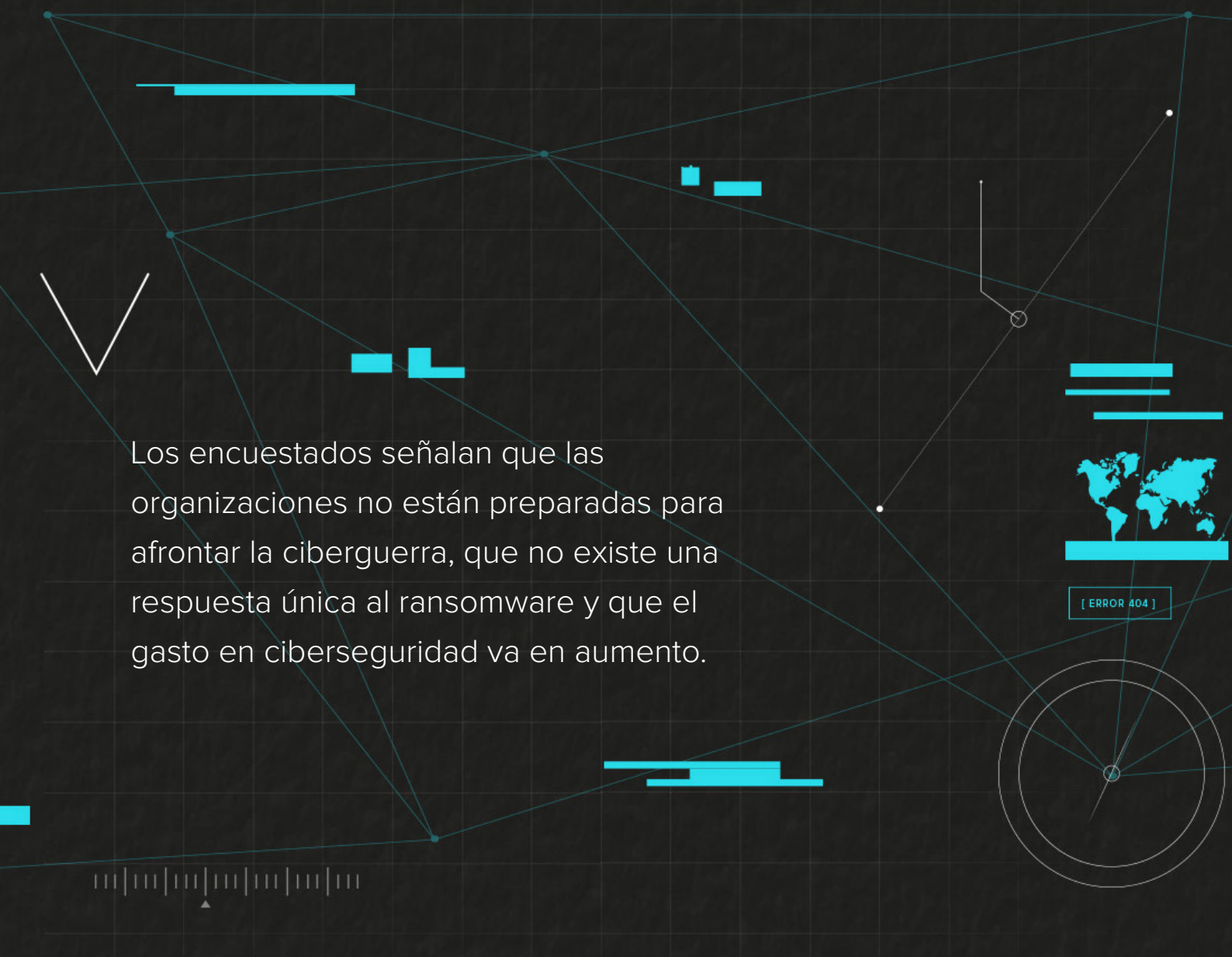
ARMIS®

EL ESTADO DE LA
CIBERGUERRA

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

OPINIÓN DE PROFESIONALES DE SEGURIDAD Y TI DE TODO EL MUNDO SOBRE LA PREPARACIÓN Y EL GASTO EN CIBERNÉTICA



Los encuestados señalan que las organizaciones no están preparadas para afrontar la ciberguerra, que no existe una respuesta única al ransomware y que el gasto en ciberseguridad va en aumento.

PRÓLOGO DE NADIR IZRAEL

CTO Y COFUNDADOR DE ARMIS

En Armis, nos complace poder compartir con usted los resultados de nuestro estudio de mercado y nuestras investigaciones globales sobre ciberguerra. Esperamos que el contenido de este estudio global, así como el de sus informes regionales paralelos, sea valioso y de su interés.

Reflexionemos sobre el contexto en el que nos desenvolvemos hoy día. Distintos **analistas prominentes**[1] pronostican que, para 2025, los ciberatacantes tendrán unos entornos de tecnología operativa que podrán usar como armas para dañar o matar a personas. Esto, que puede sonar extremo, confirma una tendencia de la ciberguerra a medida que los responsables de las amenazas pasan de la dimensión del reconocimiento y el espionaje al uso cinético de herramientas de ciberguerra. Estas ciberarmas cinéticas ya se han detectado en circulación, si bien ninguna de ellas se ha puesto en marcha aún para desatar su efecto mortífero. Un ejemplo: el malware Triton, detectado en 2017, **atacó y desactivó**[2] los controladores del sistema instrumentado de seguridad (SIS) de una planta petroquímica de Arabia Saudí, algo que, de no haberse detectado, habría contribuido a producir un desastre en toda la instalación. En febrero de 20213, un hacker intentó envenenar mediante acceso remoto las instalaciones de suministro de agua de una pequeña ciudad estadounidense del estado de Florida. Hemos sido testigos también de cómo algunos ataques de ransomware dirigidos al sector sanitario **han provocado el fallecimiento de personas**[4]. Las posibilidades de alcance de los ciberataques —intencionados o no— es incuestionable.

Si bien las ciberamenazas cinéticas son el futuro de la carrera armamentística cibernética, las ciberarmas no son ni mucho menos una novedad. En 2016, el mundo entero conoció el arsenal cibernético de la **Agencia de Seguridad Nacional**[5] estadounidense a raíz de las **filtraciones del grupo de hackers Shadow Brokers**[6], que reveló algunas de las ciberarmas más potentes e invisibles del planeta. Este arsenal cibernético filtrado, que incluía la vulnerabilidad EternalBlue, fue la base de algunos de los riesgos de mayor alcance de la historia, como NotPetya y WannaCry.

El desarrollo de estas ciberarmas también ha impulsado todo un sector, conocido como "mercado de día cero", un tenebroso grupo de investigadores, agentes y sitios web dedicados a sacar provecho de los exploits de día cero. Se desconoce cuál es el capital real exacto del sector en su totalidad, pero las listas de precios publicadas han puesto de manifiesto que el precio de un exploit sin clics en activo podría ascender a **2,5 y 2 millones de dólares para Android e iOS**[7], respectivamente.

Este panorama sigue evolucionando de manera apreciable, y ha dado un vuelco radical en los últimos cinco años, sobre todo tras la invasión rusa de Ucrania en febrero de 2022. Por tanto, los responsables de TI y de empresas deben conocer este escenario de amenazas en constante evolución para mejorar su situación de ciberseguridad y poder defenderse de estos ataques, motivo por el cual hemos elaborado el **Informe de tendencias y estado de la ciberguerra de Armis: 2022-2023**[8]. Para prepararlo, Armis encargó su propio estudio, en el que se encuestó a 6021 profesionales de TI y de seguridad de compañías con más de cien empleados con sede en EE. UU., Reino Unido, España, Portugal, Francia, Italia, Alemania, Austria, Suiza, Australia, Singapur, Japón, Países Bajos y Dinamarca. Aparte de esto, 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. Estas son algunas de las preguntas a las que respondieron los encuestados:

- ¿Diría que su organización está preparada para afrontar una ciberguerra?
- ¿Hasta qué punto está seguro de que el gobierno del país donde se encuentra puede defenderse de una ciberguerra?
- ¿Cuál es la política de su organización en cuanto al pago de rescates por un ataque de ransomware?
- ¿Qué prácticas de ciberseguridad se han puesto en marcha en su organización?

