[INFORME_DE TENDENCIAS:EN CIBERSEGURIDAD]

2024

SOFISTIC CYBERSECURITY 480

ÍNDICE

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

Manuel Ginés
Security Audit Director & RD

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

En un entorno de inestabilidad geopolítica, en plena transformación económica y digital y con la explosión de los sistemas de inteligencia artificial resoplando en nuestras nucas, la ciberseguridad ha ganado peso en las empresas y se ha afianzado como una de sus máximas prioridades. Partiendo de esa situación y siendo conscientes de que no existe una estrategia infalible, desde Sofistic, la división de ciberseguridad de la tecnológica Cuatroochenta, apostamos, una vez más, por compartir nuestros conocimientos y experiencia sobre prevención, detección y respuesta activa.

Siguiendo con el ejercicio de transparencia y divulgación, que arrancamos el año pasado con la publicación de nuestro primer estudio sobre conclusiones y recomendaciones de seguridad, presentamos el **Informe de tendencias de ciberseguridad 2024**. Una vez más, 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, durante el año 2023, a empresas tanto en Latinoamérica como en España. Esperamos que este esfuerzo se traduzca en información útil para ayudar a planificar la estrategia de seguridad de nuestros clientes, los que están valorando serlo o cualquier persona interesada en ciberseguridad.

Entendemos que se trata de minimizar riesgos y que, el actual panorama cambiante y de proliferación de vulnerabilidades, obliga a las empresas y administraciones a ser resilientes e implementar mejoras de forma constante. Conocer el origen, alcance e impacto de esas amenazas emergentes ayuda a afrontar con eficiencia esos desafíos en continua evolución. Cuando no notas la ciberseguridad es porque funciona correctamente. Lo hace con garantías y sin interrupciones. Y desde Sofistic creemos que eso es fruto de un enfoque de seguridad robusto y fiable.

Confiamos que en estas páginas encuentres las claves para desplegarlo.

[2] MUESTRA

El informe parte de una muestra suficientemente amplia y representativa del trabajo realizado por el equipo de profesionales de Sofistic en 2023. 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 150 auditorías realizadas a 45 clientes, lo que supone el análisis de 1.325 vulnerabilidades. Hemos incluido auditorías a aplicaciones (web y móviles), infraestructuras (externas e internas), código fuente e ingeniería social. Y, aunque representen un volumen menor, también hemos analizado el resultado de auditorías *red team*, wifi o de soluciones basadas en tecnología *blockchain*. Durante este 2023 hemos hecho una revisión de la categorización de las vulnerabilidades y hemos ampliado la muestra con respecto a los datos de 2022, con resultados que no se habían incluido en el informe del año anterior, hecho que puede alterar las cifras plasmadas en el informe de 2023.

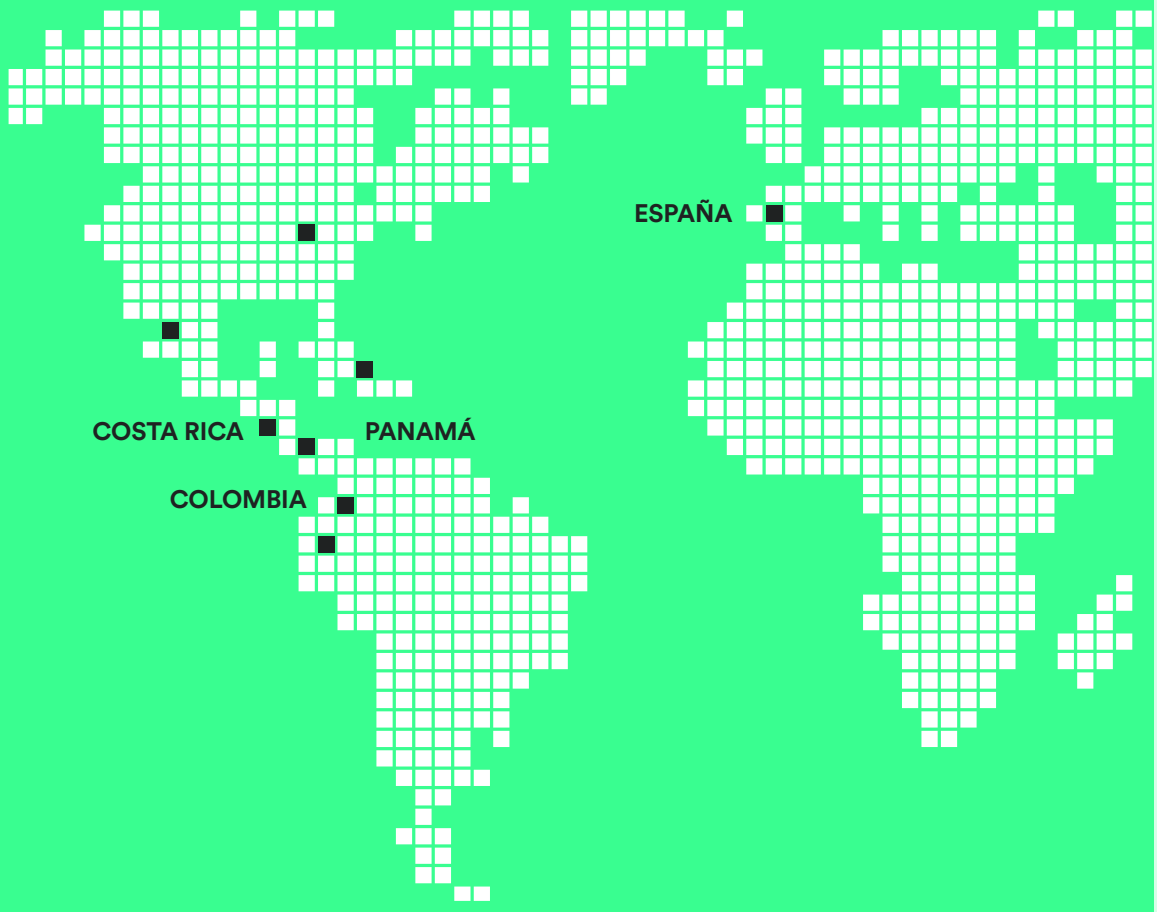
Incidentes de seguridad detectados en el SOC.

