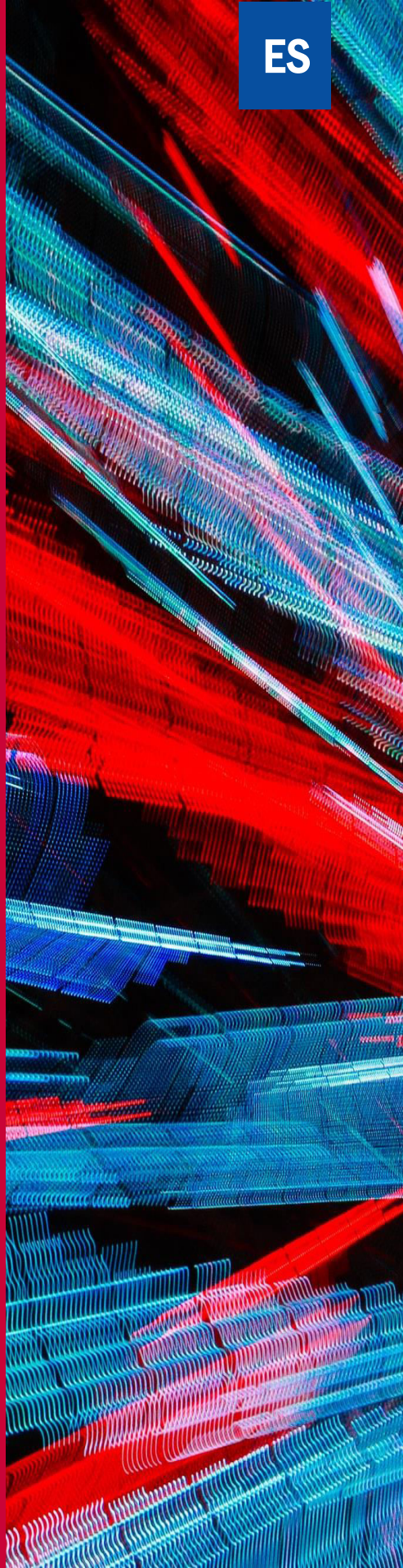
enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

ES



De enero de 2019 a abril de 2020

Tendencias emergentes

Panorama de Amenazas de la ENISA

Sinopsis

_Expectativas

Con el inicio de una nueva década podemos prever cambios importantes en la forma en que percibimos y entendemos la ciberseguridad o la seguridad del ciberespacio. El ciberespacio se define en el **ISO/IEC 27032:2012**[1] como ***«un entorno complejo que consta de interacciones entre personas, software y servicios en Internet por medio de dispositivos tecnológicos y redes conectados a ella, y que no existe en forma física»***. La protección de este entorno complejo pasará a ser aún más complicada a medida que se conecten más personas, dispositivos y sistemas, y se ejecuten más procesos y servicios en la red. También dependemos más de su fiabilidad, integridad y confianza para funcionar, relacionarnos y realizar muchas de nuestras actividades diarias. Al aumentar esta dependencia se presentarán más oportunidades para los atacantes de usar el ciberespacio para manipular, intimidar, engañar, hostigar y estafar a personas y organizaciones. La protección de las personas, empresas y organizaciones cuando usan el ciberespacio tenderá a cambiar en la próxima década: de la seguridad de redes y de los sistemas de información tradicional pasará a convertirse en un concepto más amplio que incluirá el contenido y los servicios.

Durante la década pasada, la cuarta «revolución industrial» ha acelerado significativamente el ritmo del cambio, ha transformado lo que hacen las personas, cómo lo hacen, qué capacidades se requieren, dónde se realiza el trabajo, cómo se estructuran las relaciones y cómo se organiza, distribuye y recompensa el trabajo.

Debido a la actual pandemia de COVID-19, hemos iniciado esta década con una nueva normalidad y con cambios profundos en el mundo físico y en el ciberespacio. Con el distanciamiento interpersonal o con el confinamiento, las personas tienden a usar el espacio virtual para comunicarse, relacionarse y socializar. Esta nueva normalidad introducirá nuevos retos en toda la cadena de valor digital y, en particular, en la industria de la ciberseguridad.

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.

Para hacer que la gestión del riesgo cibernético sea eficaz sería necesario considerar demasiadas variables. Un factor importante es la diversidad tecnológica que la mayoría de las organizaciones tiene hoy en día. Otro aspecto es la sofisticación de las herramientas, tácticas, técnicas y procedimientos (TTP) utilizados por los adversarios para realizar los ataques. Los atacantes se están adaptando y ajustan los TTP para adaptarse al entorno de sus víctimas y colaboran con otros para lograr sus objetivos.

