AGENCIA DE LA UNIÓN EUROPEA PARA LA CIBERSEGURIDAD

UNA EUROPA QUE OFRECE CIBERSEGURIDAD Y CONFIANZA

Estrategia de la ENISA

Junio de 2020

UNA EUROPA QUE OFRECE CIBERSEGURIDAD Y CONFIANZA

AGENCIA DE LA UNIÓN EUROPEA PARA LA CIBERSEGURIDAD

PRÓLOGO

Durante más de quince años, la Agencia de la Unión Europea para la Ciberseguridad (ENISA) ha desempeñado un papel fundamental al favorecer la aspiración de la UE de reforzar la seguridad y la confianza digitales en toda Europa, junto con los Estados miembros y las instituciones y agencias de la UE. Al unir a las comunidades, la ENISA ha logrado contribuir a mejorar la preparación de Europa y su capacidad para responder a los incidentes cibernéticos.

Al mismo tiempo, la digitalización de nuestra economía y de la sociedad ha aumentado de forma drástica, tal y como se puso de manifiesto durante la crisis de la COVID-19, cuando el viraje, colectivo y masivo, al uso de soluciones informáticas remotas resultó ser esencial para que numerosas actividades pudiesen seguir funcionando. La crisis dio una idea de hasta qué punto los autores de los ciberataques se aprovechan de nuestra dependencia de estas tecnologías. También permitió ver en qué medida ha aumentado el panorama de las ciberamenazas, que han dejado de ser ataques específicos para convertirse en nuevas formas de amenazas masivas a millones de empresas y ciudadanos, entre las que se cuenta un número cada vez mayor de sofisticados incidentes de «ransomware» (programas de secuestro de archivos a cambio de un rescate). El rápido desarrollo de los servicios y los productos digitales, desde la nube y las videoconferencias hasta la tecnología 5G y la inteligencia artificial, ha acarreado también nuevos desafíos que es necesario detectar y afrontar.

Con su mandato permanente y el incremento de sus funciones y capacidades, la ENISA está, más que nunca, destinada a asumir el liderazgo para ayudar a la UE y a sus Estados miembros a encontrarse a la altura de estos desafíos, al tiempo que comienza una nueva era para la ciberseguridad en Europa.

Para ello, la ENISA trabajará con el fin de poder anticipar tendencias pertinentes, y reunirá y compartirá competencias técnicas avanzadas y conocimientos para todos. Apoyará a la Comisión Europea y a los Estados miembros en su esfuerzo por ayudar a los agentes públicos y privados y a la ciudadanía a evitar y a gestionar los riesgos asociados con los incidentes cibernéticos. Con la aplicación del marco de certificación de la ciberseguridad, la ENISA contribuirá a que se produzca un cambio de paradigma mejorando el nivel de seguridad de las soluciones digitales desplegadas en Europa. De este modo se mejorará la capacidad de todos para elegir y confiar. La Agencia apoyará asimismo activamente a la comunidad de gestión de la ciberseguridad de Europa colaborando estrechamente y preparándose para responder unidas cuando el próximo incidente cibernético a gran escala sacuda a Europa.

En este nuevo cometido de la ENISA, la transparencia, la agilidad y la fiabilidad constituirán factores clave en su funcionamiento diario, al tiempo que cooperará más estrechamente con los Estados miembros y la Comisión Europea para armonizar enfoques. La ENISA se esforzará asimismo por mejorar su impacto medioambiental en el contexto de la actual crisis climática y por ser una entidad socialmente responsable ofreciendo un entorno laboral integrador.

El presente documento estratégico, elaborado con la participación de toda la plantilla de la ENISA, los miembros de su Consejo de Administración y su Grupo Consultivo en un proceso colaborativo e inclusivo, establece los objetivos claros que guiarán el trabajo de la ENISA en los próximos años para poder afrontar los numerosos desafíos futuros.

En nombre del Consejo de Administración

Jean-Baptiste Demaison
Presidente del Consejo de Administración

Krzysztof Silicki
Vicepresidente del Consejo de Administración

VISIÓN

Una Europa que ofrece ciberseguridad y confianza

MISIÓN

La misión de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) es lograr un elevado nivel común de ciberseguridad en toda la Unión en cooperación con la comunidad general. Para ello, actúa como un centro de conocimiento especializado en materia de ciberseguridad, reuniendo y ofreciendo asistencia y asesoramiento técnico independiente y de alta calidad a los Estados miembros y órganos de la UE sobre ciberseguridad. Contribuye al desarrollo y a la aplicación de las políticas de la Unión en materia de cibernética.