Hemos seleccionado una muestra representativa de 100.000 alertas y 1.500 incidentes entre todos los gestionados por el equipo de los SOC de Sofistic, ubicados en Panamá, Colombia y España durante el 2023.

Es una muestra suficientemente amplia que permite identificar los tipos de ataques detectados el último año.

Ámbito geográfico

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



Sectores

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

Banca y finanzas

Industria y servicios

[3] RESULTADOS

[3.1] Auditorías de seguridad

Más vulnerabilidades, pero menos críticas

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 2023 en comparación con 2022.

Auditorías	+37%
Vulnerabilidades	+26%
Criticidad	-2%

Variación 2022/23

Durante el 2023, se continúa detectando un incremento del número de auditorías ejecutadas (37%) así como de los informes derivados de esos análisis, aunque con un menor ritmo de crecimiento que en 2022 (53%). También aumenta el número de vulnerabilidades identificadas (26%), aunque disminuye ligeramente su severidad. Tendencia que se explica por la mayor preocupación y madurez en ciberseguridad de las organizaciones. Tras auditar los entornos más críticos de la compañía, conocer los resultados y aplicar mejoras, estas empresas repiten y extienden estos análisis a otras soluciones o sistemas.

3,5
auditorías por cliente

Se realizan un promedio de 3,5 auditorías por cliente, cuando hace un año la media se quedaba en 2,5.

Las auditorías web y móvil registran el mayor incremento

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

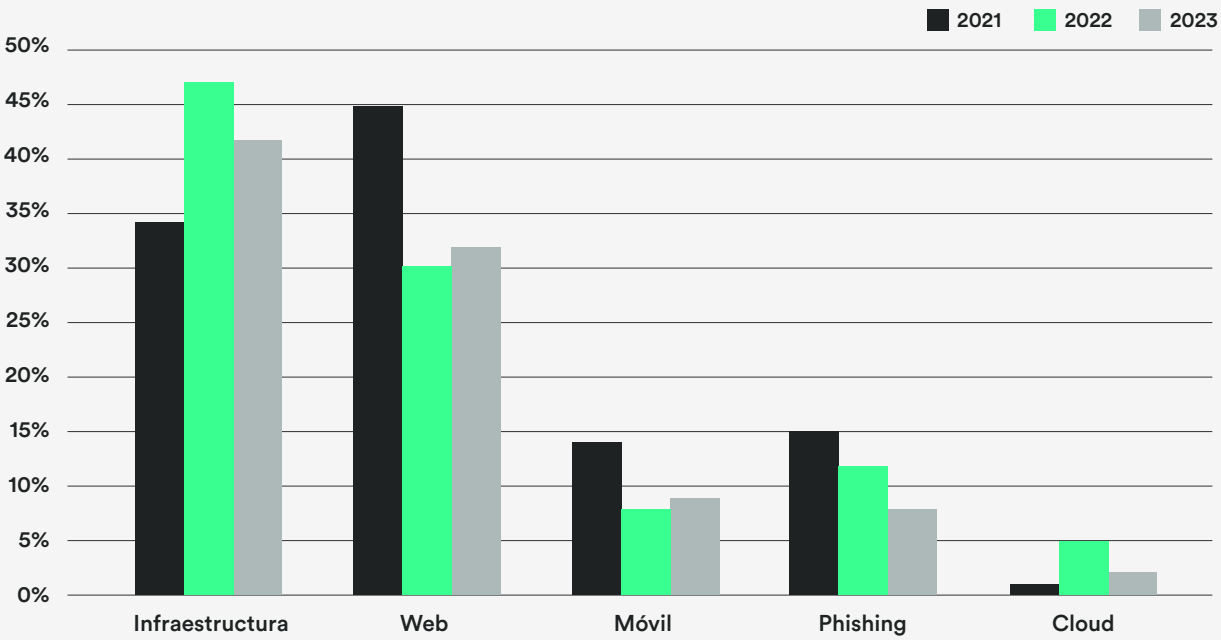
El número de auditorías de la muestra crece en prácticamente todos los ámbitos, exceptuando las de revisión de código, *phishing* y entornos *cloud*. Esta última tendencia se produce, tras un 2022 en que se registró un incremento muy remarcable de este tipo de auditorías por la creciente preocupación de la securización de las soluciones e infraestructuras en la nube, derivada de la alta demanda de los servicios *cloud* impulsada por la pandemia.