La definición de una postura de riesgo, la gestión de los datos, la aplicación de los parámetros de medida relevantes y responder al cambio son obstáculos que nos impiden crear una estrategia de gobernanza eficaz para los riesgos cibernéticos. **En la próxima década serán necesarios nuevos planteamientos a fin de dejar el análisis aislado y pasar a un análisis de tipo matricial de factores interconectados, variables y condiciones**. Esto constituye un reto importante para muchas organizaciones que intentan proteger su infraestructura, sus operaciones y datos contra adversarios más poderosos, mejor equipados y con más recursos.

Tendencias emergentes

_Diez retos para la ciberseguridad

01_Enfrentarse a riesgos sistémicos y complejos. El riesgo cibernético se caracteriza por la velocidad y por la escala de su propagación, así como por la intención potencial de los agentes de la amenaza. La interconexión de varios sistemas y redes permite que los incidentes informáticos se propaguen de forma rápida y amplia, lo que hace que sea más difícil evaluarlos y mitigarlos.

02_Difusión de la detección de IA adversaria.
La detección de amenazas que explotan la IA para lanzar ataques o evitar ser detectados constituirá un reto importante para los sistemas de defensa cibernéticos futuros.[14]

03_Reducción de errores accidentales.
Con el aumento del número de sistemas y dispositivos conectados a la red, los errores accidentales siguen siendo una de las vulnerabilidades más explotadas en los incidentes de ciberseguridad. Las nuevas soluciones para reducir estos errores serán una contribución importante para reducir el número de incidentes.

04_Amenazas a la cadena de suministro y terceros.
La cadena de suministro diversificada que caracteriza al sector de la tecnología actual proporciona nuevas oportunidades a los atacantes para aprovechar estos complejos sistemas y explotar las diversas vulnerabilidades introducidas por un ecosistema heterogéneo de terceros proveedores.[16]

05_Organización y automatización de la seguridad.
La inteligencia de las ciberamenazas y el análisis del comportamiento ganarán importancia con la automatización de los procesos y de los análisis. Invertir en automatización y organización permitirá
a los profesionales de la ciberseguridad invertir
en estrategias de ciberseguridad más robustas.

06_Reducción de los falsos positivos. Esta promesa esperada desde hace tiempo es clave para el futuro de la industria de la ciberseguridad y para la lucha contra el «hartazgo causado por las alarmas».

07_Estrategias de seguridad de confianza cero. Al haber un aumento de la presión sobre los sistemas informáticos impuesto por los nuevos requisitos comerciales, como el teletrabajo, la digitalización del modelo de empresa y la expansión de los datos, muchos encargados de la toma de decisiones ven la confianza cero como una solución práctica para proteger los activos corporativos.

08_Errores de migración a la nube de la empresa. El traslado de los datos de muchas empresas a soluciones basadas en la nube hará que aumente el número de errores de configuración, lo que, a su vez, expondrá los datos a posibles filtraciones. Los proveedores de servicios en la nube abordarán el problema implementando sistemas que identifiquen estos tipos de errores automáticamente.

09_Amenazas híbridas. Los nuevos *modi operandi* adoptan amenazas mundiales virtuales y físicas. La propagación de desinformación o noticias falsas, por ejemplo, son un elemento fijo del panorama de amenazas híbrido. El EUvsDisinfo[15] es un proyecto insignia del grupo operativo del Servicio de Acción Externa Europeo en el Este StratCom establecido para abordar la amenaza de la desinformación.

10_Aumentará el atractivo de la infraestructura en la nube como objetivo. El aumento de la dependencia en infraestructuras públicas en la nube aumentará el riesgo de apagones. La configuración errónea de los recursos en la nube sigue siendo la causa principal de los ataques a esta infraestructura, pero los ataques dirigidos directamente a los proveedores de servicios en la nube están ganando popularidad entre los piratas informáticos.

Tendencias emergente

Gasto en ciberseguridad

Según Gartner[17], muchas juntas directivas exigirán mejores datos y mejor conocimiento de los beneficios tras años de fuertes inversiones en ciberseguridad. Esto se debe principalmente a un aumento del gasto en ciberseguridad que es proporcional a la inversión en nuevas tecnologías. Según un informe de IDC[22], el gasto en ciberseguridad llegó a los 103 000 millones de dólares estadounidenses (aprox. 87 500 millones EUR) en 2019, un 9,4 % más que lo gastado el año anterior. Los encargados de la seguridad pronto serán objeto de escrutinio en relación a los resultados obtenidos durante años de inversión y son esenciales para mantener mejores datos sobre los resultados obtenidos.

