[INFORME_DE TENDENCIAS:EN CIBERSEGURIDAD]

2025

SOFISTIC CYBERSECURITY 480

Resultados de las auditorías y monitorización del SOC (Security Operations Center) a empresas realizadas por Sofistic en 2024 y recomendaciones de ciberseguridad para 2025

Marzo de 2025

ÍNDICE

[1] ¿QUÉ TE APORTA ESTE INFORME DE CIBERSEGURIDAD?

Manuel Ginés
Head of R&D

Juan Carlos García
Chief Operations Officer & SOC Director y Ph.D. in Computer Science

Las organizaciones se enfrentan a una compleja escalada de ciberamenazas, derivada de la sofisticación de los ataques, el aumento de la superficie de exposición o el uso de sistemas de inteligencia artificial generativa. Desde Sofistic, la división de ciberseguridad de la tecnológica Cuatroochenta, somos conscientes de este contexto desafiante y altamente cambiante que requiere de una respuesta rápida y eficaz. Por ello se vuelve prioritario conocer el estado del arte de la ciberseguridad, analizando las vulnerabilidades y estrategias más efectivas.

Precisamente, eso es lo que hemos hecho en la tercera edición del **Informe de tendencias de ciberseguridad 2025.** Como venimos haciendo desde 2022, hemos analizado los resultados anonimizados de las auditorías y la monitorización del SOC (Centro de Operaciones de Seguridad, en sus siglas en inglés) que ha realizado Sofistic, a lo largo de 2024, a empresas tanto en Latinoamérica como en España. Nuestro objetivo es proporcionar una visión integral que permita a las organizaciones fortalecer su defensa, optimizando recursos y actuando con eficacia.

Además de un ejercicio de transparencia y divulgación, con este informe compartimos nuestros conocimientos y experiencia sobre prevención, detección y respuesta activa. Comprender el origen, el alcance y el impacto de las amenazas es fundamental para enfrentarse a un entorno en constante evolución. La ciberseguridad es más efectiva cuando pasa desapercibida y garantiza la protección sin interrupciones. En Sofistic estamos convencidos que esto se consigue gracias a un enfoque integral de seguridad, apoyado en un equipo preparado para conocer, fortalecer y actuar de forma eficaz ante un incidente de seguridad.

[2] MUESTRA

El informe parte de una muestra suficientemente amplia y representativa del trabajo realizado por el equipo de profesionales de Sofistic en 2024. Está compuesta por los resultados de las auditorías de seguridad y de la monitorización en el SOC. A continuación, detallamos ambas muestras y su alcance geográfico y sectorial:

Vulnerabilidades encontradas en auditorías de seguridad

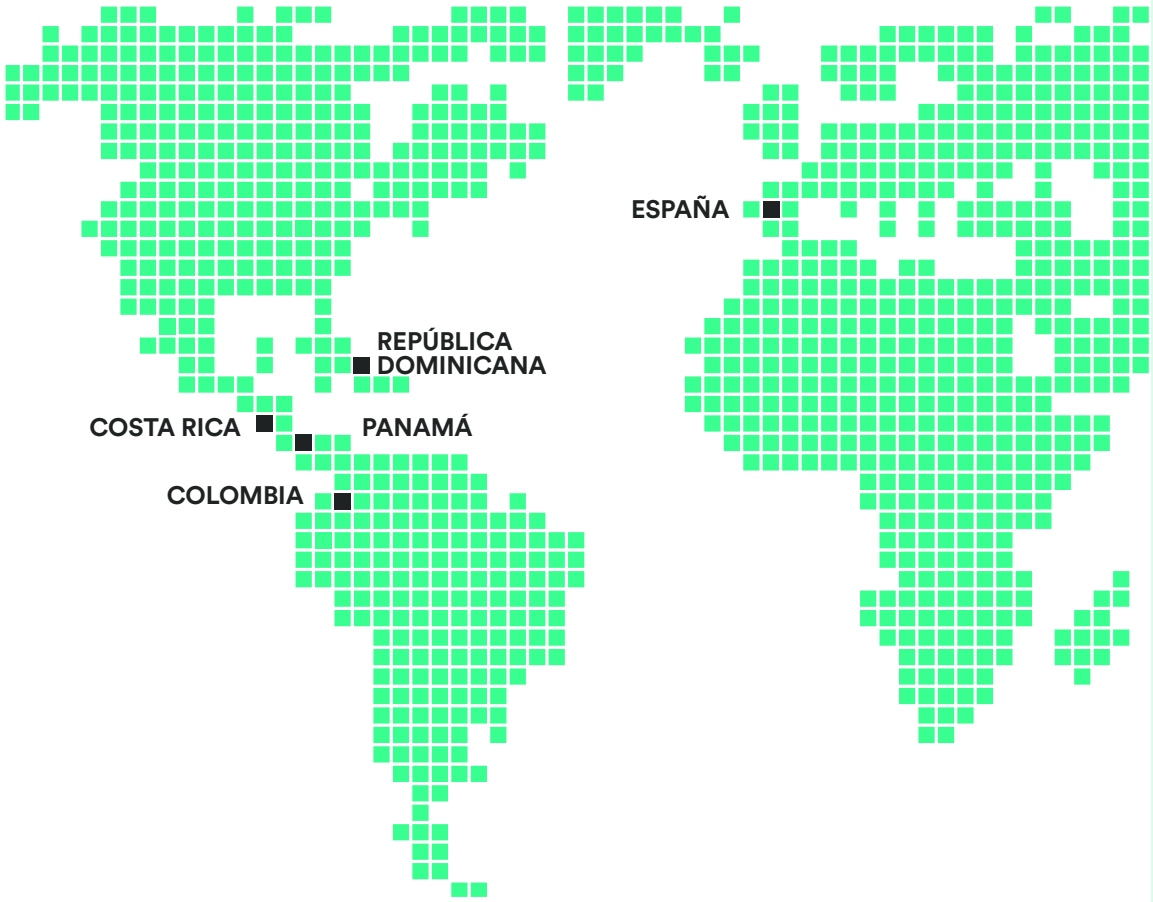
Hemos tomado una muestra de 140 auditorías realizadas a 40 clientes, lo que supone el análisis de 1.350 vulnerabilidades. Hemos incluido auditorías a aplicaciones (web y móviles), infraestructuras (externas e internas), código fuente e ingeniería social.

Casos de seguridad detectados en el SOC

Hemos seleccionado una muestra representativa de 100.000 alertas y 1.500 casos entre todos los gestionados por el equipo de los SOC de Sofistic, ubicados en España, Colombia y Panamá durante 2024. Es una muestra suficientemente amplia que permite identificar los tipos de amenazas e incidentes detectados el último año. En el análisis del resultado de esta monitorización, hay que tener en cuenta que durante este 2024 hemos hecho una revisión de la nomenclatura para ser más precisos. En informes anteriores, se utilizaba el término incidente para aglutinar los eventos gestionados y ahora se denominan casos, clasificándolos a su vez en solicitudes de información e investigaciones (RFI), ciberinteligencia (CTI), incidentes (INC) y casos de configuración (CONF).

Ámbito geográfico

Los clientes de Sofistic se distribuyen principalmente entre España y Latinoamérica, con especial presencia en países como Colombia, Panamá, Costa Rica y República Dominicana.