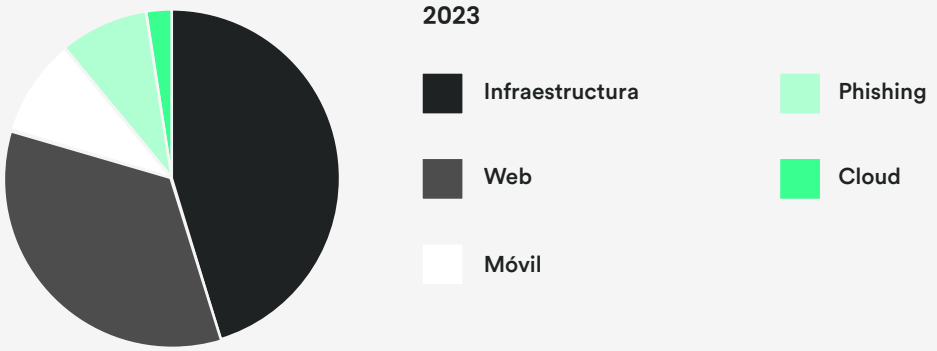
El incremento de amenazas y ataques siguen motivando las auditorías de aplicaciones web y móvil, que son las que encabezan el aumento más significativo durante 2023 con un 45% y un 44%, respectivamente. La preocupación por los sistemas de autenticación, la seguridad relacionada con los datos sensibles y la carga y descarga de archivos a través de este tipo de soluciones explican el incremento de demanda de este tipo de servicios. Le siguen las de evaluación de la seguridad de infraestructura, tanto interna como externa, que en los últimos dos años se ha multiplicado por más de 2,5 en números absolutos.

Top tipo de Auditorías por volumen	2021	2022	2023
Infraestructura	34%	47%	42%
Web	45%	30%	32%
Móvil	14%	8%	9%
Phishing	15%	12%	8%
Cloud	1%	5%	2%

Para entender bien el contexto, debemos fijarnos en el porcentaje que representa cada tipo de auditoría sobre el total de la muestra. De este modo, se observa cómo se mantiene una tendencia clara hacia la securización de las infraestructuras. 4 de cada 10 auditorías se realizan en este tipo de entornos. Las organizaciones buscan, así, proteger los activos que tienen expuestos tanto en internet como en las propias redes internas. Una vez más, el mayor grado de madurez de las compañías se refleja en análisis más sofisticados, como los de *red team*, los de entornos OT o auditorías más de nicho en soluciones *blockchain*. Son auditorías que ganan visibilidad, aunque con porcentajes bajos sobre el total.

