Informe de tendencias en ciberseguridad 2023

Resultados de las auditorías y monitorización del SOC (Security Operations Center) a empresas realizadas por Sofistic en 2022 y recomendaciones de ciberseguridad para 2023

SOFISTIC CYBERSECURITY | 480

Índice

¿Por qué otro informe de ciberseguridad?

En Sofistic, el área de ciberseguridad de la tecnológica Cuatroochenta, siempre nos debatimos entre dos estrategias de persuasión sobre cómo podemos ayudar a nuestros clientes: poniendo el foco en las amenazas, los peligros y las consecuencias de un posible ataque, o bien compartiendo conocimiento sobre estrategias de prevención y respuesta activa. A menudo combinamos las dos, pero solemos inclinarnos por huir de la clásica apelación al miedo y al desconcierto, del oscurantismo y las sudaderas con capucha con rostros ocultos. Apostamos por la divulgación, la claridad y por el hacking ético desde nuestros inicios. Lo demostramos, por ejemplo, con nuestras aportaciones a las CVE (*common vulnerabilities and exposures*) o compartiendo experiencias en foros de diferentes países, con la participación de nuestros especialistas siempre que hay oportunidad.

En esa línea de entender la ciberseguridad en positivo presentamos este *Informe de tendencias en ciberseguridad 2023*, con los resultados anonimizados de las auditorías y monitorización del SOC (Centro de Operaciones de Seguridad, en sus siglas en inglés) a empresas realizadas por Sofistic durante 2022, tanto en Latinoamérica como en España. Los hemos analizado y hemos sacado conclusiones para poder ofrecer recomendaciones de ciberseguridad a futuro. Desde el pasado otoño hemos seleccionado los indicadores que consideramos más representativos de todo 2022 y que nos aportan información de mayor valor pensando en cómo poder ayudar en materia de prevención a nuestros clientes, a los que estén pensando en serlo y a cualquier persona interesada en ciberseguridad para empresas.

En los últimos tiempos la ciberseguridad ha pasado de ser un ruido de fondo a estar en primer plano, estrepitosamente presente en el día a día. Y la mejor manera de proteger nuestras organizaciones es tomar decisiones informadas: sabiendo por dónde, cómo y por qué se pueden producir los ciberataques seguro que tendremos más resortes para minimizar riesgos. Teniendo en cuenta que el primer desafío que plantea la ciberseguridad a las empresas en la actualidad es ser conscientes de su alcance y profundidad y de que el punto más vulnerable somos las personas. En Sofistic estamos especializados en infraestructuras críticas, en el sector financiero y el sanitario, aunque la mayoría de las conclusiones se pueden hacer extensibles a cualquier organización.

Esperamos sinceramente que el esfuerzo te sea útil.

Muestra

El informe se basa en una muestra suficientemente amplia y representativa del trabajo realizado por el equipo de Sofistic en 2022, compuesta por auditorías de seguridad y resultados 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 40 clientes, lo que supone el análisis de 1.250 vulnerabilidades. Hemos incluido categorías como auditorías a aplicaciones (web y móviles), infraestructuras (externas, internas y *cloud*) y algunas con menor volumen pero que han incrementado considerablemente su presencia en los últimos tiempos, como las auditorías de blockchain o de entornos OT.

Incidentes de seguridad detectados en el SOC.

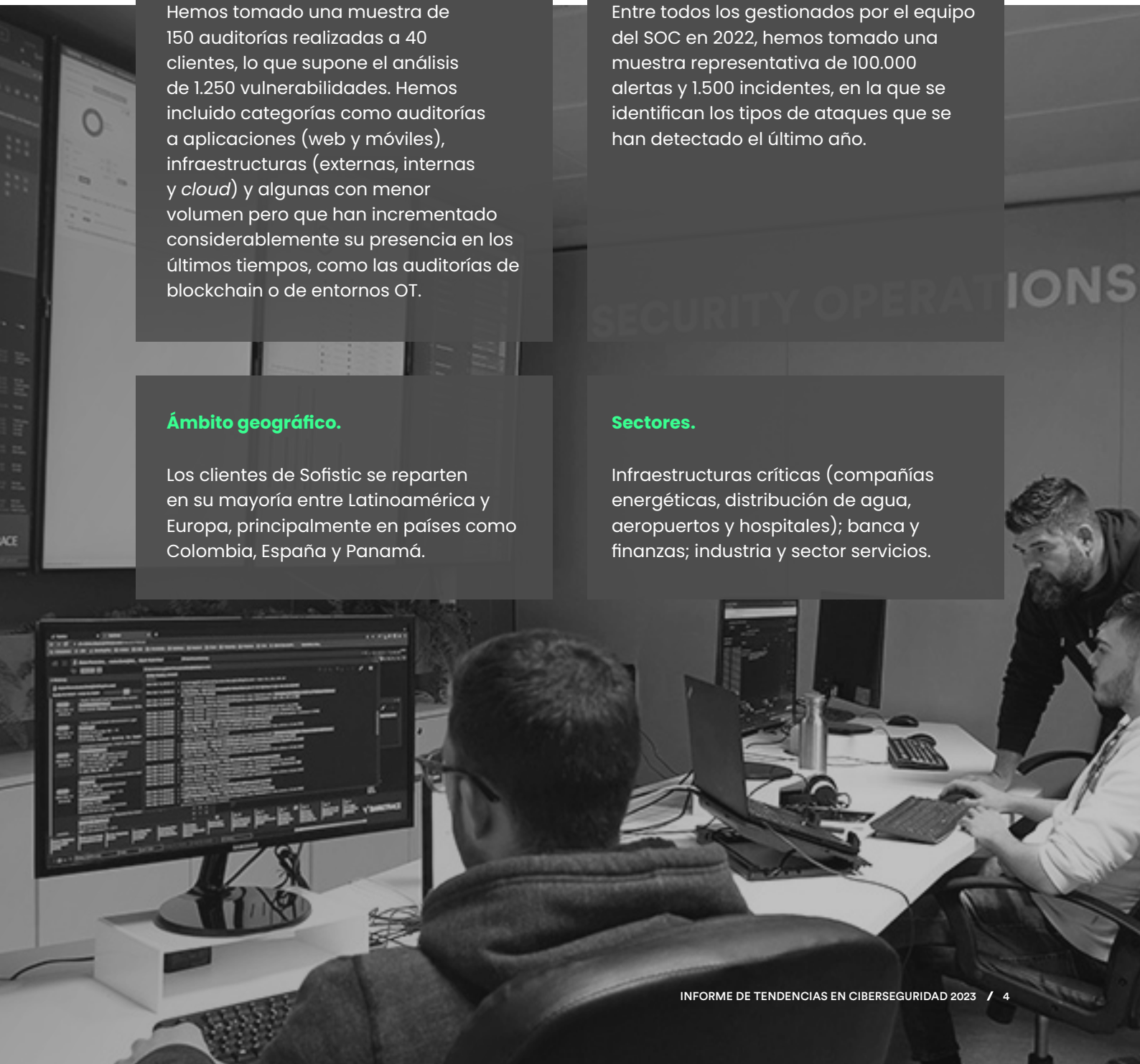
Entre todos los gestionados por el equipo del SOC en 2022, hemos tomado una muestra representativa de 100.000 alertas y 1.500 incidentes, en la que se identifican los tipos de ataques que se han detectado el último año.