Sectores

Infraestructuras críticas
(compañías energéticas, distribución de agua, aeropuertos y hospitales)

Banca y finanzas

Industria y servicios

[3] RESULTADOS

[3.1] Auditorías de seguridad

Mayor protección frente a más ataques menos críticos

Arrancamos este informe poniendo el foco en los fallos de seguridad identificados en los diferentes sistemas, a partir de las auditorías realizadas. En base a esa muestra, ya detallada, podemos ver la evolución de las vulnerabilidades en 2024 en comparación con 2023.

Auditorías	-8%
Vulnerabilidades	+2%
Criticidad	-8%

Variación 2022/24

Durante el 2024, observamos una disminución del número de auditorías ejecutadas (-8%), así como de los informes derivados de esos análisis (-8%), después de dos años de un ritmo de crecimiento destacable. Esta reducción no se explica por una menor demanda de este tipo de servicios, sino porque son organizaciones que tienen un nivel avanzado de ciberseguridad, y tras haber realizado evaluaciones a entornos o sistemas críticos, ahora no requieren de esos controles. A pesar de esta disminución, crece ligeramente el número de vulnerabilidades identificadas (+2%) respecto a 2023 y baja de forma notable (-8%) su severidad. Tendencia que empezamos a detectar en 2023 a raíz de una mayor madurez en ciberseguridad de las empresas e instituciones.

3 auditorías por cliente

Observamos que, después de auditar los entornos más críticos, identificar los resultados y acompañarlas para realizar mejoras y corregir fallos, estas empresas replican y amplían estos análisis a otras soluciones o sistemas.

Repunte de las auditorías web mientras bajan el resto

Por tipo de auditoría	Variación 2021/22	Variación 2022/23	Variación 2023/24
Web	+3%	+45%	+8%
Infraestructura	+112%	+24%	-14%
Cloud	+400%	-40%	-33%
Móvil	-10%	+44%	-23%
Phishing	+18%	-8%	-25%
Revisión código	+92%	-19%	-72%

Tras analizar la muestra de auditorías y vulnerabilidades, se detecta un aumento (+8%) de los análisis de seguridad web, mientras que en el resto se observa una disminución respecto a 2023. Esto se podría atribuir a que los servicios o páginas web de las compañías son dinámicas y en constante evolución, de manera que requieren de controles periódicos que garanticen su seguridad. Además, son puntos de exposición pública que suelen estar entre los objetivos de los ciberatacantes, por lo que las auditorías permiten mitigar posibles riesgos.

A pesar de esta tendencia, las de infraestructura continúan ocupando el primer puesto por volumen de auditorías realizadas. Es lógico que la infraestructura, compuesta por redes, servidores o dispositivos, sea el foco de la mayor parte de las evaluaciones de seguridad, ya que son la base de los sistemas tecnológicos y su fragilidad podría comprometer e interrumpir la operativa de una organización.

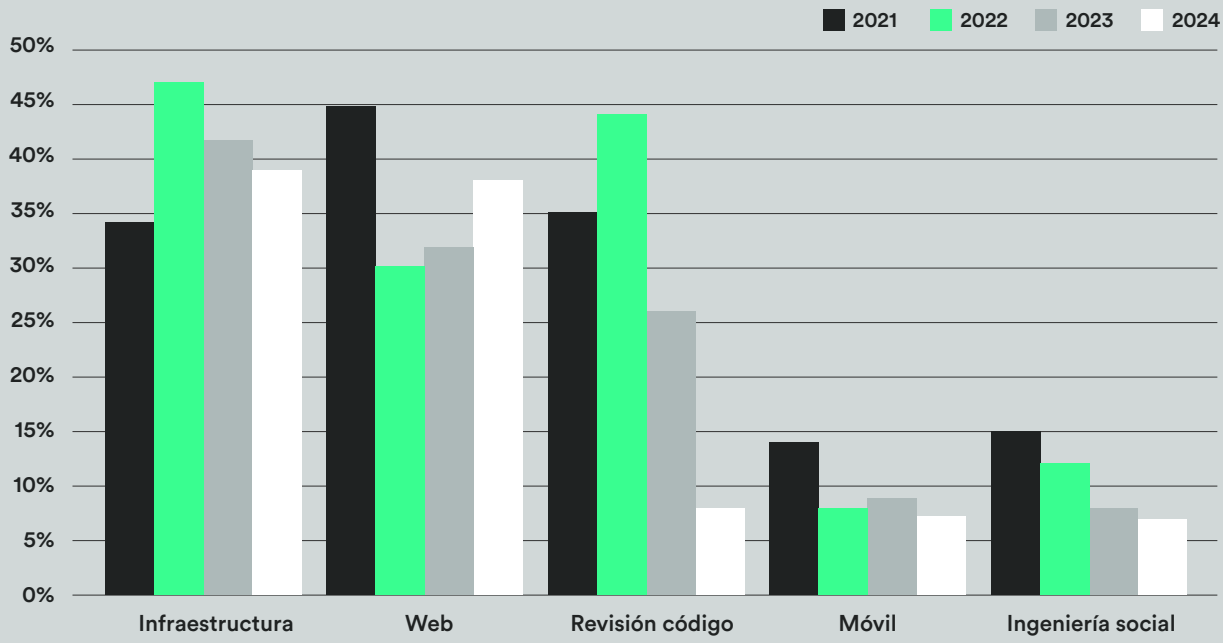
De la muestra, también se observa que las auditorías de revisión de código son las que más bajan (-72%) respecto al año anterior. Todo apunta a que, como signo de esa madurez que mencionábamos, las organizaciones han integrado, como buena práctica, herramientas de análisis de código en el flujo de desarrollo, en detrimento de este tipo de auditorías específicas. Además, se debe tener en cuenta que las revisiones de código suelen formar parte de las auditorías de aplicaciones, tanto web como móviles.

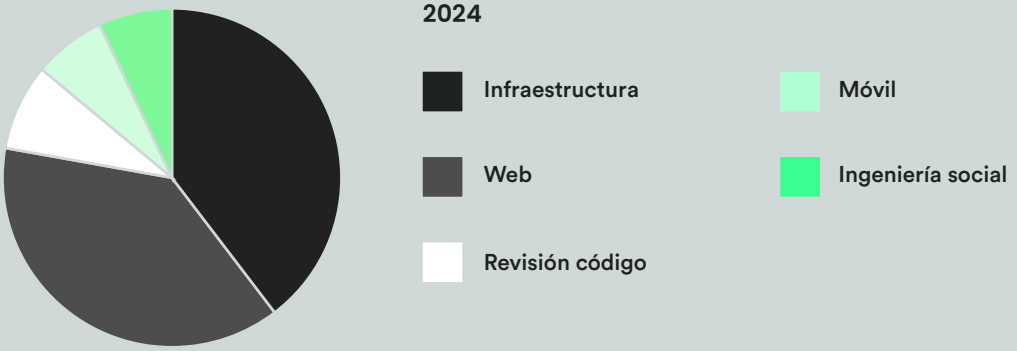
Las auditorías de infraestructura, las más frecuentes por su relevancia crítica

Top tipo de Auditorías por volumen	2021	2022	2023	2024
Infraestructura	34%	47%	42%	39%
Web	45%	30%	32%	38%
Revisión código	35%	44%	26%	8%
Móvil	14%	8%	9%	7%
Ingeniería social	15%	12%	8%	7%

