ES

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

De enero de 2019 a abril de 2020

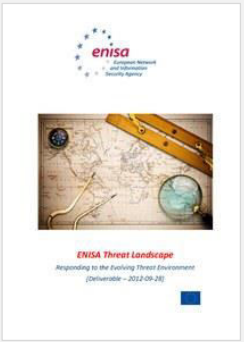
# Revisión anual

## ENISA – Panorama de Amenazas

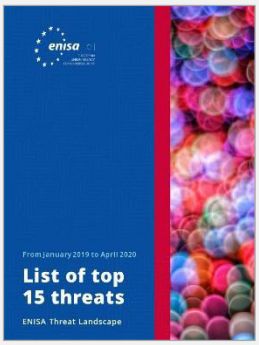
# Antes de empezar

## _ Ocho años revisando el panorama de amenazas

Este año la **Agencia de la Unión Europea para la Ciberseguridad (ENISA)** celebra el primer aniversario del Reglamento sobre la Ciberseguridad y la octava edición del informe Panorama de Amenazas de la ENISA (PAE). El Reglamento sobre la Ciberseguridad[1] moderniza y refuerza la función de la ENISA al otorgarle un mandato permanente, más recursos y nuevas tareas. Asimismo, la agencia abre un nuevo capítulo con un nuevo director ejecutivo, una nueva estrategia y una nueva estructura en la organización. Con todos estos cambios también ha llegado el momento de renovar el informe PAE y de adoptar una nueva estructura y un aspecto más moderno, dejando atrás el tipo de informe largo y estático. Con esta nueva identidad visual y nuevo formato, el informe PAE se ha convertido en un documento digital, versátil, dinámico y fácil de usar cuyo objetivo es ajustarse a las expectativas de una audiencia cada vez más numerosa y exigente.




PAE 2012




PAE 2020

Recorrido de la ENISA por el panorama de amenazas de 2012 a 2020

# _ Formato del PAE

En esta edición se hace una revisión del panorama de amenazas del período comprendido entre enero de 2019 y abril de 2020, y se ha estructurado de la forma siguiente:

**REVISIÓN ANUAL.** En este informe se ofrece una sinopsis general del panorama de amenazas y se destacan los temas más importantes a los que se hace referencia en el resto de los informes. También incluye la lista de la ENISA con las 15 amenazas principales, conclusiones y recomendaciones.

**SINOPSIS DE LA INTELIGENCIA SOBRE LAS ciberamenazas.** En este informe se resumen los temas más importantes relacionados con la comunidad dedicada a la inteligencia sobre las ciberamenazas (cyber threat intelligence, CTI) y los temas de los que se habla en varios foros.

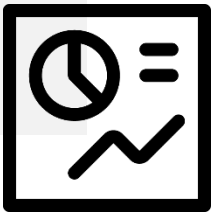
**ANÁLISIS DE LAS AMENAZAS POR SECTORES Y TEMAS.** En este informe se resume el último trabajo producido por la ENISA en el que se describe el panorama de amenazas para determinados sectores y tecnologías. Este año se presentan las conclusiones del trabajo realizado para las redes 5G, el Internet de las cosas (IdC) y los vehículos inteligentes.

**INCIDENTES PRINCIPALES EN LA UE Y EN EL RESTO DEL MUNDO.** En este informe se ofrece una sinopsis sobre los principales incidentes de ciberseguridad que están produciéndose en la UE y en el resto del mundo, y se ponen de manifiesto las lecciones que tenemos que aprender de ellos.

**TEMAS DE INVESTIGACIÓN.** En este informe se presentan los aspectos principales relacionados con la investigación e innovación en materia de ciberseguridad.

**TENDENCIAS EMERGENTES.** En este informe se identifican las tendencias emergentes y se ha centrado en los desafíos y oportunidades para el futuro en el campo de la ciberseguridad.

**LISTA DE LAS 15 AMENAZAS PRINCIPALES.** Incluye un informe por amenaza y presenta una sinopsis general, los hallazgos, los incidentes principales, los datos estadísticos, los vectores de ataque y las correspondientes medidas de mitigación.



# Antes de empezar

## Metodología

El contenido producido para el informe PAE se basa en la información disponible a partir de recursos de dominio público, principalmente de naturaleza estratégica; y cubre más de un sector, tecnología y contexto. El informe intenta ser independiente de la industria y de las empresas, y hace referencia o cita varios trabajos de investigación relacionados con la seguridad, blogs de seguridad y artículos publicados en los medios informativos, que aparecen referenciados claramente a lo largo del texto en varias notas finales.