Ámbito geográfico.

Los clientes de Sofistic se reparten en su mayoría entre Latinoamérica y Europa, principalmente en países como Colombia, España y Panamá.

Sectores.

Infraestructuras críticas (compañías energéticas, distribución de agua, aeropuertos y hospitales); banca y finanzas; industria y sector servicios.



Resultados

1. Auditorías de seguridad

Mayor concienciación, pero con más fallos críticos

El primer bloque de este informe ofrece una visión del tipo de fallos de seguridad que se han encontrado en los diferentes sistemas, aunque no se hayan explotado activamente, y evidencian los errores más comunes que se producen en las configuraciones o desarrollos. Partiendo de la citada muestra representativa de vulnerabilidades, se analiza la evolución en 2022 respecto a 2021.

Auditorías	53%
Vulnerabilidades	45%
Severidad	53%

Variación 2021/22

En cuanto a volumen, durante 2022 se aprecia un incremento significativo tanto en el número de auditorías realizadas (53%), como en el número de vulnerabilidades detectadas, a nivel absoluto y proporcionalmente, y también su severidad. Aunque es normal que las dos primeras métricas vayan de la mano, destaca que los fallos encontrados han sido de mayor riesgo, en promedio, que los de 2021. Esto significa que crece la preocupación por la ciberseguridad, ya que constatamos un aumento del número de auditorías total y el de las realizadas a cada cliente, pero también que sigue habiendo carencias en la implantación de las medidas de seguridad más críticas.

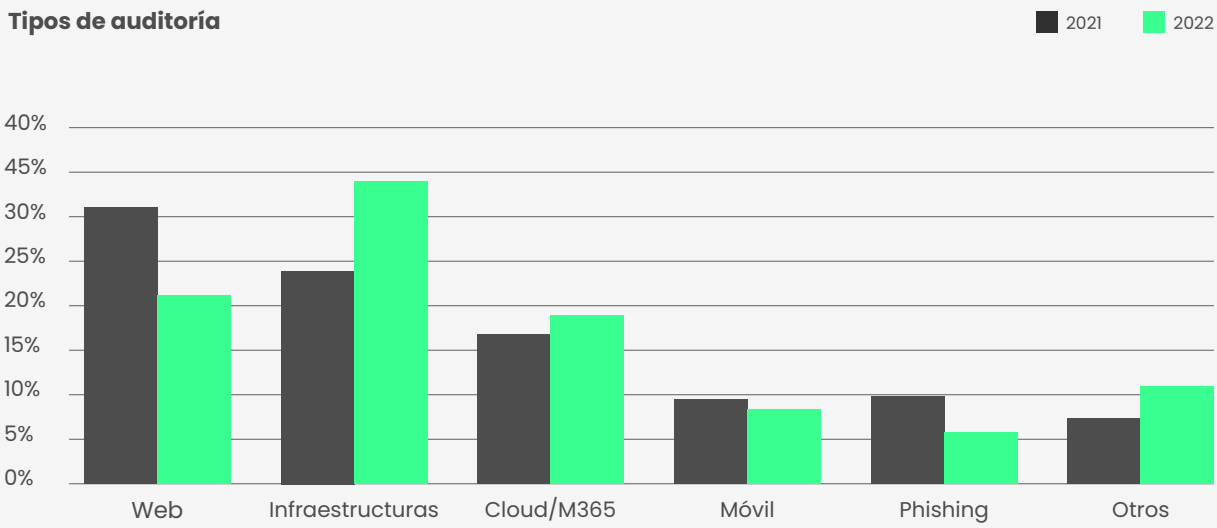
Las auditorías de infraestructuras se duplican