Nuestro objetivo es reforzar la confianza en la economía conectada, impulsar la resiliencia y la confianza en la infraestructura y los servicios de la Unión y proteger digitalmente a nuestra sociedad y a nuestra ciudadanía. Aspiramos a ser una organización activa, responsable desde el punto de vista medioambiental y social y centrada en las personas.

VALORES

Mentalidad de comunidad
La ENISA trabaja con las comunidades, respetando sus competencias y conocimientos técnicos, y fomenta las sinergias y la confianza para lograr sus objetivos de la mejor manera posible.

Excelencia
La ENISA procura disponer de los conocimientos técnicos más avanzados en su trabajo, mantiene los más elevados niveles de calidad del funcionamiento y evalúa sus resultados para intentar mejorar continuamente a través de la innovación y la anticipación.

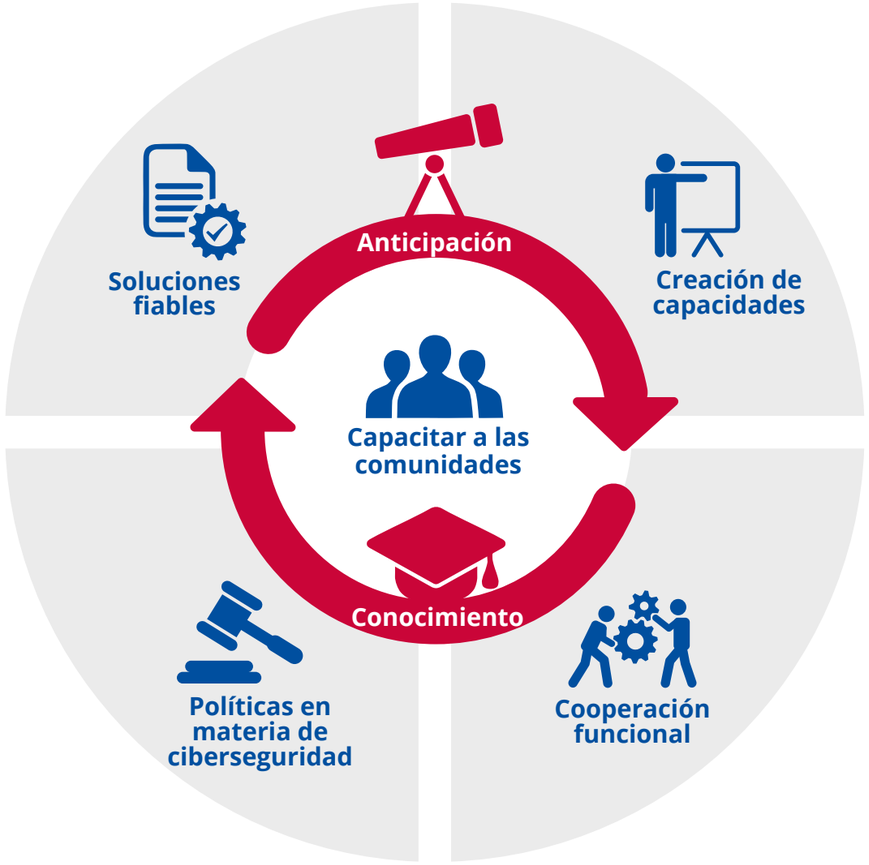
Integridad/ética
La ENISA defiende principios éticos y las obligaciones y normas de la UE pertinentes para sus servicios y su entorno de trabajo garantizando la equidad y la integración.

Respeto
La ENISA respeta los valores y los derechos fundamentales europeos que comprenden todos sus servicios y entorno de trabajo, así como las expectativas de sus partes interesadas.

Responsabilidad
La ENISA asume la responsabilidad garantizando de este modo la integración de las dimensiones social y medioambiental en prácticas y procedimientos.

Transparencia
La ENISA adopta procedimientos, estructuras y procesos abiertos, prácticos e independientes, reduciendo así el sesgo, la ambigüedad, el fraude y la opacidad.