39% **auditorías de infraestructuras**

Tipos de auditoría

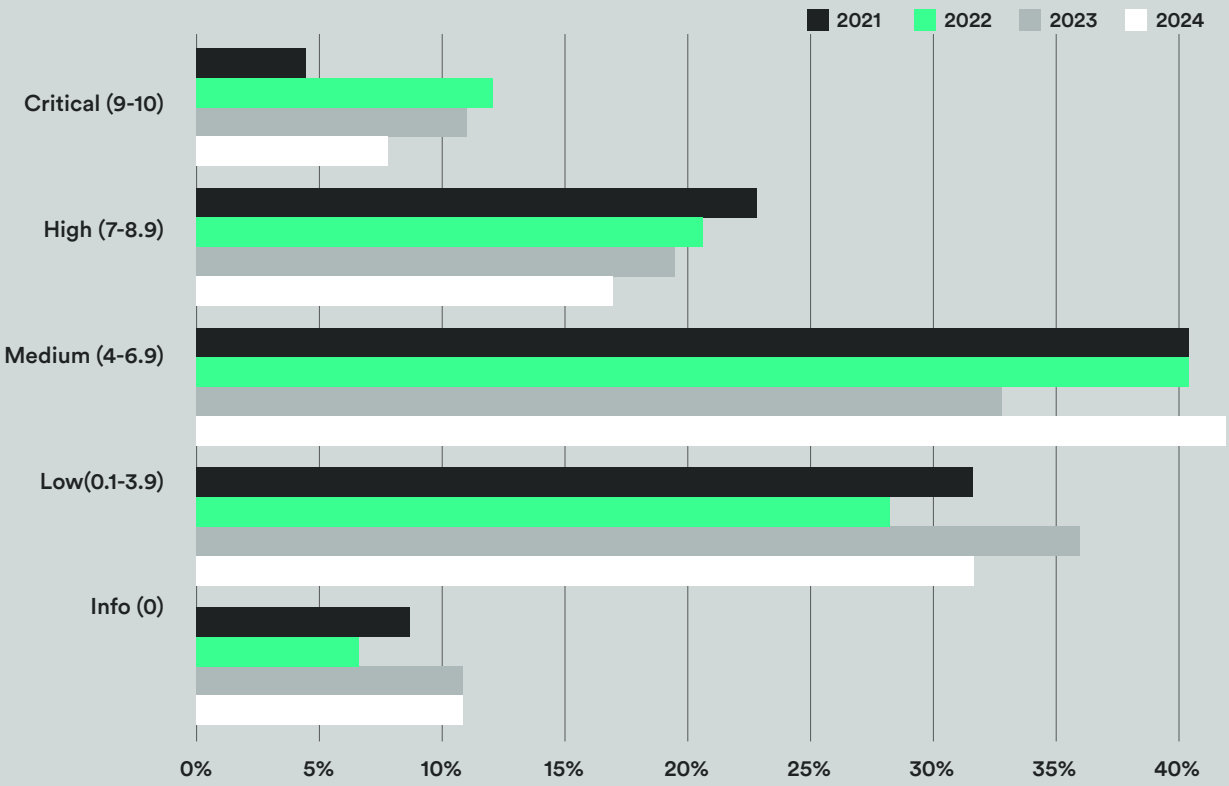




Bajan los fallos críticos o de riesgo alto, pero suben los de riesgo medio

Severidad (% del total)	2021	2022	2023	2024
Critical (9-10)	4%	11%	10%	7%
High (7-8.9)	21%	19%	18%	15%
Medium (4-6.9)	37%	37%	30%	37%
Low (0.1-3.9)	29%	26%	33%	28%
Info (0)	8%	6%	10%	10%

Severidad de las vulnerabilidades



Durante el 2024 se observa una reducción de la severidad de las vulnerabilidades detectadas, tal y como se empezó a percibir en 2023. Según la muestra de las auditorías realizadas, disminuye en 3 puntos el volumen de fallos críticos que representan el 7% del total y 3 puntos más los de riesgo alto que suponen el 15%. Es una tendencia positiva que demuestra que los fallos que comprometen sistemas, redes o datos y que pueden paralizar servicios se han corregido o mitigado. Por contra, suben en 7 puntos los fallos de riesgo medio que corresponden al mayor volumen sobre el total con un 37%. Aunque este tipo de vulnerabilidades, como la exposición de versiones de software desactualizado o el almacenamiento inseguro de contraseñas, no comprometen directamente un sistema, sí podrían ser explotadas en conjunto con otras desencadenando ataques más amplios dirigidos a poner en riesgo la seguridad de una compañía.

El **22% de las vulnerabilidades** detectadas son críticas o de alto riesgo, un porcentaje que baja 6 puntos respecto al año anterior.

Tipos de fallos

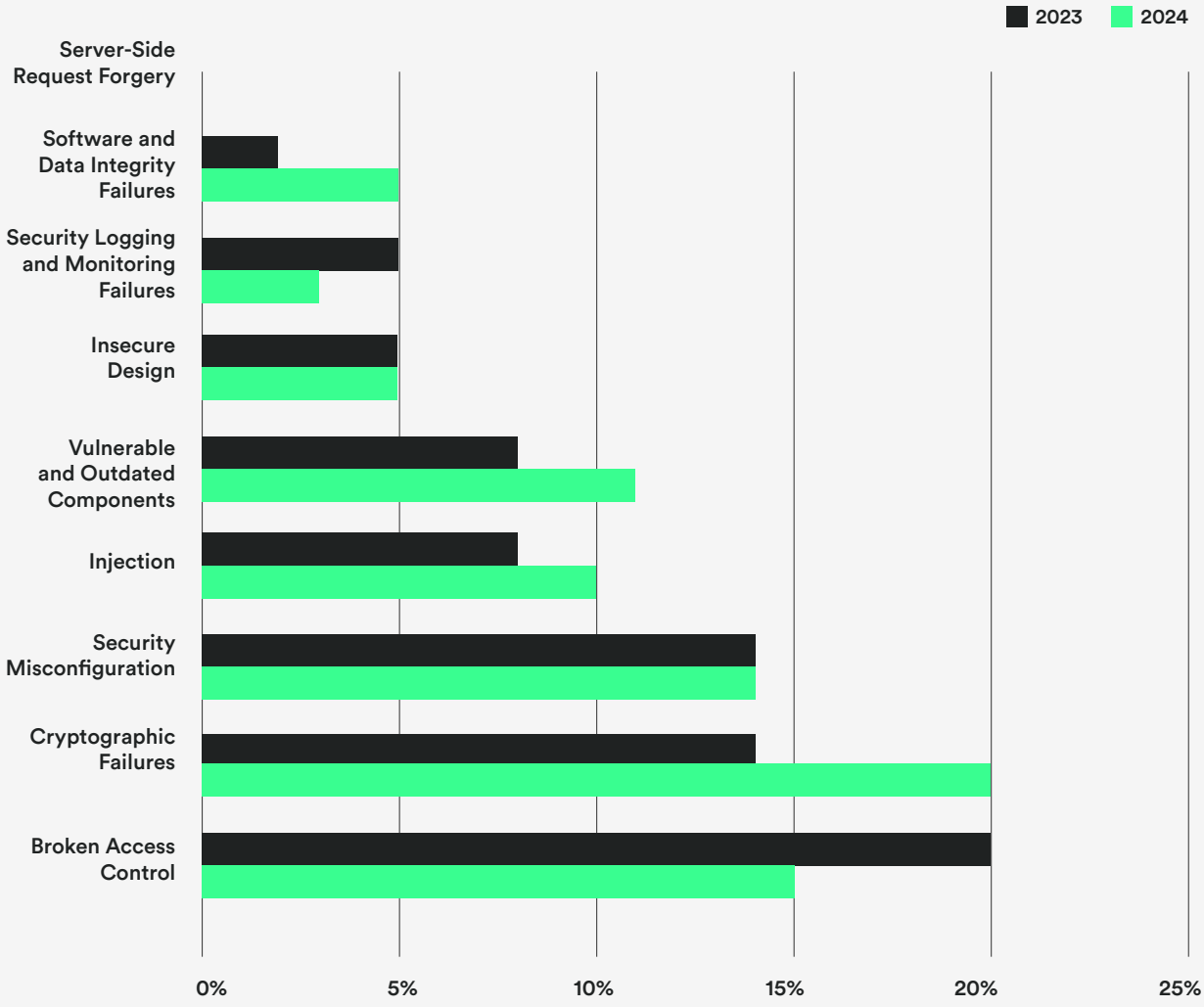
Si desglosamos y analizamos los fallos detectados por categoría de vulnerabilidad, se percibe que el ranking ha variado ligeramente respecto al año 2023. Los fallos de control de acceso, aquellos ocasionados por autorizaciones incorrectas y restricciones de acceso mal implementadas, encabezan el ranking, mientras que en 2022 estaban en segunda posición. Le siguen los fallos criptográficos, que bajan un puesto respecto al año anterior. Este tipo de debilidades se producen, por ejemplo, cuando los mecanismos de cifrado o protección de datos están mal configurados o están obsoletos y pueden ser explotados por los ciberdelincuentes. Es un tipo de vulnerabilidad frecuente en las aplicaciones web, que precisamente son los entornos en los que más ha crecido la demanda de auditorías de seguridad, según se desprende de la muestra analizada. En tercer lugar, se mantienen los fallos de configuración del sistema relacionados, por ejemplo, con una incorrecta configuración de un sistema, aplicación o servicio que podría exponer datos sensibles, permitir accesos no autorizados o facilitar la explotación de otros ataques. El resto del ranking se mantiene prácticamente igual respecto al año anterior, a excepción de los fallos de inyección, que suben una posición situándose en cuarto lugar, y los de registro y monitoreo de seguridad, que también escalan una posición hasta el séptimo puesto.