Las respuestas a estas y otras preguntas se usaron con el ánimo de saber cuál era la opinión de los profesionales de TI y de seguridad globalmente, localmente, en cada región y por países, caso a caso, para describir las siguientes tendencias. Veamos más de cerca estas conclusiones y cómo guardan relación con la forma en que las organizaciones pueden mejorar su situación de ciberseguridad para defenderse de ataques de ciberguerra.

CIBERGUERRA

/θiβer'geřa/

NOMBRE:

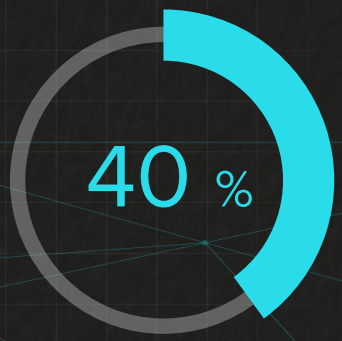
Empleo de ciberataques que provocan daños equiparables a los de una guerra de verdad y/o interrumpen servicios o sistemas vitales. Algunos efectos buscados serían el espionaje, el sabotaje, la propaganda, manipular a la opinión pública, intimidar o interrumpir servicios críticos.

ÍNDICE

¿ESTÁN PREPARADAS LAS ORGANIZACIONES PARA CAPEAR EL TEMPORAL DE LA CIBERGUERRA?

Principales conclusiones extraídas del informe global.

DE CERCA



Un 40 % de los puestos de responsabilidad (CTO, CIO y CISO) afirma haber experimentado una mayor actividad de amenazas en el mismo intervalo de tiempo. Entre estos encuestados en un puesto de responsabilidad, los pertenecientes a los sectores de la alimentación y la bebida (44 %), las telecomunicaciones (44 %), la automoción (43 %), el comercio minorista/venta al por mayor (42 %) y la tecnología (42 %) experimentaron una actividad de amenazas por encima de la media.

Según el estudio de Armis, un tercio (33 %) de las organizaciones globales no se toma en serio la amenaza de la ciberguerra. Estas organizaciones se muestran indiferentes o ajenas al impacto que la ciberguerra puede tener en ellas en términos generales, lo que da pie a brechas de seguridad. Además, las crecientes tensiones geopolíticas surgidas a raíz de la guerra de Ucrania han hecho que la amenaza de un ciberataque sea mucho más verosímil. Más del 64 % de los profesionales de TI y de seguridad encuestados por Armis admite que la guerra de Ucrania ha intensificado mucho más la amenaza de ciberguerra, y más de la mitad de los encuestados (54 %) —únicos responsables de tomar decisiones en materia 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. Ante este panorama, no es de extrañar que el 45 % de los encuestados afirme haber tenido que informar de un ataque de ciberguerra a las autoridades.

ENCUESTADOS EN PUESTOS DE RESPONSABILIDAD:

¿Ha experimentado una mayor o menor actividad de amenazas, si la ha habido, en la red en los últimos seis meses en comparación con los seis meses anteriores?

SEGMENTOS	SECTOR	MÁS	IGUAL	MENOS	N/A	NO LO SÉ
Organismos del gobierno	Gobierno, autoridades locales, agencias públicas	**39 %**	44%	14%	3%	
Servicios financieros	Servicios financieros y seguros	**20%**	70%	10%		
Sector médico y sanitario	Medicina, asistencia sanitaria, sector farmacéutico	**26%**	52%	20%	2%	
Tecnología operativa (TO)	Automoción	**43%**	33%	24%		
	Distribución, logística, transporte	**30%**	48%	19%	4%	
	Alimentación y bebida	**44%**	44%	11%		
	Fabricación, ingeniería	**40%**	30%	8%	22%	
	Petróleo, gas, minería, construcción, agricultura	**30%**	50%	15%	5%	
	Transporte	**32%**	36%	18%	14%	
	Servicios públicos: agua y energía	**15%**	62%	15%	8%	
Total de TO		**37%**	35%	12%	16%	
Otros	Beneficencia, organizaciones sin ánimo de lucro	**29%**	29%	14%	29%	
	Otro (especificar)	**33%**	43%	5%	10%	10%
	Tecnología	**42%**	25%	30%	2%	1%
Total de Otro		**42%**	25%	29%	2%	1%
Minorista	Comercio minorista/venta al por mayor	**42%**	40%	15%	3%	
Telecomunicaciones	Telecomunicaciones, comunicaciones por cable, comunicaciones por satélite	**44%**	38%	18%		
Total general		**40%**	31%	22%	6%	0,5%

Los datos privados de la plataforma de seguridad e inteligencia de activos de Armis recabados entre el 1 de junio y el 30 de noviembre de 2022 confirmaron que las tendencias anteriores 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.

El panorama de amenazas, cada vez más agravado, ha tenido un impacto palpable en los proyectos de transformación digital de todo el mundo, hasta el punto de frenar la innovación. Más de la mitad de los encuestados (55 %) afirma que sus organizaciones han paralizado o interrumpido sus proyectos de transformación digital a causa de estas amenazas. Este porcentaje es incluso mayor en países concretos como Australia (79 %), EE. UU. (67 %), Singapur (63 %), Reino Unido (57 %) y Dinamarca (56 %).

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. El sector sanitario es atractivo por la amplitud de la superficie de ataque y por el efecto que un ataque puede tener en los procesos críticos y en la seguridad y la salud de los pacientes. Las agencias gubernamentales son atractivas por los datos que atesoran, y las infraestructuras críticas siguen teniendo una gran prioridad, dada su importancia en la seguridad económica y nacional.

Con esta inquietud ante el aumento de la amenaza de la ciberguerra, y viendo el coste medio de una infracción de datos en EE. UU (**9,44 millones de dólares**[9], y 4,35 millones de dólares globalmente), no es ninguna sorpresa que los analistas del sector **hayan estimado**[10] que el gasto mundial en gestión de riesgos y seguridad se disparará un 11,3 % en 2023. Aunque hay factores que contribuyen (como los modelos de trabajo híbridos y el teletrabajo, el paso de las redes privadas virtuales al acceso mediante redes de confianza cero y el cambio a la nube), lo cierto es que todo se reduce al hecho

de que la superficie de ataque es cada vez mayor, combinado con la preponderancia de países que tienen capacidad para desarrollar ciberarmamento sofisticado. En definitiva, ¿las organizaciones digitalizadas y conectadas pueden permitirse el lujo de no aumentar el gasto en cibernética?

Pese al riesgo de que una organización pueda sufrir el impacto de la ciberguerra, la ciberdefensa y la resiliencia ante este tipo de ataques siguen siendo escasas. Son cada vez más los atacantes de estado-nación que están alejando el foco de las infraestructuras críticas para centrarlo en atacar entidades comerciales de todo tipo y tamaño. Paradójicamente, el presente estudio puso de manifiesto que casi un cuarto de las organizaciones globales (24 %) cree que no tiene la preparación adecuada para hacer frente a una amenaza de ciberguerra, y con eso y todo, el aspecto de seguridad que ocupa el último puesto entre los profesionales de TI y de seguridad es evitar un ataque de estado-nación. Por otra parte, para las organizaciones que están dispuestas a invertir en un programa de ciberseguridad contundente (más adelante veremos las tendencias de gastos) sigue siendo muy difícil dar con profesionales que sepan desenvolverse perfectamente en un puesto de ciberseguridad y que posean las aptitudes necesarias para supervisar el software y las tecnologías relacionadas. La cifra de puestos de ciberseguridad sin cubrir en todo el mundo **se disparó un 350 %**[11] entre 2013 y 2021, de un millón a 3,5 millones, y se espera que en 2025 siga habiendo el mismo número de vacantes.

¿CUÁLES SON LOS SECTORES MÁS VULNERABLES?

