ARMIS®

EL ESTADO DE LA
CIBERGUERRA

INFORME DE TENDENCIAS Y ESTADO DE LA CIBERGUERRA DE ARMIS: 2022-2023

ANÁLISIS POR PAÍSES

PENÍNSULA IBÉRICA

ÍNDICE

INTRODUCCIÓN

Si ha analizado el Informe de tendencias y estado de la ciberguerra de Armis: 2022-2023 global, sabrá que para los responsables de TI y de empresas es fundamental conocer el escenario de amenazas en constante cambio que rodea a la ciberguerra. Solo así podrán mejorar la situación de ciberseguridad para defenderse de estos ataques. Para preparar este informe, Armis encargó un estudio en el que se encuestó a 6021 profesionales de TI y de seguridad de todo el mundo con el propósito de averiguar cuáles son las tendencias mundiales de opinión de los profesionales de seguridad en torno a la ciberguerra, los patrones de ataque, los gastos en cibernética, etc. Las respuestas se obtuvieron entre el 22 de septiembre y el 5 de octubre de 2022.

Armis utilizó datos extraídos de su galardonada plataforma de seguridad e inteligencia de activos para cotejar los resultados de la encuesta con tendencias de datos reales. Los datos de la plataforma de Armis recabados entre el 1 de junio y el 30 de noviembre de 2022 confirmaron que los ciberataques no se han suavizado, sino que han empeorado. La actividad de amenazas en la base de clientes global de Armis aumentó un 15 % entre septiembre y noviembre comparado con los tres meses anteriores. De hecho, Armis concluyó que el mayor porcentaje de la actividad de amenazas se dirigió a organizaciones con infraestructuras críticas. El segundo puesto lo ostentan las organizaciones sanitarias en comparación con otros sectores.

Aparte de estas conclusiones globales, Armis ha preparado un análisis por países y conclusiones regionales para ofrecer una visión única y particular que tenga más sentido para determinados lectores en función de dónde se encuentren físicamente y los países donde estén localizadas sus empresas. **En este análisis por países veremos más de cerca las conclusiones extraídas de 751 encuestados de España (500) y Portugal (251), que pusieron en común sus puntos de vista en nuestra encuesta y que trabajan en varios sectores, como la asistencia sanitaria, la fabricación, el comercio minorista, los servicios financieros, etc.**

RESUMEN DE LAS CONCLUSIONES

Según el estudio de Armis, España es el país europeo más preocupado por la amenaza de la ciberguerra. Casi tres cuartas partes (74 %) de las organizaciones españolas muestran preocupación por los desafíos que estos eventos globales pueden plantear al país. Esta cifra supera la media mundial (67 %) y la media portuguesa (62 %), que está más próxima a la media europea (60 %). A raíz del conflicto en el continente, se ha producido un repunte de los ciberataques en la región, cosa que se vio claramente en los recientes ataques a la administración pública de España, así como a las instituciones sanitarias españolas y portuguesas.

> *"Los últimos ciberataques ponen de manifiesto que el comportamiento de los atacantes está en constante evolución y que están hallando otras formas de sortear los sistemas de detección y respuesta tradicionales. Estamos ante un escenario muy complicado en el que no existe un perímetro de seguridad definido para proteger nuestros activos. Por eso es importante conocer el estado y las tendencias de la ciberseguridad de las compañías."*
>
> **VESKU TURTIA**
> DIRECTOR REGIONAL DE ARMIS EN LA PENÍNSULA IBÉRICA

Tras analizar las respuestas de los profesionales de TI y de seguridad de las compañías de la península ibérica, Armis distingue en general cinco tendencias principales en comparación con otras regiones. A continuación examinaremos estas conclusiones en mayor profundidad y las tendencias que pueden deducirse de ellas.

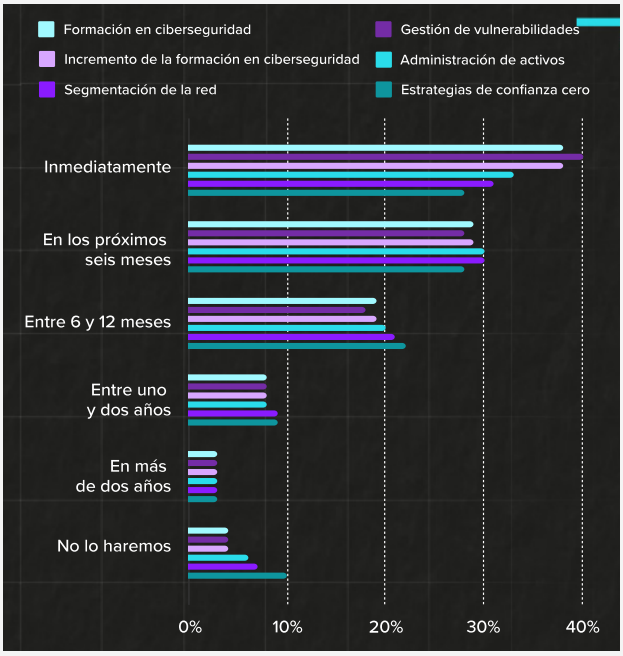
EMEA

En 2022, la región EMEA se ha visto sacudida por la invasión de la nación soberana de Ucrania. La inestabilidad geopolítica asociada a la guerra física y a la ciberguerra está teniendo una tremenda repercusión en toda la zona. La incertidumbre de la cadena de suministro, la infame crisis energética y los continuos ciberataques dirigidos a las funciones más críticas de la sociedad están contribuyendo a que se produzcan cambios en las prioridades y en la forma de gastar de numerosos sectores. El informe confirma el repunte de los ciberataques y revela que casi 3 de cada 5 organizaciones (58 %) han experimentado una o más infracciones de seguridad. Además, el 25 % de los encuestados asegura que ha habido una escala en el número de amenazas dirigidas a su organización.

