ENTHEC

kartos©

Corporate Threat Watchbots

# Objetivo Resiliencia

Buenas prácticas, claves y cumplimiento de la NIS 2

kartos®

# Índice

PAG.

# INTRODUCCIÓN

Hace ya más de una década, la Unión Europea fue consciente de la necesidad de elaborar un marco legal común sobre Ciberseguridad que estableciese la base de una estrategia compartida por los Estados miembros para luchar unidos contra la ciberdelincuencia.

Fruto de esta necesidad nació la Directiva Europea NIS 1 (Directiva sobre la Seguridad de las Redes y de la Información), que fue adoptada en 2016 por la Unión Europea (UE) con el objetivo de mejorar la Ciberseguridad en Europa y establecer un marco de cooperación entre los Estados miembros para proteger las infraestructuras críticas y los servicios digitales. Esta directiva marcó un hito en la legislación de ciberseguridad al establecer normas mínimas de seguridad cibernética a nivel europeo y promover una mayor resiliencia frente a ciberataques.

La NIS 1 buscaba garantizar la protección de los servicios esenciales, como la energía, el transporte, la salud, las telecomunicaciones y los servicios financieros, así como de los proveedores de servicios digitales, los motores de búsqueda, las plataformas de comercio en línea y los servicios en la nube. Los Estados miembros debían identificar los operadores de servicios esenciales y los proveedores de servicios digitales y garantizar que implementaran medidas adecuadas para gestionar los riesgos de ciberseguridad y notificaran incidentes significativos.

# INTRODUCCIÓN

Sin embargo, a medida que la tecnología y las ciberamenazas evolucionaron rápidamente, la Directiva NIS 1 se quedó obsoleta y resultó insuficiente para abarcar la creciente complejidad del cibercrimen.

Para solucionar estas deficiencias y actualizar el marco legal, la UE ha elaborado la Directiva NIS 2, una nueva Directiva sobre Ciberseguridad que amplía y mejora los aspectos clave de su predecesora.

En este documento analizamos el nuevo marco legal europeo en Ciberseguridad y qué aspectos clave revela como ejes de la actualización de la estrategia de Ciberseguridad común de todos los Estados miembros. Una guía para inspirar la renovación de la estrategia de cualquier organización y para abordar los retos de seguridad provocados por a las amenazas emergentes.

### Alcance limitado

La NIS 1 solo abarcaba ciertos sectores y provedores de servicios digitales, dejando fuera a otros servicios esenciales y tipos de empresas que cada vez son más vulnerables a ciberataques.

