ES

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

De enero de 2019 a abril de 2020

Análisis de las amenazas por sectores y temas

Panorama de Amenazas de la ENISA

Sinopsis

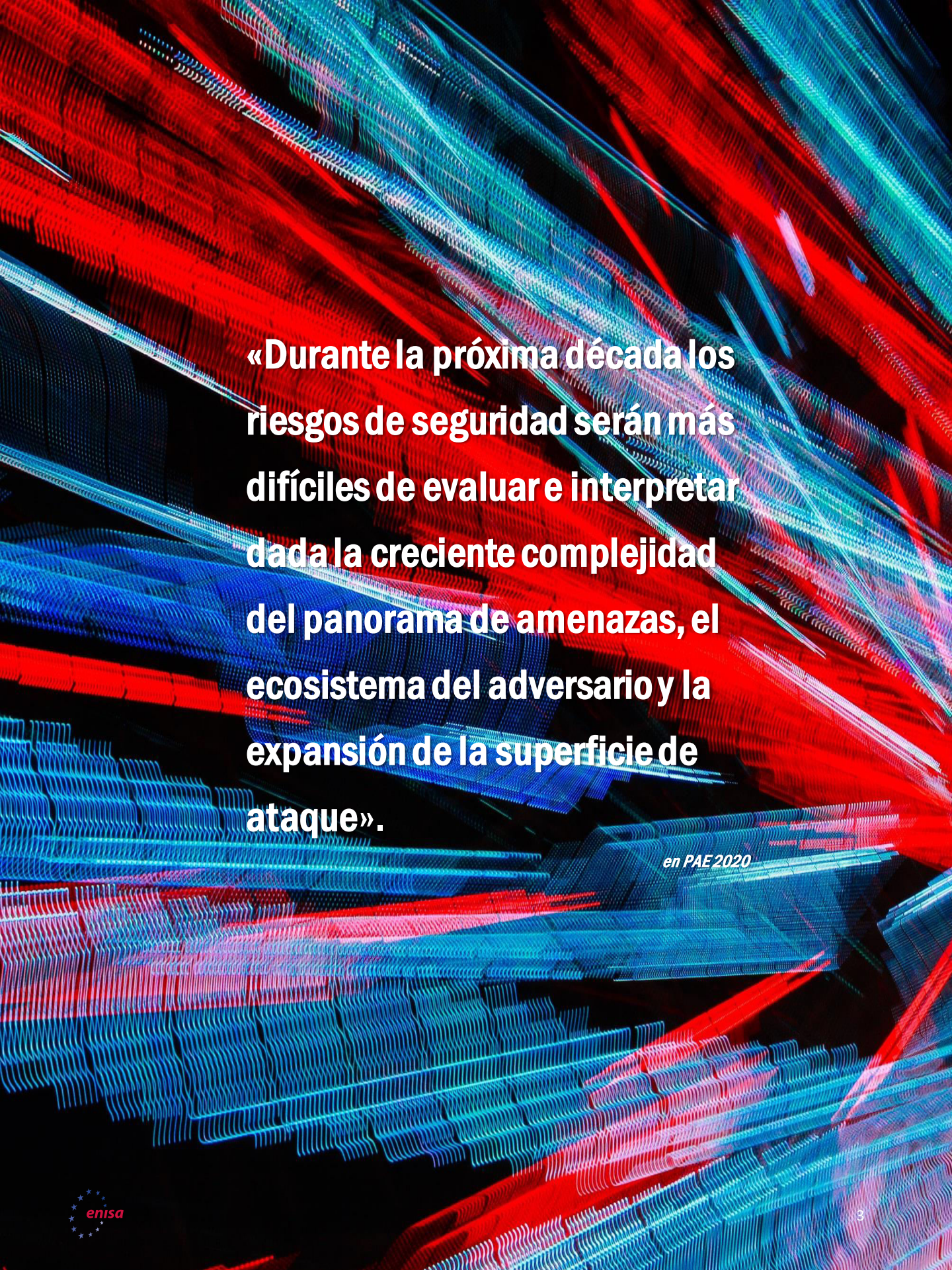
Este análisis, además de indicar las motivaciones de los adversarios, proporciona pruebas sobre las técnicas de ataque más habituales y la exposición a las amenazas aplicadas a un sector determinado, con el fin de indicar los requisitos de protección y las prioridades. En lo que respecta a los temas, el análisis de las amenazas y los retos asociados a tecnologías emergentes específicas contribuye al proceso de evaluar, valorar y mitigar los riesgos futuros.

La inteligencia contextualizada de las ciberamenazas (CTI) por sectores es una herramienta importante para sacar conclusiones sobre la previsión de ciberataques en un sector determinado.