Aunque se han tomado medidas para garantizar la protección, todavía a día de hoy menos de la mitad (44 %) de los profesionales de TI y de seguridad afirma que sus organizaciones tiene programas y procedimientos para responder a las amenazas de ciberguerra. Los encuestados calificaron a sus compañías como mal preparadas, dado que hay varias cuestiones importantes que deben abordarse:

- Solo el 46 % de los profesionales de TI y de seguridad de la región EMEA estuvo totalmente de acuerdo en que sabe a quién acudir en caso de percibir alguna actividad sospechosa.
- Solo el 76 % de los profesionales de TI y de seguridad de la región EMEA afirmó que colabora con otros miembros del sector para compartir información sobre amenazas, cifra que está por debajo de la media de las regiones de EE. UU. y Asia-Pacífico y Japón. Aunque este porcentaje es elevado, denota que todavía queda trabajo por hacer si queremos que todas las áreas estén protegidas de ciberataques.
- Solo el 33 % de los profesionales de TI y de seguridad de la región EMEA ha denunciado un acto de ciberguerra a las autoridades, por debajo de los niveles de EE. UU. (63 %) y Asia-Pacífico y Japón (61 %).
- Casi 2 de cada 10 (18 %) de los profesionales de TI y de seguridad de la región EMEA reconocen que su organización carece de un plan de contingencia en caso de que se detecte un acto de ciberguerra.
- Solo un tercio (33 %) de los profesionales de TI y de seguridad cuenta con un plan de ciberguerra validado con procedimientos recomendados, adecuado y proporcionado.
- Es más, menos de la mitad (49 %) de las compañías forma a sus empleados como algo habitual o limita los derechos de administración de red (40 %). Y una cifra aún menor ha puesto en marcha procedimientos de ciberseguridad, como crear una cultura del trabajo centrada en la seguridad (37 %), invertir en seguros de ciberseguridad (31 %) o implementar un marco de riesgos cibernéticos (31 %).

Existe una desconexión entre los niveles de confianza de preparación ante ataques de ciberseguridad (84 %) y la realidad, y acabar con esa brecha requiere invertir tanto en herramientas como en servicios. Al pedir a los profesionales de TI que seleccionaran cuándo invertirían en una serie de aspectos, dieron las siguientes respuestas:



REGULACIONES QUE MIRAN AL FUTURO

Los gobiernos, los servicios de seguridad y las autoridades competentes correspondientes siguen dando una enorme importancia a la necesidad de mejorar la situación de ciberseguridad y a la acuciante necesidad de trazar una estrategia más resiliente frente a los ciberataques. La Ley de ciberresiliencia europea, de reciente promulgación, se basa en la directiva de ciberseguridad existente de la UE de 2016, y actualiza los requisitos del bloque para que los estados miembro mejoren su ciberseguridad. Antes de que esta ley existiera, gran parte de la presión por cuestiones de ciberseguridad recaía en los usuarios de los productos, ya fueran empresas o particulares. Ahora, los fabricantes asumen una mayor responsabilidad en este ámbito. Esta responsabilidad ayuda muy mucho a poner en marcha mejoras de carácter generalizado. La UE también ha lanzado NIS2, que pone el foco en un número de sectores mucho mayor y multa, sanciona o penaliza a los que no tengan una gestión de riesgos adecuada o un mínimo de higiene cibernética y a los que se demoren en tomar las medidas correctivas que correspondan.

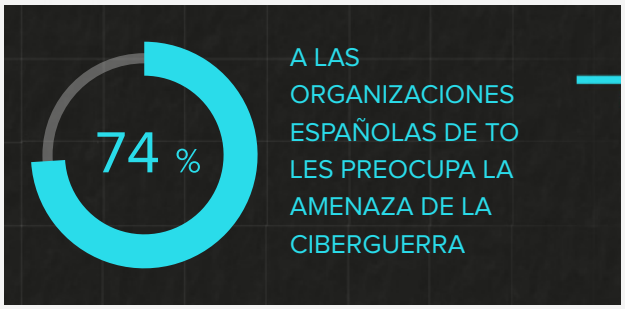
La aparición de normativas es un buen punto de partida y definitivamente contribuirá a reducir la falta de inversión en algunas herramientas y priorizar su importancia, pero aún así sigue habiendo mucho camino que recorrer para acabar con la brecha de vulnerabilidades críticas que se ha abierto como consecuencia de la proliferación exponencial de activos conectados. El 37 % de los encuestados coincide en que los dispositivos conectados tienen prioridad absoluta en caso de que se produzca un ataque de ciberguerra.

Más allá de los esfuerzos internos, entre los profesionales de TI existe la convicción de que la Unión Europea y sus países miembros también deben intensificar la cooperación con otros aliados de todo el mundo. Más de la mitad (61 %) afirmó que respaldaría el alistamiento en una liga de ciberdefensa en caso de que sus países se vieran envueltos en un conflicto de ciberguerra.