AMENAZAS A INFRAESTRUCTURAS CRÍTICAS

Con el conflicto dilatado en Ucrania, durante 2022 hemos visto cómo las agencias internacionales han emitido varias alertas sobre ciberoperaciones rusas malintencionadas dirigidas a infraestructuras críticas. Destacan Industroyer2 e InController/ PipeDream, que son herramientas de ataque modulares cuyo objetivo son las tecnologías operativas (TO) de cualquier sector, e incluyen los entornos operativos de sistemas de control de supervisión y de adquisición de datos, sistemas de control distribuidos, unidades de terminal remotas y controladores de lógica programables.

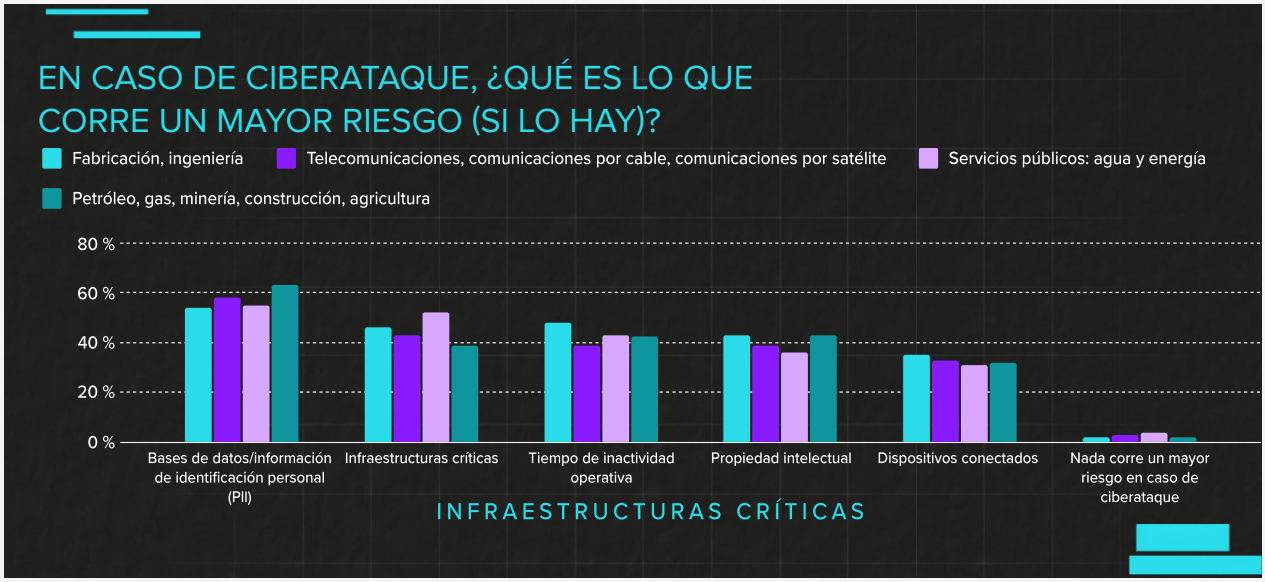
En mayo de 2021, la compañía **Colonial Pipeline**[12], que controla casi la mitad de la gasolina, el combustible para aviones y el diésel de la costa este estadounidense, sufrió un ataque de ransomware en el sistema de TI que afectó a sus operaciones de TO. El ataque a Colonial Pipeline es el ciberataque a una infraestructura crítica estadounidense más grande del que se tiene constancia hasta la fecha. Tras consultarlo con el FBI, con el Departamento de Energía (DOE), el Departamento de Seguridad Nacional (DHS) y con la Agencia de Ciberseguridad y Seguridad de las Infraestructuras (CISA), Colonial Pipeline tomó la difícil decisión de pagar el rescate en criptomonedas que exigían los hackers de DarkSide.

La compañía pensó que pagar para obtener la clave de descifrado era la mejor forma de volver a tenerlo todo en funcionamiento rápidamente y sin riesgos. Más o menos un mes después, el FBI pudo recuperar la mayor parte del pago del confiscando las bitcoins en posesión de los hackers.

Pero la ciberguerra de estado-nación no es exclusiva de países vecinos o con un conflicto en marcha, sino que los agresores pueden atacar a otros países por otros motivos, estén relacionados (suministro de armas, por ejemplo) o no con el conflicto. En 2021, EE. UU. acusó formalmente a Nobelium, un atacante de estado-nación de los servicios de inteligencia exterior rusos, de desplegar el ataque SolarWinds para filtrarse en redes gubernamentales estadounidenses y de la UE. El ataque de Nobelium alteró el escenario de amenazas de prácticamente todos los sectores. En octubre de 2022, el grupo de hackers prorruso Killnet lanzó **un sinfín de ataques de tipo DDoS**[13] contra el sector de la aviación estadounidense y reivindicó que todas las infraestructuras críticas del país deberían estar bajo un ataque persistente.

Los responsables de las empresas no han hecho oídos sordos a estas noticias de ciberataques continuados y al alza, ni tampoco a los esfuerzos de concienciación de organizaciones tanto públicas como privadas. El Informe de tendencias y estado de la ciberguerra de Armis: 2022-2023 ha revelado que el 74 % de los encuestados globales responsables de una infraestructura de TO crítica coincide en que las juntas directivas están transformando la cultura de las organizaciones hacia la ciberseguridad como respuesta a la amenaza de la ciberguerra.

De las respuestas de los sectores que más se relacionan con las infraestructuras críticas (ver tabla de abajo) se deduce la convergencia de la TI y la tecnología operativa (TO) en la Industria 4.0. Se pidió a los encuestados que seleccionaran los tres elementos con mayor riesgo en caso de ciberataque. En todos los sectores, las bases de datos y la información de identificación personal (PII) se mencionaron como las principales preocupaciones. Las infraestructuras críticas (instalaciones y equipamiento físico), el tiempo de inactividad operativa y la propiedad intelectual completaron el rango medio de las áreas en riesgo, mientras que los dispositivos conectados ocuparon el último puesto dentro de las preocupaciones de los sectores de infraestructuras críticas.



Estas respuestas señalan una serie de preocupaciones en cualquier entorno de TI[14], de TO[15], y de sistemas de control industrial[16], lo cual no es de extrañar si tenemos en cuenta la rápida convergencia de estos sistemas, antes dispares, que ha tenido lugar recientemente. Muchos de los sistemas de control industrial y de TO de las infraestructuras críticas se diseñaron hace décadas y siguen protegiéndose en gran medida con métodos heredados de diseño de red y acceso basado en roles. Como estos entornos están cada vez más interconectados y automatizados, la superficie de ataque se expande en la intersección de las redes existentes y los activos que nunca se diseñaron para conectarse a esas redes.

Esta intersección de activos conectados es lo que ha llevado a Armis a realizar investigaciones sobre vulnerabilidades de seguridad, a modo de contribución para aumentar la concienciación sobre estas vulnerabilidades y ataques que tienen impacto en las infraestructuras críticas. En marzo de 2022, el equipo de investigación de Armis dio a conocer públicamente tres vulnerabilidades de día cero con un posible impacto en más de 20 millones de dispositivos de sistemas de alimentación ininterrumpida (UPS) inteligentes de la empresa APC, que suministran energía de emergencia para activos esenciales en centros de datos, instalaciones industriales, hospitales, etc. Estas vulnerabilidades, denominadas conjuntamente TLStorm[17], permiten a los responsables de las amenazas desactivar, interrumpir y destruir estos dispositivos UPS y los activos conectados. Mediante la explotación de estas vulnerabilidades, un atacante podría convertir estos dispositivos UPS en armas, por ejemplo, manipulando el voltaje hasta que empiecen a arder, y pasar desapercibido. Estas vulnerabilidades suceden en sistemas cibernéticos físicos que unen el mundo digital y el físico, de ahí que sea tan importante detectarlas, ya que con ellas existe la posibilidad de que un ciberataque tenga consecuencias reales que pueden poner en peligro la vida y/o provocar la destrucción física de la infraestructura objeto del ataque.

