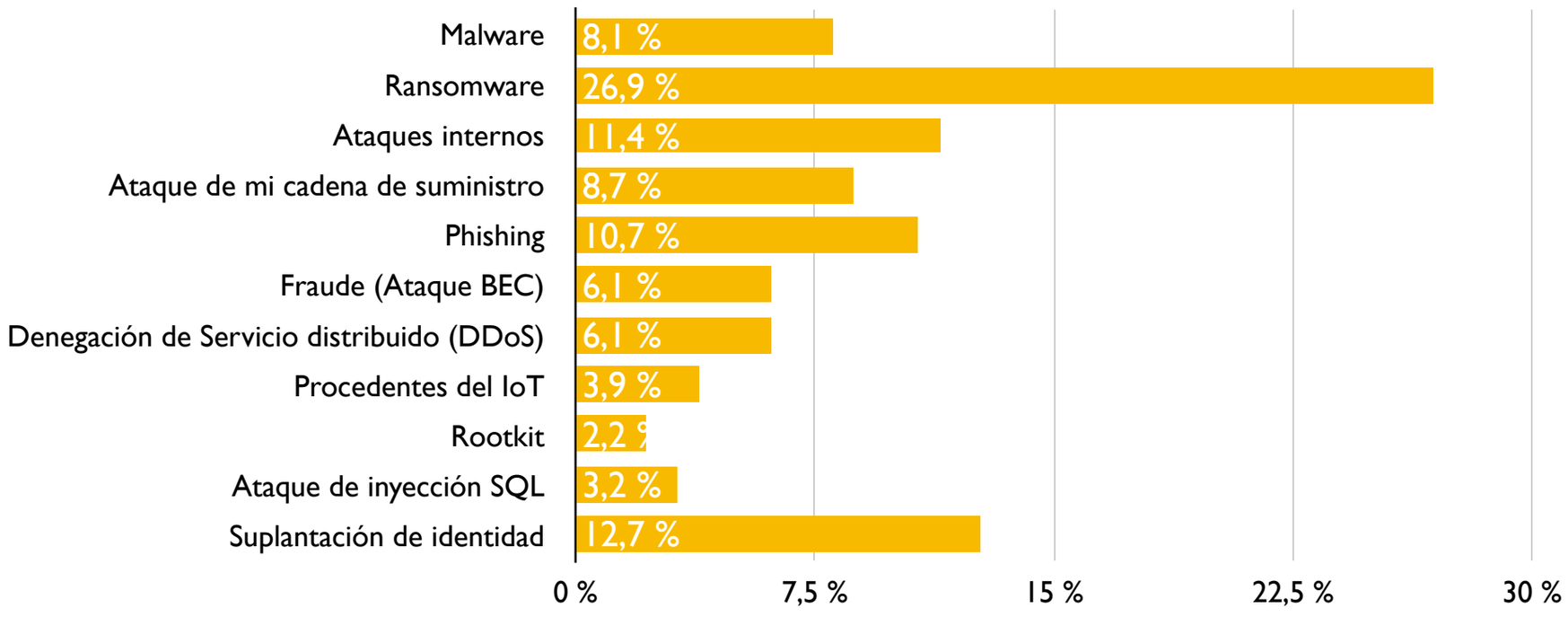
"Hay que considerar al empleado como un aliado. Y para que alguien sea un aliado en tu empresa y en cuestiones de seguridad de la información y de protección de datos, que para mí van totalmente de la mano, es fundamental enseñar"