TENDENCIAS DE ESPAÑA EXTRAÍDAS DEL INFORME DE TENDENCIAS Y ESTADO DE LA CIBERGUERRA DE ARMIS: 2022-2023

LAS ORGANIZACIONES ESPAÑOLAS SON LAS MÁS PREOCUPADAS EN EUROPA POR LA CIBERGUERRA

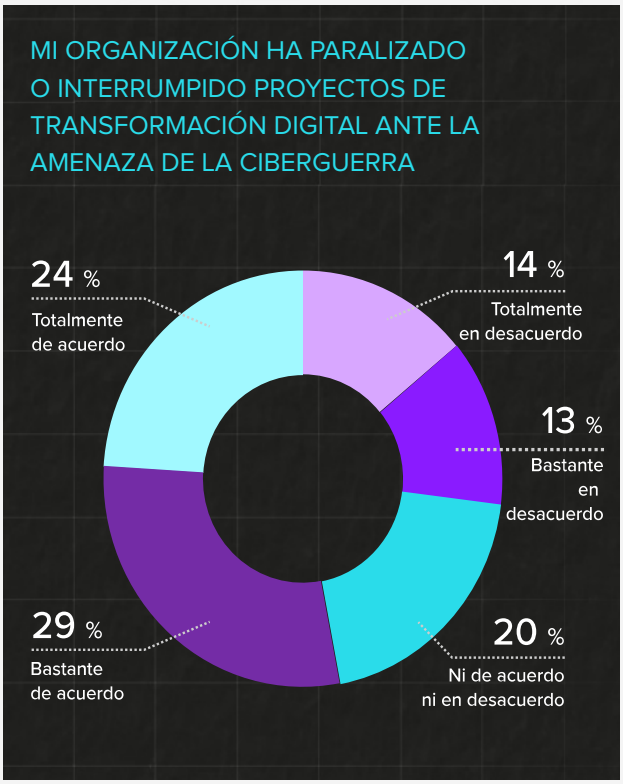
Al 74 % de las organizaciones españolas le preocupa la amenaza de la ciberguerra, cifra muy superior a la de la mayoría de las regiones y sus homólogos en Europa. Pero, a pesar de esta preocupación, más de un cuarto de las organizaciones españolas (26 %) cree que no tiene la preparación adecuada para afrontar la ciberguerra, y el aspecto de seguridad que ocupa el último puesto entre los profesionales de TI es evitar ataques de estado-nación, no solo en España, sino en todo el mundo (22 %). La protección de datos (67 %) y la detección de intrusiones (58 %) siguen siendo las principales prioridades de la región.



Las crecientes tensiones geopolíticas surgidas a raíz de la guerra de Ucrania han hecho que la amenaza de sufrir ciberataques sea mucho más verosímil. Más del 67 % de los profesionales de TI y de seguridad españoles encuestados por Armis admite que la guerra de Ucrania ha intensificado mucho más la amenaza de ciberguerra, y el 39 % de los encuestados —únicos responsables de tomar decisiones de seguridad de TI— reconoció haber experimentado una mayor actividad de amenazas en sus redes entre mayo y octubre de 2022 en comparación con los últimos seis meses, cifra bastante baja si la comparamos con el porcentaje a nivel mundial (54 %), pero que prácticamente coincide con la media europea (40 %).

EL PANORAMA DE AMENAZAS HA PARALIZADO O INTERRUMPIDO PROYECTOS DE TRANSFORMACIÓN DIGITAL EN ESPAÑA

El panorama de amenazas, cada vez más agravado, ha tenido un impacto palpable en los proyectos de digitalización, posiblemente hasta el punto de frenar la innovación. Más de la mitad de los profesionales de TI españoles (53 %) afirma que sus organizaciones han paralizado o interrumpido sus proyectos de transformación digital a causa de estas amenazas.



Del mismo modo, el 58 % de los encuestados españoles admite que la amenaza de la ciberguerra puede poner freno a la digitalización del país, una cifra incluso superior a la media europea (51 %).

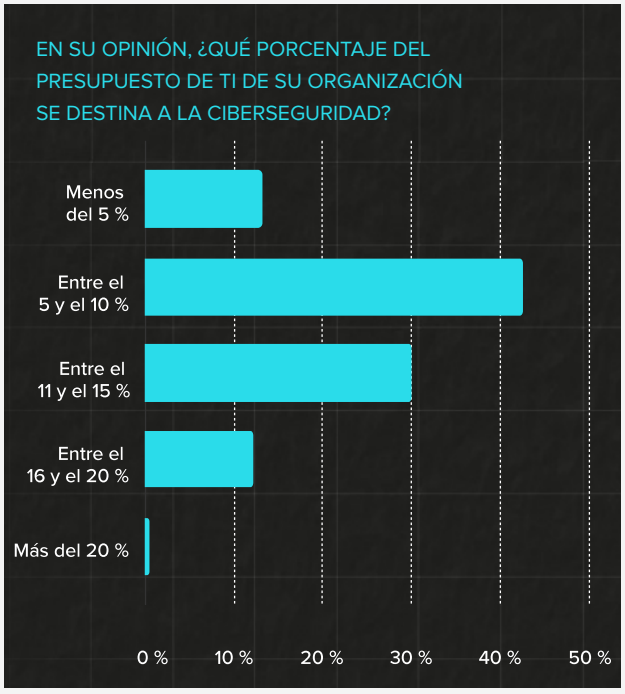
FALTA DE INVERSIÓN Y SOBERANÍA DIGITAL EN EL COMPENDIO LEGISLATIVO ESPAÑOL QUE RIGE LA CIBERSEGURIDAD