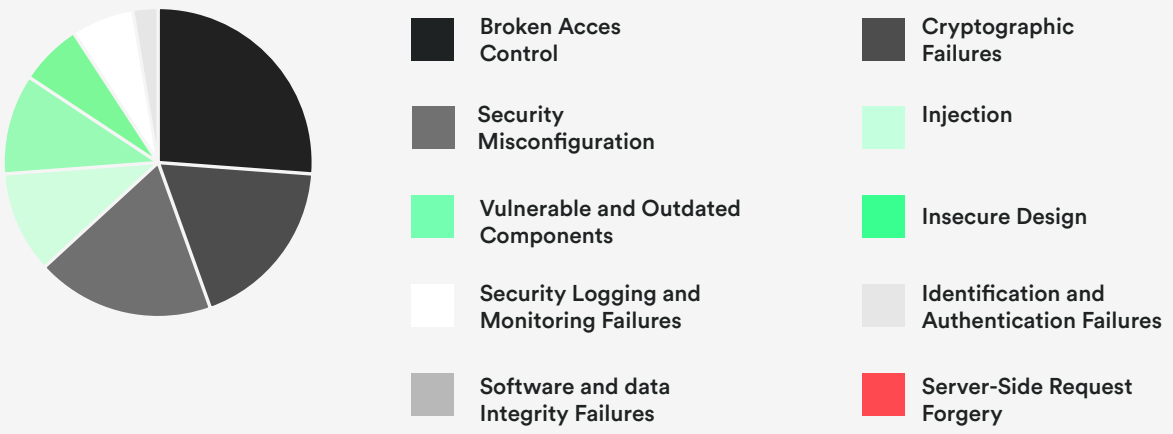
Si se analiza la evolución por volumen respecto del total, suben los fallos de registro y monitoreo, los de control de acceso o los de diseño inseguro, mientras que bajan los de integridad del software y datos, los de identificación y autenticación, los criptológicos y los de componentes vulnerables y desactualizados.

La siguiente tabla resume el peso relativo de cada categoría de incidencia y su evolución desde 2021, incluido el ranking actual de las 10 principales:

Categoría	**Volumen**							
Accionista	2021	2022	2023	2024	Variación 2022-2023	2023	2024	
Broken Access Control	21%	18%	18%	26%	+49%	2	1	+1
Cryptographic Failures	17%	25%	24%	18%	-23%	1	2	-1
Security Misconfiguration	18%	16%	16%	11%	+11%	3	3	=
Injection	14%	13%	12%	7%	-9%	5	4	+1
Vulnerable and Outdated Components	10%	13%	13%	18%	-22%	4	5	-1
Insecure Design	10%	7%	6%	10%	+16%	6	6	=
Security Logging and Monitoring Failures	2%	3%	4%	2%	+57%	8	7	+1
Identification and Authentication Failures	7%	5%	6%	0%	-55%	7	8	-1
Software and Data Integrity Failures	1%	0%	1%	6%	-100%	9	9	=
Server-Side Request Forgery	0,00%	0,00%	0,00%	0%	0%	10	10	=

Categorías de las vulnerabilidades





Phishing: la mitad de los usuarios abre correos fraudulentos, pero caen menos en la trampa

Phishing	2021	2022	2023	2024	2021 - 2022	2022 - 2023	2023 - 2024
Email abierto	50%	36%	33%	50%	-28%	-8%	+53%
Acceso enlace	29%	18%	40%	24%	-40%	+128%	-39%
Credenciales	11%	10%	20%	17%	-5%	+95%	-31%

A partir de la muestra de auditorías de ingeniería social realizadas durante el año 2024, observamos un aumento destacable del número de usuarios que interactúan con emails de phishing (+53%). Lo más reseñable es que disminuye de forma muy notable el porcentaje de personas que hacen clic en enlaces fraudulentos (-39%) y que facilitan credenciales (-31%). Estos datos demuestran que, gracias a la formación y concienciación, las personas usuarias están en alerta y han aprendido a identificar y comprobar correos con fines engañosos y, aunque los abran, no pinchan en los enlaces o ceden datos. A pesar de esta buena tendencia, aún existe un porcentaje importante de personas que caen en la trampa de los ciberdelincuentes, abriendo una brecha de seguridad. Los datos concluyen:

1 de cada 2

usuarios/as que reciben un correo de phishing lo abren

24%

accede a enlaces

17%

facilita datos

Estos datos son resultado, en parte, de las campañas de simulación de phishing que se realizan en las organizaciones, dentro de su estrategia de concienciación y formación, a los empleados para que sepan señalar y reportar correos sospechosos. Este avance en la cultura de ciberseguridad hace que, como ya apuntamos en el informe del año pasado, este tipo de acciones se focalicen en grupos determinados de las organizaciones, con roles o funciones específicas, en lugar de hacer envíos masivos a toda la plantilla. A pesar de esta mejora, no hay que obviar el auge de los casos de phishing impulsados por las herramientas de inteligencia artificial generativa (IA Gen). Estos sistemas, basados en los LLMs como ChatGPT, Copilot o la disruptiva DeepSeek, permiten a los ciberdelincuentes automatizar, personalizar y sofisticar los ataques. No sólo con texto, sino también con audio y/o vídeo, haciéndolos mucho más realistas y creíbles y, por tanto, efectivos. Las compañías deben adoptar medidas proactivas y fortalecer los mecanismos ante los *deepfakes* y la clonación de voz que facilitan fraudes y desinformación.