_Estadísticas de incidentes de un sector frente a la valoración de la exposición de sectores emergentes

La contextualización de la CTI sectorial se basa principalmente en los incidentes de ciberseguridad ocurridos en un sector. Aunque es un método estándar para los componentes de las TI y de los servicios digitales existentes y establecidos, no cubre las tecnologías emergentes. Esto se debe principalmente a que no existe información de incidentes en tecnologías que aún están en fase piloto o experimental. Para las tecnologías emergentes, la CTI se contextualiza a través de la evaluación de las amenazas de las categorías de activos relacionadas con un sector determinado. La ENISA se encarga de realizar estas evaluaciones para sectores emergentes, como el de la 5G, IoT[5] y los vehículos inteligentes[6]. La ENISA utiliza los panoramas de amenazas sectoriales y temáticos y las evaluaciones de la protección básica para contextualizar la CTI.

En este informe, aparte de la CTI sectorial que depende de datos estadísticos basados en incidentes, presentamos un resumen de la CTI evaluada para el caso de los sectores tecnológicos emergentes basándose en el trabajo de la ENISA.


«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

Sinopsis

La necesidad urgente de datos estadísticos actualizados de los incidentes por sectores

Los datos estadísticos de los incidentes por sectores son una herramienta esencial para entender la dinámica de la evolución de las amenazas, los motivos de los adversarios, la exposición de los activos y las acciones basadas en objetivos. Dada la complejidad de los ataques, las dependencias entre los activos atacados y la naturaleza multisectorial de las vulnerabilidades explotadas, los datos estadísticos sobre los incidentes presentan algo de incertidumbre inherente debida a lo siguiente.

- En las estadísticas de varios sectores vemos un número de **incidentes clasificados como «desconocido»**[12]. Este porcentaje varía del 1,5 % al 5 %. Si estos incidentes se pudieran asociar con alguno de los sectores conocidos, este porcentaje podría influir el orden de los objetivos. Es más, la cantidad significativa de técnicas de ataque desconocidas (aproximadamente un 15 %), añade más incertidumbre a la evaluación de los motivos de quienes llevan a cabo las amenazas.
- La mayoría de los **ataques requieren más de un paso** (la media es tres) para llegar a los objetivos o meta final. En muchos casos, en un mismo ataque están involucrados varios objetivos de varios sectores. Por lo tanto, un incidente que se registra en un sector puede ser el resultado de varios incidentes en otros sectores, que son los pasos intermedios del ataque. Estas dependencias entre los incidentes podrían afectar a la precisión de las estadísticas de incidentes.
- Aparte del número de incidentes por sector, un elemento importante para el análisis estadístico es la **naturaleza de las técnicas de ataque utilizadas**. Esta información podría proporcionar datos útiles sobre los vectores de ataque más usados y podría ayudar a priorizar las medidas de protección necesarias para un sector determinado.

- La materialización de las amenazas depende fuertemente de las **oportunidades existentes exploradas por los adversarios**. Debido a la pandemia de COVID-19, por ejemplo, los entornos informáticos se han descentralizado. Este hecho debilita los controles de seguridad corporativos que se aplican en la red de la empresa, lo que explica el cambio de los ataques de objetivos corporativos a objetivos particulares.[1] Este ejemplo apunta a la necesidad de «traducir» los cambios observados a estadísticas a la luz de las oportunidades emergentes.
- Las estadísticas actuales se desarrollan teniendo en cuenta varios criterios. **Las variaciones en los criterios** de las estadísticas impiden comparar los datos estadísticos de los incidentes. Por ejemplo:
    - Dependiendo de la base de datos de los recolectores de información de los contribuyentes o de las partes interesadas, los datos estadísticos pueden no cubrir todos los sectores de forma uniforme.
    - La clasificación de los incidentes podría basarse en la frecuencia de ocurrencia, independientemente de la magnitud del daño (p. ej., cantidad de datos filtrados) o su impacto.
- Un elemento esencial de las estadísticas por sectores es la **frecuencia de ocurrencia** de ataques informáticos individuales. Esto da una idea del método de ataque más habitual en un sector. Estas estadísticas podrían servir de guía para el nivel de preparación necesario o madurez de los controles de seguridad individuales que reducen la exposición a las ciberamenazas relevantes.
- En vista de todo lo mencionado sobre las estadísticas de incidentes, en este informe se proporciona una clasificación aproximada de los sectores en términos de incidentes observados, junto con una tendencia obtenida de las dinámicas emergentes de la exposición potencial de cada sector. También se incluye información sobre los vectores de ataque más populares por sector. Para ello se ha consolidado información de varias publicaciones.[1,2,3,4]