Para la producción del informe Panorama de Amenazas de la ENISA se ha seguido un doble enfoque. Primero: se ha realizado una investigación documental detallada de las publicaciones disponibles de fuentes de dominio público, como artículos de prensa, opiniones de expertos, informes de inteligencia, análisis de incidentes e informes de trabajos de investigación sobre la seguridad. Segundo: se han llevado a cabo entrevistas con los miembros del grupo de las partes interesadas del PAE, que son expertos en este campo y miembros de la comunidad de análisis de inteligencia sobre las ciberamenazas (CTI) de la UE. Este último grupo nos ayudó a confeccionar la lista de las 15 amenazas principales y a validar las suposiciones sobre las tendencias y desafíos futuros en el campo de la ciberseguridad.

También queremos dar las gracias al grupo de las partes interesadas de la CTI por toda la ayuda proporcionada para la producción de los informes durante estas ocho ediciones. Los miembros de este grupo revisan y validan el análisis producido para cada informe PAE y tienen voto en la lista anual de las 15 ciberamenazas principales.

**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.

# Qué partes debe leer cada persona

El informe PAE es parcialmente estratégico y parcialmente técnico, y presenta información relevante para lectores técnicos y no técnicos. El PAE va dirigido a diversas audiencias y adopta distintos niveles de lenguaje técnico, según el dominio y la importancia del tema para los lectores con menos conocimientos técnicos. La tabla siguiente describe el tipo de audiencia y el contenido de cada uno de los informes PAE.

| INFORME PAE | TIPO DE CONTENIDO | AUDIENCIA A LA QUE VA DIRIGIDO |
|---|---|---|
| **REVISIÓN ANUAL** | Genérico | Todas las audiencias |
| **SINOPSIS DE LA CTI** ↗ | Específico | Miembros de la comunidad CTI y profesionales. |
| **ANÁLISIS DE LAS AMENAZAS POR SECTORES Y TEMAS** ↗ | Estratégico | Expertos en gestión estratégica, encargados de la creación de políticas y toma de decisiones, analistas de riesgos, responsables de ciberseguridad y directivos. |
| **INCIDENTES PRINCIPALES EN LA UE Y EL RESTO DEL MUNDO** ↗ | Estratégico | Expertos en gestión estratégica, encargados de la creación de políticas y toma de decisiones, analistas de riesgos, responsables de riesgos y directivos. |
| **TEMAS DE INVESTIGACIÓN** ↗ | Estratégico | Expertos en gestión estratégica, encargados de la creación de políticas y toma de decisiones, analistas de riesgos, gestores de riesgos y líderes. |
| **TENDENCIAS EMERGENTES.** ↗ | Estratégico | Expertos en gestión estratégica, encargados de la creación de políticas y toma de decisiones, analistas de riesgos, gestores de riesgos y líderes. |
| **LISTA DE LAS 15 AMENAZAS PRINCIPALES** ↗ | Técnico | Responsables de seguridad de la información, responsables principales de seguridad de los sistemas de información, especialistas en ciberseguridad y analistas de CTI. |

# Las 15 amenazas principal

| Las amenazas principales en 2018 | | Tendencias evaluadas |
|---|---|---|
| 1 | *Malware* (programas informáticos malintencionados) | --- |
| 2 | Ataques basados en la *web* | ↗ |
| 3 | Ataques que afectan a aplicaciones *web* | --- |
| 4 | *Phishing* (ataques por suplantación de identidad) | ↗ |
| 5 | Denegación de servicio | ↗ |
| 6 | Correo basura (*spam*) | --- |
| 7 | *Botnets* (redes de ordenadores infectados) | ↗ |
| 8 | Filtraciones de datos | ↗ |
| 9 | Amenazas internas | ↙ |
| 10 | Manipulación física, daños, robos y pérdidas | --- |
| 11 | Filtración de información | ↗ |
| 12 | Robo de identidad | ↗ |
| 13 | Criptosecuestro | ↗ |
| 14 | *Ransomware* (programas de secuestro) | ↙ |
| 15 | Ciberespionaje | ↙ |