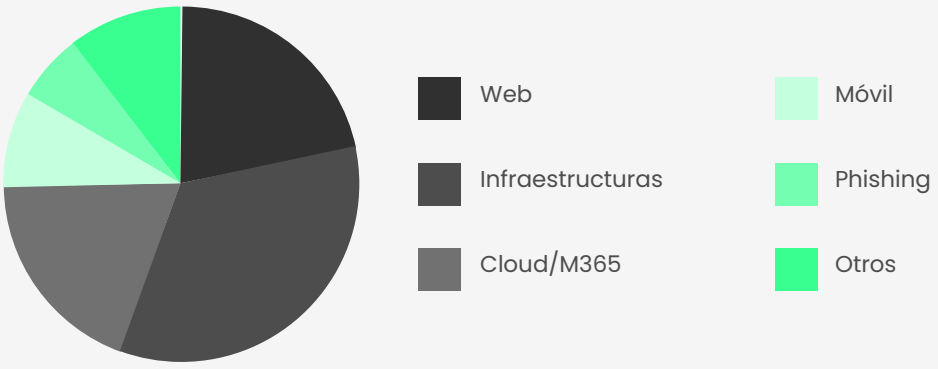
Por tipo de auditoría	Variación 2021/22
Web	3%
Infraestructuras	112%
Móvil	8%
Cloud/M365	71%
Phishing	18%
Revisión código	-16%
Blockchain	200%
RedTeam	3%
OT	100%

A nivel general, el número de auditorías de la muestra ha aumentado significativamente en todos los campos en 2022, destacando el incremento del 112% en infraestructuras y del 71% en auditorías del *cloud* y de Microsoft 365. Esta situación es consecuente con el panorama actual, donde se producen ataques constantes a redes tanto internas como externas y donde cada vez más empresas migran parte de su infraestructura a la nube, especialmente desde la pandemia, así como de un incremento de la concienciación sobre los riesgos.

Top tipo de auditorías por volumen	2021	2022
Web	31%	21%
Infraestructuras	23%	33%
Cloud/M365	16%	19%
Móvil	9%	8%
Phishing	9%	5%
Otros	7%	10%

Tipos de auditoría



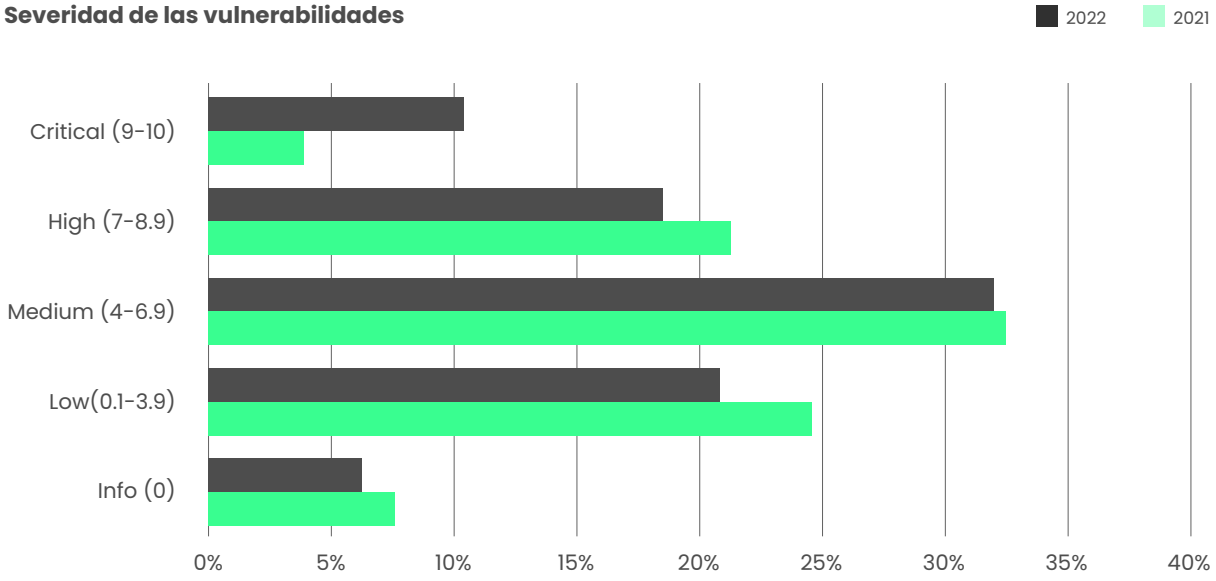


Para poner en contexto el crecimiento aislado, se debe correlacionar con el volumen, para así apreciar cómo el crecimiento de algunas áreas impacta de manera significativa en el total de la muestra. De esta forma, detectamos una clara tendencia en la preocupación por la securización de las infraestructuras, en detrimento de otras históricamente más generalizadas, como las aplicaciones web o aplicaciones móviles. Además, se atestigua el alto crecimiento de auditorías que hasta hace unos años se consideraban minoritarias o de nicho, como las de blockchain o de entornos OT, que se han triplicado y duplicado, respectivamente.

Crece la severidad de los ataques

Severidad (% del total)	2021	2022
Critical (9-10)	4%	10%
High (7-8.9)	21%	18%
Medium (4-6.9)	37%	37%
Low (0.1-3.9)	29%	25%
Info (0)	7%	5%

Severidad de las vulnerabilidades



Al analizar la severidad de las vulnerabilidades detectadas, llama la atención que las de severidad alta y las críticas representan casi el 30% de los hallazgos. Estas últimas incluso se han multiplicado por más de 2,5 con respecto a 2021, en concreto han crecido un 165%. Hay varios factores que pueden explicar esta evolución, siendo el principal el incremento de auditorías en infraestructuras, sobre todo internas, donde se suele descuidar más la seguridad al tratarse de un entorno supuestamente controlado. En segundo lugar, se observa que muchas de estas vulnerabilidades se producen en entornos que han sido auditados por primera vez, donde se suelen detectar más agujeros de seguridad que, en sucesivas auditorías, ya han sido corregidos.