Tendencias de los incidentes

SECTOR	ATAQUES/AMENAZAS MÁS POPULARES	TENDENCIAS DE INCIDENTES
Particular	• Phishing • *Malware* • Filtración de información • Robo de datos	Estable
Varias industrias	• Ataques que afectan a aplicaciones *web* • *Phishing* • *Malware*	En aumento
Administraciones públicas, defensa, servicios sociales	• *Malware* • *Phishing* • Ataques basados en la *web*	Estable, en ligero descenso
Financiero/bancario/seguros	• Ataques que afectan a aplicaciones *web* • Amenazas internas (abuso no intencionado) • *Malware* • Robo de datos	Estable
Salud/médico	• *Malware* • Amenazas internas (abuso no intencionado/errores) • Ataques que afectan a aplicaciones *web*	En aumento
Educación	• *Malware* • *Ransomware* • Ataques basados en la *web*	Estable, en ligero descenso
Información y comunicación	• Ataques que afectan a aplicaciones *web* • Amenazas internas (abuso no intencionado/errores) • *Malware*	Estable
Profesionales/ servicios digitales	• Ataques que afectan a aplicaciones *web* • Amenazas internas (abuso no intencionado/errores) • *Malware*	Estable
Artes, ocio y juegos[8]	• Ataques que afectan a aplicaciones *web* • *Malware* • Phishing	Estable
Fabricación	• *Malware* • Ataques que afectan a aplicaciones *web* • Amenazas internas (abuso no intencionado/errores)	Estable

SECTOR	FACTORES INFLUYENTES
Particular	El aislamiento debido a las medidas de confinamiento por la COVID-19 ha provocado una dispersión o descentralización de los entornos informáticos y el aislamiento de los usuarios, que son más fáciles de engañar y tienen menos controles de seguridad, que en el caso de los entornos centralizados.
Varias industrias	Los usuarios remotos por las medidas de confinamiento por la COVID-19 han facilitado los ataques por *phishing* y la filtración de información sensible (como las credenciales).
Administraciones públicas, defensa, servicios sociales	El uso de los servicios en la nube podría haber influido en la seguridad de la oferta pública. Aun así, los servicios sociales han sufrido una cantidad importante de ataques debidos a las ayudas económicas ofrecidas a la ciudadanía durante la pandemia de COVID-19.
Financiero Bancario/seguros	La complejidad del sector financiero dificulta la interpretación del panorama de amenazas, ya que distintos dominios dentro de los servicios financieros y bancarios podrían tener riesgos y ciberamenazas completamente distintas.
Salud/médico	La atención que los ciberdelincuentes han prestado a los objetivos sanitarios ha aumentado considerablemente por motivos económicos y por la importancia del sector durante la pandemia de COVID-19.
Educación	Aunque se mantiene estable, este sector fue el objetivo de campañas de ciberespionaje en 2020 debidas al interés en los resultados de las investigaciones relacionadas con la COVID-19.
Información y comunicación	Este sector se encuentra sometido a una fuerte presión constante debido a las dificultades para proteger una superficie de ataque enorme, introducida por las plataformas de los medios digitales. Para las organizaciones de medios en línea, las mayores amenazas son las de los ataques que causan daños a la reputación.
Profesional/ servicios digitales	Aunque este sector está estable, durante 2020 ha sido objetivo de varias campañas que intentaban obtener información de usuarios de los servicios digitales que teletrabajaban desde casa durante la pandemia de COVID-19.
Artes, ocio y juegos	El cambio de los modelos de negocio de licencia a suscripciones adoptado por la industria del juego ha hecho que este sector cobre interés para los ciberdelincuentes.[8]
Fabricación	Los ataques a las cadenas de suministro y a los sistemas de control industriales son la amenaza principal para las empresas del sector manufacturero, ya que pueden llegar a cerrar por completo las líneas de producción. El robo de datos de propiedad intelectual es otra de las amenazas graves para este sector.