AMENAZAS AL SECTOR SANITARIO

El sector sanitario es fundamental para los ciudadanos de cualquier país. Es vital para saber cómo funciona una sociedad, y desempeña un papel clave en el desarrollo de una nación moderna. Las consecuencias reales que pueden poner en peligro la vida cuando la seguridad de los pacientes está en jaque convierten a la asistencia sanitaria en uno de los principales objetivos de los responsables de las amenazas malintencionados. Por ejemplo, en octubre de 2022, **CommonSpirit Health[18]** sufrió un ataque de ransomware de gran magnitud en un sistema del que depende el funcionamiento de 140 hospitales y más de 1000 centros sanitarios de Estados Unidos. Al término de ese mismo año, el ataque seguía perjudicando a casi 20 millones de estadounidenses de 21 estados. Como consecuencia de ello, los sanitarios tuvieron que proporcionar asistencia sanitaria a los pacientes sin tener sus historiales médicos, lo que no deja de ser una forma realmente peligrosa de dar asistencia sanitaria. Se dio un caso, por ejemplo, en el que se administró una "megadosis" de analgésicos a un niño de tres años (quien, milagrosamente, sobrevivió) a resultas de este ataque. Antes, en 2020, un **ciberataque de proporciones mucho menores dirigido a un hospital de Düsseldorf[19]** resultó en una interrupción de la red y en la desviación de los pacientes a otros hospitales, lo que acabó con el fallecimiento de uno de ellos.

Los ataques a la asistencia sanitaria no solo son letales, sino también increíblemente caros para los sistemas sanitarios, que ya de por sí funcionan con unos presupuestos muy ajustados y que aún se encuentran en proceso de recuperarse de la sobrecarga que supuso la pandemia de la COVID-19. Los **CIO de asistencia sanitaria[20]** luchan por conservar un talento clave de tecnología y seguridad en un momento en que los teletrabajadores prefieren percibir sueldos más altos en otros sectores. Esta merma de personal cualificado surge en un punto de inflexión para las compañías sanitarias, que siguen siendo uno de los sectores más castigados por la ciberguerra y los ciberdelitos (según estimaciones actuales de IBM, el coste medio de una vulneración en el ámbito sanitario es de **10,1 millones de dólares[21]**, lo que supera la cifra de 9,44 millones calculada en todos los sectores). Cuando el sistema sanitario público irlandés **Health Service Executive[22]** sufrió un ataque con el ransomware Conti en 2021, se vieron obligados a trabajar en papel, lo que llevó a cancelar un 80 % de las citas de pacientes y a destinar un coste total estimado de 600 millones de dólares en solucionar el problema y sustituir los sistemas.

Según nuestro estudio, el 72 % de los encuestados responsables de TI en entornos médicos, farmacéuticos y de asistencia sanitaria coincide en que las juntas directivas están transformando la cultura de las organizaciones hacia la ciberseguridad como respuesta a la amenaza de la ciberguerra. Esta tendencia viene marcada por la predominancia y el goteo constante de ciberataques dirigidos al sector sanitario: el 45 %

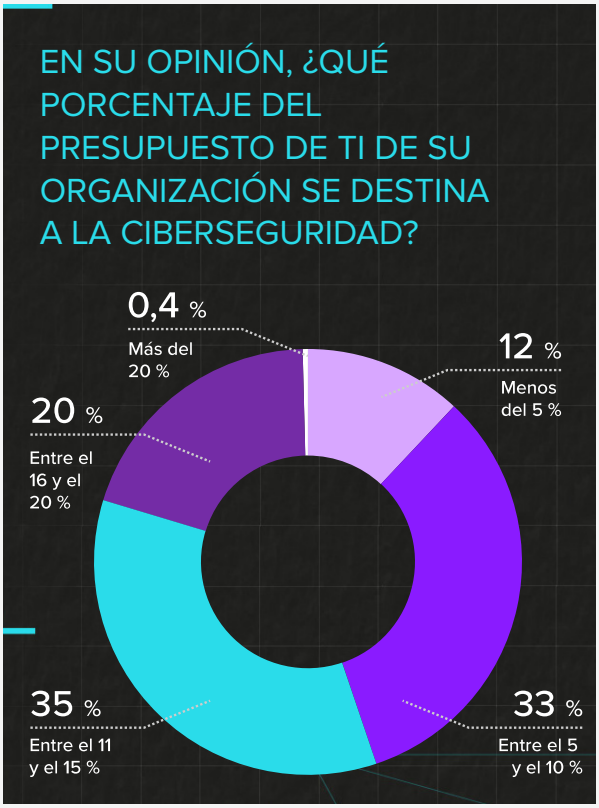
DE CERCA

Las organizaciones sanitarias globales encuestadas por Armis señalaron que su política de pago de rescates por un ataque de ransomware es la siguiente:

de los encuestados del sector señaló haber experimentado la misma actividad de amenazas en sus redes entre mayo y octubre de 2022 en comparación con los últimos seis meses, mientras que el 28 % afirmó haber experimentado una mayor actividad en el mismo intervalo de tiempo. Igualmente, los encuestados manifestaron estar bastante o muy preocupados por el impacto de la ciberguerra en sus organizaciones en general (70 %), en las infraestructuras críticas de la compañía (72 %) y en los servicios de la compañía (68 %).

Aún así, el gasto en ciberseguridad entre las organizaciones sanitarias es muy modesto en comparación con otros sectores globalmente. Casi la mitad (45 %) de las compañías sanitarias invierte menos del 10 % de sus presupuestos de TI en ciberseguridad. De media, los encuestados del ámbito sanitario globales afirmaron dedicar en torno al 11 % del presupuesto de TI de la compañía en ciberseguridad; otros mencionaron un 11-15 % (35 %) o 16-20 % (20 %) y los menos, un 20 % o más (menos del 1 %).

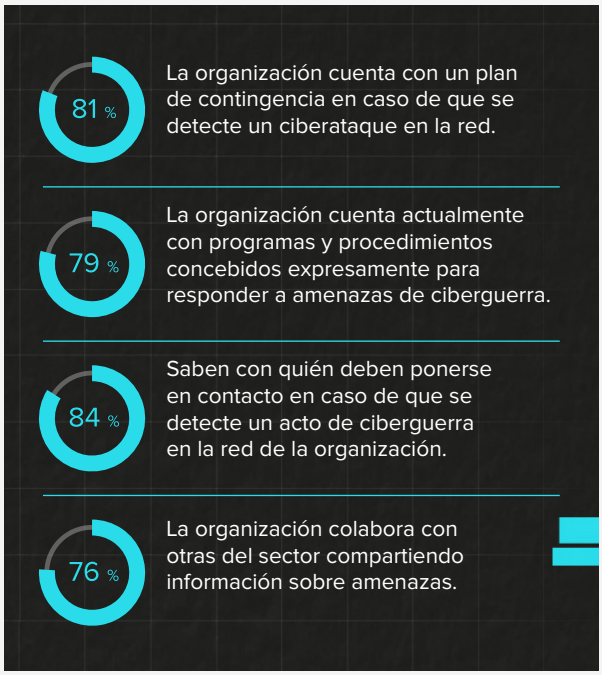
A medida que la TI sanitaria sigue avanzando y digitalizando la asistencia a los pacientes, la innovación permite lidiar con algunas de las principales dificultades a las que se enfrenta el sector sanitario, como la falta de personal, los costes al alza y problemas de cumplimiento. No obstante, el 55 % de los encuestados declaró que la amenaza de la ciberguerra puede ralentizar este proceso de digitalización. Esto puede tener un impacto notable en la vida de los pacientes, ya que no podrán beneficiarse de todas las ventajas de la digitalización si esta se ve frenada por los ciberataques. Si la digitalización no se adopta plenamente con la ciberseguridad en primer línea, estos nuevos proyectos podrían explotarse. Fijémonos en los sistemas de tubos neumáticos,



por ejemplo. Estos sistemas, que se usan en más del **80 % de los hospitales norteamericanos**[23] y se han instalado en más de 3000 centros hospitalarios de todo el mundo, automatizan la logística y el traslado de material por los hospitales a través de una red de tubos neumáticos. Su labor es fundamental en la asistencia a los pacientes y se usan prácticamente todo el tiempo. Los investigadores de Armis distinguieron nueve vulnerabilidades en estos aparatos en 2021, denominadas **PwnedPiper**[24], que si estuvieran en el punto de mira de los cibercriminales, podrían permitir que un atacante sin autenticar se hiciera con el control total de un hospital para desplegar un ataque de ransomware sofisticado o filtrar información confidencial del hospital.