| Amenazas principales en 2019-2020 | | Tendencias evaluadas | Cambio en la clasificación |
|---|---|---|---|
| 1 | *Malware* | --- | --- |
| 2 | Ataques basados en la *web* | --- | ↗ |
| 3 | *Phishing* | ↗ | ↗ |
| 4 | Ataques que afectan a aplicaciones *web* | --- | ↙ |
| 5 | Correo basura (*spam*) | ↙ | ↗ |
| 6 | Denegación de servicio | ↙ | ↙ |
| 7 | Robo de identidad | ↗ | ↗ |
| 8 | Filtraciones de datos | --- | --- |
| 9 | Amenazas internas | ↗ | --- |
| 10 | *Botnets* | ↙ | ↙ |
| 11 | Manipulación física, daños, robos y pérdidas | --- | ↙ |
| 12 | Filtración de información | ↗ | ↙ |
| 13 | *Ransomware* | ↗ | ↗ |
| 14 | Ciberespionaje | ↙ | ↗ |
| 15 | Criptosecuestro | ↙ | ↙ |

**Leyenda:** Tendencias: En descenso ↙, --- Estable, En aumento ↗ **Clasificación:** Sube ↗, --- Igual, Baja ↙

# Sinopsis

## ¿Qué cambios se han producido en el panorama?

Los años 2019 y 2020 brindaron cambios significativos en el panorama de las ciberamenazas descritas en estos informes. A estos cambios contribuyeron dos hechos significativos: las fuerzas transformadoras de carácter histórico único y que surgieron de forma abrupta por la **pandemia de la enfermedad por coronavirus del 2019 (COVID-19)**; y la tendencia en continuo aumento de las **avanzadas capacidades adversarias de los responsables de las amenazas**. Sorprendentemente, estas últimas han contribuido a amplificar el impacto de la pandemia de COVID-19 en el ciberespacio.

La pandemia de COVID-19 forzó la adopción de tecnología a gran escala para controlar una serie de aspectos críticos de la crisis, como la coordinación de los servicios sanitarios, la respuesta internacional a la propagación de la COVID-19, la adopción del teletrabajo, la educación a distancia, la comunicación interpersonal, el control de las medidas de confinamiento y las teleconferencias, entre muchas otras. Dada esta situación, los líderes empresariales han evaluado los riesgos emergentes de esta adopción (tecnológica) abrupta materializados a raíz de la transformación forzada por la pandemia de COVID-19[2]. Y la **ciberseguridad se ha enfrentado a una paradoja: haber sido tanto el desafío como la oportunidad en esta transformación**. Los cambios impuestos en el panorama de las tecnologías de la información (TI) debilitaron medidas de ciberseguridad existentes y convirtieron su rápida adaptación en un desafío. De forma simultánea, la **ciberseguridad es lo que propicia confianza en los casos de uso emergentes de los servicios digitales y, por lo tanto, tiene la oportunidad de facilitar la transformación.**

Al trabajar desde casa, los **expertos en ciberseguridad han tenido que adaptar las defensas existentes** a un nuevo paradigma de infraestructura, intentando minimizar la exposición a una serie de ataques novedosos en los que los puntos de entrada son los ordenadores personales de los empleados conectados por Internet y otros dispositivos inteligentes. También, de forma simultánea, y bajo mucha presión, han tenido que implantar soluciones basadas en componentes que previamente ofrecían menos confianza, como el acceso remoto a través de una Internet pública, los servicios en la nube, los servicios no seguros de retransmisión de vídeo y los dispositivos y aplicaciones móviles. La reacción necesaria a la pandemia de COVID-19 de garantizar la seguridad y al mismo tiempo reducir el impacto sobre las empresas, ha llevado a las organizaciones hasta los límites de su capacidad para responder a los cambios. Asimismo, muchos *modus operandi* se adaptaron rápidamente a las cambiantes pautas de trabajo, **los profesionales de la ciberseguridad terminaron trabajando al límite de sus capacidades**.

