EUROPEAN UNION AGENCY
FOR CYBERSECURITY

INFORME «PANORAMA DE AMENAZAS» DE ENISA DE 2021

De abril de 2020 a mediados de julio de 2021

OCTUBRE DE 2021

ACERCA DE LA ENISA

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. Creada en 2004 y reforzada mediante el Reglamento sobre la Ciberseguridad de la UE, la Agencia de la Unión Europea para la Ciberseguridad contribuye a la política de seguridad cibernética de la UE, mejora la fiabilidad de los productos, servicios y procesos de TIC mediante programas de certificación de la ciberseguridad, coopera con los Estados miembros y con los organismos de la UE y ayuda a Europa a prepararse para los desafíos del día de mañana en materia de ciberseguridad. A través del intercambio de conocimientos, la creación de capacidades 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 encontrar más información sobre la ENISA y su trabajo aquí: www.enisa.europa.eu.

CONTACTO

Para ponerse en contacto con los autores, utilice la dirección de correo etl@enisa.europa.eu.
Las consultas de los medios de comunicación acerca de este informe deben realizarse a través de press@enisa.europa.eu.

EDITORES

Ifigeneia Lella, Marianthi Theocharidou, Eleni Tsekmezoglou, Apostolos Malatras – Agencia de la Unión Europea para la Ciberseguridad

COLABORADORES

Claudio Ardagna, Stephen Corbiaux, Andreas Sfakianakis, Christos Douligeris

AGRADECIMIENTOS

Queremos dar las gracias a los miembros y observadores del grupo de trabajo *ad hoc* de la ENISA sobre los panoramas de ciberamenazas por sus valiosas opiniones y comentarios al validar este informe. También queremos dar las gracias al Grupo Consultivo de ENISA y a la red de funcionarios de enlace nacionales por sus valiosas opiniones.
Asimismo, queremos agradecer a los equipos de conciencia situacional y notificación de incidentes de la ENISA su contribución activa y su apoyo para consolidar diferentes datos en el panorama de amenazas.

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) 2019/881. La ENISA podrá actualizar esta publicación en cualquier momento.

Las correspondientes fuentes de terceros se citan cuando proceda. La ENISA no acepta responsabilidad alguna 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.

MENCIÓN DE COPYRIGHT

© Agencia de la Unión Europea para la Ciberseguridad (ENISA), 2021

Se autoriza la reproducción siempre y cuando se mencione la fuente. 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: 978-92-9204-536-4 - DOI: 10.2824/324797 - ISSN: 2363-3050

ÍNDICE

RESUMEN EJECUTIVO

Esta es la novena edición del informe «Panorama de amenazas» de ENISA, un informe anual sobre el panorama de ciberamenazas en el que se determinan las principales amenazas, las principales tendencias observadas con respecto a las amenazas, los agentes de riesgo y las técnicas de ataque, y en el que también se describen las medidas de mitigación pertinentes. En el proceso de mejora constante de nuestra metodología para el desarrollo de los panoramas de amenazas, el trabajo de este año ha sido apoyado por un grupo de trabajo *ad hoc* de la ENISA sobre los panoramas de ciberamenazas de nueva creación.

El informe «Panorama de amenazas» de ENISA de 2021 abarca desde abril de 2020 a julio de 2021, lo que se denomina «periodo de notificación» a lo largo del informe. Durante el periodo de notificación, las principales amenazas detectadas fueron:

- ***Ransomware* o programas de secuestro**
- ***Malware* o programas informáticos malintencionados**
- **Criptosecuestro**
- **Amenazas relacionadas con el correo electrónico**
- **Amenazas contra los datos**
- **Amenazas contra la disponibilidad y la integridad**
- **Desinformación e información errónea**
- **Amenazas no maliciosas**
- **Ataques a la cadena de suministro**

En este informe analizamos las primeras ocho categorías de ciberamenazas. Las amenazas para la cadena de suministro, la novena categoría, se analizaron en detalle, debido a su especial relevancia, en un informe específico de la ENISA titulado «ENISA Threat Landscape for Supply Chain Attacks» (informe «Panorama de amenazas» de ENISA relacionadas con los ataques a la cadena de suministro) [1].

Para cada una de las amenazas detectadas se analizan las técnicas de ataque, los incidentes considerables y las tendencias, junto con las medidas de mitigación propuestas. Por lo que respecta a las tendencias, durante el periodo de notificación destacamos lo siguiente:

- El ***ransomware*** ha sido considerado la **principal amenaza en 2020-2021.**
- **Las organizaciones gubernamentales han intensificado sus esfuerzos de protección** tanto a escala nacional como internacional.
- **Los ciberdelincuentes están cada vez más motivados por la monetización** de sus actividades, por ejemplo, *ransomware*. **La criptomoneda** sigue siendo el método de pago más común para los agentes de riesgo.
- El **descenso del *malware*** observado en 2020 continúa en 2021. En 2021, observamos un incremento de los agentes de riesgo que recurren a lenguajes de programación relativamente nuevos o infrecuentes para transferir su código.
- El volumen de **infecciones por criptosecuestro** alcanzó un **máximo histórico** en el primer trimestre de 2021, en comparación con los últimos años. Los **beneficios financieros** asociados al criptosecuestro animaron a los agentes de riesgo a perpetrar estos ataques.
- **La COVID-19 sigue siendo el principal señuelo en las campañas** de ataques a través del correo electrónico.
- Se registró un **aumento de las violaciones de la seguridad de los datos relacionadas con el sector sanitario**.

