



ES

De enero de 2019 a abril de 2020

Filtración de datos

Panorama de Amenazas de la ENISA



Sinopsis

La filtración de datos es un tipo de incidente de seguridad informática que se produce cuando se accede a información (o a parte de un sistema de información) sin la autorización debida, normalmente con malas intenciones y originando una posible pérdida o uso indebido de esa información. También incluye «errores humanos» que suelen producirse durante la configuración y el despliegue de determinados servicios y sistemas, y que pueden dejar datos expuestos de forma accidental.¹

En muchos casos, las empresas o las organizaciones no saben que se está produciendo una filtración de datos en su entorno debido a la sofisticación del ataque y, a veces, a la falta de visibilidad y clasificación en su sistema de información.² Basándonos en estudios realizados, una organización tarda aproximadamente 206 días en identificar una filtración de datos.³ Por lo tanto, el tiempo que se tarda en contener, remediar y recuperar los datos significa que se tarda más en volver a la normalidad.

A pesar de los riesgos que conlleva utilizar las infraestructuras de almacenamiento en la nube y complejos entornos internos, las organizaciones cada vez almacenan más datos⁴ de esta manera. Estos entornos están cada vez más expuestos a los distintos riesgos, de forma proporcional a la sensibilidad de la información almacenada. No resulta sorprendente que el número de filtraciones de datos aumentara en 2019 y en 2020. Los nuevos datos disponibles también sugieren que el impacto no se nota solo en el momento de descubrir la filtración, sino que el impacto económico puede durar más de 2 años después del incidente.



Conclusiones

54 % es el aumento en la cifra total de filtraciones a mediados del año 2019 con respecto a 2018.

71 % es el porcentaje de filtraciones de datos llevadas a cabo con fines económicos. Casi un 25 % tenían objetivos estratégicos a largo plazo (Estado nación/ espionaje).⁵

32 % es el porcentaje de las filtraciones de datos que conllevan actividades de *phishing* según IOCTA 2019.⁶ Un informe sugiere que los ataques de suplantación de identidad figuran en la cabeza de la lista de los mayores contribuyentes a las filtraciones de datos. El informe también menciona que el correo electrónico es el principal método de entrega del *malware* (94 %), en una cadena de eventos que desembocan en la filtración de datos.³

52 % es el porcentaje de las filtraciones de datos que conllevaron actividades de piratería informática.⁵ Otras tácticas utilizadas son los ataques de ingeniería social (33 %), *malware* (28 %) y errores o equivocaciones (21 %). Desde 2016 la piratería informática ha sido la principal responsable de las filtraciones de datos sanitarios. En 2019 casi un 59 % de las filtraciones registradas se debieron a actos de piratería informática.⁷

70 % de las filtraciones de datos exponen mensajes de correo electrónico. Aunque el nombre de usuario, la dirección de correo electrónico y las contraseñas (es decir, las credenciales) se pueden cambiar fácilmente en comparación con los datos de personales (como la fecha de nacimiento), las filtraciones de datos se centran principalmente en esta información.⁸

55 % es el porcentaje de participantes en la encuesta del Eurobarómetro que contestaron que les preocupa que delincuentes y estafadores puedan acceder a sus datos.



Cronología

2019

Enero

MEGA cloud (Nueva Zelanda) sufrió una filtración de datos que expuso 770 millones de correos electrónicos y 21 millones de contraseñas.⁹

Febrero

Un vendedor presume de que hay 620 millones de cuentas robadas de 16 sitios *web* pirateados a la venta en la *dark web*.¹⁰

Marzo

Se expusieron al público 12,5 millones de historias médicas de mujeres embarazadas de los centros de salud estatales de la India, remontándose a 2014.¹¹

Octubre

Se expuso la información de las cuentas de más de 7,5 millones de usuarios de Adobe (EE. UU.) debido a una base de datos en línea desprotegida.¹⁸

Septiembre

Mastercard (Bélgica) sufrió una filtración de datos que afectó a casi noventa mil clientes en Europa.¹⁷

Agosto

Se descubrió una filtración importante en el sistema de datos biométricos utilizado por los bancos, la policía y las empresas de defensa del Reino Unido.¹⁶