El hecho de que haya tantas altas y críticas plantea un escenario de riesgo considerable, pues implica que las organizaciones pueden tener servicios y máquinas muy expuestas, dando la opción al ciberdelincuente de tomar el control y comprometer seriamente su operativa.

Los fallos criptográficos y de control de acceso, los más comunes

Según se desprende de los resultados desglosados por categoría de vulnerabilidad, los fallos criptográficos ocupan la primera posición: ausencia de cifrado, algoritmos inseguros, uso de software desactualizado… Le siguen, en segundo lugar, los fallos de control de acceso, es decir, cómo podemos garantizar que se accede a la información correcta y, en tercero, los fallos de configuración. Todo lo cual pone de relieve que la alta complejidad tecnológica obliga a tener equipos de IT altamente cualificados.

Por otra parte, los fallos que más incremento han experimentado en 2022 respecto a 2021 han sido los relativos a los registros de actividad y los relacionados con software desactualizado y/o vulnerable.

Este escenario puede explicarse por varias razones. En primer lugar, la prevalencia de los fallos criptográficos se debe a que cualquiera de los tipos de auditoría analizados incluye, de alguna manera, sistemas criptográficos y, por tanto, es natural que se identifiquen fallos relacionados.

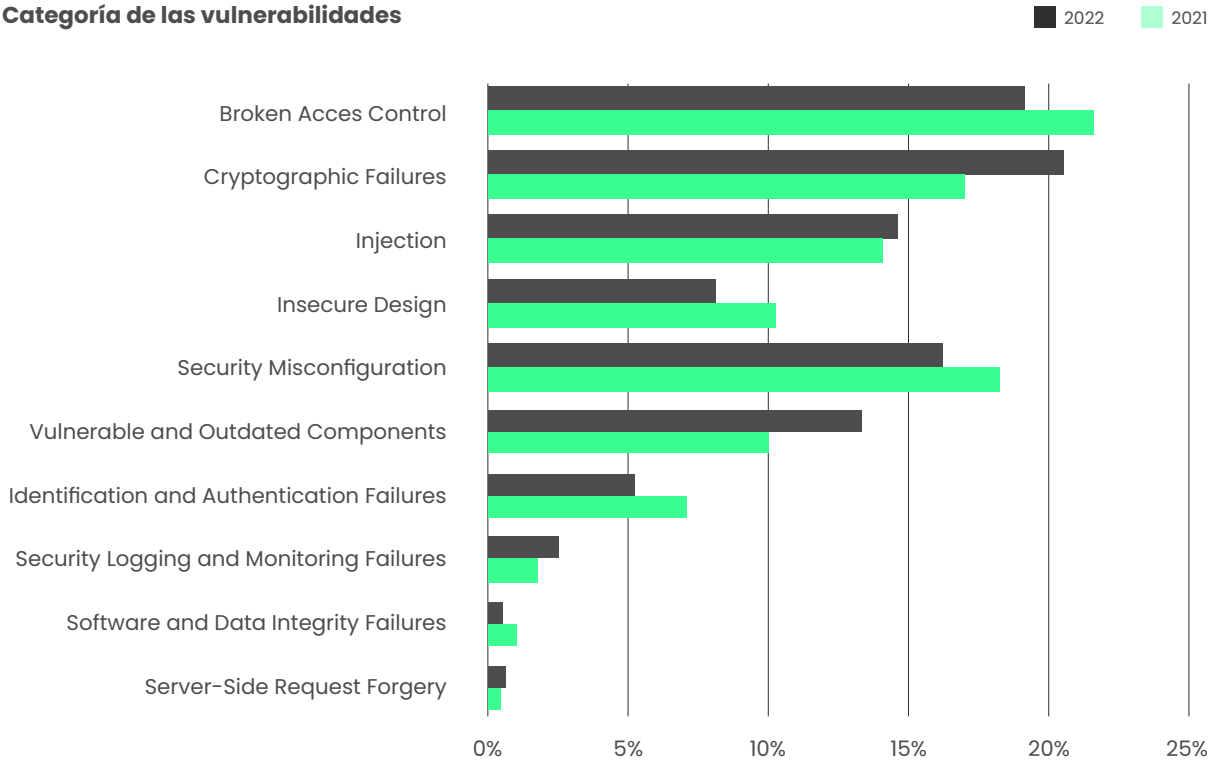
En segundo lugar, observamos que las categorías que experimentan un gran crecimiento interanual tienen un factor común: están más íntimamente relacionados con fallos de configuración o con infraestructuras. Esto concuerda con el incremento detectado anteriormente en el número de análisis de entornos *cloud*, donde prevalecen los fallos de configuración, y de infraestructuras, relacionados con software desactualizado, cifrado y control de accesos.