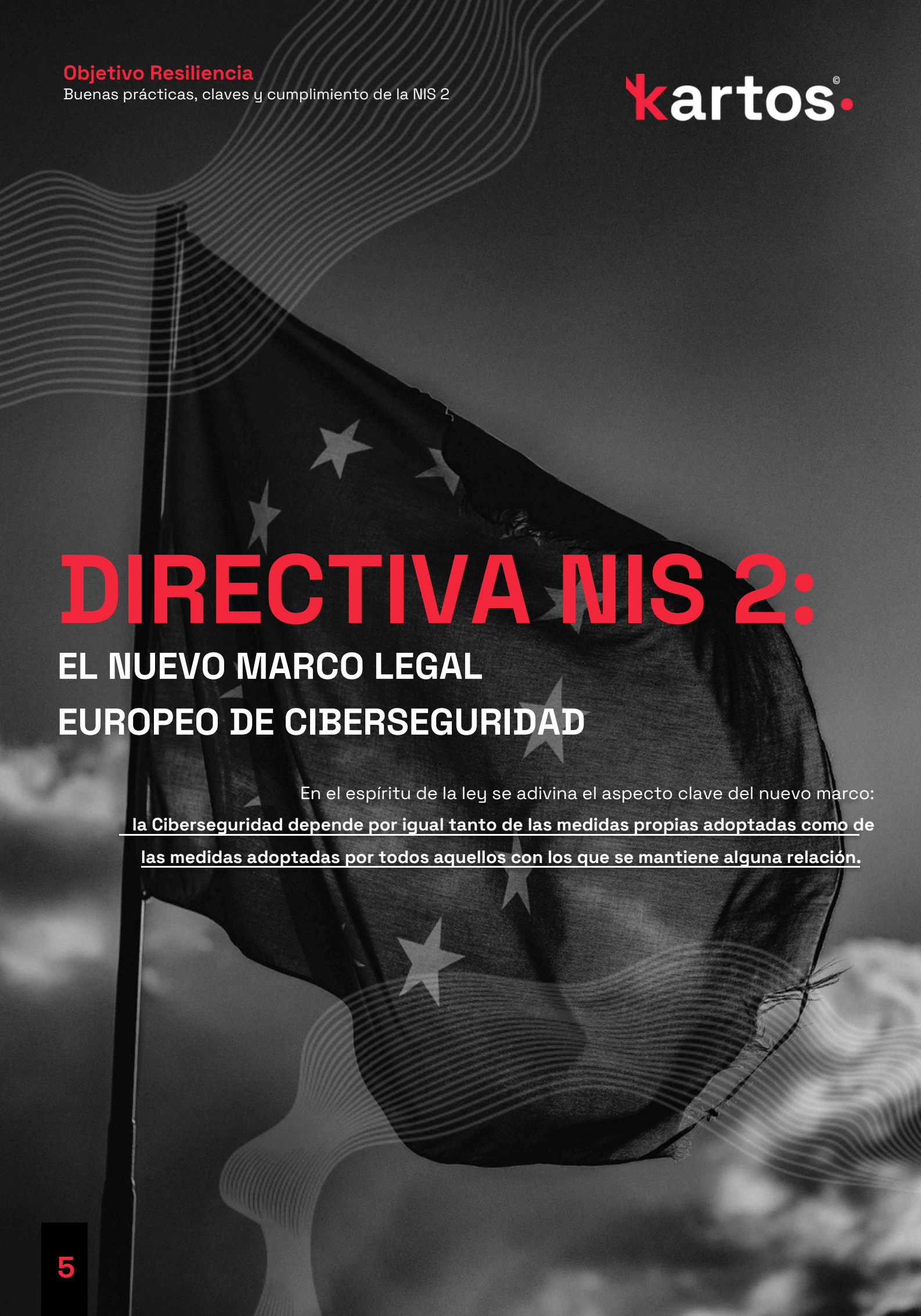
### Falta de armonización

La NIS 1 no logró unificar los enfoques de ciberseguridad entre los Estados miembros, debido a que dejaba la implantación de la mayoría de las medidas de seguridad a la voluntad de cada legislador nacional, lo que llevó a diferencias en la forma en la que se implementaron en toda la UE.

### Amenazas emergentes

Con el tiempo, han surgido nuevas y más sofisticadas ciberamenzas, como el ransomware, los ataques de denegación de servicio distribuido (DDoS) y el robo de datos a gran escala, que la NIS 1 no abordaba con eficacia.

kartos©



# DIRECTIVA NIS 2:

## EL NUEVO MARCO LEGAL EUROPEO DE CIBERSEGURIDAD

En el espíritu de la ley se adivina el aspecto clave del nuevo marco: **la Ciberseguridad depende por igual tanto de las medidas propias adoptadas como de las medidas adoptadas por todos aquellos con los que se mantiene alguna relación.**

# DIRECTIVA NIS 2

## EL NUEVO MARCO LEGAL EUROPEO DE CIBERSEGURIDAD

Con la elaboración de la Directiva NIS 2, la Unión Europea busca superar las deficiencias de la NIS 1, ofreciendo un enfoque más amplio y armonizado para proteger de forma unificada las redes y la información en toda la Unión Europea frente a las crecientes y cambiantes amenazas.

La Directiva NIS 2 entró en vigor el 27 de diciembre de 2022, después de su publicación en el Diario Oficial de la Unión Europea. Hasta el 17 de octubre de 2024, los Estados miembros tienen plazo para realizar la transposición y adoptar y publicar las medidas necesarias para dar cumplimiento a lo establecido en la Directiva.

A partir de esa fecha, este nuevo marco legal sobre Ciberseguridad estará operativo y será obligatorio en toda la Unión Europea. El objetivo principal de la NIS 2 que inspira todas sus disposiciones es la unificación de la estrategia de Ciberseguridad entre Estados miembros mediante la definición de requisitos mínimos comunes y el establecimiento de mecanismos que garanticen una cooperación eficaz entre las autoridades de los Estados miembros.