Noviembre

UniCredit (Italia) fue víctima de una filtración de datos que expuso 3 millones de registros.¹⁹

Diciembre

El proveedor de cámaras inteligentes Wyze (EE. UU.) sufrió dos filtraciones a finales de diciembre que dejaron expuestas las bases de datos durante más de dos semanas.²⁰

Enero

Se produjo una filtración de 250 millones de registros de atención y asistencia al cliente de Microsoft (EE. UU.), las fechas de estos registros se remontan a 2005.²¹

2020



— Abril

Facebook (EE. UU.) notificó una filtración de datos que expuso 540 millones de registros de usuarios en los servidores expuestos.¹²

— Mayo

First American Financial Corp. (EE. UU.) fue víctima de una filtración de cientos de millones de registros de seguros de títulos de propiedad.¹³

— Julio

Se filtraron los datos personales de clientes de tarjetas de crédito de Capital One (EE. UU.).¹⁵

— Junio

Se produjo un acceso no autorizado a los datos almacenados de clientes de Evite que tuvo como resultado la exposición de 100 millones de registros.¹⁴

— Febrero

Un servidor en la nube de Google (EE. UU.), que contenía datos personales de 200 millones de residentes de EE. UU.²²

— Marzo

La empresa de soluciones biométricas Antheus Tecnología (Brasil) sufrió una filtración de datos.²³

— Abril

Los piratas informáticos obtuvieron la información de acceso de dos empleados de Marriott (EE. UU.) y entraron en el sistema en enero de 2020.²⁴

Para las organizaciones el coste de las filtraciones de datos se prolonga durante años

Según investigadores especializados en temas de seguridad, una tercera parte de los costes relacionados con una filtración de datos se produce más de un año después del incidente. Es más, alrededor del 22 % de estos costes se producen el segundo año, y el 11 % se producen transcurridos más de dos años del incidente inicial. Estas cifras fueron más altas para las organizaciones altamente reguladas, como las de servicios financieros y servicios sanitarios, en comparación con otros sectores.³

La adopción de entornos de nube o multinube aumenta con rapidez de forma proporcional a la cantidad de datos almacenados y procesados en estos entornos.

Los pequeños errores pueden originar grandes filtraciones

Asegurar el entorno de nube sin perder toda la flexibilidad que aporta a la infraestructura y a los recursos puede ser problemático. Un solo error de configuración puede exponer todo el contenido de una base de datos sensible. Un investigador especializado en seguridad cree que la mayoría de las filtraciones de bases de datos en la nube se deben a una mala configuración y suelen ser accidentales. Netflix, Ford y TD Bank son algunos de los ejemplos, pero hay muchos más. Desde una perspectiva distinta, aunque las filtraciones de datos resultantes de ataques malintencionados siguen costando más, las filtraciones causadas por errores del sistema o humanos también representan un coste considerable, 3,24 millones de dólares estadounidenses de media (aprox. 2,74 millones EUR).³





Las filtraciones de datos cuestan más a las pequeñas empresas

El coste de las filtraciones para las organizaciones de más de 25 000 empleados en EE. UU. es de 204 dólares estadounidenses (aprox. 173 EUR) por empleado. La estimación de la cantidad total ronda los 5,11 millones de dólares estadounidenses (aprox. 4,33 millones EUR). Por el contrario, para las empresas pequeñas (de entre 500 y 1000 empleados) el coste medio es de unos 3 533 dólares estadounidenses (aprox. 3 000 EUR) por empleado. Esto representa un coste total de 2,65 millones de dólares estadounidenses (aprox. 2,24 millones EUR) para las pequeñas empresas.³

La ganancia económica es el motivo principal

Los atacantes o atacantes son los que mueven los hilos de las filtraciones de datos (aunque a veces se produzcan como resultado de un error). En lo que a esto respecta, los agentes de amenazas externos son la causa principal de las filtraciones de datos y estos incluyen actividades como las *botnets*². En este sentido, la ganancia económica se ha identificado repetidamente como la motivación principal de las filtraciones de datos perpetradas por estos grupos de agentes. El espionaje² también es uno de los motivos principales de las filtraciones de datos pero no tan importante como el de las ganancias personales o económicas. Esta tendencia fue muy similar a los resultados observados en 2010-2011.⁵