**En un corto período de tiempo los profesionales de las tecnologías de la información han tenido que responder rápidamente a los desafíos presentados por el teletrabajo, como los movimientos de datos de empresa cuando los empleados usan Internet de casa para acceder a aplicaciones en la nube, a programas informáticos corporativos, sistemas de videoconferencias e intercambio de archivos.**

La pandemia de COVID-19 aún no está enteramente controlada, y debido a la incertidumbre sobre su futura propagación, se prevé que siga siendo un desafío para los profesionales de la ciberseguridad. Es más, dado el lapso de tiempo transcurrido entre la detección de un incidente y su análisis, esta seguirá dejando su huella en el panorama de las ciberamenazas durante mucho tiempo. La pandemia de COVID-19 ha demostrado que los atacantes contaban con un nivel de capacidad que les permitió adaptarse con mucha rapidez a esta transformación. En el período de 2019 a 2020, el *modus operandi* del adversario se centró en la personalización de vectores de ataque. Los principales logros de los adversarios durante el período del informe han sido los métodos avanzados de robo de credenciales, robo masivo de credenciales (*credential-stuffing*), ataques de *phishing* muy precisos, ataques de ingeniería social avanzados, avanzadas técnicas de confusión mediante programas malintencionados y una penetración más extensa en las plataformas móviles. Si los ciberdelincuentes empiezan a combinar estos avances con la inteligencia artificial y el aprendizaje automático, en el futuro empezaremos a ver un aumento de ataques con éxito y campañas imposibles de detectar.

# Sinopsis

## _ Resumen

En la lista siguiente se resumen las tendencias principales observadas en el panorama de las ciberamenazas durante el período del informe. Estas tendencias también se examinan con detalle en todos los informes que componen el panorama de amenazas de 2020.

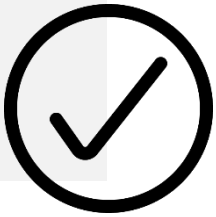
**01_ En ciberseguridad, la superficie del ataque sigue aumentando a medida que entramos en la nueva fase de la transformación digital.**

**02_ Después de la pandemia de COVID-19 habrá una nueva norma social y económica que será aún más dependiente de la existencia de un ciberespacio seguro y de confianza.**

**03_ El uso de las plataformas de redes sociales en ataques dirigidos es una tendencia importante y abarca distintos dominios y tipos de amenazas.**

**04_ Los ataques dirigidos con precisión y los ataques persistentes a datos de alto valor (p. ej., la propiedad intelectual y los secretos de Estado) están siendo planificados meticulosamente por agentes patrocinados por Estados nación.**

**05_ Los ataques de distribución masiva de corta duración y amplio impacto se están utilizando con muchos objetivos, como el robo de credenciales.**



## _ Resumen

**06_** La motivación subyacente a la mayoría de los ataques informáticos sigue siendo económica.

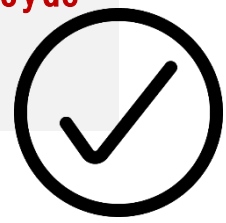
**07_** Los programas de secuestro (*ransomware)* siguen siendo generalizados y con consecuencias costosas para muchas organizaciones.

**08_** Los incidentes de ciberseguridad siguen pasando desapercibidos o se tarda mucho tiempo en detectarlos.

**09_** Con más automatización de la seguridad, las organizaciones invertirán más en preparación usando la inteligencia sobre las ciberamenazas como principal capacidad.

**10_** El número de víctimas de *phishing* sigue creciendo, ya que utiliza la dimensión humana como el eslabón más débil de la cadena.

**Con todos los cambios observados en el panorama de ciberamenazas y los desafíos creados por la pandemia de COVID-19, aún queda mucho por recorrer hasta que el ciberespacio se convierta en un entorno seguro y de confianza para todos.**