AMENAZAS A AGENCIAS GUBERNAMENTALES

Los activos son el denominador común del mundo moderno, global, digital y fragmentado en el que vivimos. En este sentido, ninguna entidad posee más activos (personas, dispositivos o software) que las agencias gubernamentales y las personas a las que quieren atender y proteger. Pese a lo sucedido en los últimos años, los encuestados globales del sector público manifiestan una aparente confianza en torno al tratamiento de la ciberguerra:



Esta creciente confianza se deba quizá a que poseen información adicional compartida entre las alianzas globales. Los países del **«Club de los cinco ojos"[25]** (Australia, Canadá, Nueva Zelanda, Reino Unido y EE. UU.) comparten actualmente recursos de inteligencia para reforzar su situación de seguridad general, sobre todo en lo tocante a la protección de los activos. Como dato de interés, si alguno de estos países se viera envuelto en un conflicto de ciberguerra, el 63 % de los encuestados globales afirmó que respaldaría el alistamiento en una liga de ciberdefensa.

Esta abrumadora exhibición de confianza de las agencias vuelve a manifestarse en esta encuesta: 9 de cada 10 (90 %) de los encuestados gubernamentales afirman con seguridad que su país cuenta con protección frente la ciberguerra. Sin embargo, cuando se detectan infracciones, el 55 % de los encuestados globales cree que las agencias gubernamentales son incapaces de asumir —y, en última instancia, reparar— los efectos adversos de los cibercriminales. Esto no pudo hacerse más patente que en abril de 2022, cuando los atacantes del grupo de ransomware ruso conocido como Conti **se hicieron con el control del gobierno de Costa Rica[26]**. Este ataque congeló con total descaro los sistemas tributarios del país subtropical, lo que causó estragos en las exportaciones y retrasó el pago de los sueldos a sus ciudadanos. A través de este ataque, Conti se las apañó para filtrar el **97 % de todos los datos sustraídos[27]**. En mayo de 2022 la situación se había agravado de tal forma que el gobierno costarricense se vio obligado a declarar el estado de emergencia.

En Estados Unidos, las agencias gubernamentales, las instituciones y los sistemas educativos han sucumbido al "efecto goteo" global de la ciberguerra. Durante la fase más aguda de la pandemia de 2020 se produjeron en Estados Unidos 79 ataques de ransomware contra agencias gubernamentales. Se calcula que estas agencias perdieron alrededor de **18 800 millones de dólares[28]** en costes de recuperación y tiempo de inactividad. Como consecuencia de ello, en el tercer trimestre de 2021 el gobierno estadounidense lanzó **StopRansomware.gov[29]**, una agresiva misión destinada a reducir el volumen general de ransomware. A través de la colaboración público-privada, las agencias gubernamentales, como las estadounidenses, albergan la esperanza de empezar a proteger, detectar y solucionar de mejor forma el impacto de los ataques de ransomware.

DE CERCA

Las organizaciones gubernamentales son las menos dispuestas de todos los sectores a pagar un rescate en caso de sufrir un ataque de ransomware; un 43 % de los encuestados señala que la política de su organización consiste en no pagar nunca, porcentaje muy por encima de la media mundial (26 %) de los encuestados cuyas organizaciones tienen políticas que establecen no pagar nunca.

¿QUÉ TENDENCIAS DE CIBERSEGURIDAD SE ESTÁN PRODUCIENDO EN TODO EL MUNDO?

NO EXISTE UNA RESPUESTA ÚNICA AL RANSOMWARE

Muchos confunden equivocadamente los ataques de ransomware con un esfuerzo dirigido meramente al robo de datos críticos, pero lo cierto es que la mayoría de las organizaciones son una diana fácil y los cibercriminales, unos oportunistas. Al fin y al cabo, extorsionar a las empresas para pagar un rescate multimillonario para que puedan reanudar sus operaciones resulta mucho más efectivo y rentable que filtrar y vender cientos de miles de datos en el mercado negro.

Independientemente de si el ransomware lo implementan atacantes de estado-nación o cibercriminales, la anatomía de un ataque de ransomware es más o menos la misma. Comienza con la penetración en el sistema, que suele suceder en forma de envío a través de un sitio web en riesgo, mediante suplantación de identidad o realizando un ataque dirigido. Ya dentro, los atacantes se desplazan lateralmente por la red, escalando privilegios y "escarbando" en la red. Mediante el uso de túneles, los atacantes establecen una conexión de mando y control que conduce finalmente a la filtración de los datos de la organización y a la ejecución del ransomware, que cifrará los datos en el sistema de destino.

DarkSide es un grupo de cibercriminales de Europa del este que desarrolló REvil, una herramienta de ransomware que comenzó inicialmente como la variante GandCrab y que es una de las plataformas de ransomware como servicio (RaaS) más conocidas a raíz del ataque a Colonial Pipeline en 2021 que comentábamos antes. Aparecieron por primera vez en abril de 2019 y estuvieron en el cenit de su actividad hasta octubre de 2021, cuando los servidores de REvil fueron hackeados en una operación conjunta entre varios países y se vieron forzados a desconectarlos. Hasta entonces, DarkSide había suministrado su malware a “afiliados” y había repartido el rescate entre los clientes que realizaban los ataques. Aparte del malware en sí, DarkSide proporcionó el mecanismo de descifrado (que sigue considerándose como uno de los sistemas de descifrado más sofisticados de todas las familias de malware), la infraestructura de los chats de la red oscura, los sitios de filtración de la red oscura y los servicios de blanqueo de dinero. Con ayuda de los agentes de acceso inicial (una nueva generación de cibercriminales que vende el acceso a una red en riesgo), los afiliados obtienen acceso a una red objeto del

DE CERCA

¿Quién paga y quién no?

Algo más de 3 de cada 10 (31 %) profesionales de TI encuestados en compañías con más de 500 empleados afirmaron que la política de sus organizaciones con respecto al pago de rescates en caso de ataque de ransomware es no pagar nunca, y lo mismo sostiene más de un quinto (23 %) de los profesionales de TI encuestados en compañías con entre 100 y 249 empleados. Las respuestas difieren cuando se realiza una comparación entre países: casi la mitad (47 %) de los profesionales de TI encuestados en EE. UU. señala que la política de sus organizaciones con respecto al pago de rescates en caso de ataque de ransomware es pagar siempre, en claro contraste con los 1 de cada 14 (7 %) de Japón que sostiene lo mismo.

ataque, inician la carga de REvil y negocian con la organización afectada para pedir un rescate para restaurar los datos cifrados.

Por si no fuera suficiente con la proliferación de ransomware y el mercado de día cero, el Secretario General de Interpol, Jürgen Stock, manifestó en mayo de 2022 su preocupación ante la posibilidad de que el ciberarmamento desarrollado por los países pudiera estar accesible en la red oscura en apenas un par de años. "Es una gran preocupación del mundo físico: armas que se usan en el campo de batalla y que mañana podrían estar usando bandas del crimen organizado", sostuvo Stock durante un encuentro **moderado por la CNBC[30]** en el Foro Económico Mundial en Davos, Suiza.

Cuando los encuestados tuvieron que responder en este estudio a la pregunta sobre la política de sus organizaciones en torno al pago de rescates en caso de ataque de ransomware, las respuestas de los profesionales de TI globales estuvieron bastante divididas. Un 24 % de los encuestados reveló que sus organizaciones siempre pagaban; un 31 %, que sus organizaciones pagaban solo cuando los datos de cliente estaban en riesgo; un 26 %, que sus organizaciones no pagaban nunca, y un 19 %, que dependía de la situación.