_ Preocupación por la seguridad de los datos con la informática cuántica

Los requisitos de criptografía desempeñan una función vital en la era de la informática cuántica y ponen de relieve temas de seguridad críticos. El 72 % de las organizaciones cree que la informática cuántica afectará estratégicamente a sus operaciones relacionadas con la criptografía (en los próximos 5 años). Según los resultados de la encuesta, al 92 % de los participantes les preocupa la exposición de datos sensibles al usar esta tecnología en la industria informática. Las estrategias principales sugeridas por los participantes para abordar estas preocupaciones fueron el cambio de la arquitectura de seguridad y el despliegue de infraestructuras de gestión clave.²⁶

_ La sanidad: un objetivo constante de los atacantes

La sanidad siguió siendo uno de los objetivos más atractivos para los ciberdelincuentes que usan técnicas de *ransomware*²⁷ y *phishing*²⁸, y contener y recuperarse del impacto de estos ataques cuestan millones de euros a estas organizaciones. En 2019, 400 empresas de servicios sanitarios notificaron una filtración de las historias médicas de los pacientes. Fue un número récord para las organizaciones sanitarias.²⁹

_ La multinube: un nuevo desafío para la seguridad de los datos

Una encuesta realizada por un investigador especializado en temas de seguridad arrojó el dato de que 9 de cada 10 empresas piensan usar o ya usan entornos de nube. Aproximadamente un 44 % de los participantes también creían que estos entornos eran complicados para implementar medidas de seguridad de datos adecuadas.²⁵



_Tipos de datos expuestos (%)

Tipo de datos	2019	2018	2017
Correo electrónico	70	44	32
Contraseña	64	39	27
Nombre	23	37	41
Varios	18	19	15
Número de la seguridad social	11	22	27
Tarjeta de crédito	11	16	19
Dirección	11	22	30
Cuenta	10	7	4
Desconocido	8	13	18
Fecha de nacimiento	8	13	12
Médicos	5	9	7
Financieros	5	13	19

Tabla 1 - Fuente: Cyber Risk Analytics⁸

Descenso continuo de las filtraciones con «presencia de tarjeta»

Según un informe de seguridad, en 2019 se identificó un descenso de las clonaciones de tarjetas en puntos de venta y en cajeros (presentando la tarjeta). Esto representa un cambio en las formas tradicionales de copia de tarjetas en cajeros² y en pagos con tarjeta en aplicaciones *web* de comercios. Aunque el número de incidentes de este tipo ha descendido, no es exacto concluir que el número de filtraciones de datos ha descendido, lo que ha ocurrido es que ha habido un cambio de vector. El descenso podría estar relacionado con la amplia implantación de tarjetas y terminales con chip y pin (también llamadas EMV).⁶

Expectativas a corto plazo

Según un investigador especializado en temas de seguridad, las organizaciones sanitarias deberían prepararse para un aumento de entre un 10 % y un 15 % en el número de filtraciones de datos en las que sus proveedores de servicios seguirán siendo el principal objetivo⁷. En términos más generales, basándose en los resultados de los primeros 6 meses de 2019, se prevé que el número de filtraciones de datos aumente a una velocidad alarmante, a pesar de que es algo que los directivos y líderes tienen presente y del intento que hacen muchas organizaciones de asegurar sus datos.⁸





Filtraciones de datos por sector y tamaño de la organización

Incidentes	Filtraciones	Pequeñas	Grandes	Desconocido
Alojamiento	61	34	7	20
Administrativos	17	6	6	5
Agricultura	2	2	0	0
Construcción	11	7	3	1
Educación	99	14	8	77
Ocio	10	2	3	5
Finanzas	207	26	19	162
Atención sanitaria	304	29	25	250
Información	155	20	18	117
Gestión	2	1	1	0
Fabricación	87	10	22	55
Minería	15	2	5	8
Otros servicios	54	6	5	43
Profesional	157	34	10	113
Públicos	330	17	83	230
Inmobiliarios	14	6	3	5
Tiendas	139	46	19	74
Comercio	16	4	8	4
Transporte	36	3	9	24
Servicios esenciales	8	2	0	6
De origen desconocido	289	0	109	180
Total	2013	271	363	1379