# DIRECTIVA NIS 2

Para subsanar las deficiencias y obsolescencias presentadas por su antecesora, la Directiva NIS 2 incorpora como ejes principales de la normativa:

### AMPLIO ALCANCE

La NIS 2 amplía su ámbito para incluir a más sectores y servicios digitales, cubriendo una gama más amplia de empresas y servicios considerados esenciales para el funcionamiento de la sociedad.

### MAYOR ARMONIZACIÓN

La NIS 2 promueve una mayor armonización de las medidas de Ciberseguridad en toda la UE para garantizar un enfoque más coherente y uniforme en la protección de las infraestructuras críticas y los servicios digitales.

### ENFOQUE EN LA RESILIENCIA

La NIS 2 hace hincapié en la necesidad de que los Estados miembros y las empresas desarrollen capacidades para resistir y recuperarse rápidamente de los ciberataques, fortaleciendo así la ciberresiliencia en toda la UE.

### IMPULSO DE LA PROACTIVIDAD

La NIS 2 enfoca la Ciberseguridad en el control y la prevención de las amenazas y los riesgos, conminando a adelantarse a los ciberataques como medida principal para evitar sus consecuencias.

### NUEVAS AMENAZAS Y TECNOLOGÍAS

La NIS 2 tiene en cuenta las amenazas emergentes y las tecnologías en evolución, como la inteligencia artificial y el Internet de las cosas (IoT), y busca abordar los desafíos que presentan para la ciberseguridad.

### RIESGOS DE TERCEROS

La NIS 2 integra la obligación de controlar los riesgos de la cadena de suministro como uno de los ejes de la eficacia de cualquier estrategia de Ciberseguridad. La idea de que la Ciberseguridad ya no es asunto de uno, tanto a nivel de Estados, como a nivel de organizaciones, es el planteamiento clave que alimenta el desarrollo normativo. Esto implica que la NIS 2 tendrá, debido al efecto cascada, influencia en un número de organizaciones más amplio del estipulado en su articulado.

### RESPONSABILIDADES Y SANCIONES

Es muy importante la novedad de que, a partir de que la NIS 2 entre en vigor en los Estados miembros, los altos cargos y los equipos directivos podrán ser considerados personalmente responsables del incumplimiento de las NIS 2 por parte de su organización. Además, la NIS 2 establece para las entidades esenciales una multa por incumplimiento que podrá llegar hasta los 10 millones de euros o el 2% de la facturación anual mundial de la empresa. Para las entidades importantes, la multa podrá llegar hasta los 7 millones de euros o el 1,4% del volumen de negocios anual mundial.

# DIRECTIVA NIS 2:
## ÁMBITO DE APLICACIÓN DE LA DIRECTIVA

Se estima que este ámbito de aplicación será, en la práctica y como consecuencia del efecto cascada, mucho más amplio que el **estricto estipulado en la Directiva debido a la obligatoriedad de controlar el riesgo de la cadena de suministro** que impone a las empresas y sectores a los que se dirige.

# DIRECTIVA NIS 2

## ÁMBITO DE APLICACIÓN DE LA DIRECTIVA

El ámbito de aplicación de la Directiva NIS 2 es más amplio y completo que el de su predecesora.

La NIS 2 abarca diversos sectores y servicios digitales para garantizar una protección integral y coordinada contra las ciberamenazas en la Unión Europea.

El objetivo principal de ampliar el ámbito de aplicación de la Directiva NIS 2 es garantizar un enfoque más coherente y completo para proteger las redes y la información en toda la Unión.

Al incluir nuevos sectores, servicios y tecnologías, la Directiva busca abordar los desafíos actuales y futuros de manera más efectiva y fortalecer la ciberresiliencia en todo el territorio europeo.

El nuevo marco legal acaba con la voluntariedad en la implementación de las medidas, obligando a los Estados miembros a incluirla en su normativa nacional y a las empresas a controlar, gestionar y supervisar los riesgos y seguir mejorando la resiliencia y la capacidad de respuesta.

# DIRECTIVA NIS 2

## ÁMBITO DE APLICACIÓN DE LA DIRECTIVA

## ORGANIZACIONES OBLIGADAS

- **EMPRESAS:**
  Medianas y grandes empresas (más de 250 empleados y con un volumen de facturación anual de 50 millones de euros en adelante)

- **ADMINISTRACIÓN:**
  Todas las Administraciones Públicas (excepto Defensa o seguridad nacional, la seguridad pública, policía, poder judicial y los parlamentos y los bancos centrales).