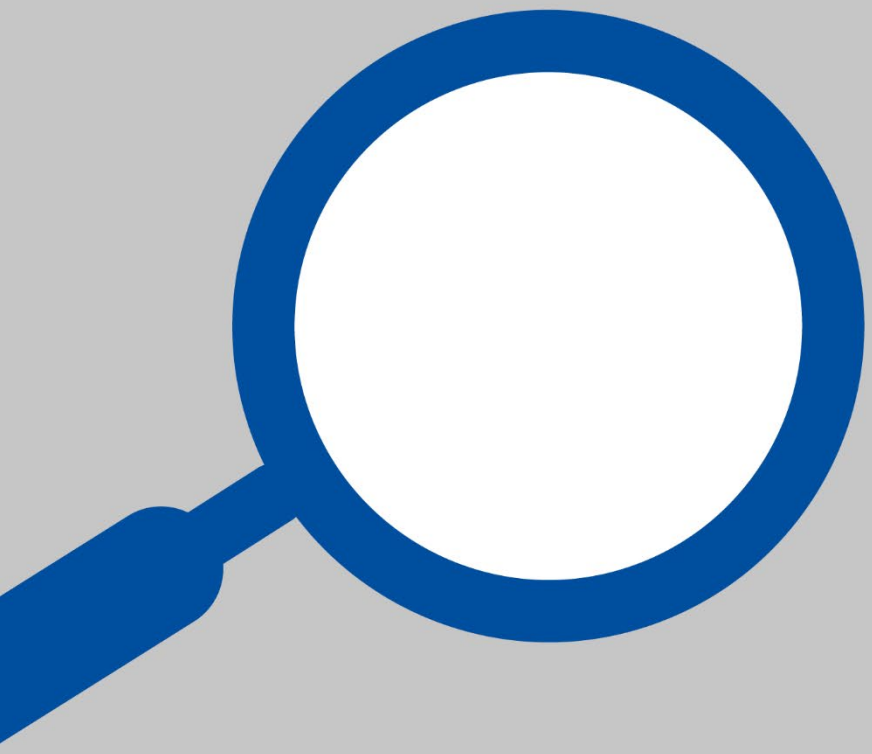
[1] Informe «Panorama de amenazas» de ENISA relacionadas con ataques a la cadena de suministro, julio de 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.

- **Las campañas de ataques distribuidos de denegación de servicio (DDoS) tradicionales** son más específicas, más persistentes y cada vez más multivectoriales en 2021. El **internet de las cosas (IdC)**, junto con las **redes móviles**, está provocando una nueva oleada de ataques DDoS.
- En 2020 y 2021, observamos un **repunte de los incidentes no maliciosos**, ya que la pandemia de COVID-19 se convirtió en un multiplicador de los **errores humanos** y los **errores de configuración de sistema**s, hasta el punto de que la mayoría de las infracciones registradas en 2020 fueron causadas por errores.

Conocer las tendencias relacionadas con los agentes de riesgo, sus motivaciones y sus objetivos ayuda enormemente a planificar las defensas de ciberseguridad y las estrategias de mitigación. Esto forma parte integral de nuestra evaluación global de amenazas, ya que permite priorizar los controles de seguridad y diseñar una estrategia específica basada en el posible impacto y la probabilidad de materialización de la amenaza. Teniendo esto en cuenta, a efectos del informe «Panorama de amenazas» de ENISA 2021, se consideran las siguientes cuatro categorías de agentes de riesgo para la ciberseguridad:

- **Agentes patrocinados por Estados nación**
- **Ciberdelincuentes**
- **Piratas informáticos contratados**
- **Hacktivistas**

Mediante un análisis continuo, la ENISA extrajo las tendencias y los puntos de interés para cada una de las principales amenazas presentadas en el informe «Panorama de amenazas» de ENISA de 2021. Los principales hallazgos y conclusiones de esta evaluación se basan en múltiples recursos disponibles públicamente que se facilitan en la bibliografía utilizada para la elaboración del presente documento. El informe está dirigido principalmente a los encargados de la creación de políticas y la toma de decisiones estratégicas, pero también será de interés para la comunidad técnica de ciberseguridad.



DESCRIPCIÓN GENERAL DEL PANORAMA DE AMENAZAS

En su novena edición, el informe «Panorama de amenazas» de ENISA ofrece una visión general del panorama de ciberamenazas. Este informe es parcialmente estratégico y parcialmente técnico, y presenta información relevante para lectores técnicos y no técnicos. El trabajo de este año ha sido apoyado por un grupo de trabajo *ad hoc* de la ENISA sobre los panoramas de ciberamenazas[2] de nueva creación.

Los ataques a la ciberseguridad han seguido aumentando durante los años 2020 y 2021, no solo en términos de vectores y cifras, sino también en términos de su impacto. La pandemia de COVID-19 también ha tenido —previsiblemente— un impacto en el panorama de ciberamenazas. Uno de los avances más duraderos derivados de la pandemia de la COVID-19 es un cambio perdurable a un modelo de oficina híbrido. Por tanto, las ciberamenazas relacionadas con la pandemia y la explotación de la «nueva normalidad» se están generalizando. Esta tendencia ha incrementado la superficie de ataque y, en consecuencia, hemos observado un aumento del número de ciberataques dirigidos a organizaciones y empresas a través del teletrabajo[3].

En general, las ciberamenazas van en aumento. El panorama de la ciberseguridad ha crecido en términos de sofisticación, complejidad e impacto de los ataques, espoleado por una presencia en línea cada vez mayor, la transición de las infraestructuras tradicionales a soluciones en línea y basadas en la nube, la interconectividad avanzada y la explotación de nuevas funciones de tecnologías emergentes como la inteligencia artificial (IA)[4][5], En particular, la amenaza para las cadenas de suministro y su importancia debido a sus efectos en cascada potencialmente catastróficos ha alcanzado la posición más alta entre las principales amenazas, hasta el punto de que la ENISA ha elaborado un panorama de amenazas específico para esta categoría de amenazas[6].