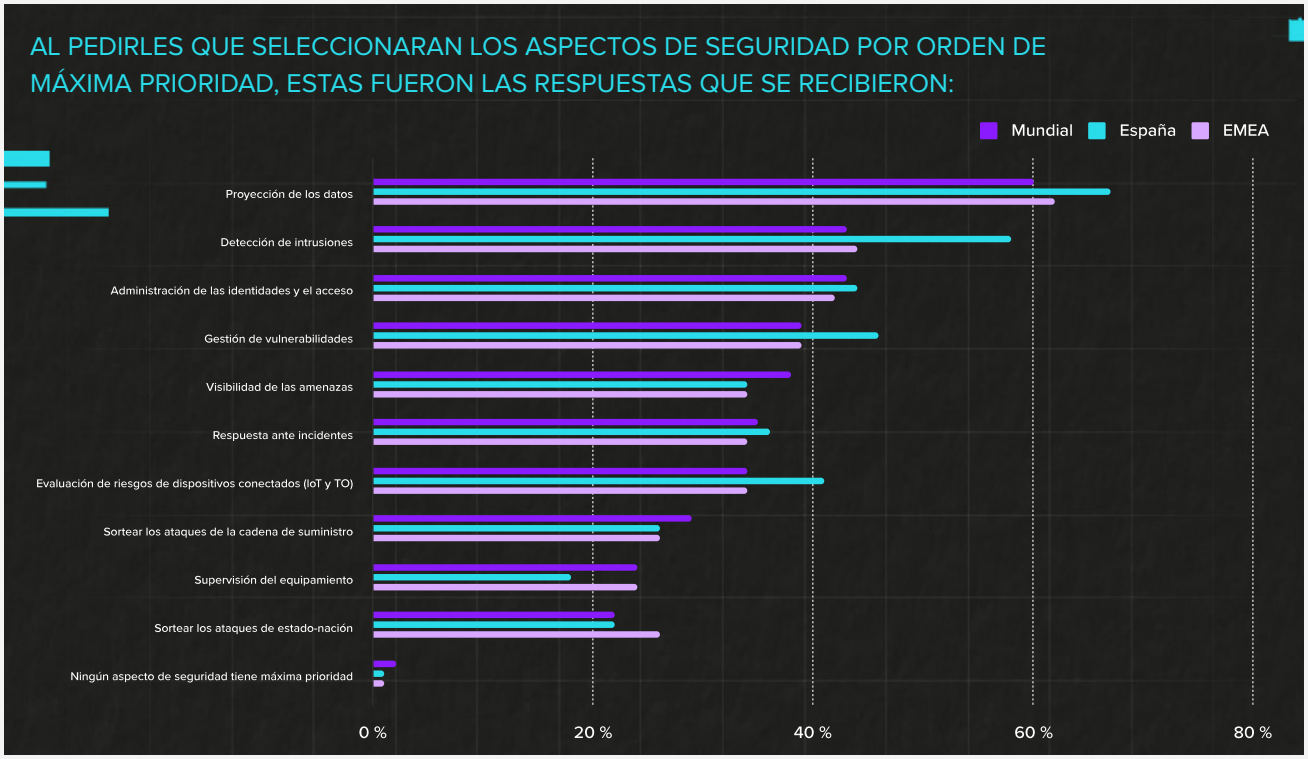
La soberanía digital es un concepto relativamente reciente que el Foro Económico Mundial describe como "la capacidad de tener el control sobre el propio destino digital", incluidos "los datos, el hardware y el software" que alguien "crea" y en los que alguien "confía". La ansiedad por el control y la privacidad de estos datos por parte de los gobiernos europeos fue un factor importante en la introducción del Reglamento General de Protección de Datos (RGPD). En lo referente a la legislación sobre ciberseguridad en España, el 83 % de los encuestados españoles coincide en que falta inversión y soberanía digital. Tradicionalmente, España siempre ha adolecido de carencias de inversión en I+D. España ocupa el 17.º puesto en Europa, con un gasto de 1,4 % de su PIB en I+D, mientras que en Europa la media es del 2,3 %. Con todo, más de la mitad (52 %) de los encuestados españoles afirma confiar en la capacidad de defensa de su gobierno ante un acto de ciberguerra, cifra similar a la de Portugal, pero inferior a la de Francia o Italia (66 % en ambos casos).

EL GASTO EN CIBERSEGURIDAD SIGUE CRECIENDO A MEDIDA QUE LAS JUNTAS DIRECTIVAS CAMBIAN LA CULTURA DE LAS ORGANIZACIONES AL RESPECTO

Las organizaciones se están replanteando su inversión en ciberseguridad en un esfuerzo por mitigar riesgos y a raíz de los últimos acontecimientos, como la pandemia o la guerra de Ucrania. Algo más de tres cuartos (77 %) de los profesionales de TI españoles encuestados coinciden en que las juntas directivas están transformando la cultura de las organizaciones hacia la ciberseguridad como respuesta a la amenaza de la ciberguerra. Esto es significativo, dado que antes este tipo de control por parte de las juntas directivas era una rara avis, mientras que ahora están asumiendo una responsabilidad conjunta por mejorar la situación de ciberseguridad de las organizaciones.

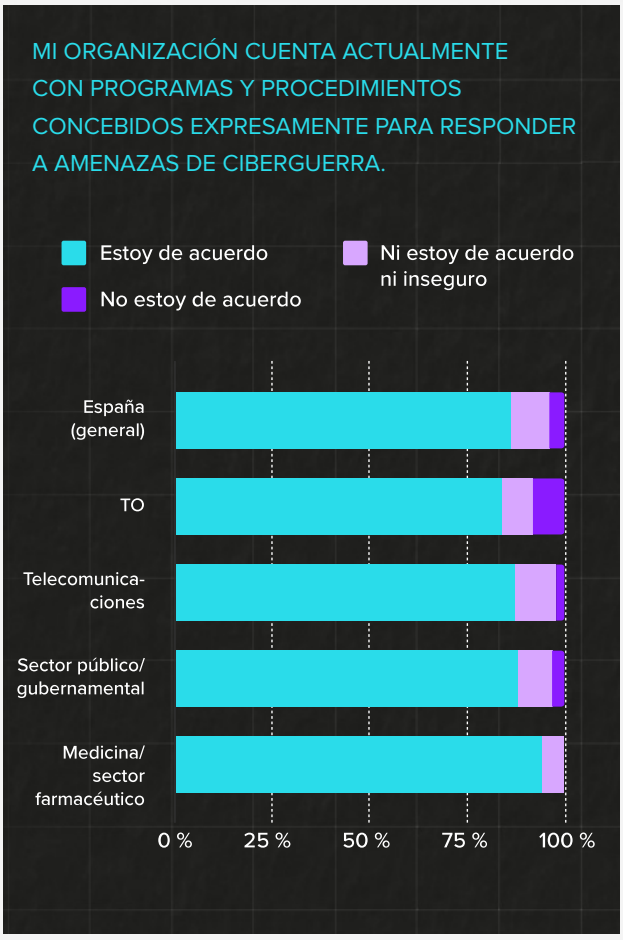
De hecho, más de 4 de cada 5 (82 %) de los profesionales de TI y de seguridad españoles encuestados afirma que es bastante probable (43 %) o muy probable (39 %) que sus compañías dediquen una mayor parte del presupuesto a ciberseguridad.