La inteligencia sobre las ciberamenazas ayudará a definir las estrategias de ciberseguridad

La inteligencia sobre las ciberamenazas (CTI)[7] intenta ayudar a las organizaciones a prepararse mejor mejorando su conocimiento sobre el panorama de amenazas. En vez de depender exclusivamente de la información generada por sistemas o canales internos (lo que se sabe sobre lo conocido) la eficacia de la CTI se determinará por el conocimiento sobre el *porqué*, el *cómo* y el *qué* que desconoce el equipo de ciberseguridad. La propuesta de valor de cualquier capacidad o programa de CTI es mejorar la preparación de la organización a fin de proteger sus activos vitales de las amenazas desconocidas.

Conocer el panorama de amenazas

Con más automatización y organización de la ciberseguridad como tendencia al alza, **los equipos de ciberseguridad dedicarán menos tiempo a vigilar actividades y más a las tareas de preparación y disponibilidad**. Una capacidad de CTI bien diseñada ofrecerá conocimiento contextualizado y viable sobre las amenazas para informar a las partes interesadas estratégicas, operativas y tácticas de toda la organización. En términos prácticos, una capacidad de CTI debería tener como objetivo responder a las siguientes cuestiones relacionadas con los requisitos de las partes interesadas y con el contexto y entorno de la organización:

- ¿Cuál es la superficie de ataque?
- ¿Cuál es el activo más valioso en términos cibernéticos?
- ¿Cuáles son las vulnerabilidades más críticas?
- ¿Cuáles son los vectores de ataque más usados?
- ¿Cómo se comportan y operan normalmente los adversarios?
- ¿Qué aspecto presenta el panorama de amenazas para:
    - el sector y el tipo de negocio que opera la organización?
    - el entorno tecnológico adoptado por la organización?
- ¿Quién tiene que actuar y qué se tiene que hacer para mitigar el riesgo que implican estas amenazas?

Falta de capacidades en ciberseguridad

La falta de profesionales con altas capacidades tecnológicas ya es un problema para la ambición de digitalización de Europa. Según un estudio[23], la falta de capacidades está dificultando las estrategias inversoras de más del 70 % de las firmas europeas; un 46 % de las firmas declara tener dificultades para cubrir puestos de trabajo debido a la falta de mano de obra cualificada en áreas clave como la ciberseguridad.

Tendencias emergentes

_Cinco tendencias con ciberamenazas

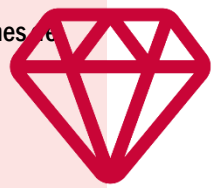
01_El *malware* se actualiza. Las variantes de las familias de *malware* se están actualizando para crear nuevas versiones con funciones y mecanismos de distribución y propagación adicionales. Por ejemplo, Emotet, un programa de *malware* diseñado inicialmente en 2014 como troyano para el sector bancario, se ha convertido ahora en uno de los distribuidores de *malware* más eficaces de 2019.[2]