# Sinopsis

## _ ¿Es más consciente la ciudadanía de la UE de los riesgos y desafíos que brinda el ciberespacio?

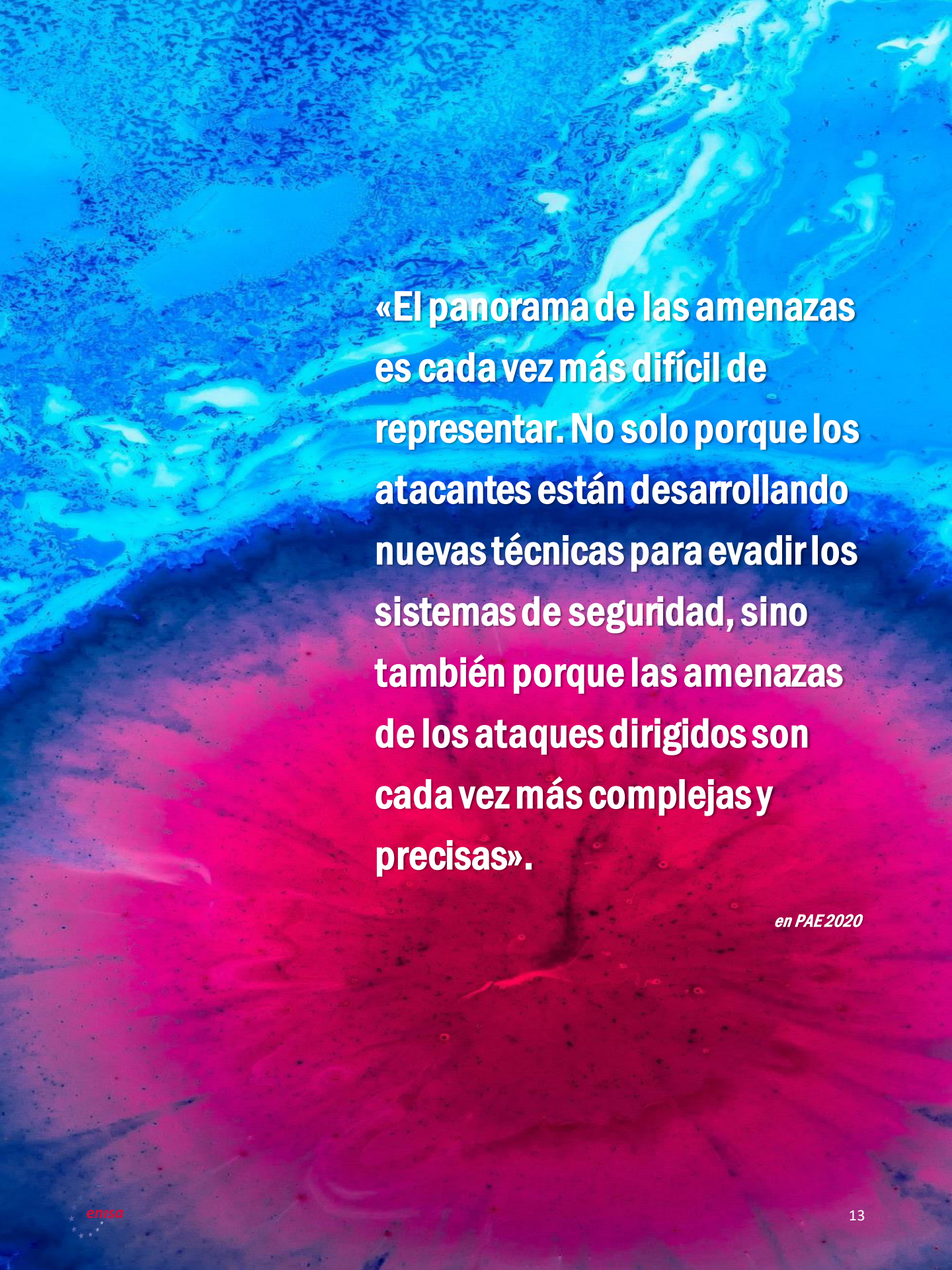
La Comisión Europea preparó una encuesta Eurobarómetro especial[4] en 2019 con el fin de conocer el grado de conocimiento, experiencias y percepciones de la ciudadanía de la UE en materia de ciberseguridad.

EUROBARÓMETRO

Los resultados de esta encuesta indican que el uso de Internet en Europa sigue aumentando, especialmente a través de los teléfonos inteligentes, y que la ciudadanía es más consciente de los peligros potenciales de conectarse a Internet.

Según los resultados de la encuesta, la desconfianza en la privacidad en línea y la seguridad han llevado a más de 9 de cada 10 usuarios de Internet a cambiar su comportamiento en línea –en la mayoría de los casos dejando de abrir mensajes de personas desconocidas, instalando programas antivirus, visitando solo sitios *web* conocidos y de confianza y usando solo sus propios ordenadores.

Aunque estos resultados son bastantes alentadores, muchos usuarios aún son víctimas de estafas en línea y de los mensajes de *phishing*. Esto revela que los ciberdelincuentes están usando ataques sofisticados que son más difíciles de detectar y de evitar. Por lo tanto, las estrategias de mitigación tienen que actualizarse periódicamente para acomodar la última información disponible (CTI) sobre las técnicas de ataque.