SECTORES EN PELIGRO PERO LISTOS PARA ACTUAR

Si bien ningún sector escapa al riesgo de sufrir un ciberataque, las infraestructuras críticas, el sector sanitario y las agencias gubernamentales están a la cabeza y son una diana muy apetitosa para los atacantes de estado-nación. En palabras de Vesku Turtia, director regional de Armis en la península ibérica: "La actividad de los atacantes de estado-nación sigue evolucionando, y las infraestructuras críticas se están convirtiendo en el principal objetivo en un escenario de ciberguerra. La amenaza constante de los ataques dirigidos a redes eléctricas, sistemas de transporte o instalaciones de agua tendrá prioridad absoluta en el futuro. En 2023 se espera que haya más ataques de ransomware y malware dirigidos y una mayor convergencia entre TI y TO, con lo cual resulta imperativo tener soluciones diseñadas para detectar, supervisar y proteger los activos digitales de la Industria 4.0, ahora y en el futuro."

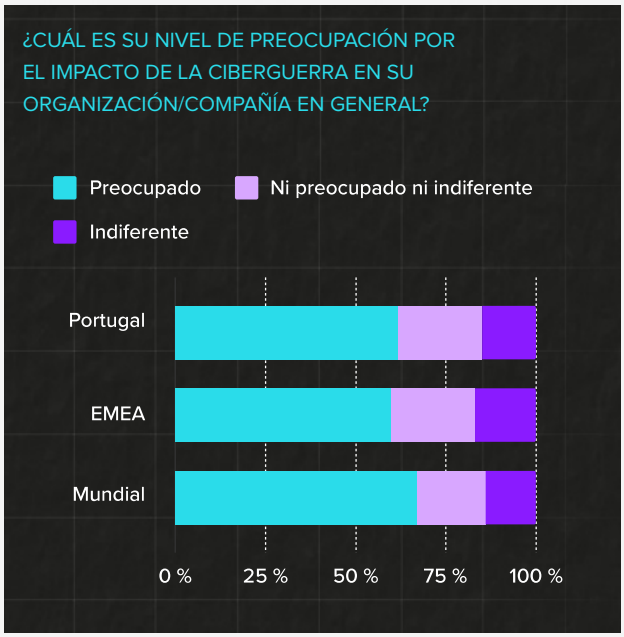


Preguntados por el nivel de preparación de sus organizaciones para responder ante la amenaza de la ciberguerra, los encuestados españoles contestaron lo siguiente:

TENDENCIAS DE PORTUGAL EXTRAÍDAS DEL INFORME DE TENDENCIAS Y ESTADO DE LA CIBERGUERRA DE ARMIS: 2022-2023

LA CIBERGUERRA PREOCUPA A LAS COMPAÑÍAS PORTUGUESAS, QUE NO CREEN ESTAR PREPARADAS PARA HACERLE FRENTE

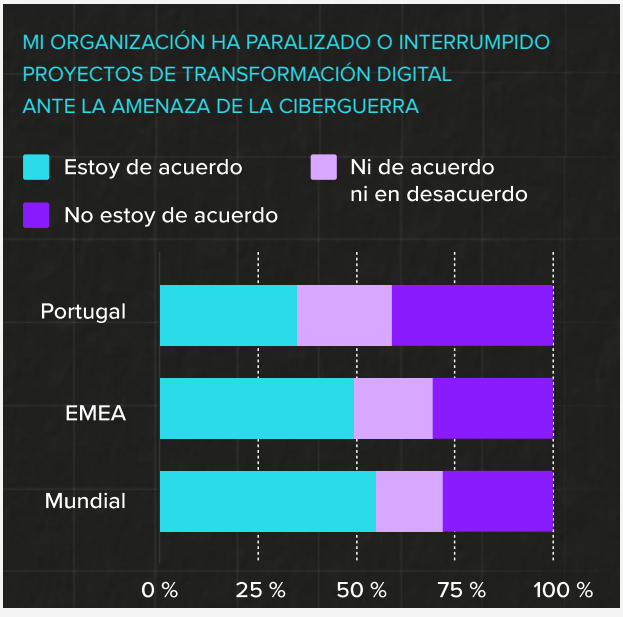
En Portugal, al 62 % de las organizaciones le preocupa el impacto de la ciberguerra en la compañía en general. Pese a ello, el 38 % de las compañías portuguesas sigue sin tomarse esta amenaza en serio, mientras que el 37 % cree que su compañía no está preparada para afrontar la ciberguerra, cifra superior a las medias europea y mundial (26 % y 24 % respectivamente).



La situación geopolítica actual ha aumentado la inquietud en torno a una posible ciberguerra, y el 67 % de los encuestados portugueses admite que la guerra en Ucrania ha supuesto una amenaza aún mayor, cifra que está ligeramente por encima de las medias europea y mundial (63 % y 64 % respectivamente). Entre los profesionales de TI encuestados, el 31 % asegura haber experimentado una mayor actividad de amenazas en sus redes entre mayo y octubre de 2022 en comparación con los últimos seis meses. Esta cifra es superior a la media europea (25 %), pero similar a la registrada a nivel mundial (31 %).