Vectores de ataque

- **PHISHING POR CORREO ELECTRÓNICO.** Hacerse pasar por un proveedor o un socio usando el correo electrónico es un premio fácil para los atacantes. Este método es el vector más usado por los ciberdelincuentes para atacar a sus víctimas y causar la mayoría de las filtraciones de datos (casi un 40 % de las filtraciones de datos en sanidad).²
- **APLICACIONES WEB Y EN LA.** Se refiere a las aplicaciones *web* que se utilizan como vector para los intentos por parte de atacantes de filtrar datos u operaciones vitales. El robo de credenciales para entrar en portales de correo electrónico en la *web* es uno de los ejemplos principales. Explotar las debilidades de los servidores de aplicaciones para inyectar o descargar programas de *malware* para el robo de información o para el secuestro de formularios, son dos ejemplos más de estos ataques.²
- **AMENAZAS INTERNAS.** Se refiere principalmente a intentos malintencionados o no autorizados de usar recursos. Cabe apuntar que, por lo general, al analizar y notificar errores de configuración o equivocaciones (errores humanos) por equipos internos también se pueden llamar «infiltrados». Aunque la mayoría de las filtraciones de datos las facilitan atacantes externos, se sigue dando el caso de que personas infiltradas con o sin acceso privilegiado desempeñan un papel fundamental en estas filtraciones.⁵