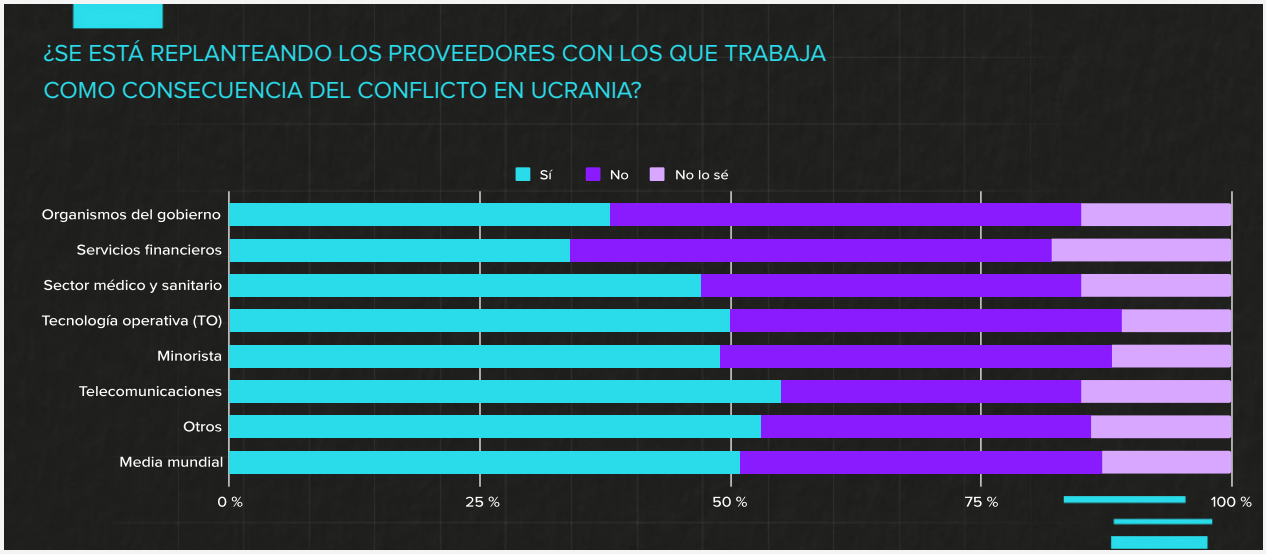
EL GASTO EN CIBERSEGURIDAD SIGUE CRECIENDO

Cuando se buscan indicios de en qué gastan su dinero de TI las empresas, no es de extrañar comprobar que lo destinan a la ciberdefensa, resiliencia y servicios de protección.

Algo más de tres cuartos (76 %) de los profesionales de TI 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.

Algo más de la mitad (51 %) de los encuestados globales reconoce haberse replanteado sus proveedores como consecuencia del conflicto en Ucrania, y prevé que sus organizaciones colaborarán con nuevos proveedores de ciberseguridad o proveedores de servicios de seguridad administrados de forma inmediata (31 %) o en los próximos seis meses (29 %). Es esencial que los proveedores estén al tanto de las tendencias de gasto y en qué parcelas de la organización son más necesarios sus servicios, así podrán asegurarse de que proporcionan las soluciones adecuadas.

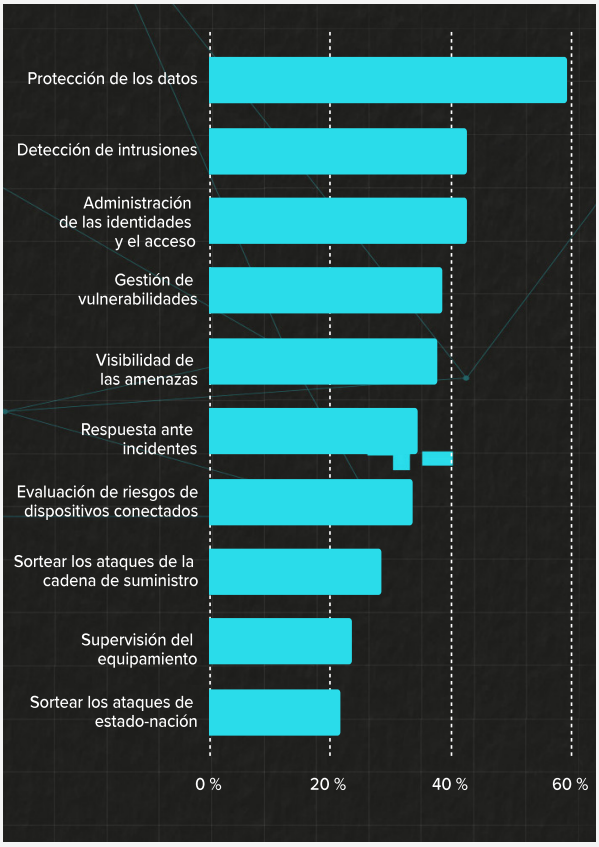
> *"La escasez de cualificaciones en ciberseguridad sigue siendo un problema muy extendido, ya que la falta de personal aumenta la demanda de servicios o soluciones, lo que hace el juego a las preciadas capacidades de los socios. La escasez de cualificaciones fortalece el mercado en ciberseguridad, sobre todo para los proveedores de servicios de seguridad administrados y para los socios que buscan reducir los riesgos del impacto empresarial mediante el desarrollo de servicios propios, que son más rentables."*
>
> **TIM MACKIE**
> VICEPRESIDENTE DE CANALES MUNDIALES EN ARMIS



Con los datos en la mano, casi 4 de cada 5 (78 %) de los profesionales de TI encuestados afirman que, ante los repentinos acontecimientos mundiales recientes y en curso (como la pandemia, el conflicto en Ucrania, etc.), es probable que sus compañías dediquen una mayor parte del presupuesto a ciberseguridad, mientras que casi 2 de cada 5 (37 %) creen que es muy probable. Así pues, ¿cuánto están gastando las organizaciones y en qué? De acuerdo con los datos que arroja este estudio, globalmente la media porcentual de presupuesto de TI asignado a ciberseguridad es del 11 %. Aquí se muestra desglosado:

Entre quienes dedican el mayor gasto, el 37 % afirma que es muy probable que la inversión aumente en breve y el 41 %, que es bastante probable. Sin embargo, las compañías que invierten menos demuestran una menor probabilidad de aumentar este gasto en breve.

Al pedirles que seleccionaran los aspectos de seguridad por orden de máxima prioridad, estas fueron las respuestas que se recibieron globalmente:



Más de 2 de cada 5 (42 %) profesionales de TI encuestados prevén que sus organizaciones invertirán en la **gestión de vulnerabilidades**[31] de forma inmediata y casi 3 de cada 10 (28 %), en los próximos seis meses. En cuanto a las inversiones en **administración de activos**[32], el 37 % de los encuestados señaló que sus compañías invertirían de forma inmediata y el 30 %, en los próximos seis meses.

Las empresas no solo están invirtiendo en soluciones de ciberseguridad, sino que están instaurando unos principios en toda la organización donde la ciberseguridad es prioritaria e invierten también en formación en ciberseguridad. Un tercio (33 %) de los profesionales de TI encuestados prevé que sus organizaciones instaurarán modelos "de **confianza cero**[33]" de forma inmediata y un 28 %, en los próximos seis meses. En cuanto a la formación en ciberseguridad, el 41 % de los encuestados globales asegura que sus organizaciones invertirán en más formación en ciberseguridad de forma inmediata y un 46 %, que lo harán durante el próximo año. Solo el 4 % de las organizaciones señala que no va a tomar ninguna medida para incrementar la formación en ciberseguridad.