## SECTORES CUBIERTOS

### ALTA CRITICIDAD

Once sectores considerados esenciales para el funcionamiento de la sociedad, de alta criticidad, a los que se aplica de forma obligatoria la normativa de la NIS 2: Energía, **Banca, Mercados Financieros, Sector Sanitario, Transporte, Infraestructura Digital, Aguas Potables, Aguas Residuales, Gestión Servicios TIC B2B, Espacio, Admin. Pública.**

### CRÍTICOS

Siete sectores considerados críticos para los que también las disposiciones de la Directiva NIS 2 serán será obligado cumplimiento: **Investigación, Química, Alimentación, Servicios Postales, Proveedores Digitales, Fabricación, Gestión de Residuos.**

**Directiva NIS 2**
ÁMBITO DE APLICACIÓN DE LA DIRECTIVA

kartos©

# DIRECTIVA NIS 2

## ÁMBITO DE APLICACIÓN DE LA DIRECTIVA

## Clasificación de Entidades

### ENTIDADES ESCENCIALES

Aquellas que pertenezcan a los sectores de alta criticidad que superen los límites máximos previstos, así como los prestadores cualificados de servicios de confianza y registros de nombres de dominio de primer nivel y proveedores de servicios de DNS, independientemente de su tamaño.

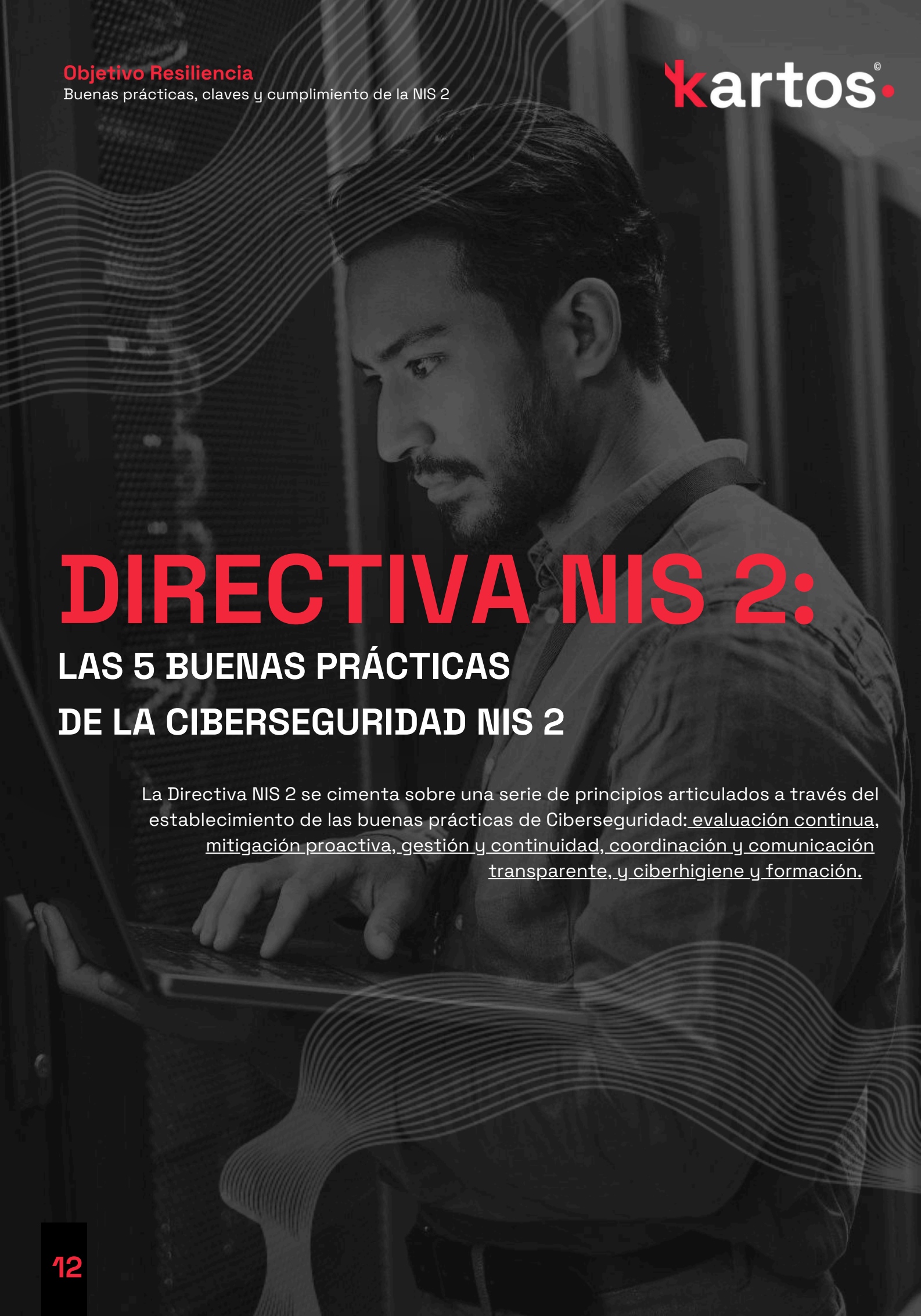
Proveedores de redes públicas de comunicaciones electrónicas o de servicios de comunicación electrónicos disponibles para el público que sean consideradas medianas empresas, entidades de la Administración pública, cualquier otra entidad perteneciente a otros sectores críticos que el Estado miembro identifique como entidad esencial, las entidades críticas identificadas por la Directiva CER, y, si así lo dispone el Estado miembro, las entidades identificadas como operadores de servicios esenciales en la anterior Directiva NIS 1.