[3.2] Incidentes detectados en el SOC

Los servicios de monitorización de la ciberseguridad

La segunda parte de nuestro informe se centra en los resultados obtenidos de la monitorización 24/7 realizada por los Security Operations Center de Sofistic, distribuidos en Colombia, España y Panamá y que permiten identificar los ataques que afectan a las organizaciones. A través de la muestra del estudio, durante 2024 constatamos un interés creciente por parte de las empresas en su apuesta por centralizar y monitorizar su seguridad a través de un centro de detección y respuesta avanzada como los que Sofistic tiene en dos continentes diferentes. Este interés responde a la necesidad crucial de las compañías por seguir fortaleciendo su seguridad mediante una detección y respuesta de alta velocidad, apoyada en un equipo altamente capacitado y con un elevado nivel de especialización.

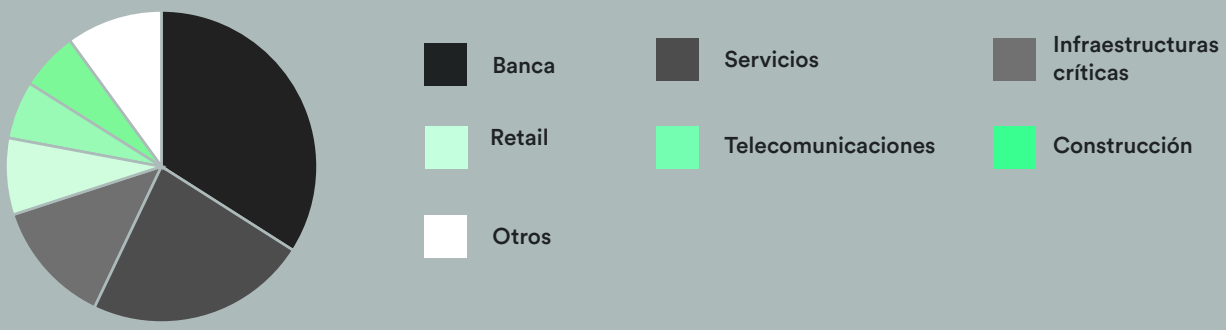
A partir de la muestra analizada, se observa una disminución de las alertas detectadas (-17%). Esta tendencia no se explica por una reducción de la actividad ciberdelictiva y de las amenazas, sino por una mejora de los sistemas de detección. Cada vez este tipo de tecnologías son capaces de identificar los riesgos y anomalías con mayor precisión, de manera que se reducen las falsas alertas. Además, este factor se combina con el mayor nivel de seguridad adquirido por las empresas a lo largo del tiempo. Lo que sí continua en ascenso, según los datos examinados, son los casos gestionados (+27%). Como ya se ha avanzado en la descripción de la muestra, durante 2024, realizamos un cambio en la nomenclatura para ganar precisión y mejorar el servicio que ofrecemos a nuestros clientes. En informes anteriores, utilizábamos el término incidente para aglutinar todos los eventos gestionados y ahora se les denomina casos, clasificándolos a su vez en solicitudes de información e investigaciones (RFI), ciberinteligencia (CTI), incidentes (INC) y casos de configuración (CONF).

-17% Alertas gestionadas

+27% Incidentes investigados

La banca y los servicios, los más precavidos

Sector	Banca	Servicios	Infraestructura crítica	Retail	Telecomunicaciones	Construcción	Otros
%	34%	23%	13%	8%	6%	6%	10%

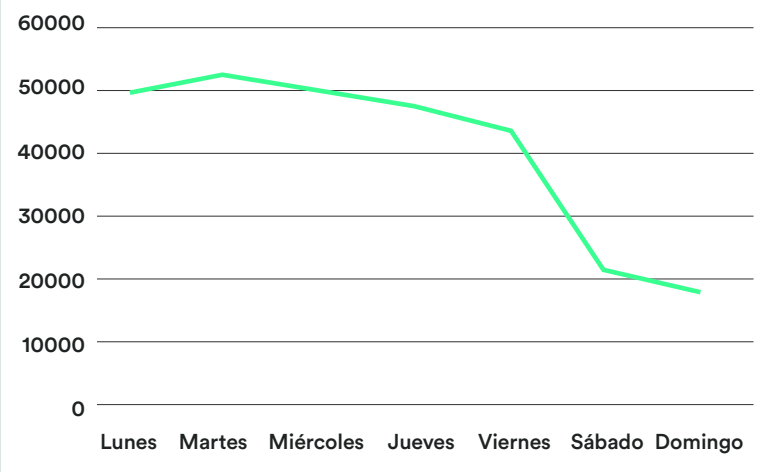


La banca es el sector que representa un mayor volumen de alertas gestionadas a través de los SOC de Sofistic, distribuidos en diferentes países. Le sigue el sector servicios, que ha bajado una posición respecto el año anterior, y las infraestructuras críticas, que ocupan la tercera posición. Cabe destacar que este ranking está influenciado por la relevancia que representan los clientes procedentes de estos sectores en la muestra analizada. Aunque baja el peso de las alertas generadas por la banca y las infraestructuras críticas, continúan siendo los ámbitos con mayor actividad. 6 de cada 10 alertas gestionadas se producen en estos dos sectores (el año pasado eran 8 de cada 10).

Este ranking se explica por la madurez y la inversión en ciberseguridad por parte de los diferentes ámbitos económicos. Tanto la banca como las infraestructuras críticas son muy activos en ciberseguridad por diferentes motivos. Son servicios esenciales, por ejemplo, de transporte, sanidad o suministros básicos y, además, cuentan con regulaciones estrictas. Todo ello ha impulsado que desde hace tiempo estén invirtiendo en ciberseguridad y en tecnologías avanzadas de detección y respuesta. Mientras, el sector servicios está tomando también mucha conciencia en los últimos años, aunque aún tiene margen de mejora en la adopción de medidas robustas de protección.

Ataques automatizados masivos para explotar brechas el fin de semana

A partir de la monitorización del SOC, podemos apreciar cómo los días entre semana se registran más casos y se generan más alertas. Estos datos indican que la superficie de ataque entre semana es mayor, con más personas trabajando y más equipos conectados.



Actualmente el cibercrimen, a través de sistemas automáticos y masivos, como los intentos de registro o los accesos a cuentas o sistemas, intenta identificar brechas y vulnerabilidades para explotarlas los fines de semana, aprovechando que son los momentos de mayor vulnerabilidad cuando hay menos personas trabajando, la concentración y atención es menor y se utilizan dispositivos con menos nivel de protección, como los teléfonos móviles. Esta tendencia indica, una vez más, que el cibercrimen no descansa y cada vez está más profesionalizado.