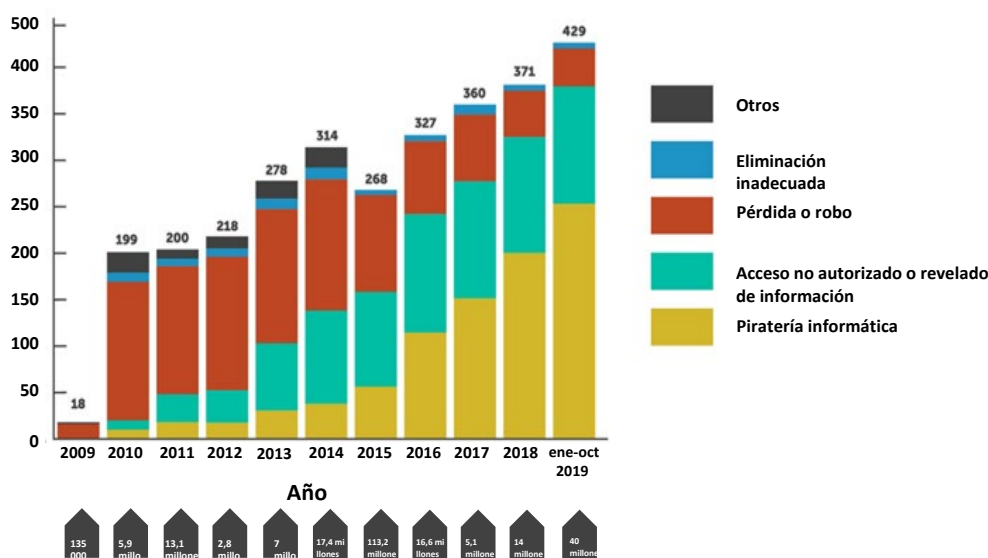


Figura 1: Entidades involucradas en una filtración. Fuente: Horizon²

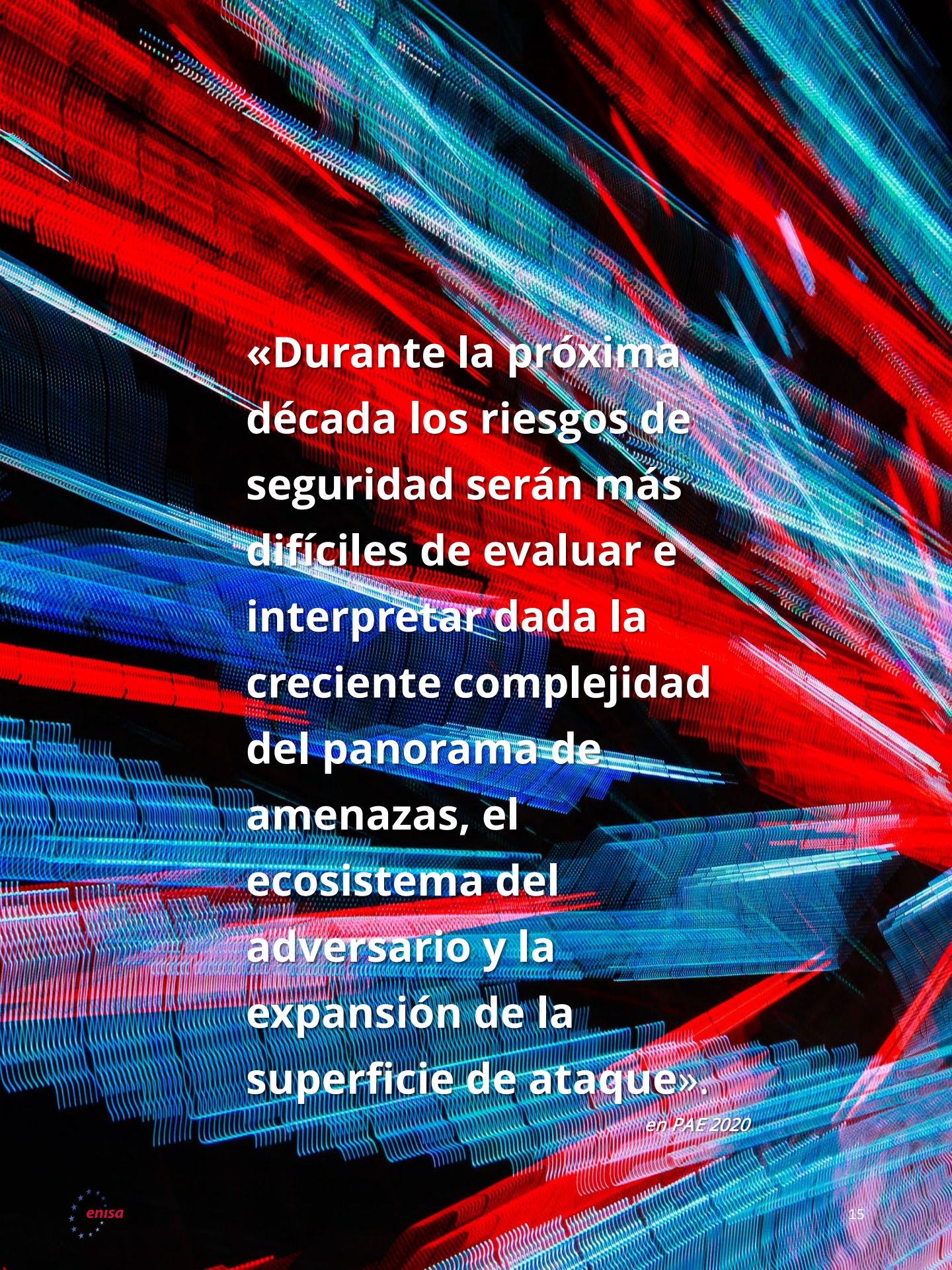
«En muchos casos, las empresas o las organizaciones no saben que se está produciendo una filtración de datos en su entorno debido a la sofisticación del ataque y, a veces, a la falta de visibilidad y clasificación en su sistema de información».

en PAE 2020

Acciones propuestas

- La filtración de datos suele ser por lo general el resultado de otras amenazas y la mitigación se solapa con otras medidas comentadas en este informe.
- Considerar invertir en herramientas de seguridad de datos híbridas centradas en operar en un modelo de responsabilidad compartida para los entornos basados en la nube.²⁶
- Desarrollar y mantener un plan de sensibilización en temas de ciberseguridad. Proporcionar formación y la simulación de escenarios para identificar los trucos de ingeniería social y de las campañas de *phishing* para el personal.⁷
- Establecer y mantener un equipo de respuesta ante incidentes y evaluar los planes de respuesta a incidentes con frecuencia.³
- Identificar y clasificar datos sensibles o personales, y aplicar medidas para cifrarlos tanto en tránsito como en almacenamiento.³ En otras palabras, desplegar capacidades de prevención de pérdida de datos.
- Aumentar la inversión en las herramientas de detección y alerta, y en la capacidad para contener y responder a una filtración de datos.
- Desarrollar y mantener políticas robustas que hagan obligatorias contraseñas seguras (gestión de contraseñas) y usar la autenticación multifactor.
- Considerar el uso de modelos que usan el método del «privilegio más bajo» para proporcionar seguridad para recursos dentro y fuera de las oficinas (p. ej. modelos de confianza cero).
- Invertir y crear políticas y planes para participar con los equipos de gobernanza, gestión de riesgos y conformidad.²⁶