Deberán cumplir con los requisitos de supervisión a partir de la introducción de NIS 2.

### ENTIDADES IMPORTANTES

Aquellas entidades que pertenezcan a los sectores de alta criticidad o a otros sectores críticos que no pueden considerarse entidades esenciales, como plataformas en línea, motores de búsqueda y servicios en la nube, entre otros.

Estarán sujetas a supervisión ex-post, lo que significa que se tomarán medidas cuando las autoridades tengan o reciban evidencias de incumplimiento.



# DIRECTIVA NIS 2:

## LAS 5 BUENAS PRÁCTICAS DE LA CIBERSEGURIDAD NIS 2

La Directiva NIS 2 se cimenta sobre una serie de principios articulados a través del establecimiento de las buenas prácticas de Ciberseguridad: evaluación continua, mitigación proactiva, gestión y continuidad, coordinación y comunicación transparente, y ciberhigiene y formación.

# DIRECTIVA NIS 2

## LAS 5 BUENAS PRÁCTICAS DE LA CIBERSEGURIDAD NIS 2

### Evaluación continua de riesgos y vulnerabilidades.

La evaluación continua de riesgos y vulnerabilidades asienta el enfoque proactivo y preventivo para fortalecer la Ciberseguridad en la UE y es la primera piedra de la construcción de la estrategia de Ciberseguridad. Implica desarrollar una estrategia corporativa de Ciberinteligencia que permita identificar y monitorizar las amenazas potenciales.

Todo ello, para evaluar su impacto y probabilidad de ocurrencia y analizar las debilidades en la estrategia de Ciberseguridad. Incluida en este principio, la Directiva determina la importancia de incluir en esta evaluación continua a la cadena de suministro y el riesgo de terceros, y establece su obligatoriedad.

### Mitigación proactiva de los riesgos y vulnerabilidades detectados.

La mitigación proactiva de riesgos y vulnerabilidades es un elemento central de la Directiva NIS 2, ya que se enfoca en prevenir y reducir el impacto de posibles ciberataques en lugar de simplemente responder a ellos después de que ocurran. Una vez detectados los riesgos y vulnerabilidades a través de la evaluación continua, deben adoptarse medidas de seguridad acordes a los niveles de riesgo identificados. Esto puede incluir la aplicación de controles de acceso más estrictos, la actualización regular de software y sistemas, el uso de cifrado de datos, el monitoreo activo de redes, la exigencia de remediación y scorings de Ciberseguridad a la cadena de suministro o la implementación de protocolos de seguridad robustos, entre otros. Es decir, hay que actuar antes de que el ataque se materialice para evitarlo o, al menos, evitar que tenga consecuencias.