OBJETIVOS ESTRATÉGICOS



OE1

Objetivo estratégico

COMUNIDADES CAPACITADAS E IMPLICADAS EN TODO EL ECOSISTEMA DE LA CIBERSEGURIDAD

Contexto

La ciberseguridad es una responsabilidad compartida. Europa aspira a conseguir un marco de cooperación transversal e integral. La ENISA desempeña un papel clave al estimular la cooperación activa entre las partes interesadas en la ciberseguridad de los Estados miembros y las instituciones y agencias de la UE. Trabaja para garantizar la complementariedad de los esfuerzos comunes, añadiendo valor a las partes interesadas, explorando sinergias y utilizando con eficacia los limitados recursos y conocimientos técnicos en materia de ciberseguridad. Debe capacitarse a las comunidades para ampliar el modelo de la ciberseguridad.

Qué queremos lograr

- Un corpus de conocimientos avanzados a escala de toda la UE sobre prácticas y conceptos de ciberseguridad que genere cooperación entre los agentes principales en materia de ciberseguridad, fomente las enseñanzas extraídas y los conocimientos técnicos de la UE y cree nuevas sinergias.
- Un ecosistema cibernético capacitado que comprenda todas las autoridades de los Estados miembros, instituciones, agencias y organismos de la UE, asociaciones, centros de investigación y universidades, industria, agentes privados y ciudadanos, ya que todos ellos desempeñan un papel para garantizar la ciberseguridad en Europa.

OE2

Objetivo estratégico

LA CIBERSEGURIDAD: UN ELEMENTO ESENCIAL DE LAS POLÍTICAS DE LA UE

Contexto

La ciberseguridad es la piedra angular de la transformación digital y una necesidad que es transversal a todos los sectores, por lo que resulta necesario tenerla en consideración en una amplia serie de iniciativas y ámbitos políticos. La ciberseguridad no debe limitarse a una comunidad especializada de expertos técnicos en cibernética. Deberá estar integrada en todos los ámbitos de las políticas de la UE. Resulta esencial evitar la fragmentación y contar con un enfoque coherente teniendo en cuenta al mismo tiempo las especificidades de cada sector.

Qué queremos lograr

- Apoyo y asesoramiento proactivo a todos los agentes pertinentes a escala de la UE integrando la dimensión de la ciberseguridad en el ciclo de la elaboración de políticas a través de directrices técnicas factibles y específicas.
- Marcos de gestión de los riesgos de la ciberseguridad en vigor en todos los sectores, supervisados a lo largo de todo el ciclo de la política en materia de ciberseguridad.

OE3

Objetivo estratégico

COOPERACIÓN EFICAZ ENTRE LOS AGENTES OPERATIVOS DENTRO DE LA UNIÓN EN CASO DE INCIDENTES CIBERNÉTICOS MASIVOS.

Contexto

Solo se podrán alcanzar los beneficios que comportan la sociedad y la economía digitales europeas en su totalidad si se cumple la premisa de la ciberseguridad. Los ciberataques no conocen fronteras. Pueden afectar a todas las capas de la sociedad y la Unión tiene que estar preparada para responder a las crisis cibernéticas y los ciberataques masivos (a gran escala y transfronterizos). Las interdependencias transfronterizas han puesto de relieve la necesidad de que exista una cooperación eficaz entre los Estados miembros y las instituciones de la UE para lograr una respuesta más rápida y la debida coordinación de los esfuerzos a todos los niveles (estratégico, operativo, técnico y comunicativo).

Qué queremos lograr

- Apoyo transfronterizo y transversal continuado a la cooperación entre los Estados miembros así como con las instituciones de la UE. Concretamente, debido a la posibilidad de que se produzcan crisis e incidentes de gran escala, apoyo a la ampliación de la cooperación técnica operativa, política y estratégica entre los agentes operativos clave para permitir respuestas rápidas, intercambio de información, conocimiento de la situación y comunicación de las crisis en toda la Unión.
- Intervención técnica rápida y exhaustiva previa solicitud de los Estados miembros para atender a las necesidades técnicas y operativas en la gestión de incidentes y crisis.

OE4

Objetivo estratégico

CAPACIDADES Y COMPETENCIAS PUNTERAS EN CIBERSEGURIDAD EN TODA LA UNIÓN

Contexto

La frecuencia y la sofisticación de los ciberataques aumenta a gran velocidad, al tiempo que las personas, las organizaciones y las industrias hacen cada vez mayor uso de tecnologías e infraestructuras de TIC. Las necesidades de competencias y conocimientos en materia de ciberseguridad superan la oferta. La UE tiene que invertir en crear competencias y talentos en ciberseguridad a todos los niveles, desde el lego hasta el profesional altamente cualificado. Las inversiones no deberían centrarse solamente en incrementar la capacitación en materia de ciberseguridad en los Estados miembros, sino también en garantizar que las diferentes comunidades operativas posean la capacidad adecuada para abordar el panorama de las amenazas cibernéticas.