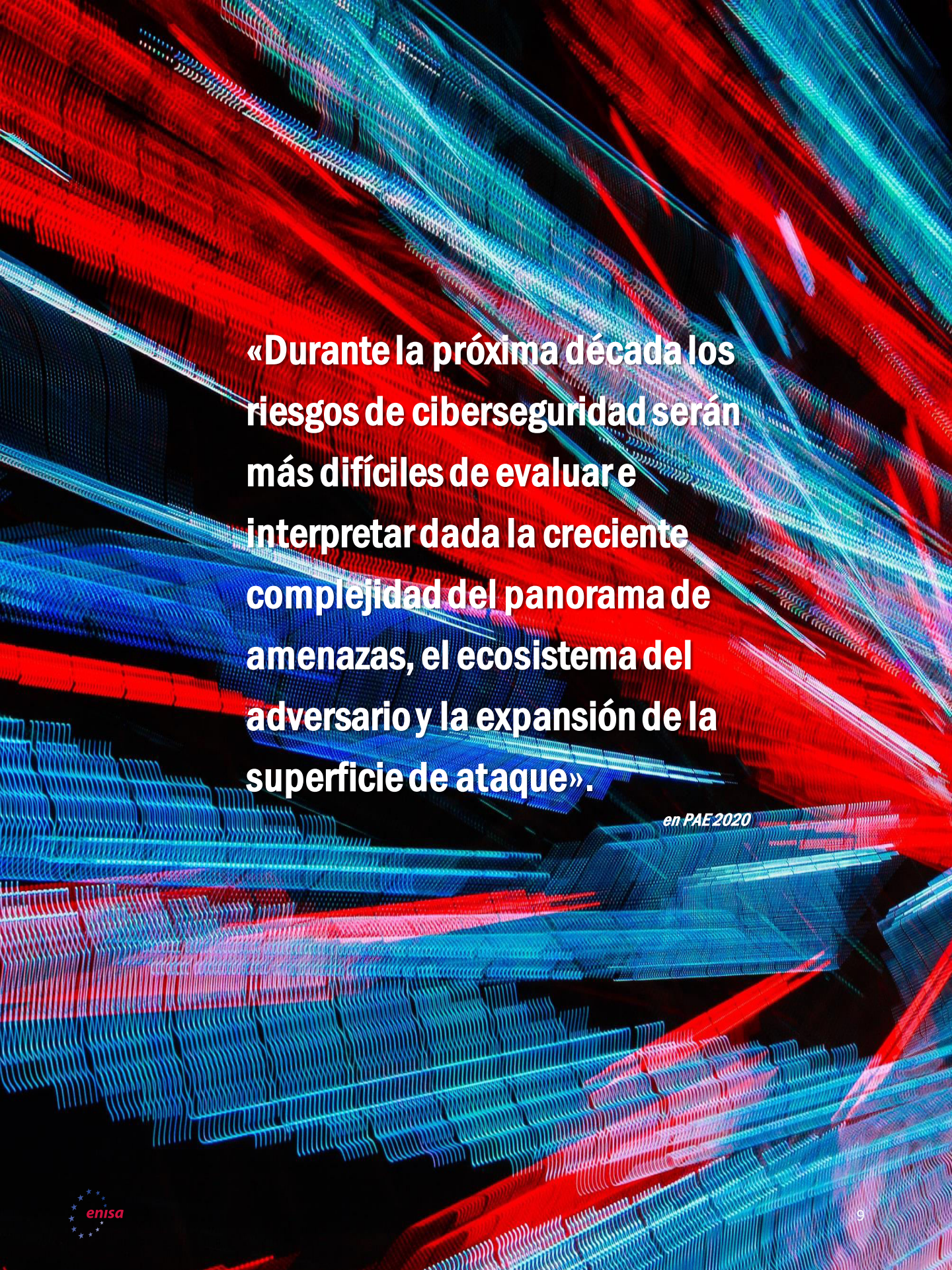
02_Las amenazas pasarán a ser totalmente móviles. Los usuarios dependen cada vez más de sus dispositivos móviles para proteger sus cuentas más sensibles. Uno de los ejemplos es el uso de 2fa (autenticación de dos factores) asociado a un autenticador de aplicación o a través de un mensaje de texto. A medida que el *malware* se va haciendo completamente móvil, las aplicaciones fraudulentas, el *SIMJacking* y los programas intrusos que afectan a los sistemas operativos convierten a estos dispositivos en el eslabón más débil y, por lo tanto, los hacen totalmente vulnerables a los ataques.

03_Los atacantes utilizan nuevos tipos de archivos, como los archivos de imagen de disco (ISO y IMG) para propagar *malware*. Los archivos DOC, PDF, ZIP y XLS siguen siendo los adjuntos más usados para propagar el *malware*, pero hay otros tipos que están ganando popularidad. En 2019 se vio que unas cuantas campañas de distribución de AgentTesla InfoStealer y NanoCore RAT utilizaban el tipo de archivo de imagen.

04_Aumento de los ataques de *ransomware* coordinados y dirigidos. En 2019 se observó un aumento de los programas intrusos de *ransomware* más sofisticados y dirigidos principalmente a organizaciones del sector público y sanitarias, y a industrias específicas. Los atacantes dedican más tiempo a recopilar inteligencia sobre las víctimas, saben exactamente qué encriptar, y consiguen perturbaciones máximas y rescates más altos.

05_Los ataques de robo masivo de credenciales serán algo generalizado. El robo masivo de credenciales (la inyección automatizada de combinaciones de nombres de usuarios o contraseñas a través de solicitudes de apertura de sesión a larga escala, dirigidas contra una aplicación *web*) proliferará como resultado de una década con un número anómalo de filtraciones de datos y billones de registros de datos personales robados.




«Durante la próxima década los riesgos de ciberseguridad 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

Tendencias emergentes

Diez tendencias emergentes en los vectores de ataque

01_ Los ataques se distribuirán de forma masiva en un corto intervalo de tiempo y con un impacto más amplio

La intención de estos ataques es afectar al número más alto de dispositivos posible para robar datos personales o bloquear el acceso a los datos al encriptar los archivos.