Tipos de auditoría

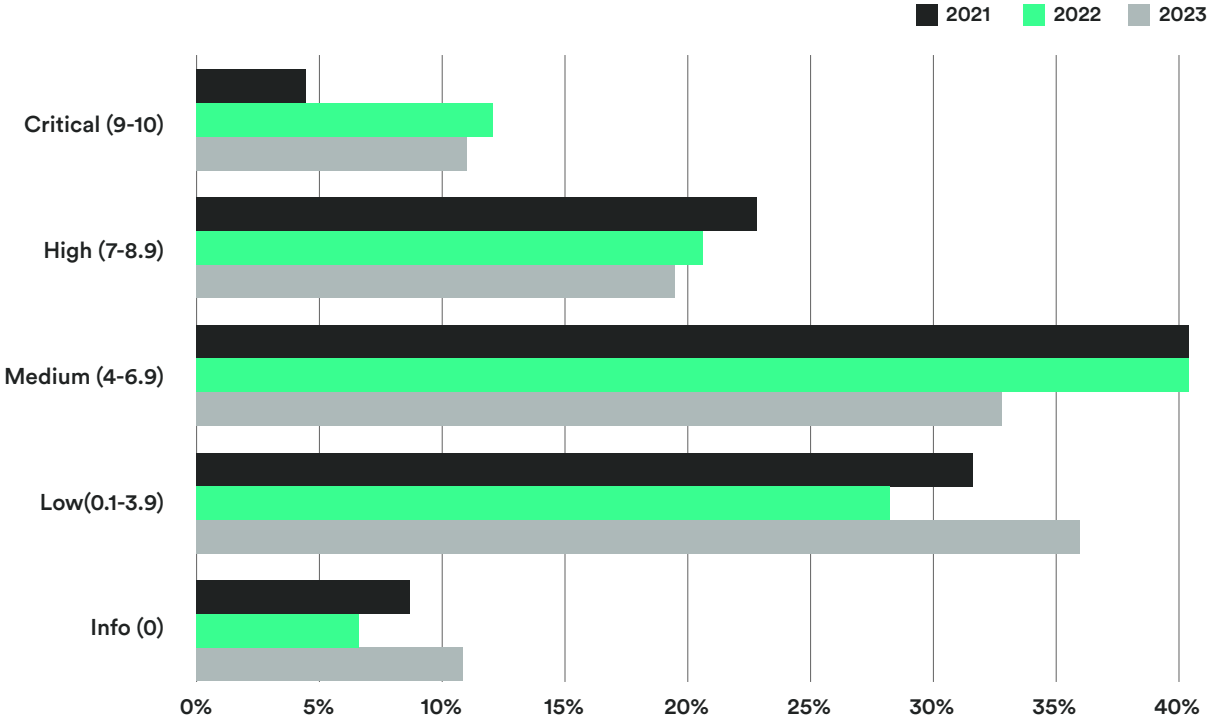




Casi un tercio de los fallos son de riesgo alto o crítico

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

Severidad de las vulnerabilidades



Analizando la severidad de las vulnerabilidades, las de riesgo alto y críticas representan casi el 30% del total de los hallazgos, el mismo porcentaje que el año 2022. Son datos preocupantes porque son fallos que pueden ocasionar graves consecuencias en una organización. A pesar de ello, la tendencia positiva es que, en el último año, se ha ralentizado el incremento de fallos críticos respecto al 2022, cuando se multiplicaron por más de 2,5. Las vulnerabilidades detectadas que experimentan un mayor crecimiento son las de riesgo bajo y, especialmente, las informativas, que se casi duplican de un año para otro. Estas últimas son las que no comportan ningún fallo de seguridad, pero sí potenciales riesgos que podrían ser explotados en un futuro como, por ejemplo, direcciones de correo electrónico localizadas en internet. Esta estabilización de la severidad de las vulnerabilidades se explica por una estandarización interna de la categorización de los fallos detectados que ya hemos mencionado, pero también a la mayor capacidad que han adquirido las organizaciones para gestionar y proteger sus activos digitales frente a amenazas.

Las vulnerabilidades críticas se suelen identificar en entornos que son auditados por primera vez. En cambio, en auditorías posteriores, ya se han corregido y se detectan otros fallos de menor riesgo, junto a otros nuevos que han podido aparecer y evolucionar.

Los fallos criptográficos y de control de acceso, en cabeza

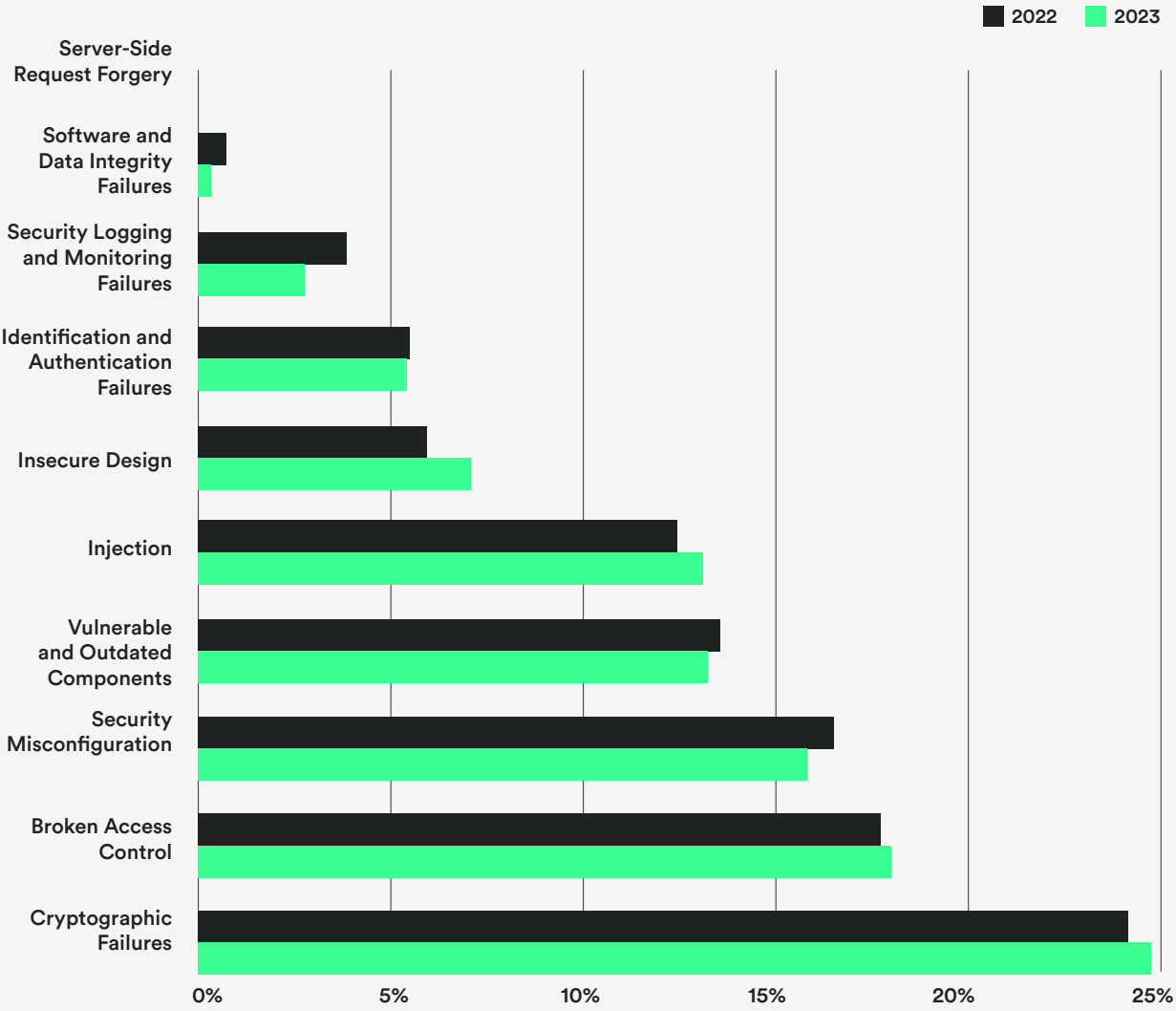
Si desglosamos los fallos detectados por categoría de vulnerabilidad, se observa que el ranking de los más comunes no ha variado respecto el 2022. Los criptográficos vuelven a ocupar la primera posición por segundo año consecutivo. La ausencia o el uso incorrecto de cifrado o de certificados en conexiones *Secure Socket Layer* (SSL) o algoritmos obsoletos son algunas de las vulnerabilidades halladas más comunes que pueden incluso permitir interceptar comunicaciones. En segundo lugar, se encuentran, de nuevo, los fallos de control de acceso. Errores que permiten a usuarios sin permisos o con limitaciones acceder a información que debería estar restringida a aquellos con mayores privilegios. Y, en tercer lugar, aparecen los fallos de configuración del sistema relacionados, por ejemplo, con los parámetros de las cabeceras HTML o las configuraciones permisivas de los dispositivos de red. Esta clasificación reafirma la gran complejidad tecnológica a la que deben enfrentarse las organizaciones con equipos IT altamente cualificados.