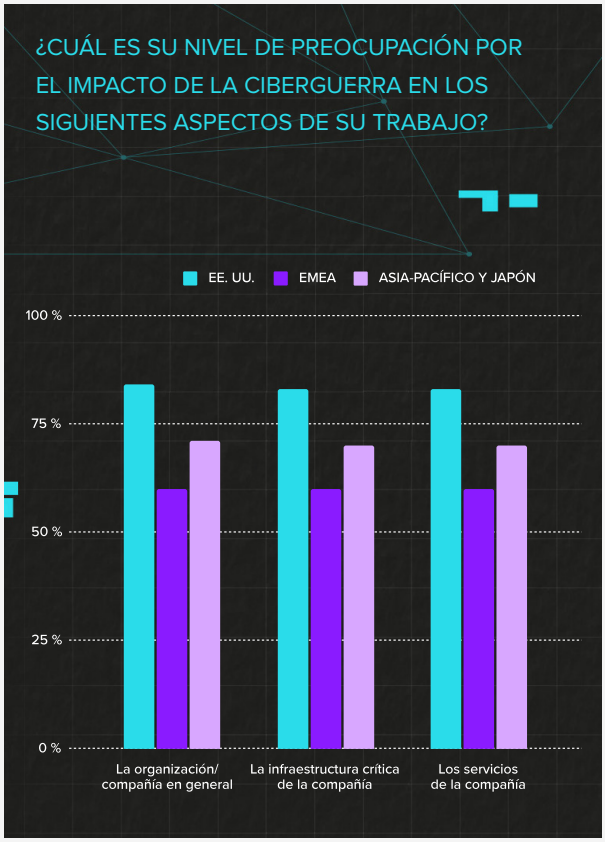
> *"Para desempeñar su labor eficazmente, los equipos de seguridad necesitan claramente un mayor grado de visibilidad contextualizada del panorama operativo de las tecnologías. El nivel de visibilidad ofrecido a los equipos de seguridad con tecnologías modernas ayuda a los CISO y a sus equipos a identificar auténticas oportunidades basadas en datos y dentro del contexto empresarial para eliminar del entorno las soluciones más antiguas que entran en conflicto y todos los gastos que estas conllevan."*
>
> **CURTIS SIMPSON**
> DIRECTOR DE SEGURIDAD DE LA INFORMACIÓN (CISO) EN ARMIS

¿CUÁLES SON LAS DIFERENCIAS REGIONALES (EE. UU., EMEA Y ASIA-PACÍFICO Y JAPÓN) DESTACABLES?

Además de las tendencias globales antes mencionadas, las diferencias regionales también fueron importantes al agrupar las respuestas de EE. UU., EMEA y Asia-Pacífico y Japón (Australia, Japón y Singapur). Por ejemplo:

PREOCUPACIÓN SOBRE EL ALCANCE DE LA CIBERGUERRA

Se preguntó a los encuestados de EE. UU., EMEA y Asia-Pacífico y Japón por su preocupación (o no) por el impacto de la ciberguerra en diferentes aspectos de su trabajo. Los encuestados de EMEA manifestaron una menor preocupación en comparación con sus homólogos de Asia-Pacífico y Japón —que mostraron mayor preocupación— y una preocupación significativamente menor que los profesionales de TI de EE. UU., que fueron quienes demostraron un mayor nivel de preocupación.



ACTIVIDAD DE AMENAZA Y NÚMERO DE INFRACCIONES EXPERIMENTADAS

- Según este estudio, los encuestados de Asia-Pacífico y Japón son los que han experimentado el menor número de infracciones de ciberseguridad; el 53 % de los encuestados de esta región señala que sus compañías han experimentado una o más infracciones de ciberseguridad. En comparación, casi 3 de cada 5 (58 %) encuestados de la región EMEA y 7 de cada 10 (73 %) de los encuestados estadounidenses señalaron que sus compañías han experimentado una o más infracciones de ciberseguridad.
- Las organizaciones estadounidenses también han experimentado la mayor tasa de aumento de la actividad de amenaza en los últimos meses (45 %), en comparación con sus homólogos en Asia-Pacífico y Japón (36 %) y EMEA (25%).

CONFIANZA EN LA PREPARACIÓN DE LA ORGANIZACIÓN

Los encuestados estadounidenses son los que muestran una mayor convicción en que sus compañías han asignado presupuesto suficiente para programas, personal y procesos de ciberseguridad, con casi 9 de cada 10 (88 %) de los encuestados que manifiestan esta convicción en EE. UU. comparado con el 78 % de Asia-Pacífico y Japón y el 76 % en EMEA. Es más, el 90 % de los encuestados estadounidenses asegura que los empleados de sus organizaciones saben a quién dirigirse en caso de detectar una actividad cibernética sospechosa, en comparación con los 4 de cada 5 (82 %) de las regiones EMEA o Asia-Pacífico y Japón.

PRÁCTICAS DE CIBERSEGURIDAD QUE YA ESTÁN EN MARCHA

- En cuanto a la inversión en seguros de ciberseguridad, las compañías estadounidenses son las que muestran una mayor probabilidad de haber invertido (45 %), seguido de Asia-Pacífico y Japón (37 %) y EMEA (31 %).
- Las respuestas sobre la importancia de formar a los empleados son similares en las tres regiones: EE. UU. (51 %), EMEA (49 %) y Asia-Pacífico y Japón (45 %).
- Respecto a la creación de una cultura del trabajo centrada en la seguridad, el 44 % de los encuestados estadounidenses señaló que en la cultura de sus compañías la seguridad tiene la máxima prioridad, frente al 37 % de los encuestados de EMEA y el 33 % de Asia-Pacífico y Japón.
- EE. UU. es la región con mayor probabilidad de tener implementado un marco de riesgos cibernéticos (43 %), frente al 34 % de los encuestados de Asia-Pacífico y Japón y el 31 % de los encuestados de EMEA.

PROTECCIÓN DE DATOS CONFIDENCIALES Y AFIANZAMIENTO DEL TRABAJO INTELIGENTE

Se preguntó a los encuestados si estaban de acuerdo o no con las siguientes afirmaciones:

- *"Mi organización conserva datos confidenciales, existe una normativa que debemos seguir y buscamos reducir al mínimo cualquier efecto negativo derivado de un evento de seguridad."*
  - » Estuvieron de acuerdo con esto: 91 % en EE. UU., 84 % en Asia-Pacífico y Japón y 83 % en EMEA.
- *"El problema de la seguridad de TI se ha convertido en un aspecto importante para los empleados con la adopción del trabajo inteligente."*
  - » Estuvieron de acuerdo con esto: 91 % en EE. UU., 85 % en Asia-Pacífico y Japón y 81 % en EMEA.

ANÁLISIS POR PAÍSES

Quienes quieran ver las diferencias regionales antes mencionadas con más detalle, el equipo de Armis ha preparado un exclusivo análisis por países más relevante para los países y territorios encuestados como parte de este estudio.

Para acceder a los informes individuales de cada país, que puede leer en inglés así como en sus versiones traducidas, visite https://www.armis.com/cyberwarfare.

1. **EE. UU.**
2. **Reino Unido**
3. **Francia**
4. **DACH** (Austria, Suiza y Alemania)
5. **Península ibérica**
6. **Italia**
7. **Dinamarca**
8. **Holanda**
9. **APJ** (Australia, Japón y Singapur)

CONCLUSIÓN

¿Por qué son importantes estas conclusiones y qué puede hacer su organización para protegerse?

Los responsables de TI y de seguridad de todo el mundo reconocen que no se están tomando en serio la amenaza de la ciberguerra, que no se sienten preparados para hacer frente a una amenaza de ciberguerra y que el aspecto de seguridad que ocupa el último puesto desde su punto de vista es evitar ataques de estado-nación. Para colmo, están viendo un aumento de las amenazas de ciberguerra como consecuencia de la guerra de Ucrania, lo que se deduce de la mayor actividad de amenaza que experimentaron en sus redes entre mayo y octubre de 2022 en comparación con los seis meses previos. Y no solo se nota más actividad —que no se toman en serio—, sino que están permitiendo que la amenaza de la ciberguerra incida en su capacidad de innovación, y reconocen que como resultado de esto se están paralizando o deteniendo proyectos de transformación digital. Sin duda, estas amenazas no son de las que pueden soslayarse, sino que hay abordarlas de frente para poder defenderse de ellas.

Anteriormente en el informe, de los encuestados que ya dedican el mayor gasto en ciberseguridad, el 37 % afirma que es muy probable que la inversión aumente en breve y el 41 %, que es bastante probable. Más de 2 de cada 5 (42 %) profesionales de TI y de seguridad encuestados prevén que sus organizaciones invertirán en la **gestión de vulnerabilidades[34]** de forma inmediata y casi 3 de cada 10 (28 %), en los próximos seis meses. En cuanto a las inversiones en **administración de activos[35]**, el 37 % de los encuestados señaló que sus compañías invertirían de forma inmediata y el 30 %, en los próximos seis meses.