Amenazas para las tecnologías emergentes

La próxima generación de comunicaciones móviles o 5G

COMPONENTES RELACIONADOS: GRUPOS DE ACTIVOS	EXPOSICIÓN A LAS AMENAZAS
Red principal	Abuso debido al acceso remoto, subidas en el tráfico de autenticación, abuso de datos de autenticación de usuario/autorización, abuso de funciones de red albergadas por terceros, abuso de funciones de interceptación legales, explotación de las interfaces de programación de aplicaciones (API), explotación de arquitecturas mal diseñadas o mal planificadas, explotación de sistemas/redes mal configurados, uso erróneo o administración errónea de las redes, sistemas y dispositivos, escenarios de estafa relacionados con interconexiones itinerantes, movimientos laterales, ataques a la memoria, manipulación del tráfico de la red, reconocimiento de la red y recolección de información, manipulación de los datos de configuración de la red, inundación malintencionada de los componentes de la red principales, desvío malintencionado del tráfico, manipulación del programador de recursos de la red, uso indebido de herramientas de auditoría, usos oportunistas y fraudulentos de los recursos compartidos, registro de funciones de red malintencionadas, vigilancia del tráfico, ataques de canal lateral.
Red de acceso	Abuso en todo el espectro de recursos, intoxicación del protocolo de resolución de direcciones (ARP), nodos de acceso a la red falsos, ataques por inundación, ataques de captura de identidades de suscriptores móviles internacionales (*IMSI-catcher*), interferencias en la frecuencia de radio, robo de identidades mediante suplantación de direcciones MAC (*MAC spoofing*), manipulación del acceso a los datos de configuración de la red, interferencias de radio, manipulación del tráfico de radio, secuestros de sesiones, fraude en la señalización, tormentas de señales.

COMPONENTES RELACIONADOS: GRUPOS DE ACTIVOS	EXPOSICIÓN A LAS AMENAZAS
Procesamiento de datos en los extremos de las redes (*multi-edge computing*)	Pasarelas MEC falsas o malintencionadas, sobrecarga de los nodos extremos, abuso de interfaces de programación de aplicaciones (API) abiertas en los extremos de las redes.
Virtualización de las funciones de red y de las redes definidas por *software*	Abuso del protocolo de interconexión de centros de datos (Date Centres Interconnect, DCI), abuso de los recursos de computación en la nube, sortear la virtualización de la red, abuso de la virtualización del anfitrión.
Infraestructura física	Manipulación de los equipos informáticos, desastres naturales que afectan a la infraestructura de la red, sabotaje o vandalismo físico de la infraestructura de la red, amenazas del personal de terceros al acceder a la infraestructura de los operadores de redes de móvil (MNO), explotación del formato de tarjeta de circuitos integrados universal (Universal Integrated Circuit Card, UICC), equipos de usuario comprometidos.
Todos los grupos de activos 5G anteriores	Denegación de servicio (DoS), filtraciones de datos, fugas, destrucción, robo y manipulación de los datos, escuchas, explotación de las vulnerabilidades de los programas y los equipos informáticos, programas informáticos con código malintencionado, compromiso de la cadena de suministros, proveedores de servicios y fabricantes, ataques y amenazas dirigidas, explotación de los puntos débiles de seguridad, procedimientos de gestión y operación, abuso de la autenticación, robo de identidades o *spoofing*.

Amenazas para las tecnologías emergentes

Internet de las cosas (IdC)

COMPONENTES RELACIONADOS: GRUPOS DE ACTIVOS	EXPOSICIÓN A LAS AMENAZAS
Factor humano	Amenazas internas, problemas del trabajo en equipo, limitaciones internas, «hacktivismo», pérdida de servicios de respaldo, corte de servicios, cortes de red, modificaciones no intencionadas, sabotaje, violación de reglas y normativas, infracción de la legislación, requisitos de contratos, incumplimiento de requisitos contractuales (p. ej., mantenimiento de programas informáticos), explotación de programas informáticos, ingeniería social, robo de identidades.
Diseño de los programas informáticos	Amenazas internas, «hacktivismo», modificaciones no intencionadas, uso erróneo o administración incorrecta de dispositivos y sistemas, sabotaje, fallos en los procesos SDLC, fallos de terceros, incumplimiento de requisitos contractuales (p. ej., mantenimiento de programas informáticos), explotación de programas informáticos, pérdidas o filtración de información.
Desarrollo de los programas informáticos	Amenazas internas, «hacktivismo», pérdida de servicios de respaldo, modificaciones no intencionadas, uso erróneo o administración incorrecta de dispositivos y sistemas, sabotaje, vandalismo y robo, vulnerabilidades de los programas informáticos, fallos en los procesos SDLC, fallos de mantenimiento, abuso de autorización, explotación de programas informáticos, manipulación de la infraestructura SDLC, pérdidas o filtraciones de información.
Despliegue de programas informáticos	Amenazas internas, «hacktivismo», pérdida de servicios de respaldo, modificaciones no intencionadas, uso erróneo o administración incorrecta de dispositivos y sistemas, sabotaje, vandalismo y robo, vulnerabilidades de los programas informáticos, fallos en los procesos SDLC, fallos de terceros, abuso de autorización, explotación de programas informáticos, manipulación de la infraestructura SDLC, denegación de servicio, manipulación de datos, pérdidas o filtración de información.