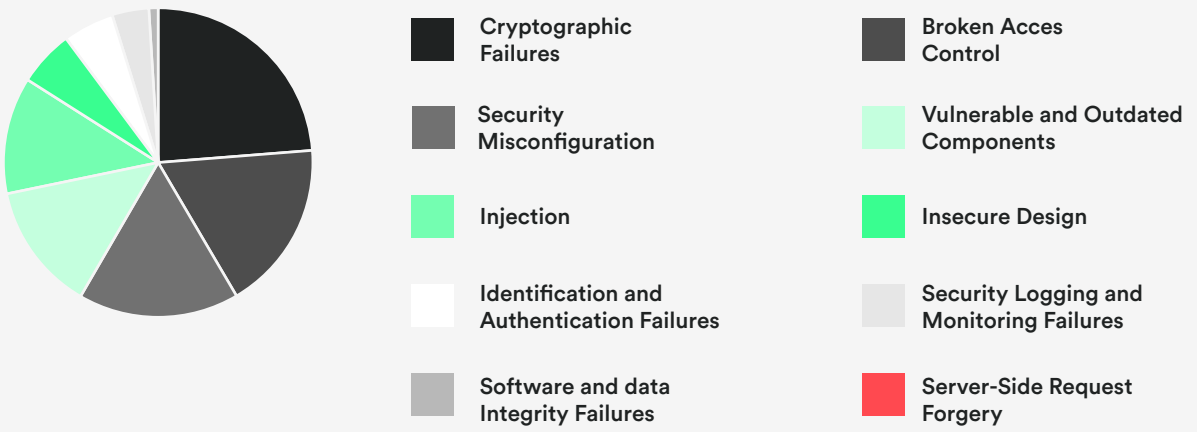
Si analizamos la evolución por volumen respecto el total, no se detecta ningún cambio substancial respecto los datos de 2022. Llama la atención la disminución de los fallos relacionados con diseño inseguro e inyección y el incremento de los fallos de configuración, especialmente los relacionados con la configuración incorrecta en el sistema de registro de eventos. Un factor que explicaría esta doble tendencia es la mayor evolución de las empresas en materia de ciberseguridad. Anteriormente, se detectaban fallos relacionados con un diseño deficiente o un desarrollo inseguro. Ahora, estos errores tienden a disminuir y se detectan más en cuestiones de configuración, que no afectan tanto al proceso de desarrollo.