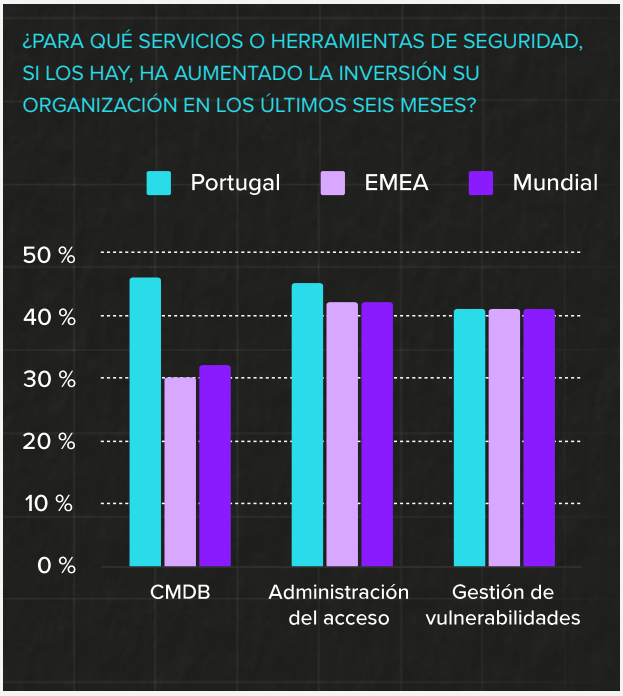
SOLO UNA PARTE DE LAS COMPAÑÍAS PORTUGUESAS ESTÁN FRENANDO SUS PROYECTOS DE TRANSFORMACIÓN DIGITAL

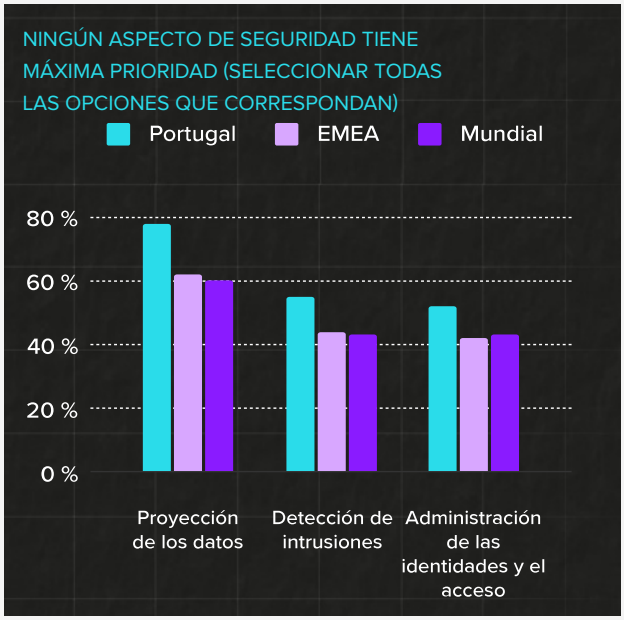
Pese a manifestar una mayor preocupación por la ciberguerra, las compañías portuguesas siguen centradas en su proceso de transformación digital. Solo el 35 % de los profesionales de TI encuestados por Armis afirma que su organización ha interrumpido o abandonado temporalmente estos proyectos, cifra que es considerablemente inferior a las medias europea (50 %) y mundial (55 %).

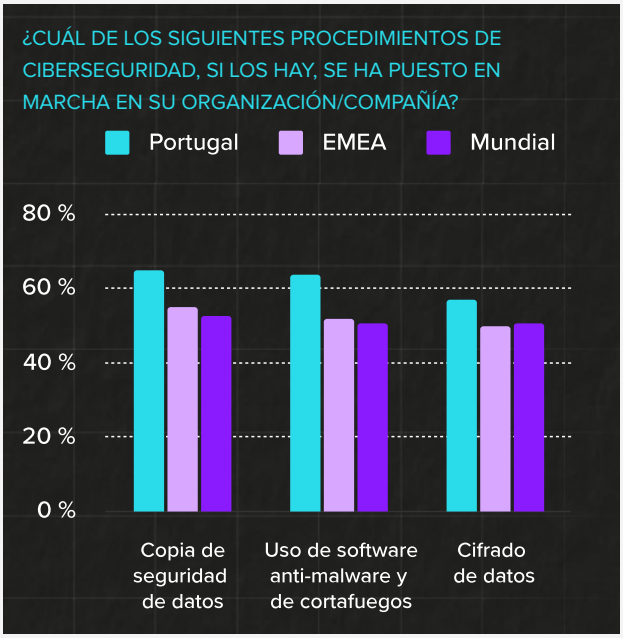


LA PROTECCIÓN DE DATOS TIENE MÁXIMA PRIORIDAD PARA LOS PROFESIONALES PORTUGUESES

Los aspectos de seguridad prioritarios para los profesionales de TI portugueses son la protección de los datos (78 % de las respuestas), la detección de intrusiones (55 %) y la administración de identidades y el acceso (52 %). En cuanto a cuáles son los servicios o herramientas de ciberseguridad cuya inversión ha aumentado en los últimos seis meses en sus organizaciones, los encuestados mencionaron las bases de datos de administración de activos (46 %), seguido de la administración del acceso (45 %) y la vulnerabilidad (41 %). Los principales procedimientos de ciberseguridad que se han puesto en marcha en las organizaciones son la copia de seguridad de datos (65 %), el uso de software anti-malware y de cortafuegos (64 %) y el cifrado de datos (57 %).