02_ Los ataques serán persistentes, muy dirigidos y planificados meticulosamente, y con objetivos bien definidos y a largo plazo

Los atacantes planifican este tipo de ataques para conseguir datos de alto valor, como información financiera, información sobre la propiedad intelectual e industrial, secretos comerciales, información clasificada, etc.

03_ Los atacantes utilizarán las plataformas digitales en ataques dirigidos

Los atacantes explorarán el potencial de las plataformas digitales para apoyar sus ataques dirigidos (p. ej., redes sociales, plataformas de juego, mensajería, difusión en continuo, etc.). Las plataformas digitales con un gran número de suscriptores son vectores de ataque eficaces y cada vez más populares entre los atacantes para actividades que van desde el robo de datos personales para ataques aislados más específicos, como los de pesca con arpón (*spear-phishing*) a la amplia distribución de *malware*.

04_ Aumentará la explotación de los procesos comerciales

Con más automatización y menos intervención humana, los procesos de empresa pueden verse alterados de forma malintencionada para generar beneficios para un atacante. Es una técnica que se conoce como «compromiso de procesos de empresa» (Business Process Compromise, BPC) y que los especialistas en ingeniería de procesos suelen infravalorar debido a la falta de una evaluación de riesgos adecuada.

05_ La superficie de ataque seguirá expandiéndose

El correo electrónico ya no es la herramienta principal y única, ni el vector de ataque principal para los ataques de *phishing*. Los atacantes utilizan ahora otras plataformas para comunicarse y atraer a sus víctimas para que estas visiten páginas *web* comprometidas. Hay una nueva tendencia emergente que usa los SMS, WhatsApp, SnapChat y sistemas de mensajes de las redes sociales.

06_ Se explotará el teletrabajo a través de los dispositivos del hogar

Cada vez hay más personas que teletrabajan y conectan sus dispositivos a redes corporativas y esto aumenta el riesgo de abrir nuevos puntos de entrada a los atacantes. Con la pandemia de COVID-19 esta tendencia obligará a los responsables de los sistemas informáticos a ajustar sus políticas de seguridad y a hacer cambios urgentes en la infraestructura informática.

07_ Los atacantes estarán mejor preparados

Los atacantes seleccionarán a sus víctimas con cuidado y harán un reconocimiento de determinados empleados para dirigirse a estos mediante ataques muy específicos de *spear-phishing* para obtener credenciales que sirvan para atacar a la organización. Cuando los atacantes consiguen acceder a un equipo, pueden emplear herramientas de pruebas de penetración como Mimikatz para obtener y explotar credenciales con privilegios elevados.

08_ Las técnicas de confusión serán sofisticadas

Los atacantes innovan continuamente para lograr amenazas más eficaces y menos susceptibles de ser detectadas. El Anibus, un troyano bancario y bot de Android se ha estado distribuyendo haciéndose pasar por una aplicación inocua, principalmente a través de Google Play Store.[1]

09_ Aumentará la explotación automatizada de sistemas y aplicaciones sin actualizar

El aumento anómalo del tráfico de Telnet al puerto 445 observado en 2019 desveló la expansión de gusanos y programas intrusos, como Eternal Blue. Telnet, que ya solo se usa en el dominio de los dispositivos IdC, experimentó los volúmenes más altos durante ese período.

10_ Las ciberamenazas se mueven hacia la periferia

Los dispositivos periféricos se despliegan en las demarcaciones entre las redes interconectadas. Hemos visto que hay una tendencia en aumento con ataques dirigidos a estos dispositivos (como los enrutadores, conmutadores y cortafuegos) que está teniendo un impacto importante en las empresas y en el ecosistema digital conectado.

Bibliografía

1. "ISO/IEC 27032:2012". ISO. https://www.iso.org/standard/44375.html

2. "Triple Threat: Emotet Deploys TrickBot to Steal Data & Spread Ryuk." 2 de abril de 2019. Cybereason. https://www.cybereason.com/blog/triple-threat-emotet-deploys-trickbot-to-steal-data-spread-ryuk-ransomware

3. "Understanding the relationship between Emotet, Ryuk and TrickBot." 14 de abril de 2019. Intel471. https://blog.intel471.com/2020/04/14/understanding-the-relationship-between-emotet-ryuk-and-trickbot/

4. "Investigating WMI Attacks". 9 de febrero de 2019. SANS. https://www.sans.org/blog/investigating-wmi-attacks/