COMPONENTES RELACIONADOS: GRUPOS DE ACTIVOS	EXPOSICIÓN A LAS AMENAZAS
Datos	Amenazas internas, «hacktivismo», pérdida de servicios de respaldo, modificaciones no intencionadas, uso erróneo o administración incorrecta de dispositivos y sistemas, sabotaje, vandalismo y robo, vulnerabilidades de los programas informáticos, fallos en los procesos SDLC, fallos de terceros, abuso de autorización, explotación de programas informáticos, manipulación de la infraestructura SDLC, denegación de servicio, manipulación de datos, pérdidas o filtración de información.
Mantenimiento	Amenazas internas, «hacktivismo», cortes de servicios, modificaciones no intencionadas, uso erróneo o administración incorrecta de dispositivos y sistemas, daños causados por terceros, sabotaje, vandalismo y robo, ataques con acceso físico, acceso forzado, requisitos de los contratos, vulnerabilidades de los programas informáticos, fallos en los procesos SDLC, fallos de terceros, incumplimiento de requisitos contractuales (p. ej., mantenimiento de programas informáticos), fallos de mantenimiento, abuso de autorización, explotación de programas informáticos, manipulación de la infraestructura SDLC, denegación de servicio, manipulación de datos, revelación, pérdidas o filtración de información.
Componentes de programas informáticos	Amenazas internas, «hacktivismo», cortes de servicios, pérdida de servicios de respaldo, modificaciones no intencionadas, uso erróneo o administración incorrecta de dispositivos y sistemas, daños causados por terceros, sabotaje, filtración de datos, vandalismo y robo, ataques con acceso físico, acceso forzado, requisitos de los contratos, vulnerabilidades de los programas informáticos, fallos en los procesos SDLC, fallos de terceros, incumplimiento de requisitos contractuales (p. ej., mantenimiento de programas informáticos), fallos de mantenimiento, abuso de autorización, explotación de programas informáticos, manipulación de la infraestructura SDLC, denegación de servicio, manipulación de datos, revelación, pérdidas o filtración de información.

Amenazas para las tecnologías emergentes

Vehículos inteligentes

COMPONENTES RELACIONADOS: GRUPOS DE ACTIVOS	EXPOSICIÓN A LAS AMENAZAS
Sensores y actuadores de vehículos	Denegación de servicio, *malware*, manipulación de datos, ataques dirigidos a OEM, actividades no autorizadas, robo de identidades, abuso de las autorizaciones, manipulación de datos, amenazas dirigidas a los sensores autónomos, amenazas contra la IA y el aprendizaje automático, sabotaje, vandalismo, robo, ataques de canal lateral, inyección de defectos, robo, fallos o mal funcionamiento de un sensor/actuador, explotación de las vulnerabilidades de los programas informáticos, secuestro del protocolo de información, ataque intermediario (*man-in-the-middle*) / secuestro de sesión, cambio de datos o de la configuración de los componentes del vehículo no intencionado, uso de la información y/o dispositivos de una fuente no fiable, uso erróneo de la configuración de los componentes del vehículo, cortes en la red, incumplimiento de los requisitos contractuales, violación de reglas y normativas, infracción de la legislación, abuso de datos personales.
Algoritmos de toma de decisiones **Unidades de control electrónico del vehículo, componentes para el procesamiento y toma de decisiones** **Infraestructura y sistemas internos de vehículos inteligentes**	Denegación de servicio, *malware*, manipulación de datos, ataques dirigidos a OEM, actividades no autorizadas, robo de identidades, abuso de las autorizaciones, manipulación de información, amenazas contra la IA y el aprendizaje automático, sabotaje, vandalismo, robo, robo, fallos o mal funcionamiento de un sensor/actuador, explotación de las vulnerabilidades de los programas informáticos, fallo o corte de servicio, secuestro del protocolo de información, reproducción de datos, ataque intermediario (*man-in-the-middle*) / secuestro de sesión, cambio de datos o de la configuración de los componentes del vehículo no intencionado, uso de la información y/o dispositivos de una fuente no fiable, uso erróneo de la configuración de los componentes del vehículo, pérdida de la señal GNSS, cortes en la red, incumplimiento de los requisitos contractuales, violación de reglas y normativas, infracción de la legislación, abuso de datos personales.