El impacto de un ataque de red en las operaciones y la reputación de una organización es el mismo tanto si procede de un atacante de estado-nación o de un cibercriminal. Es más, el protocolo de escritorio remoto, las redes de tipo BYOD (donde los usuarios pueden incorporar sus propios dispositivos), las vulnerabilidades de las redes privadas virtuales o una configuración errónea del protocolo se están convirtiendo en los puntos de entrada más habituales entre los atacantes. Esto se ha acentuado con la pandemia: en 2021, los ataques de ransomware **prácticamente se duplicaron[36]** en todo el mundo.

Disponer de unas herramientas adecuadas, además de un plan de respuesta a incidentes es solo el primer paso. Probar el plan periódicamente puede ayudar a detectar los puntos débiles de ciberseguridad de manera proactiva y a reforzar las defensas para proteger los datos críticos tanto de las empresas como de los usuarios, por no hablar de los costes millonarios que las organizaciones podrían ahorrarse por posibles filtraciones de datos.

Armis sugiere poner en marcha las siguientes medidas en todas las organizaciones:

- Independientemente de las herramientas y las técnicas que una organización decida usar, muchas organizaciones necesitarán ayuda para mitigar los efectos de un ataque mediante la ejecución de un plan de respuesta a incidentes. Algo bastante recomendable suele ser que la organización tenga de retén un equipo de respuesta a incidentes para reducir los costes y acelerar la respuesta a los incidentes.
- Cuando se detecta un ataque, es fundamental reducir su efecto al mínimo. El aislamiento del dispositivo afectado sigue siendo la estrategia predominante en la mayoría de las organizaciones. Existen diferentes técnicas de aislamiento, y casi todas las herramientas de detección y respuesta de terminales incluyen funciones de aislamiento de dispositivos.

Gracias a ello, los responsables de la respuesta a incidentes podrán aislar equipos concretos del resto de la red.

- Tener un proceso y una estrategia de copia de seguridad en condiciones constituye también una línea de defensa esencial frente a los ataques de estado-nación y los cibercriminales. Las organizaciones deben garantizar que la solución que decidan usar sea resistente a los ataques e incluya funciones de supervisión continua y de comprobación de la integridad.
- Una organización resiliente frente a ciberataques también invertirá en formar a sus empleados para concienciarlos sobre la seguridad. Asegúrese de que los empleados reciban formación cada cierto tiempo sobre cómo identificar correos electrónicos malintencionados, y proporcione unos mecanismos de comunicación que sean fáciles de usar.

Las organizaciones deben operar siguiendo la máxima de que la actividad de los atacantes de estado-nación o cibercriminales va a tener éxito. A fin de cuentas, a los responsables de las amenazas malintencionados les basta con poder acceder a la red de una organización en cualquiera de sus intentos, mientras que los equipos de TI y de seguridad necesitan una defensa que funcione el 100 % de las veces para evitar estos ataques.

Así pues, ¿qué pueden hacer las organizaciones? La forma más adecuada de mejorar la situación de seguridad y solucionar incidentes rápidamente 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.

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.**

DATOS DEMOGRÁFICOS DEL INFORME

Para preparar este informe, Armis encargó un estudio a Censuswide, en el que se encuestó a 6021 profesionales de TI y de seguridad de compañías con más de cien empleados con sede en EE. UU., Reino Unido, España, Portugal, Francia, Italia, Alemania, Austria, Suiza, Australia, Singapur, Japón, Países Bajos y Dinamarca. Las respuestas se obtuvieron entre el 22 de septiembre y el 5 de octubre de 2022.

ENCUESTADOS POR PAÍS	
Australia	511
Austria	100
Dinamarca	50
Francia	501
Alemania	501
Italia	500
Japón	501
Holanda	52
Portugal	251
Singapur	501
España	500
Suiza	50
Reino Unido	1003
EE. UU.	1000

ENCUESTADOS POR PUESTO/ROL	
Director de información (CIO)	432
Director de seguridad de la información (CISO)	241
Director de tecnología (CTO)	530
Especialista en asistencia informática	229
Administrador de base de datos	457
Analista de seguridad de la información	392
Jefe de proyectos de tecnología de la información (TI)	1831
Administrador de red	394
Arquitecto de redes	260
Otros	346
Analista de sistemas	493
Desarrollador web	416

ENCUESTADOS POR SEGMENTO	
Gobierno, autoridades locales, agencias públicas	369
Servicios financieros y seguros	120
Medicina, asistencia sanitaria, sector farmacéutico	255
TO (automoción, distribución, logística, alimentación y bebida, fabricación, petróleo, gas, construcción, minería, agricultura, transporte)	1415
Tecnología y otros	3133
Comercio minorista y venta al por mayor	295
Telecomunicaciones	434

NOTAS FINALES

1. https://www.gartner.com/en/newsroom/press-releases/2021-07-21-gartner-predicts-by-2025-cyber-attackers-will-have-we
2. https://www.csoonline.com/article/3654833/u-s-charges-russian-government-agents-for-cyber-attacks-on-critical-infrastructure.html
3. https://www.wired.com/story/oldsmar-florida-water-utility-hack/
4. https://www.washingtonpost.com/politics/2021/10/01/ransomware-attack-might-have-caused-another-death/
5. https://www.nsa.gov/
6. https://www.nytimes.com/2016/08/17/us/shadow-brokers-leak-raises-alarming-question-was-the-nsa-hacked.html
7. https://arstechnica.com/information-technology/2019/09/for-the-first-time-ever-android-0days-cost-more-than-ios-exploits/
8. https://www.armis.com/cyberwarfare/
9. https://www.ibm.com/reports/data-breach
10. https://www.gartner.com/en/newsroom/press-releases/2022-10-13-gartner-identifies-three-factors-influencing-growth-i
11. https://www.einpresswire.com/article/556075599/cybersecurity-jobs-report-3-5-million-openings-through-2025
12. https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html
13. https://www.darkreading.com/attacks-breaches/us-airports-cyberattack-crosshairs-pro-russian-group-killnet
14. https://www.armis.com/cybersecurity-asset-management/
15. https://www.armis.com/ot-device-security/
16. https://www.armis.com/ics-risk-assessment/
17. https://www.armis.com/research/tlstorm/
18. https://www.healthcaredive.com/news/commonspirit-health-ransomware-cyberattack/634011/
19. https://www.securityweek.com/german-hospital-hacked-patient-taken-another-city-dies
20. https://www.beckershospitalreview.com/healthcare-information-technology/a-war-for-talent-cios-detail-the-challenges-of-retaining-health-it-professionals.html
21. https://www.ibm.com/reports/data-breach
22. https://www.bankinfosecurity.com/irish-ransomware-attack-recovery-cost-estimate-600-million-a-16931
23. https://www.swisslog-healthcare.com/-/media/swisslog-healthcare/documents/products-and-services/transport/translogic-pts/pts-513-swisslog-healthcare-delivers-unmatched-innovation.
24. https://www.armis.com/research/pwnedpiper/
25. https://www.zdnet.com/article/five-eyes-advisory-warns-more-malicious-russian-cyber-activity-incoming/
26. https://www.bleepingcomputer.com/news/security/how-conti-ransomware-hacked-and-encrypted-the-costa-rican-government/
27. https://www.bleepingcomputer.com/news/security/costa-rica-declares-national-emergency-after-conti-ransomware-attacks/
28. https://www.americancityandcounty.com/2021/03/22/report-ransomware-attacks-cost-local-and-state-governments-over-18-billion-in-2020/
29. http://stopransomware.gov
30. https://www.cnbc.com/2022/05/23/military-cyberweapons-could-become-available-on-dark-web-interpol.html
31. https://www.armis.com/avm/

32. https://www.armis.com/armis-asset-management/

33. https://www.armis.com/zero-trust/

34. https://www.armis.com/avm/

35. https://www.armis.com/armis-asset-management/

36. https://www.securitymagazine.com/articles/97166-ransomware-attacks-nearly-doubled-in-2021#:~:text=Ransomware%20attacks%20rose%20by%2092.7,nation%2Dstate%20cyberattacks%20and%20more.

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®