5. "RDP Abuse and Swiss Army Knife Tool Used to Pillage, Encrypt and Manipulate Data". 18 de diciembre de 2019. Bitdefender. https://labs.bitdefender.com/2019/12/rdp-abuse-and-swiss-army-knife-tool-used-to-pillage-encrypt-and-manipulate-data/

6. "Europe's huge privacy fines against Marriott and British Airways are a warning for Google and Facebook". 10 de julio de 2019. CNBC. https://www.cnbc.com/2019/07/10/gdpr-fines-vs-marriott-british-air-are-a-warning-for-google-facebook.html

7. "This is how we might finally replace passwords". 27 de mayo de 2019. C | Net. https://www.cnet.com/news/this-is-how-we-might-finally-replace-passwords/

9. "Authentication standards to help reduce the world's over-reliance on passwords." FIDO. https://fidoalliance.org/overview/

10. "How Much Cyber Sovereignty is Too Much Cyber Sovereignty?" 3 de octubre de 2019. Council on Foreign Relations. https://www.cfr.org/blog/how-much-cyber-sovereignty-too-much-cyber-sovereignty

11. "Conceptualising Cyber Arms Races". 2016. NATO. https://ccdcoe.org/uploads/2018/10/Art-10-Conceptualising-Cyber-Arms-Races.pdf

12. "Journalism, 'Fake News' and Disinformation: A Handbook for Journalism Education and Training" 2018. UNESCO. https://en.unesco.org/fightfakenews

13. "The Big Connect: How Data Science is Helping Cybersecurity". 12 de junio de 2019. Info Security Group. https://www.infosecurity-magazine.com/blogs/data-science-helping-cybersecurity-1/

14. "Are You Ready For The Age Of Adversarial AI? Attackers Can Leverage Artificial Intelligence Too". 9 de enero de 2020. Forbes. https://www.forbes.com/sites/forbestechcouncil/2020/01/09/are-you-ready-for-the-age-of-adversarial-ai-attackers-can-leverage-artificial-intelligence-too/#2a76dee14703

15. https://euvsdisinfo.eu/

16. "FBI Alerts Companies of Cyber Attacks Aimed at Supply Chains". 21 de febrero de 2020. Bitsight. https://www.bitsight.com/blog/fbi-alerts-companies-of-cyber-attacks-supply-chains

17. "Gartner Identifies the Top Seven Security and Risk Management Trends for 2019". 5 de marzo de 2019. Gartner. https://www.gartner.com/en/newsroom/press-releases/2019-03-05-gartner-identifies-the-top-seven-security-and-risk-ma

18. "Android banking trojan." 3 de octubre de 2019. Cyare. https://cyware.com/news/exploring-the-nature-and-capabilities-of-anubis-android-banking-trojan-6ea7dec4

19. "5 Top Trends for Mobile Cyber Security in 2020". 9 de enero de 2020. Corrata. https://corrata.com/5-top-trends-for-mobile-cyber-security-in-2020/

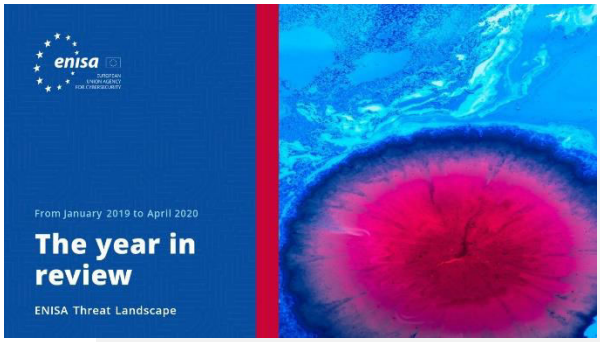
20. "Malicious Attachments Remain a Cybercriminal Threat Vector Favorite". 27 de agosto de 2020. Threat Post. https://threatpost.com/malicious-attachments-remain-a-cybercriminal-threat-vector-favorite/158631/

21. "10 trends shaping the future of work". Octubre de 2019. EPSC. https://op.europa.eu/en/publication-detail/-/publication/e77a1580-0cf5-11ea-8c1f-01aa75ed71a1/language-en/format-PDF/source-121729338

22. "Global security spending to top $103 billion in 2019, says IDC", 20 de marzo de 2019. ZDNet. https://www.zdnet.com/article/global-security-spending-to-top-103-billion-in-2019-says-idc/

23. "Insights into skills shortages and skills mismatch. learning from Cedefop's European skills and jobs survey". 2018. CEDEFOP. https://www.cedefop.europa.eu/files/3075_en.pdf