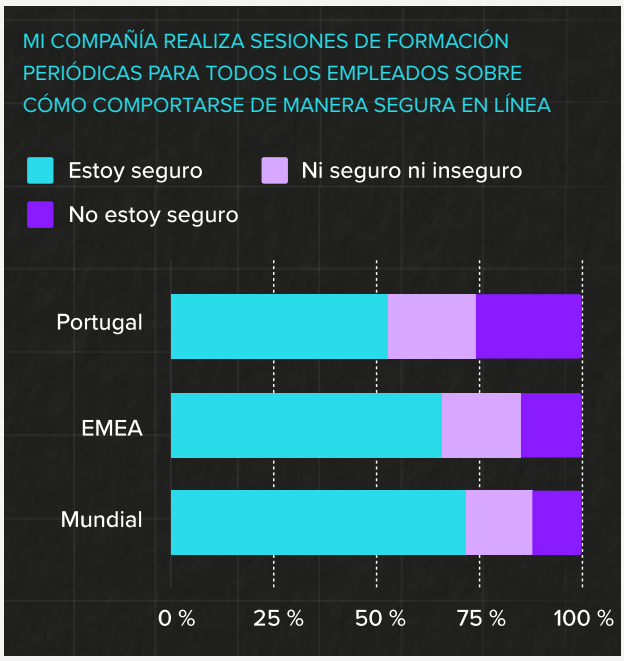






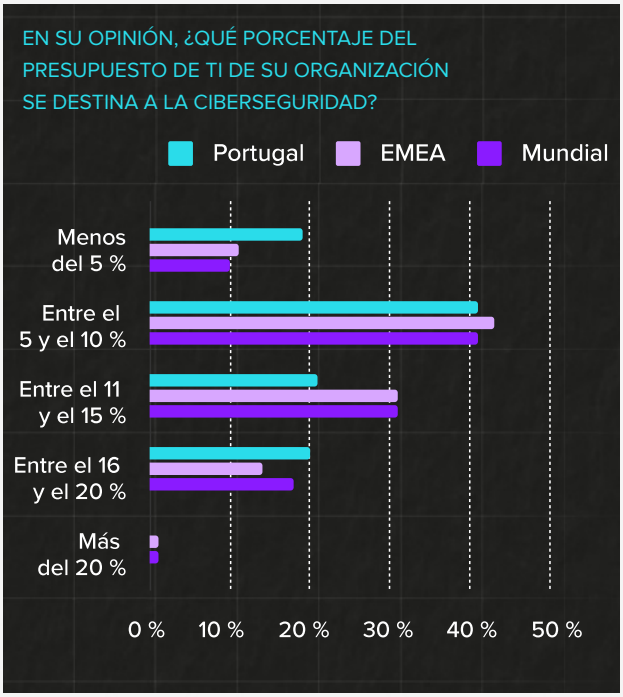
LAS COMPAÑÍAS PORTUGUESAS INVIERTEN EN FORMAR A SUS EMPLEADOS EN SEGURIDAD EN LÍNEA, PERO TODAVÍA QUEDAN COSAS QUE HACER EN ESTE ÁMBITO

La formación ha sido otro punto de interés de las compañías lusas. Al ser preguntados si sus compañías realizan sesiones de formación periódicas para todos los empleados sobre cómo comportarse de manera segura en línea, el 77 % de los profesionales de TI respondió afirmativamente.



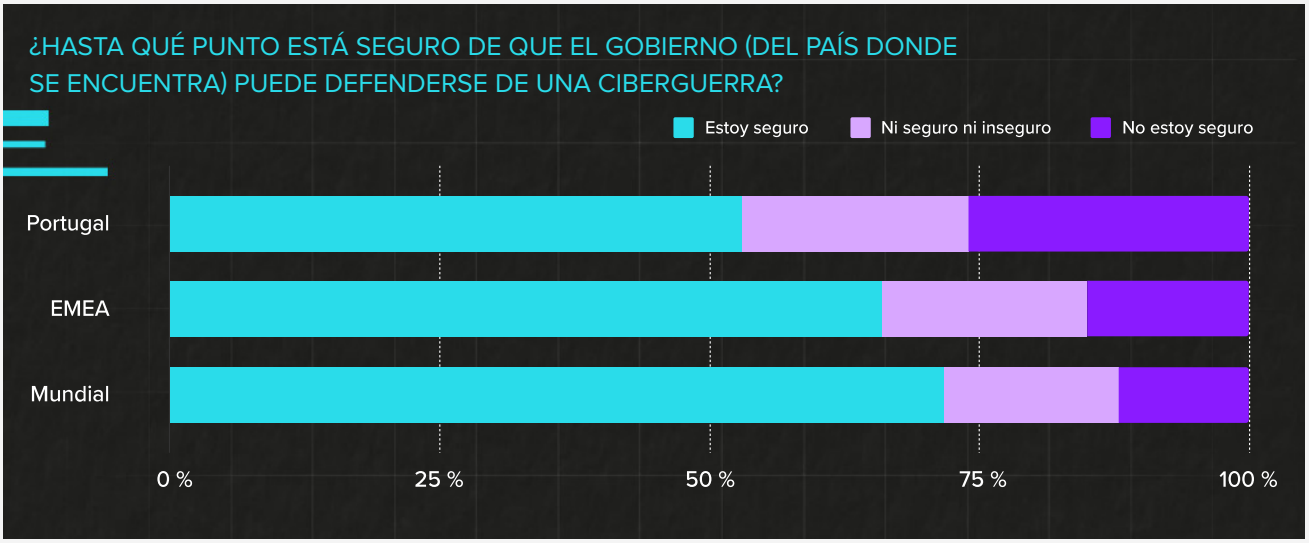
LA MAYORÍA DE LAS COMPAÑÍAS PORTUGUESAS DEBE DEDICAR UNA MAYOR PARTE DEL PRESUPUESTO A LA CIBERSEGURIDAD

En vista de los últimos acontecimientos, como la pandemia o la guerra de Ucrania, el 78 % de los encuestados portugueses considera que es probable que sus organizaciones dediquen una mayor parte del presupuesto a ciberseguridad. Actualmente, una parte nada desdeñable de las compañías portuguesas asigna solo entre un 5 y un 10 % de su presupuesto de TI a la ciberseguridad (41 %).



LOS PORTUGUESES CONFÍAN EN LA CAPACIDAD DE DEFENSA DE SU GOBIERNO ANTE UN ACTO DE CIBERGUERRA

Al preguntarles si confían en la capacidad de defensa de su gobierno ante un acto de ciberguerra, el 53 % de los profesionales de TI y de seguridad portugueses manifestó tener confianza. El estudio de Armis incluye también dos preguntas específicas para el mercado portugués acerca del nuevo marco legal para la seguridad del ciberespacio de ese país. Al preguntarles si el nuevo marco ha cambiado la forma en que las compañías lidian con las medidas de ciberseguridad, el 53 % de los profesionales de TI y de seguridad portugueses respondió afirmativamente. Al preguntarles si las compañías deberían ser multadas si no tienen planes de seguridad frente a ciberataques, el 67 % de los encuestados respondió afirmativamente.