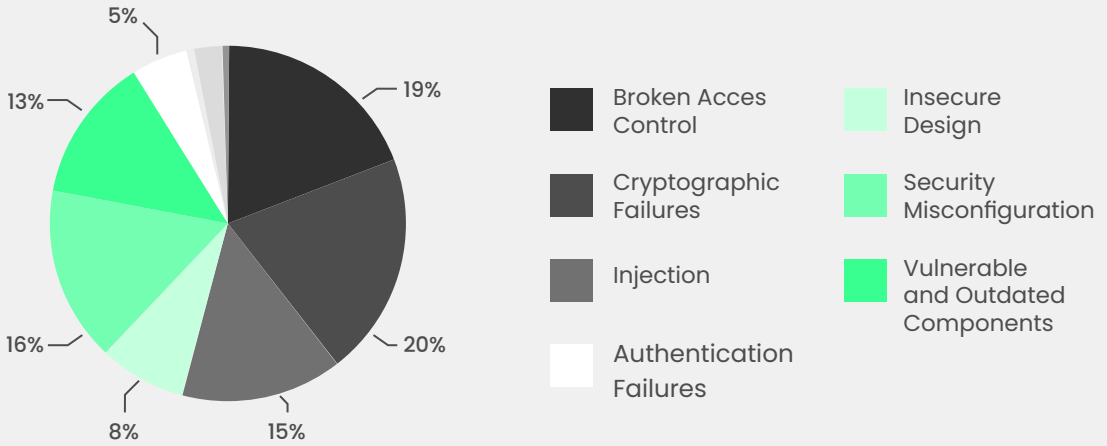
Por el contrario, descienden los fallos de seguridad por diseño, integridad y sistemas de autenticación. Respecto a los dos primeros, el principal motivo es que comienza a haber una mayor sensibilización a la hora de la definición y diseño de las arquitecturas, así como un mayor control y securización del software nuevo. Por otro lado, los sistemas de autenticación han sido durante mucho tiempo uno de los puntos más débiles, pero esta tendencia se ha ido revirtiendo poco a poco al utilizar sistemas adicionales para reforzar este proceso, como las librerías específicas para la autenticación multifactor (MFA o 2FA).

La siguiente tabla resume el peso relativo de cada categoría de incidencia y su evolución de 2021 a 2022, incluido el ranking actual de las 10 principales:

Categoría	Volumen			Puesto		
	2020	2021	Variación	2021	2022	
Cryptographic Failures	17%	20%	18%	3	1	↑2
Broken Access Control	20%	19%	-8%	1	2	↓1
Security Misconfiguration	17%	16%	-9%	2	3	↓1
Injection	14%	14%	3%	4	4	=0
Vulnerable and Outdated Components	10%	13%	32%	6	5	↑1
Insecure Design	10%	7%	-23%	5	6	↓1
Identification and Authentication Failures	7%	5%	-26%	7	7	=0
Security Logging and Monitoring Failures	1%	2%	70%	8	8	=0
Software and Data Integrity Failures	0%	0%	-39%	9	9	=0
Server-Side Request Forgery	0%	0%	10%	10	10	=0

Categoría de las vulnerabilidades





Phishing: menor índice de clicks, pero aún se introducen credenciales

Phishing	2021	2022	Variación
Emails abiertos	49%	35%	-28%
Enlace abierto	29%	17%	-40%
Introducción de credenciales	10%	10%	-5%

Por último, respecto a las auditorías de ingeniería social, en 2022 hemos detectado un descenso general de usuarios que interactúan con los emails de phishing, reduciéndose el número de los que abren los emails y aquellos que, aun abriéndolo, hacen clic en enlaces de los emails fraudulentos. Sin embargo, continúa habiendo un importante número que sí facilita datos, por ejemplo, introduciendo información en un formulario, sobre el que apenas hemos notado mejora en los resultados.

2. Incidentes detectados en el SOC

Los servicios de monitorización de la ciberseguridad, en alza

En este segundo bloque nos centramos en la perspectiva del SOC (Security Operations Center), que permite identificar no tanto los fallos, sino los ataques reales que se están produciendo sobre las organizaciones. Tomando como referencia la muestra del estudio, las empresas que han apostado por centralizar y monitorizar su ciberseguridad en un centro de detección y respuesta 24/7 como el de Sofistic han crecido un 200% en el último año, lo que pone de manifiesto el creciente interés por abordarla de una forma integral.

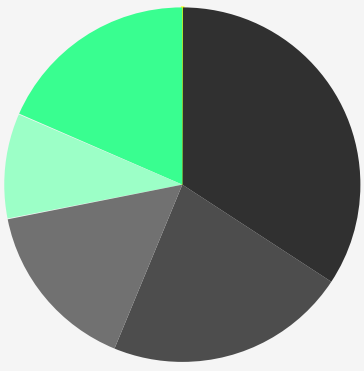
Además, se ha detectado un fuerte incremento, proporcionalmente en el último año, tanto en el número de alertas gestionadas (250%) como en el número de incidentes investigados (300%), lo que confirma la intensa actividad cibercriminal registrada en 2022 a nivel global.

Alertas gestionadas **250%**

Incidentes investigados **300%**

Bancos e infraestructuras críticas, los más previsores

Sectores	%
Finanzas	34%
Infra. Crítica	22%
Industrial	16%
Retail	9%
Otros	19%



El sector financiero y el de las infraestructuras críticas aglutinan el 56% de las empresas gestionadas en el SOC de Sofistic, seguidos a distancia por el sector industria y el *retail*. Aunque cualquier sector puede ser objetivo de la cibercriminalidad, realmente hay una gran diferencia en el volumen de ataques registrados en ciertos sectores, lo que se corresponde con el perfil de clientes que contratan los servicios de ciberseguridad de Cuatroochenta.

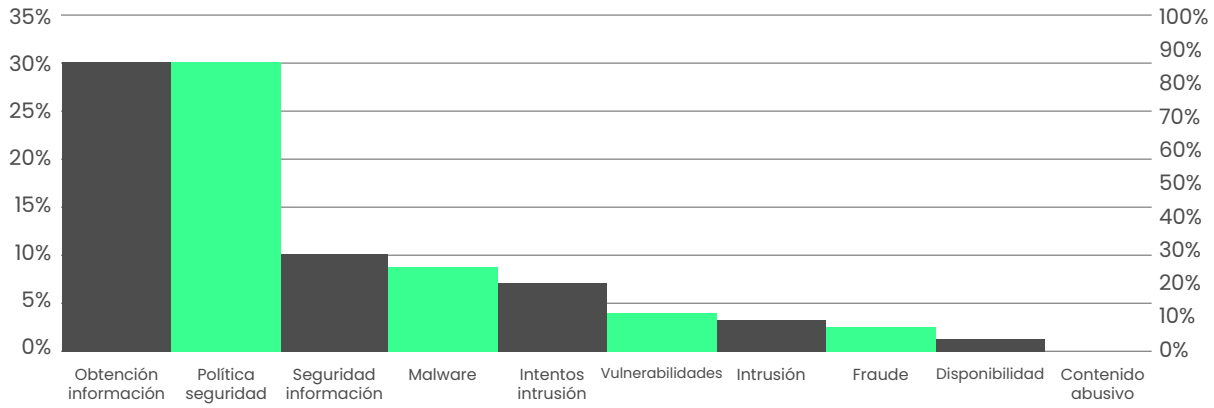
Por un lado, los bancos y entidades financieras son el primer objetivo de los ciberdelincuentes por razones económicas, que es la principal motivación de su actividad fraudulenta.