COMPONENTES RELACIONADOS: GRUPOS DE ACTIVOS	EXPOSICIÓN A LAS AMENAZAS
Funciones del vehículo **Sensores y actuadores de vehículos** **Unidades de control electrónico del vehículo, componentes para el procesamiento y toma de decisiones**	Denegación de servicio, *malware*, manipulación de datos, ataques dirigidos a OEM, actividades no autorizadas, robo de identidades, abuso de las autorizaciones, manipulación de información, amenazas contra los sensores autónomos, amenazas contra la IA y el aprendizaje automático, sabotaje, ataques de canal lateral, inyección de defectos, robo, fallos o mal funcionamiento de un sensor/actuador, explotación de las vulnerabilidades de los programas informáticos, fallo o corte de servicio, secuestro del protocolo de información, reproducción de datos, ataque intermediario (*man-in-the-middle*) / secuestro de sesión, cambio de datos o de la configuración de los componentes del vehículo no intencionado, uso de la información y/o dispositivos de una fuente no fiable, uso erróneo de la configuración de los componentes del vehículo, batería del vehículo descargada, cortes en la red, incumplimiento de los requisitos contractuales, violación de reglas y normativas, infracción de la legislación, abuso de datos personales.
Gestión de los programas informáticos **Unidades de control electrónico del vehículo, componentes para el procesamiento y toma de decisiones** **Componentes de la comunicación del vehículo**	Denegación de servicio, *malware*, manipulación de datos, ataques dirigidos a OEM, actividades no autorizadas, robo de identidades, abuso de las autorizaciones, sabotaje, ataques de canal lateral, inyección de defectos, robo, fallos o mal funcionamiento de un sensor/actuador, explotación de las vulnerabilidades de los programas informáticos, fallo o corte de servicio, secuestro del protocolo de información, ataque intermediario (*man-in-the-middle*) / secuestro de sesión, cambio de datos o de la configuración de los componentes del vehículo no intencionado, uso de la información y/o dispositivos de una fuente no fiable, cortes en la red, incumplimiento de los requisitos contractuales, violación de reglas y normativas, infracción de la legislación, abuso de datos personales.
Componentes de la comunicación dentro del vehículo	Denegación de servicio, *malware*, manipulación de datos, ataques dirigidos a OEM, actividades no autorizadas, robo de identidades, abuso de las autorizaciones, manipulación de información, sabotaje, ataques de canal lateral, inyección de defectos, robo, fallos o mal funcionamiento de un sensor/actuador, explotación de las vulnerabilidades de los programas informáticos, secuestro del protocolo de información, reproducción de datos, ataque intermediario (*man-in-the-middle*) / secuestro de sesión, cambio de datos o de la configuración de los componentes del vehículo no intencionado, uso de la información y/o dispositivos de una fuente no fiable, uso erróneo de la configuración de los componentes del vehículo, cortes en la red, incumplimiento de los requisitos contractuales, violación de reglas y normativas, infracción de la legislación, abuso de datos personales.

Amenazas para las tecnologías emergentes

_ Vehículos inteligentes

COMPONENTES RELACIONADOS: GRUPOS DE ACTIVOS	EXPOSICIÓN A LAS AMENAZAS
Redes y protocolos de comunicación. **Unidades de control electrónico del vehículo, componentes para el procesamiento y toma de decisiones** **Componentes de la comunicación del vehículo**	Denegación de servicio, *malware*, manipulación de datos, ataques dirigidos a OEM, actividades no autorizadas, robo de identidades, abuso de las autorizaciones, sabotaje, robo, fallos o mal funcionamiento de un sensor/actuador, explotación de las vulnerabilidades de los programas informáticos, secuestro del protocolo de información, reproducción de datos, ataque intermediario (*man-in-the-middle*) / secuestro de sesión, cambio de datos o de la configuración de los componentes del vehículo no intencionado, uso de la información y/o dispositivos de una fuente no fiable, uso erróneo de la configuración de los componentes del vehículo, cortes en la red, incumplimiento de los requisitos contractuales, violación de reglas y normativas, infracción de la legislación, abuso de datos personales.
Componentes externos cercanos **Infraestructura y sistemas internos de vehículos inteligentes**	Denegación de servicio, *malware*, manipulación de datos, ataques dirigidos a OEM, actividades no autorizadas, robo de identidades, abuso de las autorizaciones, manipulación de información, sabotaje, vandalismo, robo, explotación de las vulnerabilidades de los programas informáticos, fallo o corte de servicio, secuestro del protocolo de información, ataque intermediario (*man-in-the-middle*) / secuestro de sesión, cambio de datos o de la configuración de los componentes del vehículo no intencionado, uso de la información y/o dispositivos de una fuente no fiable, pérdida de la señal GNSS, cortes en la red, incumplimiento de los requisitos contractuales, violación de reglas y normativas, infracción de la legislación, abuso de datos personales.