¿HASTA QUÉ PUNTO ESTÁ SEGURO DE QUE EL GOBIERNO (DEL PAÍS DONDE SE ENCUENTRA) PUEDE DEFENDERSE DE UNA CIBERGUERRA?
Estoy seguro
Ni seguro ni inseguro
No estoy seguro
Portugal
EMEA
Mundial
0 %
25 %
50 %
75 %
100 %

¿POR QUÉ SON IMPORTANTES ESTAS CONCLUSIONES?

Informe de tendencias y estado de la ciberguerra de Armis: Los resultados del Informe de tendencias y estado de la ciberguerra de Armis: 2022-2023 han puesto de manifiesto la creciente preocupación de las organizaciones en torno a la frecuencia y gravedad —cada vez más agudas— de los ciberataques, así como ante la amenaza de la ciberguerra. El panorama de amenazas, que no hace más que aumentar en complejidad y sofisticación, está teniendo impacto en diferentes áreas empresariales de todos los sectores. Pese a ello, sigue habiendo diferencias en cuanto a la celeridad y las prioridades con las que se trazan y adoptan estrategias de ciberseguridad.

"La ciberguerra es el futuro del terrorismo hasta arriba de esteroides, ya que constituye un método de ataque rentable y asimétrico que requiere una vigilancia ininterrumpida y gastos para defenderse de ella..." "La ciberguerra clandestina ya es casi cosa del pasado: actualmente, los atacantes de estado-nación lanzan ciberataques con total descaro, a menudo con el objetivo de recopilar información, interrumpir las operaciones o destruir completamente los datos. Según estas tendencias, todas las organizaciones deberían considerarse a sí mismas como posibles objetivos de ataques de ciberguerra y, por tanto, conviene que protejan sus activos en consecuencia."

NADIR IZRAEL
CTO Y COFUNDADOR DE ARMIS

"La inestabilidad geopolítica actual, unida a la invasión rusa de Ucrania, ha acelerado también el repunte de ciberataques. Algunos sectores fundamentales para la economía y la sociedad, como la asistencia sanitaria, las infraestructuras críticas y las industrias, están especialmente expuestos a este riesgo, por lo que es de suma importancia que estén bien protegidos."

"Las organizaciones de la península ibérica, que todavía están en proceso de transformación y adaptación a nuevos modelos de trabajo híbridos y teletrabajo, deberán invertir en ciberseguridad para que la adopción de nuevas tecnologías suceda sin riesgos y con total seguridad."

VESKU TURTIA
DIRECTOR REGIONAL DE ARMIS EN LA PENÍNSULA IBÉRICA

¿QUÉ PUEDE HACER SU ORGANIZACIÓN PARA PROTEGERSE?

Así pues, ¿qué pueden hacer las organizaciones? La forma más adecuada de mejorar la situación de seguridad y solucionar incidentes rápidamente en la organización es contar con una detección temprana y una supervisión constante. Y es que si no sabemos que hay un problema, no podremos corregirlo. Siguiendo esta analogía, si no podemos ver un activo, no podremos protegerlo. Y aquí es precisamente donde Armis puede ser de ayuda.

PLATAFORMA DE INTELIGENCIA DE ACTIVOS DE ARMIS

La **plataforma de inteligencia de activos de Armis** proporciona una visibilidad y seguridad unificadas de cualquier tipo de activo, incluida la tecnología de la información (TI), Internet de las cosas (IoT), la tecnología operativa (TO), Internet de las cosas médicas (IoMT), la nube y el IoT móvil, tanto si están administrados como sin administrar. La solución de Armis, una plataforma de software como servicio (SaaS) sin agentes, se integra sin complicaciones en sus pilas de TI y seguridad actuales para ofrecer con rapidez la inteligencia contextual que necesita para mejorar su situación de seguridad, sin causar ningún tipo de interrupción en las operaciones o flujos de trabajo en curso. Armis ayuda a los clientes a protegerse de los peligros cibernéticos y operativos que pasan desapercibidos, disparar la productividad, optimizar el uso de recursos e innovar con nuevas tecnologías sin riesgos para expandir el negocio. Sea cual sea la amenaza o acción de ciberguerra.

Regístrese hoy mismo para realizar una **evaluación de riesgos de seguridad** y descubra qué activos son los más vulnerables a un ataque. Sírvase de estas conclusiones para priorizar su estrategia de mitigación de riesgos y garantizar el pleno cumplimiento de los marcos normativos que requieren que se identifiquen y prioricen todas las vulnerabilidades.

Si desea solicitar una demostración personalizada de Armis, visite: armis.com/demo.

Para seguir analizando las conclusiones del Informe de tendencias y estado de la ciberguerra de Armis: 2022-2023 en una escala global, visite: **armis.com/cyberwarfare.**

EL ESTADO DE LA

CIBERGUERRA

ACERCA DE ARMIS

Armis, la compañía de visibilidad y seguridad de activos líder del sector, posee la primera plataforma de inteligencia de activos unificada del mercado, diseñada para solucionar los problemas de la nueva superficie de ataque extendida que crean los activos conectados. Las empresas de la lista Fortune 100 confían en nuestra protección constante y en tiempo real para ver el contexto integral de todo tipo de activos administrados y sin administrar en dispositivos IoT, TI o en la nube, dispositivos médicos (IoMT), tecnología operativa (TO), sistemas de control industrial (ICS) y 5G. Armis proporciona una administración de los activos cibernéticos pasiva, gestión de riesgos y aplicación de políticas automatizadas. Armis es una empresa privada con sede en California.

armis.com

info@armis.com

20230110-1

ARMIS®