«Durante la próxima década los riesgos de seguridad serán más difíciles de evaluar e interpretar dada la creciente complejidad del panorama de amenazas, el ecosistema del adversario y la expansión de la superficie de ataque».

en PAE 2020

Bibliografía

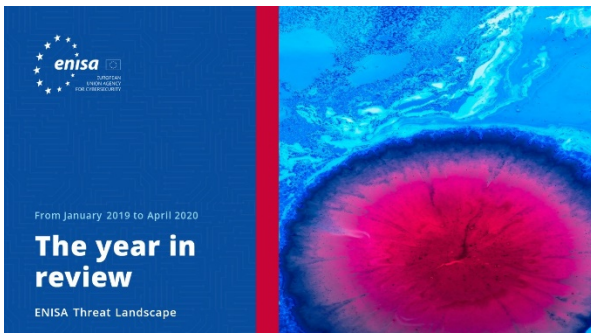
1. "What is data breach?" Norton. <https://us.norton.com/internetsecurity-privacy-data-breaches-what-you-need-to-know.html>
2. "What is data breach?" Malwarebytes. <https://www.malwarebytes.com/data-breach/>
3. "Cost of Data Breach Report." 2019. IBM Security, Ponemon Institute. <https://www.ibm.com/security/data-breach>
4. Dhritimaan Shukla, Kush Wadhwa. "Data breach – threat landscape. Unauthorised exposure of an organisation's critical data." PWC India. <https://www.pwc.in/consulting/forensic-services/data-breach-threat-landscape.html>
5. "Verizon Data Breach Investigations Report." 2020. Verizon. <https://enterprise.verizon.com/resources/reports/dbir/>
6. Catherine De Bolle. "Internet Organised Crime Threat Assessment (IOCTA)." 2019. European Cyber Crime Centre (EC3), Europol. <https://www.europol.europa.eu/iocta-report>
7. "2020 Healthcare Cybersecurity Horizon Report." 2020. Fortified Health Security. <https://fortifiedhealthsecurity.com/wp-content/uploads/2019/12/Fortified-Health-Security-2020-Horizon-Report.pdf>
8. Inga Goddijn. "2019 Midyear QuickView Data Breach Report – Cyber Risk Analytics." Agosto de 2019. <https://pages.riskbasedsecurity.com/hubfs/Reports/2019/2019%20MidYear%20Data%20Breach%20QuickView%20Report.pdf>
9. Troy Hunt. "The 773 Million Record "Collection #1" Data Breach." 17 de enero de 2019. TroyHunt. <https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/>
10. Chris Williams. "620 million accounts stolen from 16 hacked websites now for sale on dark web, seller boasts." 11 de febrero de 2019. The Register. https://www.theregister.com/2019/02/11/620_million_hacked_accounts_dark_web/
11. Catalin Cimpanu. "Indian govt agency left details of millions of pregnant women exposed online." 1 de abril de 2019. ZDNet. <https://www.zdnet.com/article/indian-govt-agency-left-details-of-millions-of-pregnant-women-exposed-online/>
12. "Losing Face: Two More Cases of Third-Party Facebook App Data Exposure." 3 de abril de 2019. UpGuard. <https://www.upguard.com/breaches/facebook-user-data-leak>
13. "First American Financial Corp. Leaked Hundreds of Millions of Title Insurance Records." 24 de mayo de 2019. KrebsonSecurity. <https://krebsonsecurity.com/2019/05/first-american-financial-corp-leaked-hundreds-of-millions-of-title-insurance-records/>
14. "Data Incident, Evite." 14 de mayo de 2019. Evite. <https://www.evite.com/security/update>
15. "Information on the Capital One Cyber Incident." 23 de septiembre de 2019. CapitalOne. <https://www.capitalone.com/facts2019/>
16. Josh Taylor. "Major breach found in biometrics system used by banks, UK police and defence firms." 14 de agosto de 2019. The Guardian. <https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms>
17. Neil Hodge. "Mastercard reveals data breaches in third-party loyalty program." 27 de agosto de 2019. Compliance Week. <https://www.complianceweek.com/data-privacy/mastercard-reveals-data-breaches-in-third-party-loyalty-program/27614.article>
18. Catalin Cimpanu. "Adobe left 7.5 million Creative Cloud user records exposed online." 26 de octubre de 2019. ZDNet. <https://www.zdnet.com/article/adobe-left-7-5-million-creative-cloud-user-records-exposed-online/>