Lecturas



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

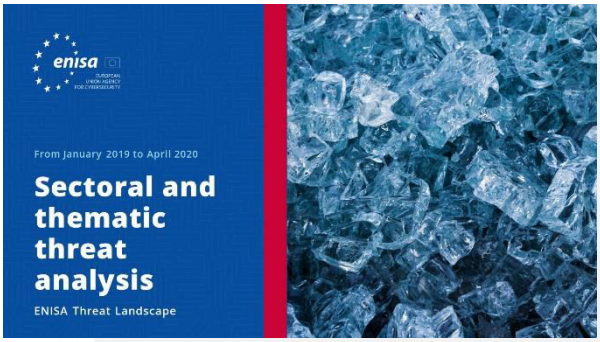
Informe Panorama de Amenazas de la ENISA
Lista de las 15 amenazas principales

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.



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 **Tendencias emergentes**

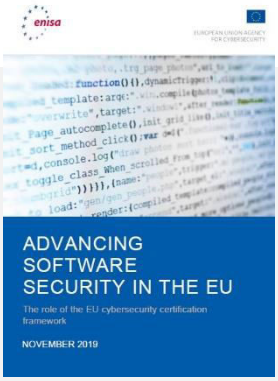
Principales tendencias en ciberseguridad observadas entre enero de 2019 y abril de 2020.

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.

Otras publicaciones



Avance de la seguridad del software en la UE

Presenta elementos clave de seguridad de los programas informáticos y ofrece un resumen conciso de los planteamientos más relevantes existentes y de los estándares en el panorama de desarrollo de programas informáticos seguros.

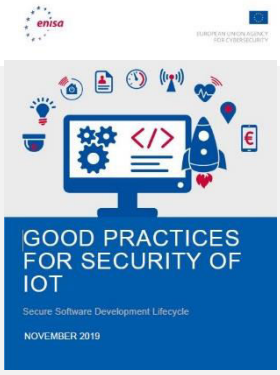
LEER EL INFORME

ENISA: buenas prácticas para la seguridad de los vehículos inteligentes

Buenas prácticas para la seguridad de los vehículos inteligentes, vehículos conectados y semiautónomos para mejorar la experiencia del usuario y mejorar la seguridad del vehículo.

.