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				Puesto			
Accionista	2021	2022	2023	Variación 2022-2023	2021	2022	2023	
Cryptographic Failures	17%	25%	24%	-2%	3	1	1	=
Broken Access Control	21%	18%	18%	-2%	1	2	2	=
Security Misconfiguration	18%	16%	16%	+5%	2	3	3	=
Vulnerable and Outdated Components	10%	13%	13%	+2%	6	5	4	-1
Injection	14%	13%	12%	-5%	4	4	5	+1
Insecure Design	10%	7%	6%	-15%	5	6	6	=
Identification and Authentication Failures	7%	5%	6%	+1%	7	7	7	=
Security Logging and Monitoring Failures	2%	3%	4%	+39%	8	8	8	=
Software and Data Integrity Failures	1%	0%	1%	+123%	9	9	9	=
Server-Side Request Forgery	0,00%	0,00%	0,00%	0%	10	10	10	=

Categorías de las vulnerabilidades





Phishing: se triplican los clics y la introducción de credenciales

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

A partir de la muestra de auditorías de ingeniería social realizadas durante el 2023, detectamos una ligera disminución de los usuarios que interactúan con emails de *phishing* (-8%). A pesar de esta tendencia, preocupa especialmente el incremento del número de los que hacen clic en enlaces fraudulentos y los que facilitan credenciales, ya que se han triplicado respecto a 2022. Los datos concluyen que:

3 de cada 10

usuarios/as que reciben un correo de phishing lo abren

40%

accede a enlaces

20%

facilita datos

Aunque detectamos una reducción de este tipo de campañas que ponen a prueba la concienciación y las habilidades de seguridad del personal de una organización, se ha ampliado el radio de cobertura a departamentos o áreas que tradicionalmente no estaban tan vinculados al sector IT o a las políticas de ciberseguridad y protección. De media, se están registrando 375 envíos por campaña, mientras que en 2022 esta cifra se quedaba en 232 emails. Se trata de replicar, a través de estas pruebas de seguridad, las prácticas que están llevando a cabo los ciberdelincuentes, tanto con campañas globales y masivas como de investigación, obteniendo información pública personal de las posibles víctimas para intentar engañarlas. Para todo ello, además, se están apoyando en herramientas de inteligencia artificial generativa (AI Gen) que están facilitando y perfeccionando los ataques de ingeniería social.

[3.2] Incidentes detectados en el SOC

Los servicios de monitorización de la ciberseguridad

En esta segunda parte del informe nos focalizamos en los resultados obtenidos de la vigilancia realizada por el *Security Operations Center*, que permite identificar los ataques que afectan a las organizaciones. A partir de la muestra del estudio, observamos que continúa creciendo el número de empresas que apuestan por centralizar y monitorizar su ciberseguridad a través de un centro de detección y repuesta 24/7 como el de Sofistic. En el último año se ha detectado un fuerte incremento evidenciando el interés de las compañías por fortalecer su seguridad mejorando la detección y respuesta temprana de amenazas.

Además, se continúa constatando un aumento remarcable y proporcional, tanto en el número de alertas gestionadas (475%) como en el número de incidentes investigados (322%). Una tendencia que se explica por ese mayor grado de madurez de las organizaciones, que hace que cuenten con más herramientas de protección y detección. También influye la creciente actividad delictiva, reportada y detectada por diversos organismos a nivel mundial, que hace que proliferen las alertas.

+475% Alertas gestionadas

+322% Incidentes investigados

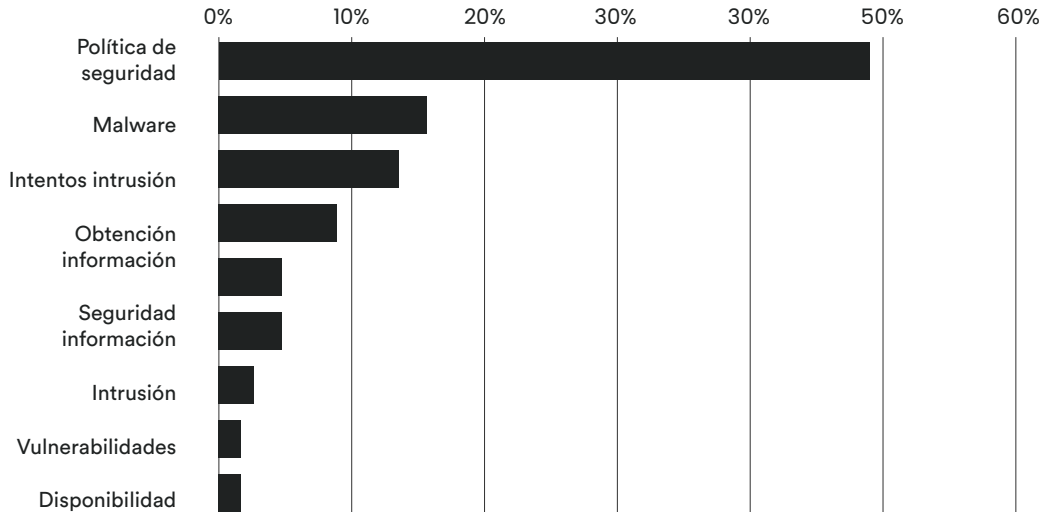
Los proveedores de servicios y los bancos, los más proactivos

Sector	Servicios	Banca	Retail	Infraestructura crítica	Salud	Otros
%	31%	25%	15%	8%	2%	18%

Más de la mitad de las alertas, motivadas por la interacción del usuario

Tipos de casos	%
Política de seguridad	47%
Malware	14%
Intentos intrusión	13%
Obtención de información	9%
Seguridad información	5%
Intrusión	5%
Fraude	3%
Vulnerabilidades	2%
Disponibilidad	2%