19. Charlie Osborne. "UniCredit reveals data breach exposing 3 million customer records." 28 de octubre de 2019. ZDNet. <https://www.zdnet.com/article/unicredit-reveals-data-breach-exposing-3-million-customer-records/>
20. Chris Isidore. "Smart camera maker Wyze hit with customer data breach." 30 de diciembre de 2019. CNN. <https://edition.cnn.com/2019/12/30/tech/wyze-data-breach/index.html>
21. Davey Winder. "Microsoft Security Shocker As 250 Million Customer Records Exposed Online." 22 de enero de 2020. Forbes. <https://www.forbes.com/sites/daveywinder/2020/01/22/microsoft-security-shocker-as-250-million-customer-records-exposed-online/#2d3f9dca4d1b>
22. Paul Bischoff. "US property and demographic database of 200 million records leaked on the web." 5 de marzo de 2020. comparitech. <https://www.comparitech.com/blog/vpn-privacy/200-million-us-database-leaked/>
23. Jim Wilson. «Brasil: Millions of Records Leaked, Including Biometric Data." 11 de marzo de 2020. Safety Detectives. <https://www.safetydetectives.com/blog/antheus-leak-report/>
24. Zack Whittaker. "Marriot says 5.2 million guest records were stolen in another data breach." 1 de abril de 2020. Techcrunch. <https://techcrunch.com/2020/03/31/marriott-hotels-breached-again/?renderMode=ie11>
25. "2019 Thales Data Threat Report – Global Edition" Thales Security, 2019. <https://cpl.thalesgroup.com/data-threat-report>
26. "2020 Thales Data Threat Report – Global Edition" Thales Security, 2020. <https://cpl.thalesgroup.com/data-threat-report>
27. Laura Paine. "2019 Verizon DBIR Shows Web Applications and Human Error as Top Sources of Breach." 8 de mayo de 2019. Veracode. <https://www.veracode.com/blog/security-news/2019-verizon-dbir-shows-web-applications-and-human-error-top-sources-breach>

Lecturas relacionadas



LEER EL INFORME



Informe Panorama de Amenazas de la ENISA **Revisión anual**

Un resumen de las tendencias en materia de ciberseguridad durante el período de enero de 2019 a abril de 2020.



LEER EL INFORME



Informe Panorama de Amenazas de la ENISA **Lista de las 15 amenazas principales**

Lista de la ENISA con las 15 amenazas principales durante el período de enero de 2019 a abril de 2020.



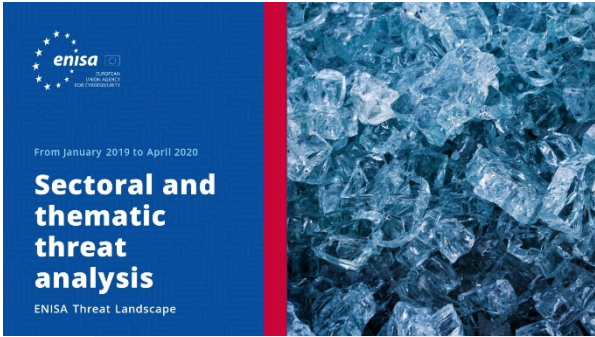
LEER EL INFORME



Informe Panorama de Amenazas de la ENISA **Temas de investigación**

Recomendaciones sobre temas de investigación de varios cuadrantes de la ciberseguridad y de la inteligencia sobre las ciberamenazas.