«El panorama de las amenazas es cada vez más difícil de representar. No solo porque los atacantes están desarrollando nuevas técnicas para evadir los sistemas de seguridad, sino también porque las amenazas de los ataques dirigidos son cada vez más complejas y precisas».
en PAE 2020

# Expectativas

## Es probable que los agentes patrocinados por un Estado-nación...

| TENDENCIA | DESCRIPCIÓN | AMENAZA |
|---|---|---|
| → | **Sigan** utilizando el ciberespacio para lanzar ataques contra los procesos electorales de otros países poniendo en peligro los sistemas democráticos y los derechos humanos.[5] | **Ataques contra los derechos humanos y los sistemas democráticos** |
| → | **Sigan** acosando a los partidos de la oposición y vigilando a su población mediante la manipulación de la información en redes sociales, junto con campañas con programas espía (*spyware*). | **Ataques contra los derechos humanos y los sistemas democráticos** |
| ↗ | **Lancen** campañas de desinformación sofisticadas[6] diseñadas para influir en las percepciones o para manipular opiniones en favor de un programa político determinado o con objetivos de especulación financiera. | **Campañas de desinformación** |
| ↗ | **Aumenten** la carrera armamentista cibernética[7] en un intento de desarrollar capacidades cibernéticas. Cuando el ciberespacio se considera un dominio de guerra, es probable que los Estados nación busquen armas cibernéticas a través de agentes patrocinados en preparación para conflictos de carácter cibernético. | **Carrera armamentista cibernética descontrolada** |
| ↗ | **Persigan** objetivos estratégicos como: obtener secretos industriales mediante espionaje, obtener ventajas en la toma de decisiones políticas, financiar el régimen a través del fraude financiero, realizar operaciones de información facilitadas por la informática y, finalmente, debilitar o desmoralizar al adversario mediante actividades desestabilizadoras o destructivas. | **Robo de datos** |

# Es probable que los ciberdelincuentes...

| TENDENCIA | DESCRIPCIÓN | AMENAZA |
|---|---|---|
| → | **Sigan** utilizando a los adolescentes y adultos jóvenes como objetivo para los ataques con sextorsión (chantaje por cámara *web*) que tendrán efectos psicológicos y, en última instancia, físicos en las víctimas.[8] | **Sextorsión (chantaje por cámara *web*)** |
| ↗ | **Aumenten** el número de ataques de ciberacoso durante la pandemia de COVID-19 y después de ella, ya que los adolescentes utilizan cada vez más las plataformas para fines personales o educativos.[9] | **Ciberacoso** |

# Es probable que los ciberdelincuentes...

| TENDENCIA | DESCRIPCIÓN | AMENAZA |
|---|---|---|
| ↗ | **Aumenten** el uso de herramientas de IA para crear reproducciones hiperrealistas (imágenes, audio y vídeo), también conocidas popularmente como «ultrafalsificaciones» (del inglés *deep-fakes*), para defraudar a empresas. | **Ultrafalsificaciones** |
| → | **Mejoren** las tácticas que comprometen a los procesos empresariales para obtener beneficios financieros. | **Compromiso de los procesos empresariales (CPE)** |
| → | **Bajen** un nivel en la organización –por debajo del nivel ejecutivo– para comprometer los mensajes de correo electrónico la empresa. | **Compromiso de los mensajes de correo electrónico de la empresa (CCE)** |
| → | **Aumenten** el uso de los proveedores de servicios gestionados (PSG) para distribuir programas informáticos malintencionados (*malware*). | **Programas informáticos malintencionados (*malware*)** |