Alertas por tipo



La monitorización del SOC de Sofistic pone de manifiesto que la interacción del usuario tiene un peso importante en la generación de alertas, tanto relacionadas con las políticas de seguridad o la seguridad de la información como de *malware*. Las alertas más frecuentes (47%), según los datos de la muestra, son las que están vinculadas con la vulneración de las políticas de seguridad de la organización, como podría ser el uso de aplicaciones no permitidas o de servicios VPN no autorizados, el acceso a servicios no aprobados o malas prácticas. A parte de las alertas de *malware*, de intentos de intrusión u obtención de información, también son reseñables las vinculadas con la seguridad de la información. Sería el caso, por ejemplo, de una posible exfiltración, del borrado de ficheros o de una modificación o acceso no autorizado. Estos datos demuestran la necesidad de seguir concienciando tanto a organizaciones como al personal para detectar posibles amenazas y hacer un buen uso de la información.

El 13% de los incidentes investigados son de severidad crítica o alta

Severidad (% total)	
Crítica	2%
Alta	11%
Media	63%
Baja	21%
Info	3%

A partir de la monitorización del SOC se observa la misma tendencia detectada en las auditorías de seguridad sobre la severidad de las vulnerabilidades. En el caso de los incidentes gestionados, los datos confirman que el 63% son de severidad media. Representan el mayor volumen, seguidos de los de baja severidad, confirmando así la visión global de una mayor madurez en las estrategias de ciberseguridad de las organizaciones. Aun así, hay que poner el foco en los más preocupantes: los de severidad alta (11%) y crítica (2%) que pueden llegar a comprometer la operativa de las compañías.

[4] CONCLUSIONES

Los hallazgos detectados en las auditorías de seguridad y la monitorización del SOC de Sofistic van en la línea de los informes publicados por diversos organismos especializados y de referencia en ciberseguridad. Los ciberataques son uno de los cinco principales riesgos para este 2024, junto al cambio climático, la desinformación generada por la IA, la polarización política y social y la crisis del coste de la vida, según ha hecho público el Foro Económico Mundial. Los datos de nuestro análisis indican que, aunque los riesgos y las vulnerabilidades crezcan, la capacidad de respuesta de las organizaciones también está aumentando. Eso responde a que las empresas están entendiendo que deben ser resilientes y que, para una protección robusta y efectiva, deben apostar por una inversión estratégica en ciberseguridad. Es por eso que, en nuestro informe, recogemos las principales conclusiones que pueden ayudar en la toma de decisiones futuras:

Crece el número de vulnerabilidades y se estabiliza la severidad. La inestabilidad geopolítica, por las guerras en Ucrania y Gaza, y la sofisticación de los ataques impulsados por las nuevas herramientas de inteligencia artificial generativa están promoviendo la proliferación de ciberamenazas. Este entorno en creciente riesgo y constante evolución precisa que las organizaciones sigan fortaleciéndose y perfeccionando sus estrategias de ciberseguridad para identificar las vulnerabilidades más críticas.

El 28% de las vulnerabilidades detectadas en auditorías son críticas o de alto riesgo. Aunque la severidad de los ataques se haya estancado, preocupa que casi un tercio de los riesgos identificados tengan potencial para causar impactos severos en las organizaciones.

La mayor coordinación entre negocio y ciberseguridad afianza una protección efectiva contra las amenazas. A través de la actividad de las auditorías y la monitorización del SOC observamos cómo las empresas están integrando la ciberseguridad en su estrategia, de manera que aumenta su madurez para implementar medidas de protección sólidas y responder de forma rápida y ágil a los posibles incidentes. Además, esta colaboración fomenta la cultura de seguridad en toda la compañía, que es fundamental para cualquier entorno digital en continua evolución.

Las principales vulnerabilidades detectadas continúan siendo:

1. **Fallos criptográficos** relacionados con la ausencia o uso incorrecto de cifrado, como por ejemplo, acceder a una página web usando HTTP en lugar de HTTPS, el uso de algoritmos inseguros o software desactualizado.

2. **Fallos de control de acceso** en los que los usuarios sin privilegios pueden acceder a información o sistemas a los que no están autorizados.

3. **Fallos de configuración** que confirman que la seguridad del sistema no depende únicamente de la tecnología, sino también de unos protocolos actualizados y seguros. Como ya apuntamos hace un año, esta complejidad, además, precisa de equipos profesionales IT altamente cualificados.

4. **Fallos de componentes vulnerables y obsoletos de software** que pueden ser explotados y exponer un sistema a amenazas por su falta de mantenimiento y actualización.

Se dispara el número de personas que pinchan en enlaces fraudulentos o introducen credenciales. La mayor sofisticación, la automatización y la personalización de los ataques, impulsados por la IA generativa, y la falta de formación o conciencia de una parte de las plantillas explican que se hayan multiplicado por 3 las personas que hacen clic en enlaces o proporcionan datos en emails de *phishing*.

Siguen creciendo las alertas e incidentes gestionados en el SOC. Los datos obtenidos por el servicio de monitorización del SOC de Sofistic reafirman que el número de alertas e incidentes gestionados se ha incrementado de forma muy remarcable, multiplicándose por 6 y por 4, respectivamente. Una tendencia que responde a la actividad global de cibercriminalidad según los datos recopilados por diversos organismos internacionales.