Informe Panorama de Amenazas de la ENISA **Análisis de las amenazas por sectores y temas**

Análisis contextualizado de las amenazas durante el período de enero de 2019 a abril de 2020.

[LEER EL INFORME](#)



Informe Panorama de Amenazas de la ENISA **Tendencias emergentes**

Principales tendencias en ciberseguridad observadas entre enero de 2019 y abril de 2020.

[LEER EL INFORME](#)



Informe Panorama de Amenazas de la ENISA **Sinopsis de la inteligencia sobre las ciberamenazas**

Situación actual en materia de inteligencia sobre las ciberamenazas en la UE.

[LEER EL INFORME](#)

¿Quiénes somos?

— La agencia

La Agencia de la Unión Europea para la Ciberseguridad (ENISA) es la agencia de la Unión cuyo objetivo es alcanzar un elevado nivel común de ciberseguridad en toda Europa. La agencia se estableció en 2004, se ha visto reforzada por el Reglamento sobre la Ciberseguridad y contribuye a la política cibernética de la UE, mejora la fiabilidad de los productos, servicios y procesos de TIC con programas de certificación de la ciberseguridad, coopera con los Estados miembros y los organismos de la UE y ayuda a Europa a prepararse para los desafíos cibernéticos del futuro. A través del intercambio de conocimientos, la capacitación y la sensibilización, la Agencia coopera con sus partes interesadas clave para fortalecer la confianza en la economía conectada, para impulsar la resiliencia de la infraestructura de la Unión y, por último, para proteger digitalmente a la sociedad y a la ciudadanía de Europa. Puede encontrarse más información sobre la ENISA y su labor en www.enisa.europa.eu.

Colaboradores

Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) y *todos los miembros del grupo de partes interesadas de la CTI (inteligencia sobre las ciberamenazas) de la ENISA*: Andreas Sfakianakis, Christian Doerr, Jart Armin, Marco Riccardi, Mees Wim, Neil Thaker, Pasquale Stirparo, Paul Samwel, Pierluigi Paganini, Shin Adachi, Stavros Lingris (CERT EU) y Thomas Hemker.

Editores

Marco Barros Lourenço (ENISA) y Louis Marinos (ENISA).

Datos de contacto

Las consultas acerca de este informe deben realizarse a través de enisa.threat.information@enisa.europa.eu.

Las consultas de los medios de comunicación acerca de este informe deben realizarse a través de press@enisa.europa.eu.



Nos gustaría conocer su opinión sobre este informe

Le pedimos que dedique unos minutos a rellenar el cuestionario. Para acceder al cuestionario haga clic [aquí](#).



Aviso legal

Salvo que se indique lo contrario, la presente publicación refleja las opiniones e interpretaciones de la ENISA. Esta publicación no constituye en ningún caso una medida legal de la ENISA ni de los organismos que la conforman, a menos que se adopte en virtud del Reglamento (UE) 526/2013. La información tampoco refleja necesariamente el estado actual de la técnica y la ENISA se reserva el derecho a actualizarla en todo momento.

Las correspondientes fuentes de terceros se citan cuando proceda. La ENISA declina toda responsabilidad por el contenido de las fuentes externas, incluidos los sitios *web* externos a los que se hace referencia en esta publicación.

Esta publicación tiene un carácter meramente informativo. Además, debe poder accederse a la misma de forma gratuita. Ni la ENISA ni ninguna persona que actúe en su nombre aceptan responsabilidad alguna en relación con el uso que pueda hacerse de la información incluida en la presente publicación.

Aviso de copyright

© Agencia de la Unión Europea para la Ciberseguridad (ENISA), 2020
Reproducción autorizada siempre que se indique la fuente.

Copyright de la imagen de la portada: © Wedia. Para utilizar o reproducir fotografías o cualquier otro material de cuyos derechos de autor no sea titular la ENISA, debe obtenerse el permiso directamente de los titulares de los derechos de autor.

ISBN: 978-92-9204-354-4

DOI: 10.2824/552242



Vasilissis Sofias Str 1, Maroussi 151 24, Attiki, Grecia
Tel.: +30 28 14 40 9711
info@enisa.europa.eu
www.enisa.europa.eu



Reservados todos los derechos. Copyright

ENISA 2020.

<https://www.enisa.europa.eu>