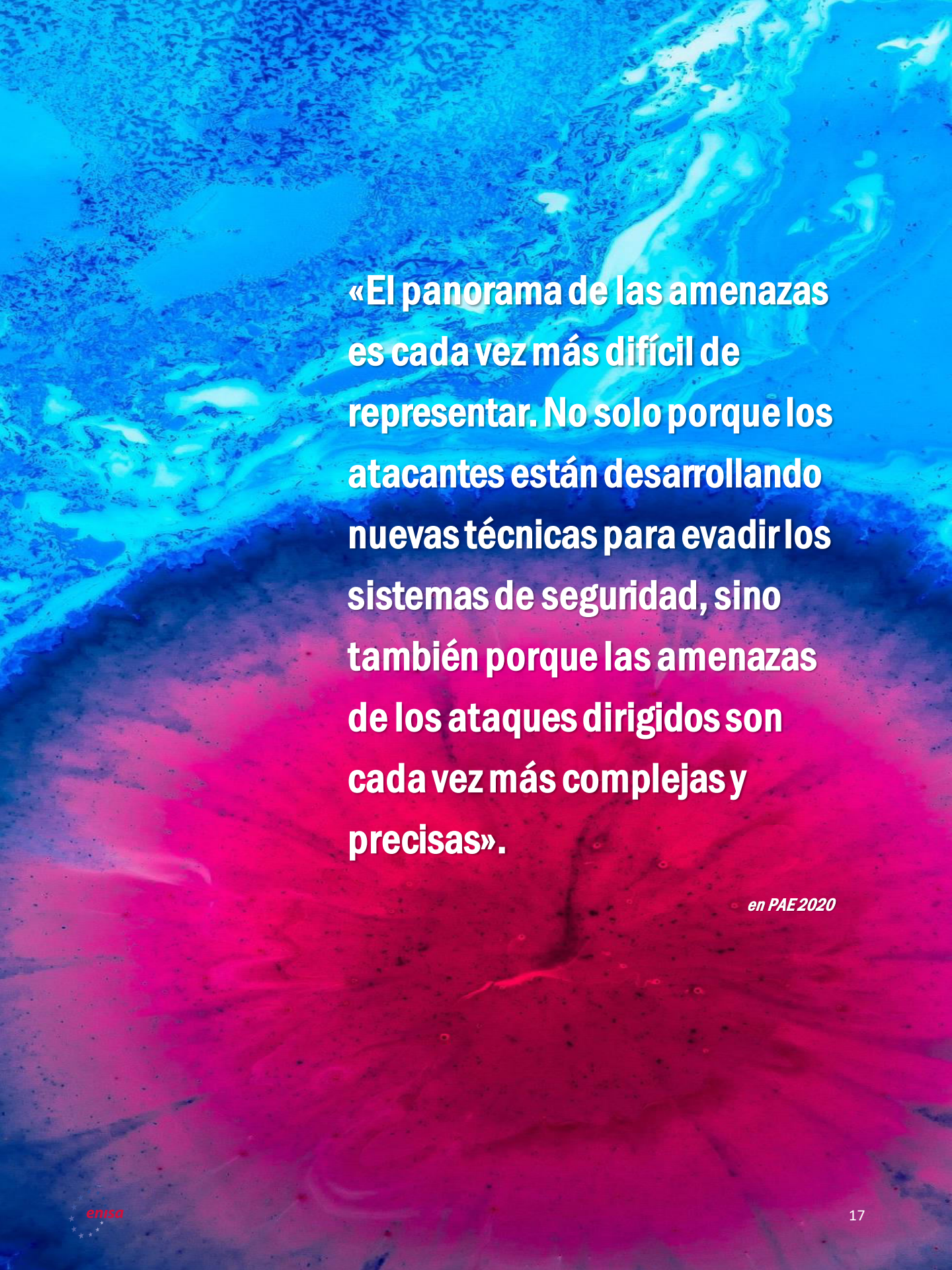
LEER EL INFORME



Buenas prácticas en la seguridad de IdC: ciclo de desarrollo de software seguro

Seguridad en IdC con un enfoque especial a las directrices de desarrollo de programas informáticos.

LEER EL INFORME


«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

¿Quiénes somos

La agencia

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

Colaboradores

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

Editores

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

Datos de contacto

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

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

Nos gustaría conocer su opinión sobre este informe

Le pedimos que dedique unos minutos a rellenar el cuestionario. Para acceder al cuestionario haga clic aquí.

Aviso legal

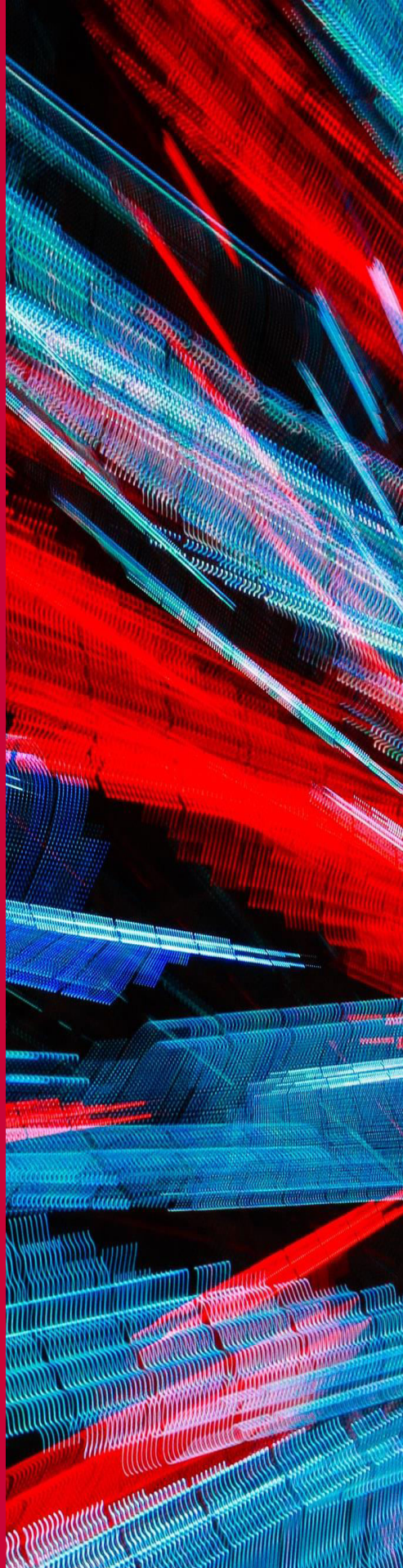
Salvo que se indique lo contrario, la presente publicación refleja las opiniones e interpretaciones de la ENISA. Esta publicación no constituye en ningún caso una medida legal de la ENISA ni de los organismos que la conforman, a menos que se adopte en virtud del Reglamento (UE) 526/2013. La información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

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

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

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