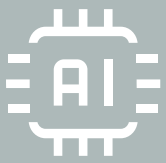
La interacción del usuario genera el mayor volumen de alertas de seguridad. La monitorización del SOC pone de manifiesto que el 47% de las alertas están relacionadas con las políticas de seguridad, como por ejemplo el uso de aplicaciones o servicios no autorizados. La seguridad de la información, como el borrado de ficheros o un acceso no autorizado, es otra de las tipologías de alertas más comunes.

[5] RECOMENDACIONES DE CIBERSEGURIDAD PARA 2024

El análisis de las tendencias en ciberseguridad registradas en 2023 nos lleva a plantear una serie de recomendaciones prácticas para minimizar riesgos en 2024:

Estrategia Managed Detection & Response (MDR).

Un enfoque integral que incluya tanto la detección como la respuesta a incidentes permite tener una mayor visibilidad sobre la superficie de ataque. Se trata de monitorizar en tiempo real, identificar de forma temprana amenazas y mitigarlas rápidamente para reducir su impacto. A esa estrategia, se deben sumar los servicios activos de seguridad que garanticen la configuración de los sistemas y redes, así como su actualización y las auditorías de seguridad periódicas que permiten hacer correcciones y mejorar las medidas de seguridad.



Incorporar tecnologías avanzadas con inteligencia artificial es estratégico para detectar y contener vulnerabilidades en tiempo real.

Este tipo de herramientas, basadas en técnicas de IA como el *machine learning*, permiten identificar patrones de comportamiento, que permitan agilizar la detección de amenazas y, por tanto, reducir la exposición y el riesgo de las organizaciones. Este tipo de soluciones deben estar gestionadas por analistas con experiencia y conocimiento que permitan garantizar los máximos resultados.

***

Gestión de la identidad y de los accesos.

La verificación y autenticación de la identidad de los usuarios y las usuarias, tanto internos como externos, se ha convertido en una prioridad para garantizar la seguridad, la privacidad, la eficiencia de los procesos y las transacciones en línea, así como para proteger los activos de una compañía. El despliegue de un modelo *Zero Trust* es una de las vías más efectivas para mitigar estos riesgos, especialmente en entornos híbridos o en remoto.

Formación y concienciación.

Visto el aumento tan destacable del número de usuarios que interactúan con emails de *phishing* y el potencial que tienen las herramientas de inteligencia artificial generativa para generar incluso *deepfakes* o *vishing*, las organizaciones deben seguir apostando por la formación continua en ciberseguridad de toda la plantilla. Una formación extensible a las políticas de seguridad y seguridad de la información, ya que muchas de las alertas de seguridad están motivadas por la interacción de los propios usuarios.

[6] QUIÉNES SOMOS

SOFISTIC CYBERSECURITY

En **Sofistic**, la unidad de ciberseguridad de Cuatroochenta, estamos especializados en el sector bancario, salud e infraestructuras críticas. Contamos con clientes relevantes en estos sectores 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 más de 15 años maximizando la protección y respuesta, sin interferir en la eficacia del negocio.

Tanto los empleados como la compañía cuentan con un amplio número certificaciones de seguridad, entre las que destacan ISO 27001, ENS, ioXt y SOC 2 Tipo II. Reconocimientos que reafirman nuestro compromiso con la excelencia en ciberseguridad y que se suman a la colaboración con entidades internacionales (FIRST) y nacionales (CSIRT.es) para el intercambio de información que ayude a otras empresas a estar más protegidas.

Contamos con **Sofistic ONE**, un nuevo servicio que aglutina todo nuestro conocimiento para ofrecer la mejor protección. Se basa en nuestro servicio de monitorización (*Managed Detection*) o monitorización y respuesta (*Managed Detection & Response*) que se ofrece desde nuestros tres SOC distribuidos en dos continentes y tres países diferentes que permiten una respuesta global 24/7. Estos servicios se complementan con otros que se adaptan a las necesidades de los clientes. Los principales son:

Threat Intelligence para analizar, recopilar y detectar eventos relevantes en diversas fuentes de información tanto internas como externas.

Threat Hunting para captar amenazas ocultas, mediante la infección con un *malware* propio, el análisis de brechas de seguridad públicas o con la detección del uso fraudulento de la marca.

Playbooks que permiten optimizar tanto los tiempos análisis de información, como los tiempos de respuesta ante incidentes.

Pentest continuo para poner a prueba la infraestructura local o *cloud* en búsqueda de vulnerabilidades.

480

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

Sus desarrollos cuentan con más de 20 millones de personas usuarias en 24 países. Con oficina central en el parque tecnológico Espaitec de la Universitat Jaume I de Castelló de la Plana (España), cuenta con sedes propias en Barcelona, Burgos, Lugo, Madrid, València, Raleigh/Durham, Bogotá, Panamá, Santo Domingo y San José, en las que trabajan más de 280 personas. Cuatroochenta cotiza en BME Growth como 480S desde octubre de 2020.

480

SOFISTIC
CYBERSECURITY

cuatroochenta.com