## Gestión de crisis y continuidad del negocio.

El primer objetivo es evitar que el ciberataque ocurra, pero para el caso de que sea inevitable, la Directiva NIS 2 establece la necesidad de desarrollar procedimientos eficaces de gestión de crisis para garantizar la máxima continuidad operativa en caso de incidente. Las organizaciones están obligadas a elaborar planes y procedimientos de respuesta a incidentes bien definidos y a tenerlos testados y actualizados. Esto asegura que, en caso de un ciberataque o incidente de seguridad, exista una respuesta rápida y coordinada para mitigar el impacto y restaurar la operatividad normal del negocio lo antes posible.

- Desarrollo de un Plan de Gestión de Crisis detallado con designación de roles y responsabilidades, la secuencia de acciones a seguir y los protocolos de comunicación con la autoridad competente y las partes interesadas.
- Desarrollo de un Plan de Recuperación y Continuidad del Negocio detallado enfocado en las acciones para mantener o restablecer la operatividad dentro del plazo de tiempo admisible y garantizar la continuidad de los servicios esenciales.
- Realización de pruebas y simulacros para testar los planes,verificar su efectividad, familiarizar a los trabajadores con el procedimiento y detectar los puntos de mejora.
- Colaboración con las autoridades competentes para evitar la propagación y mejorar la respuesta al incidente.
- Evaluación post-incidente para analizar los fallos e identificar los puntos a mejorar o cambiar.

## Coordinación y comunicación rápida y transparente de los riesgos, vulnerabilidades e incidentes.

La Directiva NIS 2 estipula que las entidades están obligadas a notificar a las autoridades pertinentes cualquier incidente significativo que se produzca. Las entidades afectadas deberán seguir un procedimiento determinado:

- **Notificación inicial – Alerta temprana:** en un plazo de 24 horas desde que se haya tenido constancia del incidente la entidad deberá comunicarlo al CSIRT o, en su defecto, a la Autoridad Competente designada.

- Notificación intermedia – Actualización: pasadas 72 horas desde la detección del incidente, la entidad deberá actualizar el estado del incidente exponiendo una evaluación inicial.
- Notificación final – Presentación informe: en el plazo máximo de un mes después de la notificación del incidente, la entidad deberá presentar un informe final que recoja una descripción detallada del mismo (incluyendo gravedad, impacto, tipo de amenaza que haya provocado el incidente, medidas paliativas aplicadas y en curso y, si aplica, repercusiones transfronterizas).

Además, se promueve la comunicación continua, rápida y transparente en materia de Ciberseguridad tanto entre los Estados miembros, como entre las autoridades competentes y las organizaciones o entre las partes interesadas o potencialmente afectadas ya sea directa o indirectamente. Este intercambio de información sobre vulnerabilidades e incidentes debe ser rápido, abierto y transparente.

## Ciberhigiene y formación.

La Directiva NIS 2 se centra en aumentar la concienciación y las capacidades de los ciudadanos y las organizaciones de la Unión para protegerse contra las amenazas cibernéticas y contribuir a un entorno digital más seguro y resiliente.

- **Ciberhigiene:** Prácticas y hábitos de ciberseguridad que los usuarios deben seguir para proteger sus dispositivos y datos. Esto incluye el uso de contraseñas seguras y únicas, la actualización regular de software y aplicaciones, la activación de la autenticación de dos factores, la precaución al pinchar en enlaces o descargar archivos y el uso de redes wi-fi seguras.
- **Formación y concienciación** en ciberseguridad a los usuarios y al personal de las organizaciones. Las empresas son responsables en capacitar a sus empleados para identificar y reportar posibles incidentes de seguridad, así como para seguir los procedimientos de seguridad establecidos.
- **Educación:** La NIS 2 aboga por la inclusión de la ciberhigiene en los planes de estudio educativos. La enseñanza de habilidades básicas de seguridad cibernética desde una edad temprana es fundamental para formar una generación de usuarios más conscientes y seguros en el entorno digital.
- **Sensibilización pública** en la importancia de la ciberseguridad a través de campañas de concienciación y comunicación sobre temas de ciberseguridad.

kartos©

# DIRECTIVA NIS 2:

## ELEMENTOS CLAVE DE LA NIS 2

- INNOVACIÓN, IA Y AUTOMATIZACIÓN
- AMENAZAS EMERGENTES Y TECNOLOGÍAS AVANZADAS
- PROTECCIÓN DE DATOS
- CADENA DE SUMINISTRO
- FIGURA DEL CISO
- ORGANISMOS VINCULADOS