Cabe señalar que en esta edición del informe «Panorama de amenazas» de ENISA se ha prestado especial atención al impacto de las ciberamenazas en diversos sectores, en particular los mencionados en la Directiva sobre Ciberseguridad (Directiva SRI). Ofrece información interesante sobre las particularidades de cada sector en lo que respecta al panorama de amenazas, así como sobre las posibles interdependencias y áreas de importancia. Según esta información, los paisajes de amenazas sectoriales merecen una mayor atención.

Este año los defensores de la cibercomunidad y los encargados de la creación de políticas también han dado pasos notables. La comunidad mundial ha comenzado a darse cuenta de la importancia de la comunicación y la cooperación en el examen y el seguimiento de los ciberdelincuentes, y el *ransomware* (la amenaza más importante para el periodo de notificación del informe «Panorama de amenazas» de ENISA de 2021) se ha convertido en particular en uno de los principales puntos del orden del día de las reuniones sobre estrategia entre los líderes mundiales.

Los lectores de ediciones anteriores del informe observarán una diferencia en el inventario de las principales amenazas. Este año, la ENISA dio un paso atrás y consolidó las categorías de amenazas para promover la integración y la mejora de la representación de amenazas similares. Esto forma parte de las iniciativas en curso hacia una taxonomía de amenazas renovada y ayudará a establecer las tendencias metodológicamente en los próximos años.

[2] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ad-hoc-working-group-cyber-threat-landscapes
[3] IBM – Cost of a Data Breach Report 2020 (Informe de IBM del coste de una brecha de seguridad en los datos de 2020) - https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/
[4] Panorama de amenazas de IA de ENISA: https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges
[5] https://www.stealthlabs.com/blog/top-10-cybersecurity-trends-in-2021-and-beyond/
[6] Informe «Panorama de amenazas» de ENISA relacionadas con ataques a la cadena de suministro, julio de 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

El informe «Panorama de amenazas» de ENISA de 2021 se basa en una serie de fuentes de información de código abierto y de inteligencia sobre amenazas. En él se determinan las principales amenazas, tendencias y hallazgos, y se ofrecen estrategias de mitigación de alto nivel pertinentes. La ENISA trabaja actualmente en la consolidación de la metodología para la elaboración de informes sobre el panorama de amenazas, con vistas a promover la transparencia y la coherencia en el trabajo.

1.1. PRINCIPALES AMENAZAS

Durante 2020 y 2021 surgieron y se materializaron una serie de ciberamenazas. Sobre la base del análisis presentado en este informe, en el informe «Panorama de amenazas» de ENISA de 2021 se determinan y analizan los ocho principales grupos de amenazas siguientes (véase Gráfico 1). Estos ocho grupos de amenazas se destacan por su importancia durante el periodo de notificación, su popularidad y el impacto que ha tenido su materialización.

- ***Ransomware* o programas de secuestro**
  El *ransomware* es un tipo de ataque malicioso en el que los atacantes cifran los datos de una organización y exigen un pago para restablecer el acceso. El *ransomware* ha sido la principal amenaza durante el periodo de notificación, con varios incidentes muy destacados y ampliamente divulgados. La importancia y el impacto de la amenaza del *ransomware* también se pone de manifiesto en una serie de iniciativas políticas conexas puestas en marcha en la Unión Europea (UE) y en todo el mundo.

- ***Malware* o programas informáticos malintencionados**
  El *malware* es *software* o ***firmware*** cuyo objetivo es llevar a cabo un proceso no autorizado que tendrá repercusiones negativas en la confidencialidad, integridad o disponibilidad de un sistema. La amenaza de *malware* lleva muchos años copando los primeros puestos de la lista de amenazas, si bien su importancia ha disminuido durante el periodo de notificación del informe «Panorama de amenazas» de ENISA de 2021. El uso de nuevas técnicas de ataque y algunos logros importantes de los responsables del cumplimiento de la ley han tenido un impacto en las operaciones de agentes de riesgo relevantes.

- **Criptosecuestro**
  El criptosecuestro o la criptominería oculta es un tipo de ciberdelincuencia en el que un delincuente utiliza secretamente la capacidad informática de una víctima para generar criptomonedas. Dada la proliferación de las criptomonedas y su creciente adopción por parte del público en general, se ha observado un aumento de los incidentes de ciberseguridad correspondientes.

- **Amenazas relacionadas con el correo electrónico**
  Los ataques relacionados con el correo electrónico son un conjunto de amenazas que aprovechan las debilidades de la psique humana y los hábitos cotidianos, en lugar de las vulnerabilidades técnicas de los sistemas de información. Curiosamente, y a pesar de las numerosas campañas de sensibilización y de educación contra este tipo de ataques, la amenaza persiste en un grado notable. Aumentan en particular los ataques al correo electrónico de las empresas y las técnicas avanzadas y sofisticadas para obtener ganancias monetarias.

- **Amenazas contra los datos**
  Esta categoría abarca fugas de datos o violaciones de la seguridad de los datos. Una violación de la seguridad de los datos o fuga de datos es la divulgación de datos sensibles, protegidos o confidenciales a entornos que no son de confianza. Las violaciones de la seguridad de los datos pueden producirse como resultado de un ciberataque, un trabajo desde dentro, o una pérdida o exposición no intencionada de los datos. La amenaza sigue siendo alta, ya que el acceso a los datos es el principal objetivo de los atacantes por numerosas razones, como la extorsión, el rescate, la difamación, la información errónea, etc.