Qué queremos lograr

- Estructuras educativas, experiencia profesional y competencias en materia de ciberseguridad armonizadas para atender a las necesidades, en constante aumento, de competencias y conocimientos sobre ciberseguridad en la UE.
- Un buen nivel básico de competencias y conocimientos en materia de ciberseguridad en toda la UE incorporando al mismo tiempo la cibernética en nuevas disciplinas.
- Buena preparación y competencias probadas con la capacidad adecuada para gestionar el entorno de las amenazas en constante evolución en toda la UE.

OE5

Objetivo estratégico

ALTO NIVEL DE CONFIANZA EN SOLUCIONES DIGITALES SEGURAS

Contexto

Los servicios y productos digitales comportan tanto beneficios como riesgos, y estos últimos han de ser detectados y mitigados. En el proceso de evaluar la seguridad de las soluciones digitales y garantizar su fiabilidad, resulta esencial adoptar un enfoque común, con el objetivo de encontrar un equilibrio entre las necesidades de la sociedad, el mercado, la economía y la ciberseguridad. Una organización neutra que actúe de forma transparente aumentará la confianza de los clientes en las soluciones digitales y el entorno digital en general.

Qué queremos lograr

- Un entorno digital seguro desde el punto de vista cibernético en toda la UE, donde los ciudadanos puedan confiar en los procesos, servicios y productos de TIC, a través de la aplicación de programas de certificación en ámbitos tecnológicos clave.

OE6

Objetivo estratégico

PREVISIÓN DE DESAFÍOS PARA LA SEGURIDAD EMERGENTES Y FUTUROS

Contexto

Numerosas tecnologías nuevas, tanto las más recientes como las que pronto se adoptarán de forma generalizada, se beneficiarían de la utilización de métodos de previsión. A través de un proceso estructurado que permita el diálogo entre las partes interesadas, los responsables políticos podrían definir estrategias de mitigación temprana que mejorasen la resiliencia de la UE frente a las amenazas para la ciberseguridad y hallasen soluciones para abordar los desafíos emergentes.

Qué queremos lograr

- Comprender los patrones y las tendencias emergentes utilizando escenarios futuros y prospectivos que contribuyan a mitigar los desafíos cibernéticos de nuestras partes interesadas.
- Realizar una evaluación inicial de los retos y los riesgos que comporta la adopción de las opciones futuras emergentes, y la adaptación a estas, colaborando al mismo tiempo con las partes interesadas en estrategias adecuadas de mitigación.

OE7

Objetivo estratégico

GESTIÓN EFICAZ Y EFICIENTE DE LOS CONOCIMIENTOS Y DE LA INFORMACIÓN SOBRE CIBERSEGURIDAD PARA EUROPA

Contexto

El combustible que alimenta la máquina de la ciberseguridad es la información y el conocimiento. A fin de lograr que los profesionales de la ciberseguridad puedan perseguir nuestros objetivos de un modo eficaz, trabajar en un entorno en constante cambio (en términos de avances digitales y en relación con los agentes) y afrontar los retos de nuestro tiempo, necesitamos un proceso continuo de recogida, organización, resumen, análisis, comunicación y mantenimiento del conocimiento y la información sobre ciberseguridad. Todas las fases resultan esenciales para garantizar que la información y el conocimiento se compartan y se expandan dentro del ecosistema de la ciberseguridad de la UE.

Qué queremos lograr

- La gestión compartida de la información y el conocimiento para el ecosistema de la ciberseguridad en la UE en una forma accesible, personalizada, oportuna y aplicable, con la metodología, las infraestructuras y las herramientas adecuadas acompañadas de métodos de garantía de la calidad con el objetivo de mejorar continuamente los servicios.

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 fortalecida por el Reglamento sobre la Ciberseguridad de la UE, la Agencia de la Unión Europea para la Ciberseguridad 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 futuros en materia de cibernética. 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. Más información sobre la ENISA y su labor en www.enisa.europa.eu.

TP-02-20-759-ES-N

ENISA
Agencia de la Unión Europea para la Ciber-seguridad

Oficina de Atenas
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Grecia

Oficina de Heraklion
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Grecia

enisa.europa.eu