## INNOVACIÓN, IA Y AUTOMATIZACIÓN

La NIS 2 establece la obligación de los Estados miembros de fomentar el uso de toda tecnología innovadora, incluida la inteligencia artificial, que pueda mejorar la detección y la prevención de ciberataques, permitiendo que los recursos se desvíen de manera más eficaz hacia la lucha contra los mismos.
Para ello, se promoverán, dentro de las Estrategias Nacionales de Ciberseguridad, las actividades de investigación y desarrollo encaminadas a facilitar el uso de dichas tecnologías, en particular las relativas a herramientas automatizadas o semiautomatizadas en materia de Ciberseguridad, y, en su caso, el intercambio de datos necesarios para formar a los usuarios de esas tecnologías y mejorarlas.

## AMENAZAS EMERGENTES Y TECNOLOGÍAS AVANZADAS

La Directiva NIS 2 tiene en cuenta las ciberamenazas y las tecnologías en evolución, como la IA, el Internet de las cosas (IoT) y las redes 5G.

Esto asegura que la legislación esté actualizada y sea relevante para los desafíos actuales y futuros en el campo de la Ciberseguridad.

## PROTECCIÓN DE DATOS

La Directiva NIS 2 fomenta el pleno aprovechamiento de los principios de protección de datos desde el diseño y por defecto, así como de las medidas más avanzadas de seguridad y preservación de la intimidad, como la seudonimización y el cifrado, para la protección de los datos personales.

Además, establece que el uso de cualquier tecnología de Ciberseguridad, incluida la inteligencia artificial, debe cumplir el Derecho de la Unión en materia de protección de datos, incluidos los principios de protección de datos de exactitud, minimización de datos, equidad y transparencia, y de seguridad de datos, como el cifrado avanzado.

## ORGANISMOS VINCULADOS

**Autoridades Competentes:**
Designadas por cada Estado miembro, supervisarán las entidades a través de inspecciones, análisis de seguridad o auditorías.
**Punto de contacto único:**
Designado por cada Estado miembro, asegurará la cooperación transfronteriza entre todas las administraciones

## CADENA DE SUMINISTRO

La Directiva NIS 2 establece la obligación de hacer frente a los riesgos de ciberseguridad provenientes de la cadena de suministro de una entidad. La relación con los proveedores resulta especialmente importante debido a la prevalencia de incidentes en los que las entidades han sido víctimas de ciberataques y en los que agentes malintencionados han podido comprometer la seguridad de los sistemas de redes y de información de una entidad aprovechándose de las vulnerabilidades que afectan a productos y servicios de terceros. Las pequeñas y medianas empresas cada vez sufren más ataques contra las cadenas de suministro debido al menor rigor de sus medidas para la gestión de riesgos de ciberseguridad y de su gestión de los ataques y al hecho de que tienen unos recursos de seguridad limitados. Tales ataques a las cadenas de suministro no solo afectan a las pequeñas y medianas empresas y sus operaciones de forma aislada, sino que también pueden tener un efecto en cascada en el marco de ataques más importantes contra las entidades a las que han suministrado. Por ello, la Directiva conmina además a los Estados miembros a ayudar a las pequeñas y medianas empresas a hacer frente a los retos a los que se enfrentan en sus cadenas de suministro, a través de sus Estrategias Nacionales de Ciberseguridad.

## FIGURA DEL CISO

La Directiva NIS 2 establece la obligación de las empresas a las que va dirigida de contar con un Responsable de Seguridad, una persona debidamente cualificada y con dedicación exclusiva que gestione la Ciberseguridad corporativa y forme parte de la dirección. Representa una gran oportunidad para que los CISO refuercen su posición, ya que la NIS 2 introduce la noción de responsabilidad de la dirección en la gestión de los riesgos de ciberseguridad, así como fuertes sanciones para los infractores.

La NIS 2 obliga a las entidades esenciales y a las importantes a establecer un enfoque proactivo en la gestión de riesgos y la protección de datos y sistemas críticos que implica que el CISO adopte el papel de guía y líder enlas decisiones técnicas y de negocio que deban tomarse, así como de divulgador de las políticas de Ciberseguridad.

kartos©

**CSIRT:** Equipos de Respuesta a Incidentes de Seguridad Informática que prestarán asistencia a las entidades esenciales e importantes afectadas por cualquier incidente y difundirán alertas, avisos e información sobre ciberamenazas, vulnerabilidades e incidentes entre las entidades implicadas en la Directiva NIS 2.