- **Amenazas contra la disponibilidad y la integridad**
  La disponibilidad y la integridad son el objetivo de un sinfín de amenazas y ataques, entre los que destacan las familias de ataques de denegación de servicio (DoS) y los ataques de aplicación web. El ataque DDoS, estrictamente relacionado con los ataques basados en la web, es una de las amenazas más importantes para

los sistemas de TI, ya que se centra en su disponibilidad agotando los recursos, lo que ocasiona una disminución del rendimiento, la pérdida de datos y las interrupciones del servicio. La amenaza ocupa sistemáticamente un lugar destacado en el panorama de amenazas de la ENISA, tanto por su manifestación en incidentes reales como por su potencial para causar un gran impacto.

- **Desinformación e información errónea**
  Las campañas de desinformación e información errónea están creciendo, impulsadas por el mayor uso de las plataformas de redes sociales y los medios en línea, así como por el aumento de la presencia de personas en línea debido a la pandemia de COVID-19. Este grupo de amenazas aparece por primera vez en el informe «Panorama de amenazas» de ENISA; sin embargo, su importancia en el espacio cibernético es grande. Las campañas de desinformación e información errónea se utilizan frecuentemente en ataques híbridos para reducir la percepción general de confianza, una importante defensora de la ciberseguridad.

- **Amenazas no maliciosas**
  Las amenazas suelen considerarse actividades voluntarias y maliciosas provocadas por enemigos que tienen motivaciones para atacar un objetivo concreto. Esta categoría abarca las amenazas en las que las intenciones maliciosas no son evidentes. Se basan principalmente en errores humanos y errores de configuración de los sistemas, pero también pueden referirse a catástrofes físicas dirigidas a infraestructuras de TI. Debido a su naturaleza, estas amenazas tienen una presencia constante en el panorama anual de amenazas y constituyen una preocupación importante para las evaluaciones de riesgos.

Gráfico 1: Informe «Panorama de amenazas» de ENISA de 2021 - Principales amenazas

Cabe señalar que las amenazas mencionadas abarcan categorías y la recopilación de amenazas, consolidadas en los ocho ámbitos mencionados anteriormente. Cada uno de los grupos de amenazas se analiza más a fondo en un capítulo específico de este informe, que profundiza en sus particularidades y proporciona información más específica, hallazgos, tendencias, técnicas de ataque y vectores de mitigación.

1.2. TENDENCIAS PRINCIPALES

En la lista siguiente se resumen las tendencias principales observadas en el panorama de ciberamenazas durante el periodo de notificación. Estas tendencias también se examinan con detalle en los distintos capítulos que componen el informe «Panorama de amenazas» de ENISA de 2021.

- Proliferaron los **ataques muy sofisticados e impactantes a la cadena de suministro**, como pone de relieve el informe «Panorama de amenazas» de ENISA relacionadas específicamente con los ataques a la cadena de suministro. Los **proveedores de servicios gestionados** son objetivos de alto valor para los ciberdelincuentes.
- **La COVID-19 impulsó el ciberespionaje** y creó **oportunidades para los ciberdelincuentes**.
- **Las organizaciones gubernamentales han intensificado sus esfuerzos de protección** tanto a escala nacional como internacional. Los gobiernos han redoblado sus esfuerzos para entorpecer la labor de los agentes patrocinados por Estados nación y emprender acciones legales contra ellos.
- **Los ciberdelincuentes están cada vez más motivados por la monetización** de sus actividades, por ejemplo, *ransomware*. **La criptomoneda** sigue siendo el método de pago más común para los agentes de riesgo.
- Los ciberataques **cada vez afectan más a las infraestructuras críticas**.
- **Los ataques mediante mensajes de *phishing* y los ataques de fuerza bruta a servicios de escritorio remoto** siguen siendo los dos **vectores de infección por *ransomware*** más habituales.
- La atención prestada a los **modelos de negocio de tipo *ransomware* como servicio** ha aumentado en 2021, lo que dificulta la atribución adecuada a cada uno de los agentes de riesgo.
- La aparición de esquemas de ***ransomware* de triple extorsión** aumentó notablemente a lo largo de 2021.
- **El descenso del *malware*** observado en 2020 continúa en 2021. En 2021, observamos un incremento de los agentes de riesgo que recurren a lenguajes de programación relativamente nuevos o infrecuentes para transferir su código.
- **El *malware* dirigido a entornos de contenedores** ha adquirido mucha más prevalencia, con nuevas evoluciones como la ejecución de malware sin archivos desde la memoria.
- Los desarrolladores de *malware* siguen encontrando formas de dificultar la **aplicación de ingeniería inversa y el análisis dinámico**.
- El volumen de **infecciones por criptosecuestro** alcanzó un **máximo histórico** en el primer trimestre de 2021, en comparación con los últimos años. Los **beneficios financieros** asociados al criptosecuestro animaron a los agentes de riesgo a perpetrar estos ataques.
- **El volumen de minería de criptomonedas y las actividades de criptosecuestro han alcanzado un máximo histórico** en 2021.
- Podemos observar que se está produciendo un **cambio del criptosecuestro basado en navegador al criptosecuestro basado en archivos**.
- **La COVID-19 sigue siendo el principal señuelo en las campañas** de ataques a través del correo electrónico.
- **Los ataques al correo electrónico de las empresas** han **aumentado**, han adquirido **sofisticación** y se han vuelto más **específicos**.
- El modelo de negocio de **suplantación de identidad como servicio (PhaaS)** está adquiriendo prevalencia.
- Los agentes de riesgo desviaron su atención hacia la **información sobre vacunas** en el contexto de las amenazas para los datos y la información.
- Se registró un **aumento de las violaciones de la seguridad de los datos relacionadas con el sector sanitario**.
- Los ataques distribuidos de denegación de servicio (DDoS) tradicionales están evolucionando hacia **redes móviles y el internet de las cosas (IdC).**
- **La denegación de servicio de rescate (RDoS)** constituye la nueva frontera de los ataques de denegación de servicio.
- **La puesta en común de recursos en entornos virtualizados** actúa como amplificador de los ataques DDoS.
- En 2021 las **campañas DDoS** se han convertido en campañas más específicas, mucho más persistentes y cada vez más multivectoriales.