COMPONENTES RELACIONADOS: GRUPOS DE ACTIVOS	EXPOSICIÓN A LAS AMENAZAS
Servidores, sistemas y computación en nube **Infraestructura y sistemas internos de vehículos inteligentes**	Denegación de servicio, *malware*, manipulación de datos, ataques dirigidos a OEM, actividades no autorizadas, robo de identidades, abuso de las autorizaciones, manipulación de información, sabotaje, explotación de las vulnerabilidades de los programas informáticos, fallo o corte de servicio, secuestro del protocolo de información, reproducción de datos, ataque intermediario (*man-in-the-middle*) / secuestro de sesión, cambio de datos o de la configuración de los componentes del vehículo no intencionado, uso de la información y/o dispositivos de una fuente no fiable, pérdida de la señal GNSS, cortes en la red, incumplimiento de los requisitos contractuales, violación de reglas y normativas, infracción de la legislación, abuso de datos personales.
Información	Denegación de servicio, *malware*, manipulación de datos, ataques dirigidos a OEM, actividades no autorizadas, robo de identidades, abuso de las autorizaciones, manipulación de información, amenazas contra los sensores autónomos, amenazas contra la IA y el aprendizaje automático, sabotaje, vandalismo, robo, ataques de canal lateral, inyección de defectos, robo, fallos o mal funcionamiento de un sensor/actuador, explotación de las vulnerabilidades de los programas informáticos, fallo o corte de servicio, secuestro del protocolo de información, reproducción de datos, ataque intermediario (*man-in-the-middle*) / secuestro de sesión, cambio de datos o de la configuración de los componentes del vehículo no intencionado, filtración de información, uso de la información y/o dispositivos de una fuente no fiable, uso erróneo de la configuración de los componentes del vehículo, pérdida de la señal GNSS, cortes en la red, incumplimiento de los requisitos contractuales, violación de reglas y normativas, infracción de la legislación, abuso de datos personales.
Humanos	Denegación de servicio, *malware*, manipulación de datos, ataques dirigidos a OEM, actividades no autorizadas, robo de identidades, abuso de las autorizaciones, manipulación de información, sabotaje, vandalismo, robo, fallos o mal funcionamiento de un sensor/actuador, explotación de las vulnerabilidades de los programas informáticos, fallo o corte de servicio, secuestro del protocolo de información, reproducción de datos, ataque intermediario (*man-in-the-middle*) / secuestro de sesión, cambio de datos o de la configuración de los componentes del vehículo no intencionado, filtración de información, uso de la información y/o dispositivos de una fuente no fiable, uso erróneo de la configuración de los componentes del vehículo, pérdida de la señal GNSS, batería del vehículo descargada, cortes en la red, incumplimiento de los requisitos contractuales, violación de reglas y normativas, infracción de la legislación, abuso de datos personales.

Bibliografía

1. "April 2020 Cyber Attacks Statistics". 3 de junio de 2019. HACKMAGEDDON. https://www.hackmageddon.com/2020/06/03/april-2020-cyber-attacks-statistics/

2. "Data Breach Investigation Report" 2019. Verizon. https://enterprise.verizon.com/resources/reports/dbir/

3. "CIRCL - Operational Statistics" 2019. CIRCL. https://www.circl.lu/opendata/statistics/

4. "Survey: The Third Annual Study on the State of Endpoint Security Risk". 2020. https://engage.morphisec.com/2020-endpoint-security-risk-study