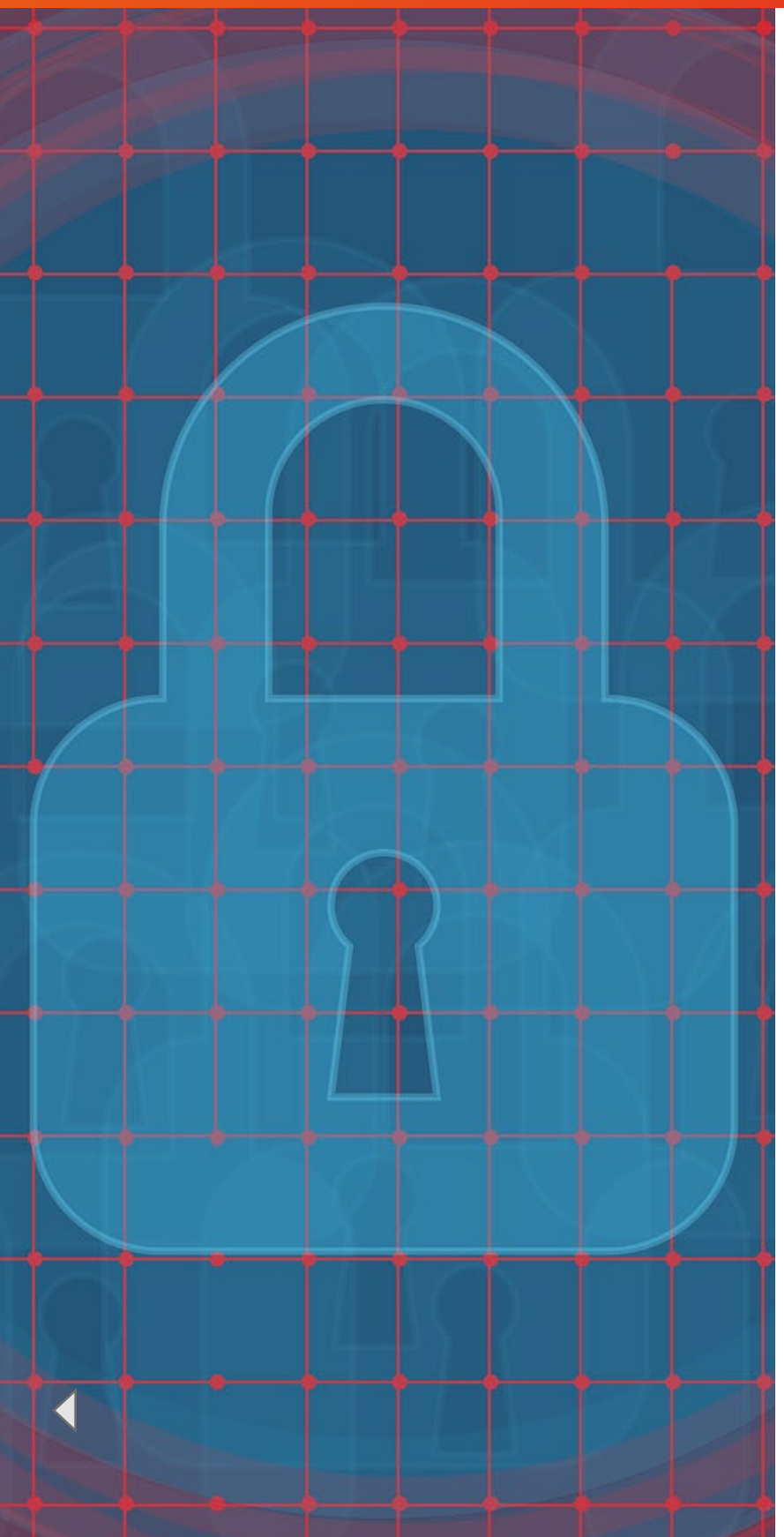
Gustavo Lozano García, CISO, ING

¿Qué tipo de ataque le preocupa más?

Los ciberataques se han multiplicado en los últimos años, pero hay amenazas que preocupan más que otras. El ransomware es, desde hace unos años, una de las que más preocupa. Indican los expertos que el ransomware ha descendido, pero a cambio de ser más dirigido y más peligroso. De once amenazas propuestas, un 26,9% de las respuestas han seleccionado el ransomware como el tipo de ataque que les preocupa más, seguido de la suplantación de identidad (12,7%), los ataques internos (11,4%) o el phishing (10,7%).

Los rootkits, o paquetes de software malicioso diseñados para permitir el acceso no autorizado a un equipo o a otro software, que fueron muy populares hace una década, parecen estar pasando a mejor vida. Además de utilizados por los ciberdelincuentes para acceder a los equipos, fueron utilizados por avezados usuarios para hacer lo que se denominaba un "jailbreak" en iOS o "rooting" en Android con el fin de obtener permisos de superusuario, algo que el fabricante bloquea principalmente por razones comerciales, pero también para proteger la seguridad del dispositivo. La utilización de este tipo de equipos modificados en entornos empresariales fue un dolor de cabeza para los responsables de seguridad. Hoy, sólo preocupa al 2,2%.