- **La desinformación basada en la inteligencia artificial (IA)** ayuda a los ciberdelincuentes a llevar a cabo sus ataques.
- **El *phishing* se sitúa en el centro de los ataques de desinformación** y explota en gran medida las creencias de las personas.
- La **información errónea y la desinformación** constituyen el núcleo de las actividades de la ciberdelincuencia y están aumentando a un ritmo sin precedentes.
- **El modelo de negocio de desinformación como servicio (DaaS)** ha crecido significativamente, al calor del creciente impacto de la pandemia de COVID-19 y la necesidad de disponer de más información.
- En 2020 y 2021, observamos un **repunte de los incidentes no maliciosos**, ya que la pandemia de COVID-19 se convirtió en un multiplicador de los **errores humanos** y los **errores de configuración de sistemas**, hasta el punto de que la mayoría de las infracciones registradas en 2020 fueron causadas por errores.
- Se ha producido un **repunte en los incidentes de seguridad en la nube no maliciosos**.

1.3. PROXIMIDAD DE LAS PRINCIPALES AMENAZAS CON RESPECTO A LA UE

Un aspecto importante que debe tenerse en cuenta en el contexto del informe «Panorama de amenazas» de ENISA es la proximidad de un ciberataque con respecto a la Unión Europea (UE). Esto es especialmente importante para ayudar a los analistas a evaluar la importancia de las ciberamenazas, correlacionarlas con posibles vectores y agentes de riesgo e incluso para guiar la selección de vectores de mitigación específicos adecuados. De acuerdo con la clasificación propuesta para la política común de seguridad y defensa (PCSD)[7], clasificamos las ciberamenazas en cuatro categorías, como se muestra en el **Cuadro 1**.

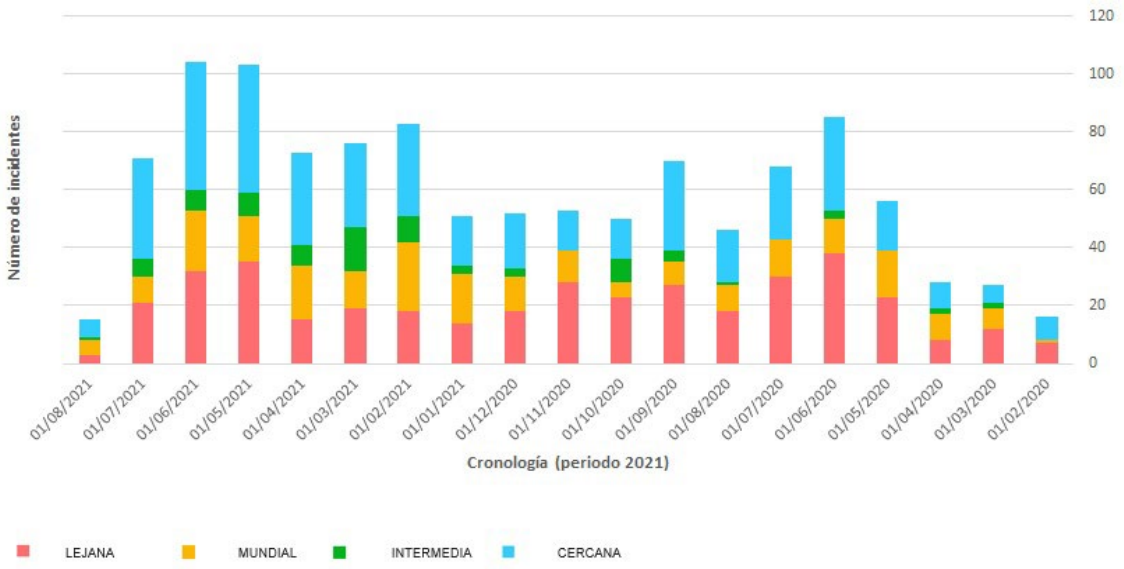
Cuadro 1: Clasificación de la proximidad de las ciberamenazas

Proximidad	Afectados
CERCANA	Redes y sistemas afectados, controlados y protegidos dentro de las fronteras de la UE. Población afectada dentro de las fronteras de la UE.
INTERMEDIA	Redes y sistemas considerados esenciales para los objetivos operativos en el ámbito del mercado único digital de la UE y los sectores de la Directiva SRI, pero cuyo control y protección dependen de las autoridades públicas o privadas de instituciones de terceros países. Población afectada en zonas geográficas cercanas a las fronteras de la UE.
LEJANA	Redes y sistemas que, de verse afectados, tendrán un impacto crítico en los objetivos operativos en el ámbito del mercado único digital de la UE y los sectores de la Directiva SRI. El control y la protección de estas redes y sistemas son ajenos a las autoridades públicas o privadas de las instituciones de la UE o de los Estados miembros. Población afectada en zonas geográficas alejadas de la UE.
MUNDIAL	Todas las áreas mencionadas

En el Gráfico 2 se muestra una cronología de los incidentes relacionados con las principales categorías de amenazas notificadas en el informe «Panorama de amenazas» de ENISA de 2021. Cabe señalar que la información contenida en el gráfico se basa en información procedente del dominio público y es el resultado de un trabajo realizado por la ENISA en el ámbito de la conciencia situacional[8].