El 10% de los casos gestionados son de severidad crítica o alta

	Crítica	Alta	Media	Baja	Infi
Severidad (% total)	1%	9%	70%	12%	8%

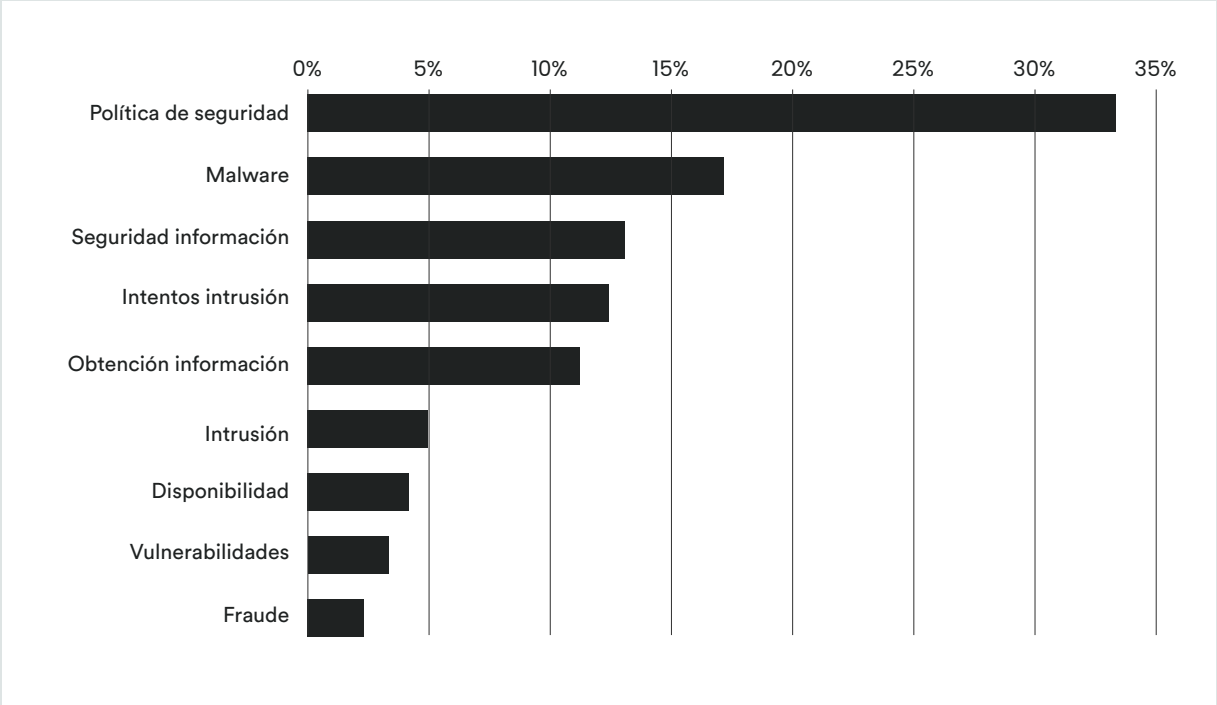
En la misma línea de la tendencia detectada en las auditorías, a través de la monitorización del SOC se observa un aumento de 7 puntos en el volumen de casos de severidad media que representan el 70% del total. También se registra un pequeño descenso de los casos críticos y de seguridad alta, que son los más prioritarios porque pueden comprometer la operativa de una organización. Como ya hemos avanzado, esta tendencia responde a una mayor madurez de las compañías. Las organizaciones llevan tiempo ya invirtiendo en ciberseguridad y, tras corregir y mejorar los puntos más críticos, ahora ponen el foco en otras vulnerabilidades de menor riesgo, pero que igualmente es necesario abordar porque pueden ser la base de ataques más complejos.

El acceso a servicios no autorizados, el principal motivo

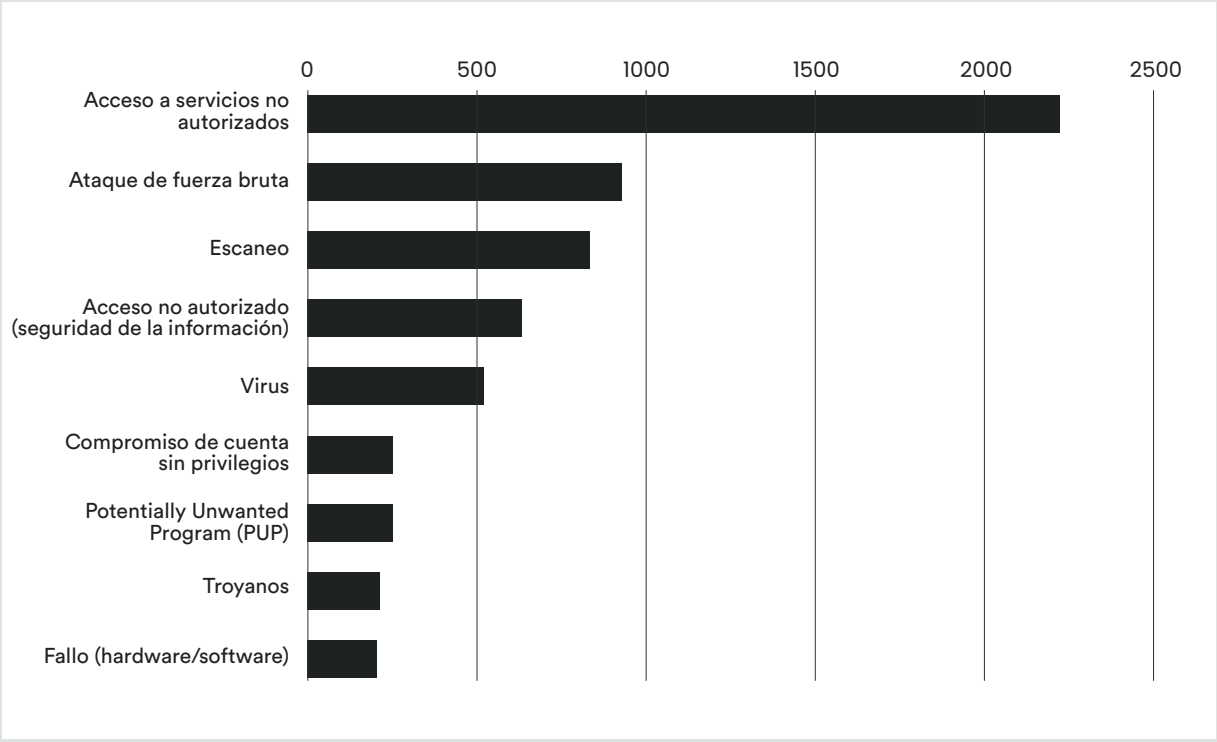
Tipo de casos por categoría principal	**%**
Política de seguridad	33%
Malware	17%
Seguridad de la información	13%
Intentos intrusión	12%
Obtención de información	11%
Intrusión	5%
Disponibilidad	4%
Vulnerabilidades	3%
Fraude	2%

Tipo de casos por subcategoría	**%**
Acceso a servicios no autorizados	29%
Ataque de fuerza bruta	12%
Escaneo	10%
Acceso no autorizado (seguridad de la información)	8%
Virus	7%
Compromiso de cuenta sin privilegios	3%
Potentially Unwanted Program (PUP)	3%
Troyanos	3%
Fallo (hardware/sofware)	3%

Casos por categoría principal



Casos por subcategoría



Una vez más, la monitorización del SOC concluye que las políticas de seguridad continúan encabezando la mayor parte de los casos gestionados (33%). La inmensa mayoría son por accesos a servicios no autorizados (29% respecto al total). También, aunque en menor medida, por abusos de privilegios, herramientas de acceso remoto, cambios en infraestructura o sistemas desactualizados. Cada vez es más frecuente que las empresas con una madurez de protección avanzada tengan sus propias normas y políticas de seguridad con un alto nivel de detalle. Así, los sistemas de alerta se adaptan a esas reglas, casos de uso y modelos para que generen avisos cuando se incumplen. Esta circunstancia explicaría en parte el alto porcentaje de volumen de casos derivados de las políticas de seguridad.

En segundo lugar, destacan por volumen los casos de malware (17%), motivados principalmente por virus, programas potencialmente no deseados (PUP) y troyanos. En tercera posición, se sitúan los casos de seguridad de la información, que suben dos puestos en el ranking. Es el caso, por ejemplo, de accesos no autorizados a información, modificación y/o borrado de datos sin autorización o exfiltración, es decir, el robo o transferencia no permitida de información. También son remarcables los intentos de intrusión, que son los ataques de fuerza bruta o la explotación de vulnerabilidades conocidas.