Las infraestructuras críticas, por su parte, son objetivo de otra tipología de ciberdelincuentes, que no buscan tanto la recompensa económica, sino la posibilidad de interferir o desestabilizar las infraestructuras de un país, atacando, por ejemplo, a los sistemas informáticos de la distribución de agua o energía, aeropuertos, hospitales… Prácticas que han proliferado, especialmente, como consecuencia de la invasión de Rusia a Ucrania en febrero de 2022.

Sustraer información de valor para extorsionar

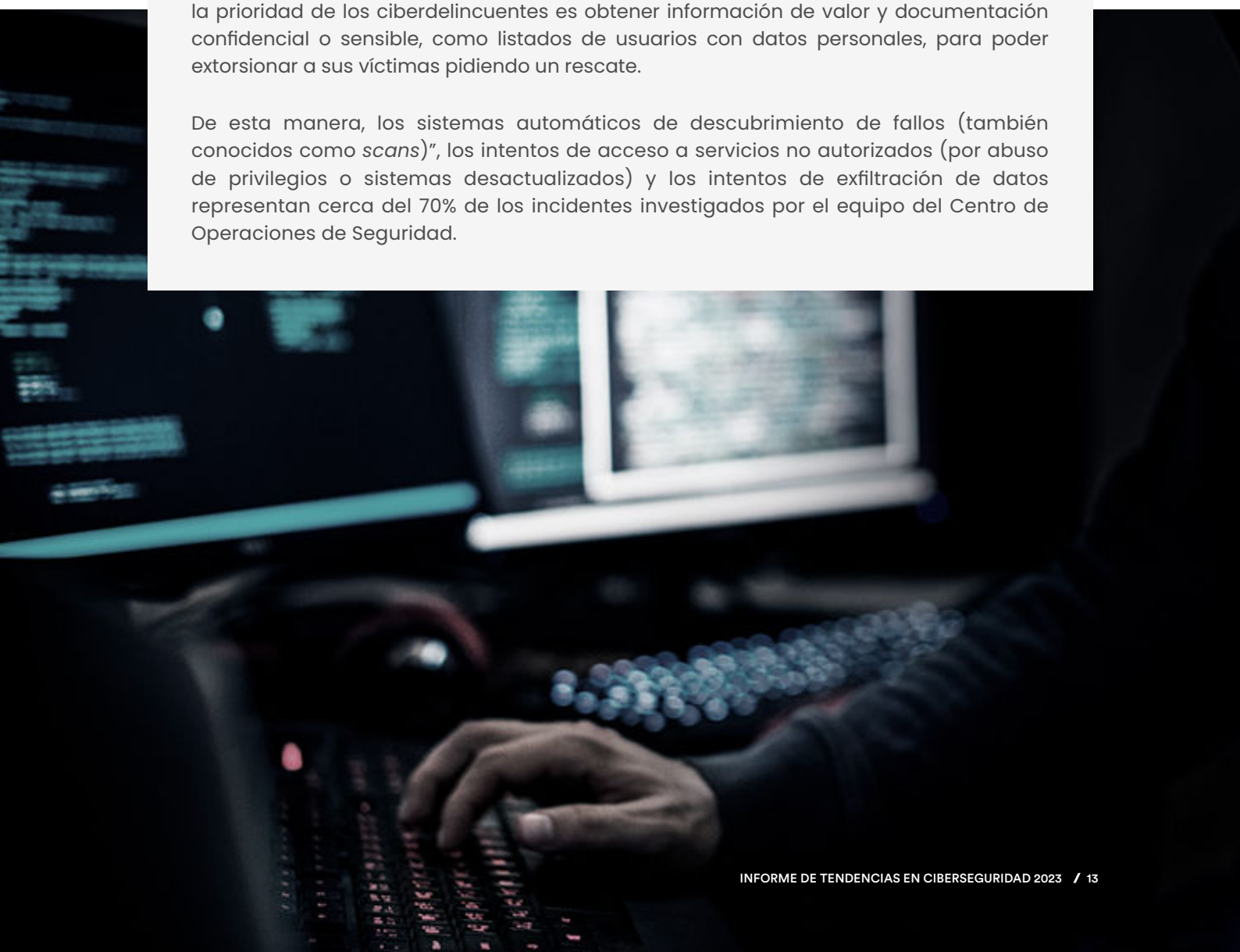
Tipo de incidente	%
Obtención información	31%
Política seguridad	31%
Seguridad información	10%
Malware	9%
Intentos intrusión	8%
Vulnerabilidades	4%
Intrusión	3%
Fraude	3%
Disponibilidad	1%
Contenido abusivo	0%

Incidentes por tipo



La tipología de incidentes investigados por el SOC de Sofistic pone de manifiesto que la prioridad de los ciberdelincuentes es obtener información de valor y documentación confidencial o sensible, como listados de usuarios con datos personales, para poder extorsionar a sus víctimas pidiendo un rescate.