[7] https://www.europarl.europa.eu/RegData/etudes/STUD/2017/603175/EPRS_STU(2017)603175_EN.pdf
[8] De conformidad con el artículo 7, apartado 6, del Reglamento sobre la Ciberseguridad de la UE https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

Gráfico 2: Cronología de los incidentes observados relacionados con amenazas importantes del informe «Panorama de amenazas» de ENISA (conciencia situacional basada en información procedente del dominio público) en términos de su proximidad.



Como pone de manifiesto el gráfico anterior, en 2021 se ha registrado un mayor número de incidentes en comparación con 2020. En particular, en la categoría CERCANA se registra un número cada vez mayor de incidentes observados relacionados con las amenazas principales, lo que implica su importancia en el contexto de la UE. Como era de esperar, las tendencias mensuales (que no se muestran en el gráfico para favorecer la brevedad) son bastante similares entre las distintas clasificaciones, ya que la ciberseguridad no conoce fronteras y, en la mayoría de los casos, las amenazas se materializan en todos los niveles de proximidad. Cabe destacar que, durante los últimos meses cubiertos por el informe «Panorama de amenazas» de ENISA de 2021, se ha observado una mayor proximidad CERCANA respecto a la UE, tendencia que la ENISA seguirá supervisando para determinar su evolución y su relación con las actividades de los agentes de riesgo y los vectores de amenaza en curso.

1.4. PRINCIPALES AMENAZAS POR SECTOR

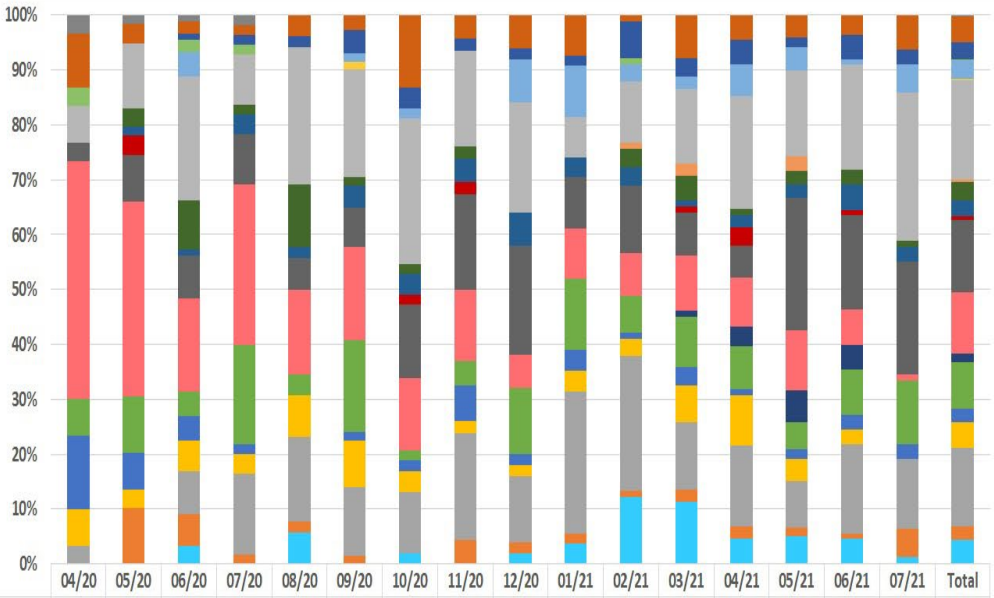
Las ciberamenazas no suelen limitarse a un sector concreto y en la mayoría de los casos afectan a más de uno de ellos. Efectivamente, en muchos casos las amenazas se manifiestan aprovechando las vulnerabilidades de los sistemas de TIC subyacentes que se utilizan en diversos sectores. Sin embargo, hay que tener en cuenta tanto los ataques selectivos como los que aprovechan las diferencias en cuanto a madurez de la ciberseguridad en distintos sectores y la popularidad y prominencia de determinados sectores. Estos factores contribuyen a que las amenazas se manifiesten como incidentes en sectores específicos, de ahí la importancia de analizar en profundidad los aspectos sectoriales de las amenazas y los incidentes observados. Además, las tendencias observadas en cada sector y las dependencias intersectoriales son observaciones que pueden extraerse de dicho análisis.