# Conclusiones y recomendaciones

## Conclusiones y recomendaciones para políticas

- Durante las últimas décadas los responsables de las políticas y los expertos en tecnología han habitado en dos mundos separados y han hablado idiomas distintos. Para afrontar los retos de la digitalización ambas partes deben **trabajar juntas** desde la base y desarrollar un enfoque común. Debido a que la mayor parte de la tecnología actual está conectada al ciberespacio, la contribución de los expertos en ciberseguridad en muchos de estos debates es de fundamental importancia.
- Con el aumento de la innovación tecnológica y la rápida expansión del ciberespacio, las políticas efectivas y exhaustivas de ciberseguridad de la UE adquieren una importancia vital. **Políticas de ciberseguridad maduras** proporcionarán la capacidad de seguridad necesaria en todos los niveles de la sociedad: administraciones, infraestructuras vitales, empresas, sector terciario y particulares. La capacidad de seguridad debe ser eficaz y flexible para poder enfrentarse a los nuevos retos a medida que van surgiendo para poder afrontar la naturaleza en continua evolución del ciberespacio.
- Dado el aumento en el número de partes interesadas de la UE y de los Estados miembros que participan en las actividades de CTI, la **cooperación y la coordinación** de las actividades de la UE en este campo es clave. La ENISA promoverá la cooperación con varias partes interesadas y hará el primer intento de identificar los requisitos de CTI de varios grupos de partes interesadas, especialmente en la UE (es decir, la Comisión, las instituciones, los órganos y organismos, y los Estados miembros).
- La CTI debe considerarse la herramienta principal de **preparación para la ciberseguridad** y para facilitar enfoques basados en riesgos. La integración de la CTI con los procesos de gestión de la seguridad ayudará a multiplicar su difusión en áreas relacionadas y aumentará la agilidad de procesos que suelen ser largos, como el de las certificaciones y el de la evaluación de riesgos. Por otra parte, la CTI se considerará un elemento facilitador de las decisiones de emergencia necesarias en la gestión de crisis.
- La relevancia de la CTI para las decisiones estratégicas y políticas está ampliamente aceptada y se considera esencial para facilitar la **conexión a la información geopolítica** y a los sistemas físicos cibernéticos. Esto permitirá incluir a la CTI en los procesos de toma de decisiones de toda la UE y también permitirá la expansión de su contexto para identificar amenazas híbridas.

# Conclusiones y recomendaciones para empresas

- Durante 2019 aumentó el número de **laboratorios de pruebas y campos de maniobras virtuales**[10] en oficinas y en ofertas en la nube. Se trata de recursos importantes para formar al personal, simular ataques y probar diversas estrategias de defensa. Todo en entornos virtuales multiusos.
- Aunque algunos criterios y requisitos de CTI han sido desarrollados para diversos perfiles de usuario de CTI, será necesario establecer **requisitos similares** para desarrollar más productos, servicios y herramientas para esta materia. Los proveedores de servicios de CTI necesitarán tener más en cuenta los requisitos de los usuarios para facilitar la adopción de productos y servicios de CTI.
- La inversión en algunos conceptos básicos de CTI, particularmente los relacionados con la **madurez de la CTI y las jerarquías de la amenaza**, es muy útil para la adopción de inteligencia sobre las ciberamenazas. Los proveedores necesitarán orientar su oferta hacia varios niveles de madurez de CTI para facilitar su uso eficiente en organizaciones de distintos tamaños y presupuestos.
- A largo plazo parece que **OpenCTI**[11] podría ser una buena solución para resolver la fragmentación de la oferta de CTI dada su capacidad inherente para integrar fuentes de inteligencia de varios tipos en un único entorno de herramientas. Los proveedores de CTI necesitarán tender los «puentes» necesarios en sus productos para permitir su integración en OpenCTI. La Agencia Europea de Defensa (AED) fue la que definió inicialmente, en 2013, el concepto de «campo de maniobras virtual o *cyber range*» en el informe «Common staff target for military cooperation on cyber ranges in the European Union» como un entorno multiusos para respaldar tres procesos primarios: desarrollo de conocimiento, garantía y difusión.

# Conclusiones y recomendaciones

## Conclusiones y recomendaciones relacionadas con la investigación y la educación

- La UE debe seguir invirtiendo en **I+D en ciberseguridad** haciendo hincapié en las iniciativas de investigación a largo plazo y de alto riesgo. La investigación a largo plazo y la innovación son un ejercicio costoso y fuera del alcance de la mayoría de las organizaciones del sector privado.
- La expansión del conocimiento y experiencia en ciberseguridad es fundamental para mejorar la preparación y la resiliencia. La UE debe seguir **capacitando** a través de la inversión en programas de formación en materia de ciberseguridad, certificaciones profesionales, ejercicios y campañas de concienciación.
- Los trabajos de investigación en el campo a la ciberseguridad deben incluir expertos de disciplinas sociales, comportamiento y economía. La **investigación multidisciplinar** en el campo de la ciberseguridad debe promoverse e incentivarse en toda la UE.
- Es necesario evaluar y representar en un contexto más amplio los resultados de los proyectos de investigación realizados en el campo de la ciberseguridad a fin de identificar los **solapamientos y las lagunas** y hacerlos comparables a los productos, servicios y prácticas comerciales existentes. Esto ayudaría a difundir estos resultados a los grupos de usuarios.
- Es necesario desarrollar nuevos planteamientos para la adopción del conocimiento de CTI en los dominios que se puedan beneficiar de ello. **Los campos de maniobras virtuales (*cyber-ranges*), las amenazas híbridas y las evaluaciones geopolíticas son unos ejemplos**. Las sinergias logradas podrían impulsar casos de usos y calidad del contenido de una forma multidireccional.
- Debe estudiarse más a fondo el uso de la **inteligencia artificial (IA)** y del aprendizaje automático (AA) en el campo de la CTI. Así se podría reducir el número de pasos manuales en el análisis de la CTI y aumentaría el valor de las funciones de aprendizaje automático en las actividades de inteligencia sobre las ciberamenazas.
- Deberá promoverse la provisión y el uso de material de CTI de fuentes de dominio público. Esto facilitaría el **intercambio de conocimientos**, pero también reduciría el umbral de las capacidades de CTI necesarias.