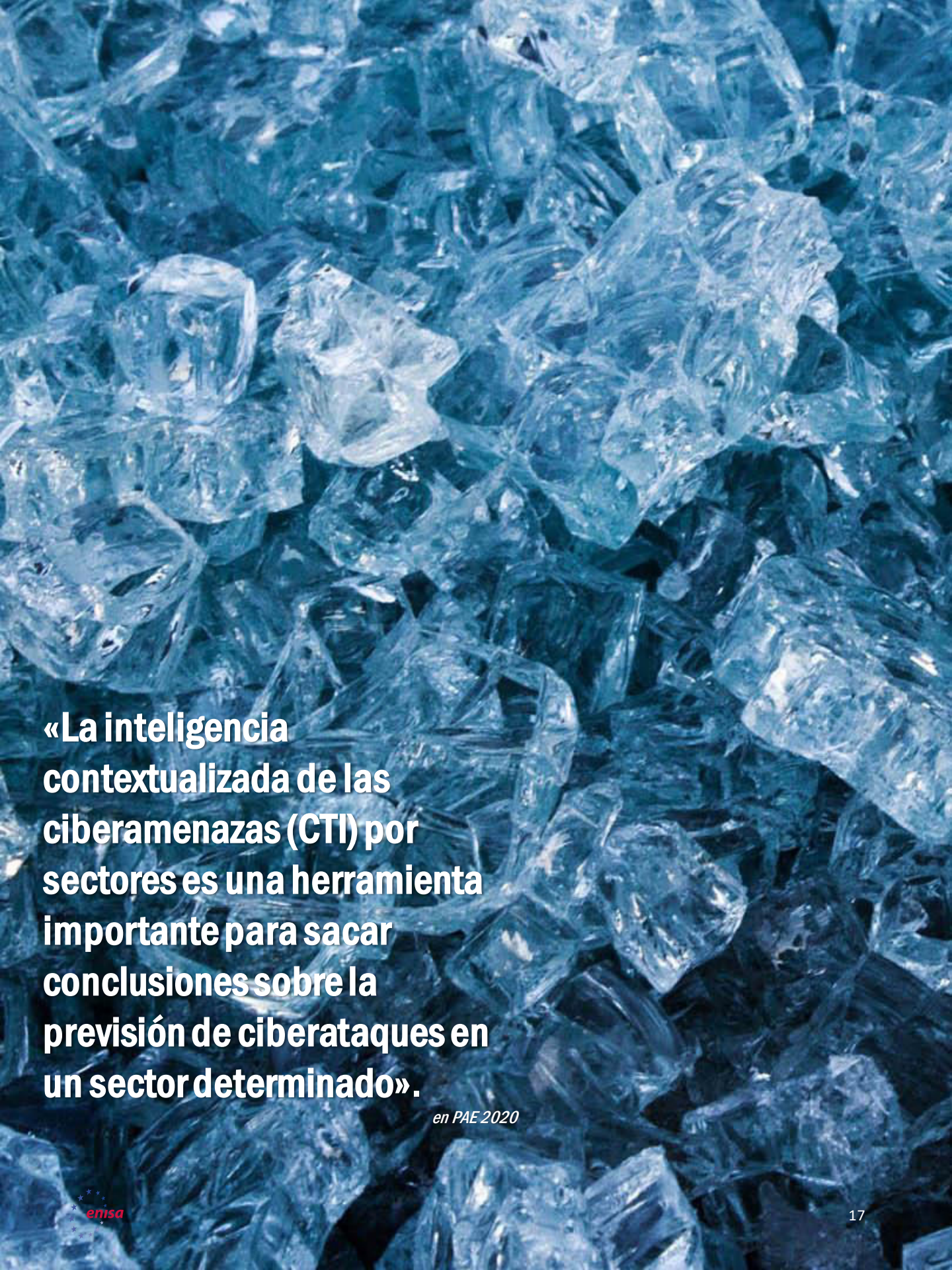
5. "Good Practices for Security of IoT - Secure Software Development Lifecycle". 19 de noviembre de 2019. ENISA. https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1

6. "ENISA good practices for security of Smart Cars". 25 de noviembre de 2019. https://www.enisa.europa.eu/publications/smart-cars

7. El orden seleccionado de los sectores se ha realizado consolidando los datos estadísticos de varios informes basados en incidentes. Proporcionan valores medios del período de este informe (2019 - al primer trimestre de 2020) y puede que se desvíe ligeramente de los valores presentados en los informes mensuales o trimestrales.

8. "Player vs. Hacker: Cyberthreats to Gaming Companies and Gamers'. 16 de marzo de 2020. Security Intelligence. https://securityintelligence.com/posts/player-vs-hacker-cyberthreats-to-gaming-companies-and-gamers/

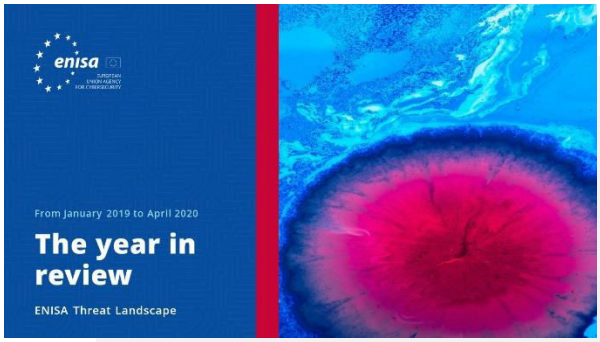
9. Cabe mencionar que la exposición a las amenazas se ha evaluado utilizando categorías de amenazas detalladas desarrolladas por la ENISA (ver https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view) y se utilizan para diversas evaluaciones sectoriales. Debido a la falta de datos de incidentes para los sectores emergentes, la evaluación de las amenazas se hace con más profundidad para obtener un enfoque más exhaustivo.



«La inteligencia contextualizada de las ciberamenazas (CTI) por sectores es una herramienta importante para sacar conclusiones sobre la previsión de ciberataques en un sector determinado».

en PAE 2020

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 **Incidentes principales en la UE y en el resto del mundo**

Incidentes de ciberseguridad principales que se han producido entre enero de 2019 y 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 contra 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) n.° 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.

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

enisa
EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

https://www.enisa.europa.eu