En los gráficos 3 y 4 se destacan los sectores afectados por incidentes observados sobre la base de la información procedente del dominio público y son el resultado de un trabajo realizado por la ENISA en el ámbito de la conciencia situacional[9]. Se refieren a incidentes relacionados con las principales amenazas del informe «Panorama de amenazas» de ENISA de 2021. Este es el primer intento de la ENISA de delimitar el impacto de las amenazas en sectores específicos. En los próximos años y en futuras ediciones del informe «Panorama de amenazas» de

[9] De conformidad con el artículo 7, apartado 6, del Reglamento sobre la Ciberseguridad de la UE (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN)

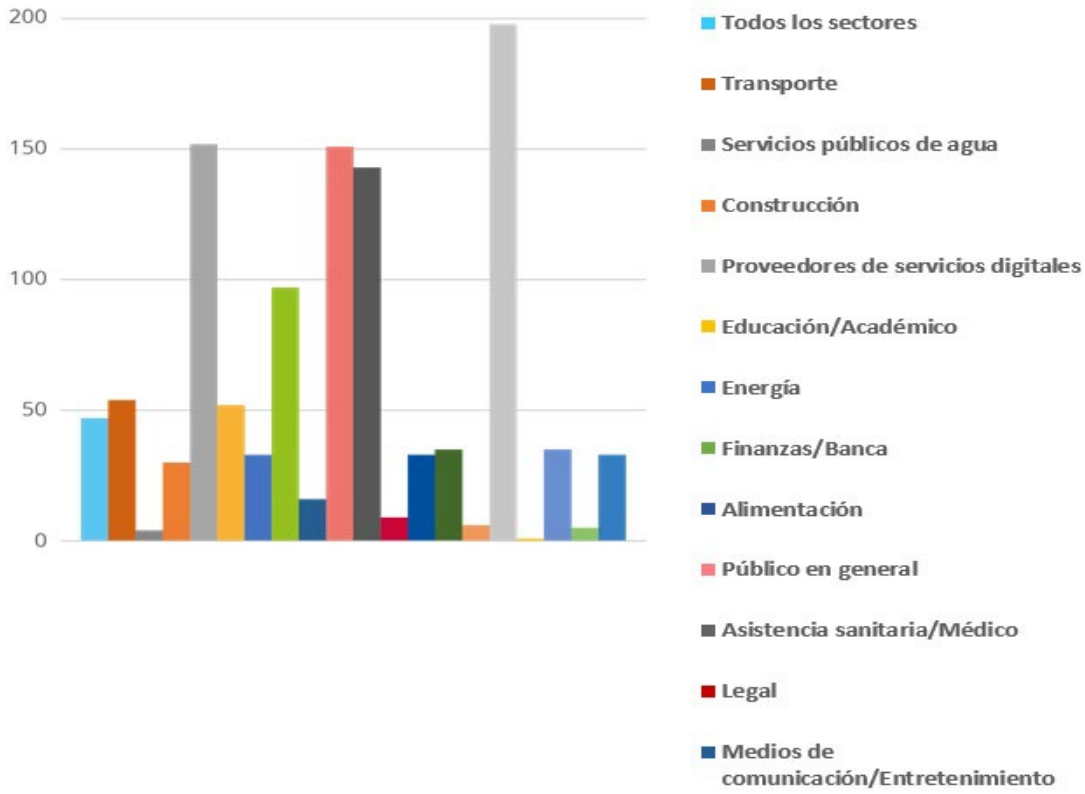
ENISA, se hará todo lo posible por armonizar los sectores con los mencionados en la Directiva sobre Ciberseguridad (Directiva SRI) y en la propuesta para su revisión (Directiva SRI 2.0).

Gráfico 3: Cronología de los incidentes observados relacionados con las principales amenazas del informe «Panorama de amenazas» de ENISA en términos del sector afectado.



	04/20	05/20	06/20	07/20	08/20	09/20	10/20	11/20	12/20	01/21	02/21	03/21	04/21	05/21	06/21	07/21	Total
Servicios públicos de agua	1	1	1	1													2
Transporte	3	2	2	1	2	2	7	2	3	4	1	7	4	5	4	5	49
Personas específicas			1	1	1	3	2	1	1	1	6	3	4	2	5	2	33
Espacial	1		2	1							1						4
Cadena de suministro de software			4			1	1		4	5	3	2	5	5	1	4	35
Semiconductores						1											1
Administración pública/Gobierno	2	7	20	5	13	14	14	8	10	4	10	12	18	19	21	21	189
Servicios postales y de mensajería											1	2		3			6
Militar		2	8	1	6	1	1	1			3	4	1	3	3	1	33
Medios de comunicación/Entretenimiento		1	1	2	1	3	2	2	3	2	3	1	2	3	5	2	32
Legal		2					1	1				1	3		1		7
Asistencia sanitaria/Médico	1	5	7	5	3	5	7	8	10	5	11	7	5	29	19	16	137
Público en general	13	21	15	16	8	12	7	6	3	5	7	9	8	13	7	1	117
Alimentación												1	3	7	5		16
Finanzas/Banca	2	6	4	10	2	12	1	2	6	7	6	8	7	6	9	9	89
Energía	4	4	4	1		1	1	3	1	2	1	3	1	2	3	2	25
Educación/Académico	2	2	5	2	4	6	2	1	1	2	3	6	8	5	3		48
Proveedores de servicios digitales	1		7	8	8	9	6	9	6	14	22	11	13	10	18	10	151
Construcción		6	5	1	1	1		2	1	1	1	2	2	2	1	4	24
Todos los sectores			3		3		1		1	2	11	10	4	6	5	1	47

Gráfico 4: Sectores específicos por número de incidentes (de abril de 2020 a julio de 2021)



Durante este periodo de notificación, un gran número de incidentes afectaron a la administración pública y el Gobierno, así como a los proveedores de servicios digitales. Esto último es de esperar dada la prestación horizontal de los servicios para este sector y, por tanto, su impacto en muchos otros sectores. También hemos observado un número significativo de incidentes que afectan a los usuarios finales y no necesariamente a un sector concreto. El sector sanitario también fue objeto de importantes ataques, y esta actividad muestra signos de aumento en los últimos meses del periodo de notificación (mayo-julio de 2021). Curiosamente, el sector financiero se enfrenta a un número constante de incidentes a lo largo del año. La cadena de suministro de *software* también muestra un aumento del número de incidentes durante 2021, lo que constituye una observación en el informe «Panorama de amenazas» de ENISA relacionadas con la cadena de suministro[10].