De esta manera, los sistemas automáticos de descubrimiento de fallos (también conocidos como *scans*)", los intentos de acceso a servicios no autorizados (por abuso de privilegios o sistemas desactualizados) y los intentos de exfiltración de datos representan cerca del 70% de los incidentes investigados por el equipo del Centro de Operaciones de Seguridad.



Conclusiones

Los resultados de la muestra de las auditorías de seguridad y de la monitorización del SOC de Sofistic son coherentes con los informes anuales de 2022 que están publicando diferentes organismos especializados en ciberseguridad en lo que va de año. Como conclusión general, el incremento de ataques a todo tipo de empresas, pero especialmente a las que se dedican a una actividad y manejan información más sensible, ha terminado por concienciarlas hasta el punto de entender la ciberseguridad como una inversión estratégica y no como un gasto. No obstante, nuestro informe también permite sacar conclusiones que nos pueden ayudar a tomar decisiones de futuro:

- **La ciberseguridad se asienta como un proceso más dentro de las empresas.** En 2022 ha crecido significativamente el número de empresas que han decidido realizar auditorías de diferente índole por primera vez; compañías que ya destinaban recursos humanos y económicos han solicitado más auditorías y, por último, también son más las empresas que han apostado por integrar servicios de monitorización o gestión de sus herramientas a través del servicio del SOC. Cada vez más se entiende la ciberseguridad como un proceso de mejora continua, que nos ayuda a identificar dónde están las vulnerabilidades y cuáles son los pasos que tenemos que dar para resolverlas, mitigarlas o asumirlas, en base a un análisis de riesgos y un plan específico.

- **Crece el número de vulnerabilidades y su severidad**. Casi el 30% de las vulnerabilidades detectadas en 2022 son de severidad alta y crítica, y las segundas son las que más han aumentado multiplicándose por 2,5, lo que habla de un riesgo muy patente de alteración para la operativa de las empresas, que generalmente tiene que ver con un déficit de actualización en las infraestructuras.

- **La securización de infraestructuras y entornos *cloud*, protagonista.** En base al tipo de auditorías más solicitadas en 2022 se determina que, precisamente, la principal tendencia ha sido proteger las infraestructuras externas e internas (sobre todo estas últimas, porque suelen estar más descuidadas) y también los entornos *cloud*.

- Las principales vulnerabilidades detectadas en **infraestructuras externas e internas** se concentran en:

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

Fallos de control de acceso, donde usuarios sin privilegios pueden acceder a recursos que no deberían.

Fallos de configuración, lo que revela que la alta complejidad tecnológica obliga a tener equipos IT altamente cualificados, que no siempre tienen la opción de realizar formación continua, así como protocolos actualizados y seguros.

Acceso a través de VPN y wifi inseguras. Brechas por las que pueden llegar a acceder personal externo a la empresa o empleados díscolos

- **En entornos *cloud*, gran parte de los hallazgos están relacionados con políticas y configuraciones deficientes, exceso de permisos y una gestión de los registros *(logs)* insuficiente.** No sólo debemos tener en cuenta qué fuentes se recogen, sino cómo vamos a gestionar dichos logs, aplicar políticas coherentes, sin olvidarnos de cómo vamos a gestionar los accesos y permisos de los usuarios. Según nuestras auditorías, este es uno de los fallos con mayor impacto sobre la infraestructura.

- **Las auditorías de blockchain y OT, un reto en auge.** Su incremento es un reflejo de la apuesta de muchas organizaciones por incorporar estas tecnologías en su infraestructura, lo que supone un importante reto desde el punto de vista de la ciberseguridad. Las auditorías de blockchain son complejas por la propia tecnología y por el hecho de que cada empresa tiene necesidades muy concretas, haciendo que cada proyecto difiera mucho de una a otra. Los entornos OT, por su parte, tienen su dificultad en la propia interconexión de los dispositivos, ya que muchos de ellos usan protocolos de comunicación propietarios y el acceso al conocimiento es más limitado. Además, la experiencia en nuestros clientes ha evidenciado que existe la falsa sensación de que los entornos OT están aislados del resto de sistemas IT, y por tanto de sus riesgos, cuando en la gran mayoría de los casos ese aislamiento no es completo. Por esa razón, se recomienda seguir el criterio de *Zero Trust* y proteger los sistemas entendiendo que la red pueda ser vulnerada.

- **Las plantillas, mejor formadas sobre ingeniería social pero todavía con brechas.** El aumento de las auditorías de ingeniería social, enfocadas a conocer y mejorar el grado de concienciación de las plantillas en materia de ciberseguridad, es un hecho muy positivo, ya que las personas son el principal vector de ataque de los ciberdelincuentes: a mayor grado de concienciación, mayor capacidad de resiliencia ante un ciberataque. Lo más representativo es que el porcentaje de usuarios que interaccionan con un email fraudulento desciende considerablemente, aunque no en la misma proporción aquellos que finalmente facilitan información o introducen los datos en formularios.

- **Más alertas e incidentes gestionados en el SOC.** Los datos obtenidos por el servicio de monitorización del SOC de Sofistic confirma que el número de alertas e incidentes gestionados se ha incrementado de forma considerable, multiplicándose por 2,5 y por 3, respectivamente; como apuntábamos, en la línea de los datos de actividad global de cibercriminalidad recopilados por diversos organismos internacionales.