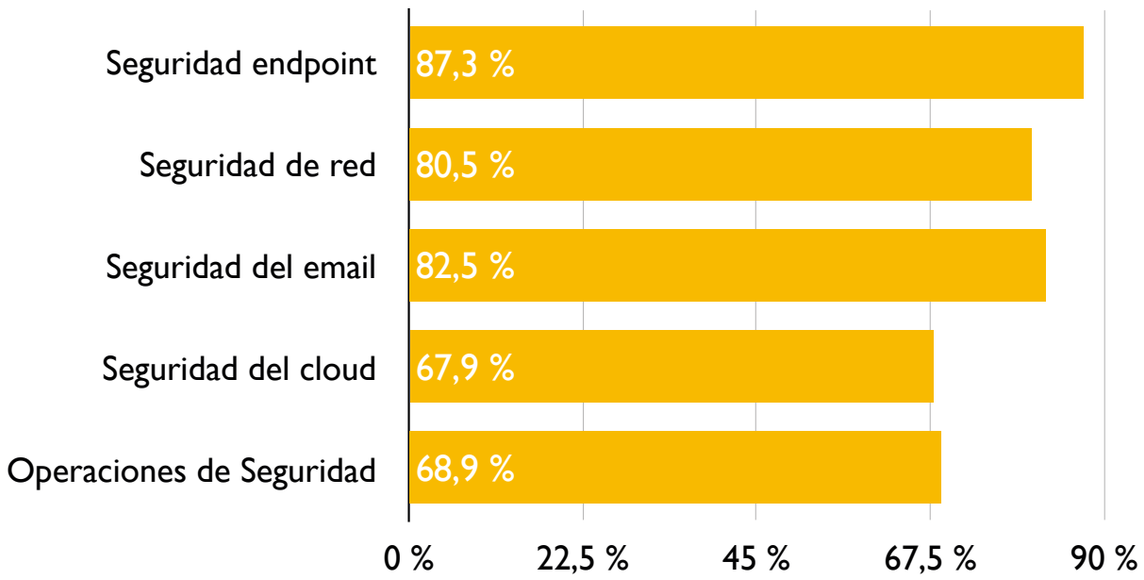


¿Qué tipo de tecnologías tiene implantadas?

En este estudio se plantearon una serie de tecnologías de seguridad básicas que toda empresa debería, en mayor o menor medida, tener implementadas. Los datos recogidos no sorprenden.

Un 87,3% de los encuestados tienen implementaciones de seguridad endpoint en sus empresas. También es amplia la adopción de seguridad de red, existente en el 80,5% de los negocios, pero preocupa más la seguridad del email, que está disponible en el 82,5% de las empresas españolas. No es mala opción teniendo en cuenta que el correo electrónico es uno de los principales vectores de ataque utilizados por los ciberdelincuentes.

La seguridad del cloud (67,9%) y las Operaciones de Seguridad (68,9%) (SecOps), que mantienen y restauran las garantías de seguridad del sistema a medida que los adversarios directos lo atacan, también son tecnologías utilizadas, aunque en menor medida.



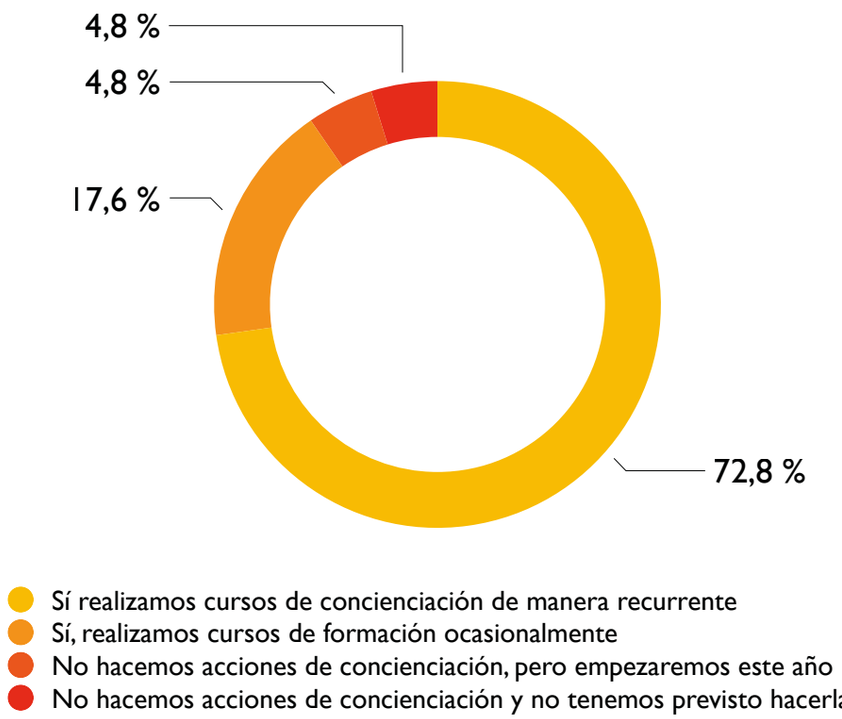
Formación y concienciación del usuario

Por muy buenas tecnologías que una empresa tenga implementadas, el error humano puede ser fatal. Hace años que los planes de formación y concienciación de los empleados forman parte de los planes de seguridad de muchas empresas.