1.5. METODOLOGÍA

El informe «Panorama de amenazas» de ENISA de 2021 se basa en la información disponible de fuentes abiertas, principalmente de carácter estratégico, y en las propias capacidades de inteligencia sobre amenazas de la ENISA, y abarca 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 investigadores sobre 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. El informe «Panorama de amenazas» de ENISA de 2021 abarca desde abril de 2020 a julio de 2021, lo que se denomina «periodo de notificación» a lo largo del informe.

Para la elaboración de dicho informe se ha utilizado el siguiente enfoque. A lo largo del periodo pertinente, la ENISA, mediante la conciencia situacional, recabó una lista de los incidentes graves publicados en fuentes abiertas. Esta lista sirvió como base para la elaboración de la lista de amenazas principales, así como para el material básico de varias tendencias y estadísticas del informe.

[10] Informe «Panorama de amenazas» de ENISA relacionadas con ataques a la cadena de suministro, julio de 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

Posteriormente, la ENISA y expertos externos realizaron 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. Mediante un análisis continuo, la ENISA extrajo las tendencias y los puntos de interés para cada una de las principales amenazas presentadas en el informe «Panorama de amenazas» de ENISA de 2021. Los principales hallazgos y conclusiones de esta evaluación se basan en múltiples recursos disponibles públicamente que se facilitan en la bibliografía utilizada para la elaboración del presente documento.

Dentro del informe, tratamos de diferenciar entre lo que han comunicado nuestras fuentes y lo que representa nuestra evaluación. (Lo hacemos utilizando específicamente la frase «en nuestra evaluación»). Por último, al realizar una evaluación, transmitimos la probabilidad utilizando palabras que expresan una estimación de la probabilidad (por ejemplo, probablemente, muy probablemente, sin duda)[11].

El marco MITRE ATT&CK®[12] se utilizó en este informe para destacar las tácticas y técnicas de ataque pertinentes para una amenaza determinada (véase el anexo A). Para cada táctica de ATT&CK®, se presentan las técnicas utilizadas por el adversario. Esto puede dar lugar a una lista de medidas de mitigación de ATT&CK[13] que pueden aplicarse. MITRE ATT&CK® es una base de conocimientos, un lenguaje común para tácticas y técnicas contradictorias basadas en observaciones del mundo real. La base de conocimientos de MITRE ATT&CK® se utiliza como base para el desarrollo de metodologías y modelos de amenazas específicos en el sector privado, en la Administración y en la comunidad de productos y servicios de ciberseguridad.

El informe fue validado por el grupo de trabajo *ad hoc* sobre los panoramas de ciberamenazas de la ENISA[14], creado en abril de 2021, un grupo formado por expertos de entidades públicas y privadas europeas e internacionales.

Para el desarrollo de futuros informes «Panoramas de amenazas» de ENISA, la Agencia está en proceso de formalizar una nueva metodología, con vistas a promover la transparencia y sentar las bases de procesos estructurados y bien alineados. En esta perspectiva, la metodología para los panoramas de amenazas se hará pública en el futuro, junto con una revisión de la taxonomía de amenazas.

1.6. ESTRUCTURA DEL INFORME

El informe «Panorama de amenazas» de ENISA de 2021 ha mantenido la estructura de los informes anteriores, utilizando una estructura similar para destacar las principales ciberamenazas en 2021. Los lectores de informes pasados notarán que las categorías de amenazas se han consolidado en consonancia con un avance hacia una nueva taxonomía de amenazas de ciberseguridad que se utilizará en el futuro.

Este informe se estructura del siguiente modo:

En el **capítulo 2** se analizan las tendencias relacionadas con los agentes de riesgo (es decir, agentes patrocinados por Estados nación, ciberdelincuentes, piratas informáticos contratados y hacktivistas).
En el **capítulo 3** se analizan los principales hallazgos, incidentes y tendencias relacionados con el *ransomware*.
En el **capítulo 4** se presentan los principales hallazgos, incidentes y tendencias relacionados con el *malware*.
En el **capítulo 5** se describen los principales hallazgos, incidentes y tendencias relacionados con el criptosecuestro.
En el **capítulo 6** se destacan los principales hallazgos, incidentes y tendencias relacionados con las amenazas relacionadas con el correo electrónico.
En el **capítulo 7** se analizan los principales hallazgos, incidentes y tendencias relacionados con las amenazas contra los datos.
En el **capítulo 8** se presentan los principales hallazgos, incidentes y tendencias relacionados con las amenazas contra la disponibilidad y la integridad.

[11] CIA - Words of Estimate Probability (Palabras de probabilidad estimativa) https://www.cia.gov/static/0aae8f84700a256abf63f7aad73b0a7d/Words-of-Estimative-Probability.pdf
[12] MITRE ATT&CK® , https://attack.mitre.org/
[13] https://attack.mitre.org/mitigations/enterprise /
[14] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ad-hoc-working-group-cyber-threat-landscapes

En el **capítulo 9** se subraya la importancia de las amenazas híbridas y se describen los principales hallazgos, incidentes y tendencias relacionados con la desinformación y la información errónea.
En el **capítulo 10** se analizan los principales hallazgos, incidentes y tendencias relacionados con las amenazas no maliciosas.
En el **anexo A** se presentan las técnicas empleadas habitualmente para abordar cada amenaza, sobre la base del marco MITRE ATT&CK®.
En el **anexo B** se incluyen los incidentes considerables por amenaza, observados durante el periodo de notificación.