[4] CONCLUSIONES

Los resultados de nuestro análisis a la muestra de auditorías de seguridad y la monitorización del SOC de Sofistic coinciden con otros informes de referencia de organismos especializados en ciberseguridad. El cibercrimen está aprovechando las tensiones geopolíticas, los conflictos comerciales y las rivalidades económicas. Eso sumado a las tecnologías emergentes, la dependencia de las cadenas de suministro y la sofisticación de los ataques impulsados por IA intensifican la complejidad del panorama de la ciberseguridad, según ha destacado recientemente el Foro Económico Mundial. Conocer y comprender este contexto es clave para mejorar la inversión en la estrategia de seguridad y tener mayor capacidad de respuesta. Los datos de nuestro informe señalan que las compañías están entendiendo esa prioridad para ser más resilientes y hacer frente a estos desafíos. Con esta premisa, también queremos recoger las principales conclusiones que pueden ayudarte a orientar tus decisiones futuras:

Mayor monitorización ante ataques menos críticos. A pesar de la complejidad del ecosistema y de la escalada de amenazas y vulnerabilidades, la mayor madurez de las compañías en ciberseguridad hace que se vayan corrigiendo vulnerabilidades críticas o de alto riesgo que pueden comprometer la operativa de las organizaciones, además de mejorar la monitorización de las amenazas. Por contra, las empresas deben continuar adoptando medidas para mitigar fallos de riesgo medio que podrían acabar abriendo la puerta a ataques de mayor impacto.

Las principales vulnerabilidades detectadas son por este orden:

1. **Fallos de control de acceso** motivados por autorizaciones incorrectas o restricciones de acceso mal implementadas que permiten a usuarios o sistemas sin autorización acceder a datos, aplicaciones o recursos restringidos.

2. **Fallos criptográficos** producidos por mecanismos de cifrado o protección de datos mal configurados u obsoletos que pueden exponer datos sensibles, comprometiendo la confidencialidad o integridad de la información.

3. **Fallos de configuración** que muestran debilidades en los ajustes de seguridad y que pueden abrir las puertas a los ciberdelincuentes. Este tipo de vulnerabilidades confirman la complejidad de la gestión de la ciberseguridad requiriendo equipos profesionales IT con alta especialización y cualificación.

4. **Fallos de inyección** que permiten que los atacantes tomen el control de un sistema o entorno insertando código malicioso para alterar su funcionamiento a través de comandos no autorizados.

Más usuarios interactúan con correos de phishing, pero caen menos en la trampa. La formación ha impulsado avances en la cultura de ciberseguridad que permiten que las personas usuarias tengan suficientes nociones para identificar señales ante un mail engañoso. A pesar de la mayor concienciación, un 24% hace clic en enlaces fraudulentos y un 17% facilita credenciales. Acciones que pueden dar acceso a los ciberdelincuentes y comprometer los sistemas de una organización, con graves repercusiones económicas, legales o de reputación.

Los principales casos gestionados por el SOC están motivados por:

1. **Acceso a servicios no autorizados:** una persona usuaria o sistema accede a una aplicación, red o recurso sin los permisos adecuados, por errores en la configuración o credenciales comprometidas, por ejemplo.

2. **Ataques de fuerza bruta:** los ciberdelincuentes prueban múltiples combinaciones de contraseñas de forma repetitiva y automatizada para acceder a un entorno, sistema o red.

3. **Escaneo:** a través de un escaneo de red, se detectan equipos o servicios expuestos que podrían ser explotados por los ciberatacantes.

4. **Acceso no autorizado por seguridad de la información:** se produce cuando una persona usuaria o sistema accede o modifica datos sin los permisos adecuados, ya sea por configuraciones deficientes ya sea por credenciales robadas.

Ataques masivos automatizados para explotar brechas el fin de semana.

A partir de la monitorización del SOC se observa una mayor incidencia de casos entre semana que se explicaría por una mayor superficie de ataque, coincidiendo con una mayor actividad en las organizaciones. A través de sistemas automáticos y masivos, el cibercrimen intenta identificar brechas y vulnerabilidades para explotarlas los fines de semana, aprovechando que son los momentos de mayor vulnerabilidad en las compañías con menor actividad y menos personas trabajando.

[5] RECOMENDACIONES DE CIBERSEGURIDAD PARA 2025

El análisis de las tendencias en ciberseguridad registradas en 2024 nos lleva a plantear una serie de recomendaciones prácticas para minimizar riesgos en 2025. La creciente regulación normativa, como la directiva de seguridad de redes y sistemas de información NIS2 o el reglamento DORA que legisla la ciberseguridad en el sector financiero, hace que buena parte de estas medidas propuestas sean obligatorias para mejorar la gestión y garantizar la continuidad operativa de las organizaciones ante incidentes digitales. Además, las previsiones de gasto mundial en productos y servicios de ciberseguridad apuntan a un crecimiento de un 13%, según las estimaciones de McKinsey. Con este contexto es importante conocer hacia dónde deberían focalizarse las próximas inversiones:

Diseñar estrategias de ciberseguridad integrales buscando la máxima eficiencia y eficacia.

El aumento de la complejidad de las amenazas aconseja adoptar una propuesta interconectada capaz de identificar las vulnerabilidades existentes a través de auditorías, de fortalecer la seguridad utilizando tecnologías específicas y de monitorizar de forma ininterrumpida un entorno. Todo con el objetivo de acelerar la detección y respuesta a incidentes mitigando cualquier impacto.

Poner atención en los modelos de inteligencia artificial.

Esta tecnología supone tanto un riesgo como una oportunidad en la gestión de la ciberseguridad. Los ciberdelincuentes la están aprovechando para personalizar sus ataques de ingeniería social multiplicando las probabilidades de éxito. Al mismo tiempo, las compañías deben integrarla para predecir posibles ciberataques y guiarlas en la investigación y respuesta a incidentes. Eso sí, cualquier compañía, sea del sector que sea, debe extremar las precauciones para evitar otras vías de ataque a través de los sistemas LLM, como podría ser la exfiltración de datos, el compromiso de modelos o la fiabilidad y consistencia de las respuestas. Conscientes del potencial de esta tecnología, desde Sofistic estamos desarrollando junto al INCIBE una solución pionera de gestión de alertas cloud, asistida por IA, para agilizar la respuesta a ciberataques. Se trata de un proyecto que ejemplifica la colaboración público-privada para reforzar el ecosistema de ciberseguridad.

Evaluar los riesgos de los proveedores e involucrar en la ciberseguridad a toda la cadena de suministro.

Los ciberdelincuentes buscan todos los posibles vectores de ataque, incluidas las debilidades de proveedores y colaboradores. Ante este escenario, es importante exigir el mismo nivel de ciberseguridad a todo el entorno externo y red de proveedores, para evitar que un incidente se extienda o utilicen esa brecha para llegar a tu infraestructura.

Fortalecer la cultura de seguridad.

La sofisticación de los ataques de phishing, impulsados por IA generativa, obliga no sólo a implementar controles tecnológicos y procesos administrativos sólidos. Las compañías deben implementar programas continuados de formación y concienciación para capacitar a todas las personas empleadas que permitan reducir riesgos.

[6] QUIÉNES SOMOS

En **Sofistic**,la unidad de ciberseguridad de Cuatroochenta, estamos especializados en el sector bancario y las infraestructuras críticas. Contamos con clientes relevantes en estos ámbitos en Colombia, Panamá, Costa Rica, República Dominicana y España.