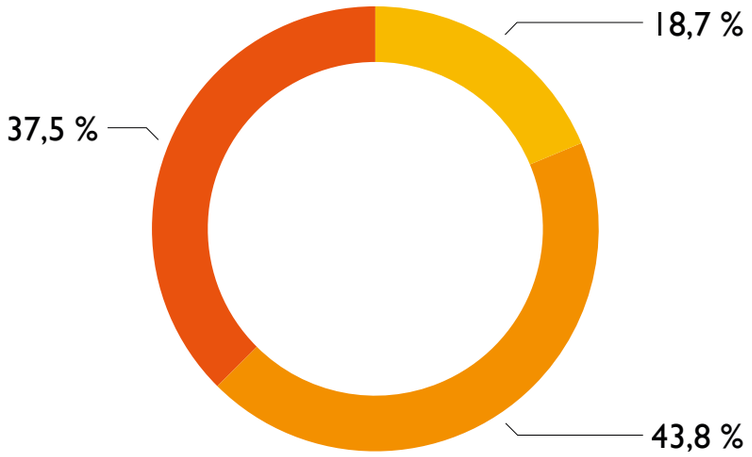
Entre otras cosas, estos planes ayudan a los usuarios a detectar un phishing que lleve a un robo de credenciales, que a su vez permita un acceso no autorizado, que termine en una brecha de seguridad, que deje escapar información sensible. Un desastre.

En el 90,4% de las empresas se realizan planes de formación y concienciación. Los más efectivos son los recurrentes, que son la opción del 72,8% de las empresas, mientras que un 17,6% opta por formación y concienciación de una manera más ocasional.

Del 9,6% de las empresas que aún no concienciación a sus empleados en ciberseguridad, la mitad planea hacerlo y la otra mitad no tiene intención de adoptarlo.



Estado de ciberseguridad en España



Asesoramiento externo

La ciberseguridad es un asunto complejo. No sólo desde el punto de vista tecnológico habida cuenta de la cantidad de herramientas que se utilizan, sino desde el punto de vista de normativas, más o menos dependiendo del sector en el que se trabaje.

Sólo el 18,7% de las empresas trabajan todo internamente, y un 81,3% buscan asesoramiento tecnológico y legal fuera de la empresa.

La mayoría, un 43,8% opta por solicitar asesoramiento en la parte legal y de cumplimiento, mientras que un 37,5% opta por solicitar asesoramiento en la parte tecnológica.

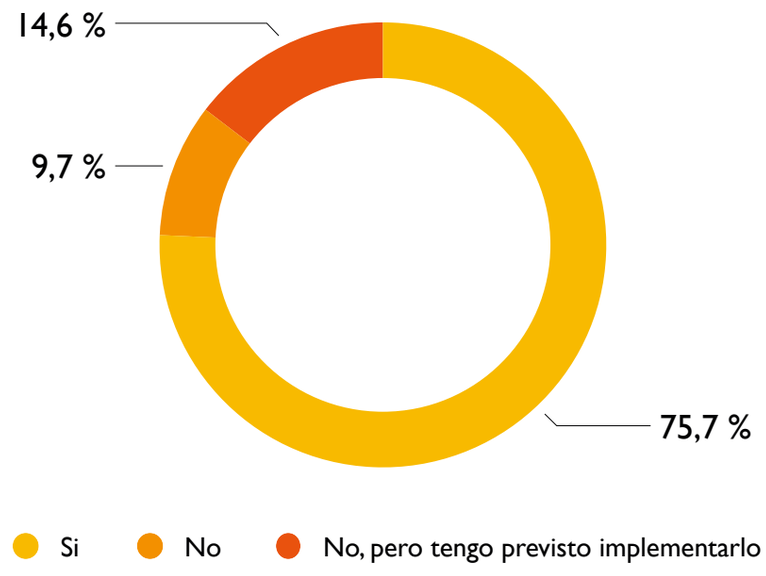
PCI DSS, HIPAA, GDPR, ISO… la lista de normativas que las empresas deben cumplir hoy en día es tan larga como tediosa. En cuanto a las tecnologías, ya sabemos lo rápido que avanzan.