**«La sofisticación de las capacidades de amenaza aumentó en 2019, y hubo muchos adversarios que usaron programas intrusos, robo de credenciales y ataques multietapa».**

***en PAE 2020***

# Bibliografía


**1.** «Reglamento sobre la Ciberseguridad». Abril, 2019. Parlamento y Consejo de la UE https://eur-lex.europa.eu/eli/reg/2019/881/oj

**2.** "COVID-19 Risks Outlook: A Preliminary Mapping and its Implications". 19 de mayo de 2020. WEF. https://www.weforum.org/reports/covid-19-risks-outlook-a-preliminary-mapping-and-its-implications

**3.** «Comunicación conjunta al Parlamento europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. La lucha contra la desinformación acerca de la COVID-19: contrastando los datos». Junio de 2020. Comisión Europea. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52020JC0008

**4.** «Special Eurobarometer 499: Europeans' attitudes towards cyber security». 29 de enero de 2020. https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG

**5.** «EUvsDosinfo» https://euvsdisinfo.eu/european-elections-2019/

**6.** «Manipulating Social Media to Undermine Democracy». 2017. Freedom House. https://freedomhouse.org/report/freedom-net/2017/manipulating-social-media-undermine-democracy

**7.** «Conceptualising Cyber Arms Races» 2016. NATO CCD COE. https://ccdcoe.org/uploads/2018/10/Art-10-Conceptualising-Cyber-Arms-Races.pdf

**8.** «How online 'sextortion' drove one young man to suicide». 8 de febrero de 2018. Hoy. https://www.today.com/parents/how-online-sextortion-drove-one-young-man-suicide-t122735

**9.** «Cyberbullying may increase during COVID-19 pandemic, expert says». 30 de marzo de 2020 Healio. https://www.healio.com/news/pediatrics/20200330/cyberbullying-may-increase-during-covid19-pandemic-expert-says

**10.** La Agencia Europea de Defensa (AED) fue la que definió inicialmente, en 2013, el concepto de «campo de maniobras virtual o *cyber range*» en el informe «Common staff target for military cooperation on cyber ranges in the European Union» como un entorno multiusos para respaldar tres procesos primarios: desarrollo de conocimiento, garantía y difusión.

**11.** Open CTI. https://www.opencti.io/en/

**«La CTI se ha establecido firmemente en el dominio de la ciberseguridad como herramienta esencial para mejorar la agilidad y la eficiencia contra los ataques informáticos».**

***en PAE 2020***

# Lecturas relacionadas


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

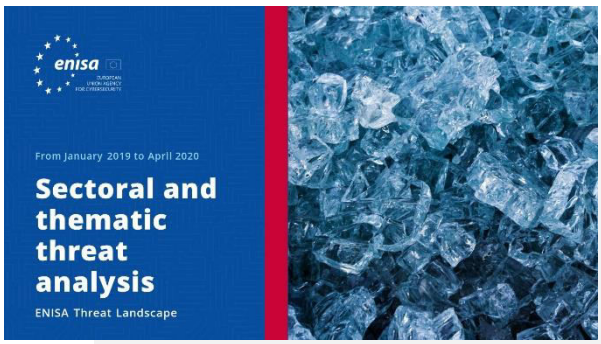
Lista de la ENISA con las 15 amenazas principales durante el período de enero de 2019 a abril de 2020.

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 ciberamenazas.

LEER EL INFORME




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 **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 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 de ciberseguridad común para 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 las 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.

## 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. Esta publicación tampoco refleja necesariamente la información más actual 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