Ofrecemos tanto protección preventiva y proactiva como una respuesta eficaz a los incidentes apoyándonos en el software más avanzado. Contamos con profesionales altamente cualificados para identificar y detener ataques, simplificar la seguridad y minimizar el riesgo. Tenemos una amplia experiencia y una trayectoria de 18 años maximizando la protección y respuesta, sin interferir en la eficacia del negocio.

Tanto los empleados como la compañía cuentan con un amplio número de certificaciones de seguridad, entre las que destacan ISO 27001, ISO 9001, ENS y SOC 2 Type II. Estos reconocimientos reafirman que cumplimos con los estrictos criterios de seguridad, disponibilidad, integridad, confidencialidad y privacidad de los datos, ajustándonos al RGPD o las diferentes normativas locales de Protección de Datos Personales. Además, colaboramos con entidades de referencia internacional (FIRST) y nacional (CSIRT.es y Red Nacional de SOC) para el intercambio de información que ayude a otras empresas a estar más protegidas y formamos parte de alianzas estratégicas (ioXt) para fomentar la confianza en productos IoT. Todo ello es una muestra de nuestro compromiso con los estándares de calidad y ciberseguridad más avanzados.

En Sofistic, combinamos tecnología avanzada con inteligencia artificial aplicada a la ciberseguridad para ofrecer un enfoque proactivo y eficaz en la protección de las organizaciones:

Auditorías de seguridad evaluamos el estado real de la seguridad de una organización, detectando vulnerabilidades antes de que los ciberdelincuentes puedan explotarlas. A través de pruebas avanzadas de intrusión y simulaciones de ataques reales, ayudamos a fortalecer la postura de ciberseguridad de nuestros clientes.

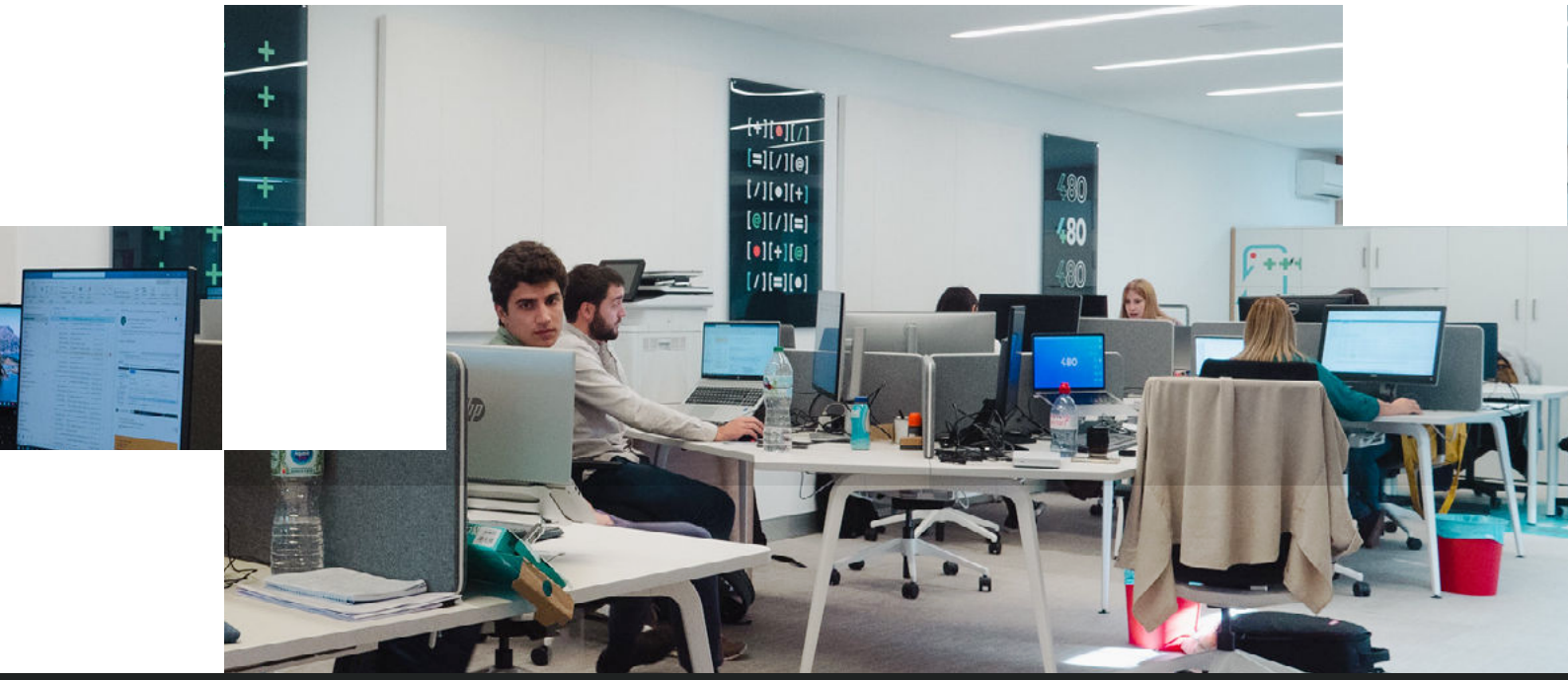
Servicios MSSP *(Managed Security Services Provider)*: más allá de la implementación de herramientas, gestionamos y optimizamos la seguridad de las organizaciones, asegurando su evolución frente a nuevas amenazas. Nuestro equipo de profesionales proporciona asistencia experta y mantenimiento preventivo, garantizando el máximo rendimiento y una resiliencia sólida ante ciberataques.

***Managed Detection & Response* (MDR):** desde nuestros SOC en Europa y Latinoamérica, ofrecemos detección y respuesta de amenazas en tiempo real 24/7, combinando tecnologías de seguridad líderes en el mercado y el uso de algoritmos avanzados en IA, analizando y detectando comportamientos anómalos antes de que supongan un riesgo para las empresas.

Cuatroochenta es una empresa tecnológica especializada en soluciones digitales *cloud* y **ciberseguridad** para mejorar el rendimiento de las organizaciones.

Además de proteger infraestructuras críticas y entidades financieras a través de Sofistic; la compañía también es **Proveedora de Software Independiente** (ISV) a través de las aplicaciones de Facility Management & Services FAMA y CheckingPlan y la plataforma de ticketing Escena Online; **Revendedora de Valor Añadido** (VAR) con las soluciones de gestión empresarial Microsoft y Zoho; y prestadora de **Servicios de Valor Añadido** (VAS) con su división de desarrollo a medida 480:DEV.

Sus desarrollos cuentan con más de 20 millones de personas usuarias en 32 países. Con oficina central en el parque tecnológico Espaitec de la Universitat Jaume I de Castelló de la Plana (España), cuenta con oficinas en Madrid, Barcelona, València, Burgos, Lugo, Málaga, Bogotá, Panamá, Ciudad de México, Santo Domingo y San José, en las que trabajan más de 270 personas. Cuatroochenta cotiza en BME Growth como 480S desde octubre de 2020.



En la elaboración del informe han participado:

Manuel Ginés, Head of R&D de Sofistic
Juan Carlos García, CCO & SOC Director de Sofistic
Arturo Beltran, CISO de Cuatroochenta
Patrick Campillo, MD/MDR Team Leader de Sofistic
Bárbara Villuendas, Branded Content Manager de Cuatroochenta

480

SOFISTIC
CYBERSECURITY