¿Haces uso de servicios de monitorización de SOC?

El SOC, o centro de operaciones de seguridad, es el que ayuda a las empresas a tener el control sobre lo que está sucediendo con la seguridad de sus empresas. Está compuesto por una plataforma tecnológica y un equipo técnico y humano que está altamente cualificado y posee las herramientas necesarias para, monitorizar, analizar, prevenir y dar respuesta ante cualquier incidente de seguridad. Gracias al SOC se acelera y simplifica la detección de amenazas, la respuesta a incidentes y la gestión del cumplimiento normativo a las empresas.

Los sistemas de información generan millones de eventos y alertas desde los procedentes de sistemas de seguridad como el firewall, waf, IDS/IPS, control de accesos, etc., a los generados por otras plataformas o servicios, como ERP o el DNS. Por eso, los SOC se han convertido en parte indispensable de la operativa de seguridad. Así lo entienden, al menos el 75,7% de los profesionales encuestados, que aseguran hacer uso de servicios de monitorización de SOC.

Del 24,3% de empresas que no lo hacen, un 14,6% tiene previsto implementar este tipo de servicios.



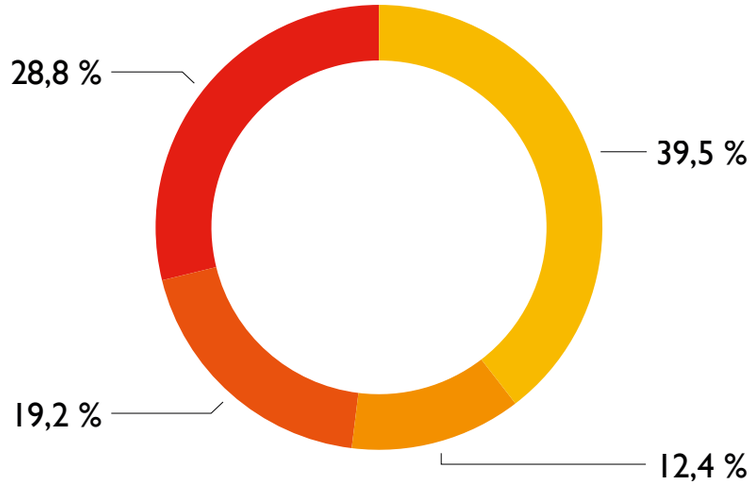
¿Qué aspectos valora más a la hora de trabajar en una empresa?

Tras el salario económico, la capacidad de teletrabajar es, para el 28,8% de los encuestados, el aspecto que más valora a la hora de trabajar en una empresa. No es tema baladí teniendo en cuenta que contratar y retener a profesionales del mundo de la ciberseguridad se está convirtiendo en un verdadero dolor de cabeza para las empresas.

La pandemia abrió las puertas al trabajo remoto, que por otra parte ya era más o menos habitual en muchas empresas. Ahora se avanza hacia lo híbrido, lo que supone un reto desde el punto de vista de la ciberseguridad.

Después del salario económico y la capacidad de trabar desde casa, la flexibilidad horaria es, para el 19,2% de los encuestados el tercer elemento a tener en cuenta a la hora de trabajar en una empresa.

Para un 12,4% también cuenta lo que se conoce como salario emocional, que incide directamente en el rendimiento de los profesionales y, por tanto, en la competitividad de la compañía. Aquí entra desde ofrecer un seguro médico, formación, servicio de cafetería gratis, etc.



- Salario económico
- Salario emocional (Seguro médico, Formación, servicio de cafetería...)
- Flexibilidad horaria
- Capacidad de teletrabajo

Estado de ciberseguridad en España

Niveles de inversión

Lo último que se les ha pedido a los encuestados para este estudio es que indiquen los niveles de inversión en ciberseguridad para este año que, según datos de un informe de IDC alcanzará los 1.749 millones de euros, un 7,7% más que en 2021.

El 44% de las empresas han mantenido los mismos niveles de inversión que el año pasado, mientras que un 51,3% los han aumentado en mayor o menor medida. Sólo un 3,8% los han reducido, y un 0,9% asegura que empezará a invertir.

Respecto a las empresas que invierten más en ciberseguridad este año, un 32% aumenta sus niveles de inversión un 20% más que el años pasado; un 11,6% entre el 21% y el 50%; y un 6,7% habrá aumentado su inversión cuando acabe el año más de un 51%.