- **El ransomware, la mayor preocupación y con razón.** La mayoría de los incidentes investigados en el SOC de Sofistic se centran en el abuso de los privilegios (tanto los intentos de acceso no autorizados como el abuso de permisos), explotar vulnerabilidades en sistemas expuestos sin actualizar o intentar exfiltrar información. Una tipología de incidentes que están relacionados con diferentes fases de los ataques de ransomware, lo que refrenda que el secuestro de datos sea, hoy en día, la mayor preocupación para los responsables de ciberseguridad o IT de cualquier compañía.

Recomendaciones de ciberseguridad para 2023

El análisis de las tendencias en ciberseguridad registradas en 2022 nos lleva a plantear una serie de recomendaciones prácticas para minimizar riesgos en 2023:

- **Revisar configuraciones y monitorización.** Los entornos *cloud* siguen ganando relevancia, en cualquiera de sus opciones: empresas que migran todo al *cloud*, empresas en modo híbrido que combinan *cloud* y sistemas *on-premise* (alojados dentro de la organización) y empresas que usan entornos multi-*cloud* a través de diferentes proveedores. En cualquier caso, las recomendaciones de seguridad son similares:

- ***Firewall* para servidores y servicios *cloud*.** Hace unos años era lógico disponer de una gran infraestructura en las oficinas para dar cabida a todos los equipos de trabajo y servidores, por lo que uno de los proyectos más relevantes era escoger un buen *firewall* que garantizara la seguridad de las conexiones. En la actualidad, dada la tendencia a tener todos los servicios en el *cloud*, es más importante disponer de soluciones SASE (Secure Access Service Edge) o CASB (Cloud Access Security Brokers), que además encajan con la estrategia Zero Trust, una de las principales estrategias que están adoptando las empresas.

- ***Zero Trust.*** La evolución y sofisticación de los ataques, junto con entornos cada vez más complejos donde se desdibuja completamente el perímetro de seguridad, hacen que las estrategias tradicionales pierdan eficacia. La premisa de este paradigma es que, de entrada, no debemos confiar en nada y que siempre debemos validar, aprovechando toda la información contextual posible (credenciales, red, ubicación, equipo, comportamiento...), que el usuario es quien dice ser y que tiene permisos para realizar la acción que pretende, en base a un esquema de mínimos privilegios. Este paradigma cobra especial relevancia en entornos híbridos y/o en aquellos donde prevalece el teletrabajo.

- **Acceso remoto.** Con la progresiva implantación del modelo de trabajo híbrido, las empresas se ven obligadas a dar acceso a sus recursos de forma remota, lo que abre nuevos vectores de ataque. Más allá de las habituales conexiones VPN, encontramos soluciones ZTNA (Zero Trust Network Access) que habilitan el acceso microsegmentado y seguro a aplicaciones privadas por parte de los usuarios desde cualquier ubicación y dispositivo, evitando el riesgo de que éstas se encuentren accesibles de forma abierta en internet.

- **Proteger credenciales sin bloquearlo todo.** La gestión de la identidad digital ya representa en sí mismo todo un reto porque, a medida que crece el número de servicios que usamos en nuestra empresa, aumentamos el número de credenciales. Según la mayoría de los estudios, el uso fraudulento (por robo o exposición) de las credenciales está relacionado con el 90% de los incidentes. Podemos mejorar esta gestión con el apoyo de herramientas que nos permitan unificar la autenticación, segregar los permisos siguiendo el principio del mínimo privilegio, utilizar múltiples factores e identificar accesos de riesgo.

- **Concienciar, formar y procedimentar.** Todavía es elevado el número de personas que interaccionan con emails fraudulentos y, si a esto le unimos que cada vez se observan más ataques de los denominados "*fileless*" (se ejecutan directamente en la memoria del equipo dificultando la labor de detección por parte de los antivirus tradicionales), el riesgo es aún mayor. Hay que seguir apostando no solo por la concienciación, sino por la formación constante en ciberseguridad para los empleados y que ésta se traduzca en procedimientos claros que realmente se cumplan.

Quiénes somos

Sofistic, la división de ciberseguridad de Cuatroochenta, está especializada en sectores críticos, ofreciendo tanto protección preventiva y proactiva como una respuesta eficaz a los incidentes apoyándose en el software más avanzado. Cuenta con una amplia experiencia y una trayectoria de 14 años minimizando riesgos y maximizando la protección y la 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 ISO27001 y ENS.

Entre los servicios de Sofistic destacan:

Security Operations Center (SOC) para monitorizar la ciberseguridad de empresas e instituciones en Europa y América. Un centro redundante 24/7, con sedes en España y Panamá, para detectar y dar una respuesta integral a ciberamenazas de forma ininterrumpida.

Auditoría de seguridad. Pentest o auditoría de seguridad informática que simula un ciberataque a los sistemas de la empresa. A través del hacking ético nuestros profesionales analizan las posibles brechas y descubren hasta dónde podría acceder un atacante.

MSSP. Servicios de seguridad gestionados en la modalidad MDR (*Managed Detection and Response*), basados en inteligencia artificial y aprendizaje automático para prevenir amenazas en sistemas y dispositivos con el software más avanzado de Crowdstrike, Darktrace y Exabeam.

Microsoft Security. Implantamos las herramientas de ciberseguridad de Microsoft en todo tipo de clientes, desde pequeñas empresas a grandes infraestructuras críticas como aeropuertos o entidades financieras.

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 10 millones de personas usuarias en 21 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, València, Madrid, Burgos, Lugo, Bogotá, Panamá, Santo Domingo, San José y Raleigh, en las que trabajan más de 280 personas. Cuatroochenta cotiza en BME Growth como 480S desde octubre de 2020.

En la elaboración del informe han participado

Manuel Ginés (CIO de Sofistic)

Juan Carlos García (SOC manager y country manager de Sofistic en España)

David Hernández (responsable de comunicación de Cuatroochenta)

SOFISTIC

CYBERSECURITY

480