**Red de CSIRT**: Formada por representantes de los CSIRTs y el Equipo de Respuesta a Emergencias Informáticas de las instituciones, órganos y organismos de la Unión (CERT-EU) para el intercambio de información de incidentes, amenazas...

**Grupo de Cooperación:** Formado por representantes de los Estados miembro, la Comisión y ENISA, proporcionará a las autoridades competentes orientación con la transposición y aplicación de la Directiva, desarrollará y ejecutará de políticas sobre divulgación coordinada de vulnerabilidades, y servirá para el intercambio de buenas prácticas e información relacionada con la aplicación de la Directiva, ciberamenazas, etc.

**Red europea de organizaciones de enlace para la crisis de ciberseguridad (EU-CyCLONe):** Formada por la Autoridades de Gestión de Crisis de Ciberseguridad de los Estados miembros y la Comisión, tendrá un papel de observador en caso de ciberincidentes susceptibles de tener un impacto significativo en los servicios y actividades incluidos en la Directiva NIS 2, sirviendo de respaldo en la gestión coordinada de los incidentes y crisis de Ciberseguridad a gran escala.

kartos©

# DIRECTIVA NIS 2:

## CUMPLIMIENTO DE LA NIS 2: VENTAJAS DE LA MONITORIZACIÓN DE LA SUPERFICIE EXTERNA

Gran parte de la innovación de la Directiva NIS 2 se basa en el concepto de **Ciberinteligencia de Amenazas:** monitorizar, descubrir, analizar y controlar los riesgos tanto propios como de terceros para implantar una estrategia de Ciberseguridad proactiva en la organización.

La capacidad de prevenir y anular ciberataques es hoy el combustible del crecimiento sostenible de cualquier negocio y cualquier Estado. Y así se reconoce en el espíritu que guía la redacción de la Directiva NIS 2.

**La monitorización continua y automatizada de la información filtrada y otras amenazas de la superficie** externa corporativa (Internet, Dark Web y Deep Web) utilizando Inteligencia Artificial (IA), puede jugar un importante papel en el cumplimiento de la Directiva Europea NIS 2 por parte de las organizaciones. Esta Directiva busca fortalecer la Ciberseguridad en la Unión Europea (UE), y la IA aplicada a la vigilancia de la superficie externa ayuda a identificar y abordar proactivamente los riesgos de Ciberseguridad en un entorno digital en constante evolución.

El concepto de superficie de ataque externa corporativa hace referencia al conjunto de activos digitales y datos que están expuestos y son accesibles desde el exterior de la organización, es decir, aquellos que pueden ser detectados y alcanzados por cualquiera que sepa buscarlos. Esto incluye sitios web públicos, repositorios, foros, mercados, servidores, bases de datos, dispositivos conectados a la red y cualquier otro recurso digital accesible desde la web pública.

# DIRECTIVA NIS 2

## CUMPLIMIENTO DE LA NIS 2: VENTAJAS DE LA MONITORIZACIÓN DE LA SUPERFICIE EXTERNA

### IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES PROPIAS

La monitorización continua y automatizada de la superficie externa corporativa permite a las organizaciones identificar amenazas y vulnerabilidades en tiempo real y de forma continua. Mediante la utilización de técnicas avanzadas de IA, se pueden escanear y analizar fuentes en línea, incluyendo redes sociales, foros de hacking y mercados de la Dark Web, para buscar menciones de la organización, sus activos o datos confidenciales. Si se detecta información filtrada, credenciales de acceso expuestas o detalles de vulnerabilidades, el sistema de monitorización alerta al equipo de seguridad para tomar medidas inmediatas y anular el riesgo.

### CUMPLIMIENTO CON LA NOTIFICACIÓN DE INCIDENTES

La Directiva NIS 2 establece la obligación para las entidades esenciales y las entidades importantes de notificar incidentes significativos a las autoridades competentes. La monitorización continua y automatizada de la superficie de ataque externa facilita la detección temprana de vulnerabilidades e incidentes y la recopilación de información relevante para cumplir con los plazos de notificación establecidos en la Directiva.

### RESPUESTA PROACTIVA A INCIDENTES

La monitorización continua y en tiempo real, junto con la utilización de tecnologías de IA, permiten automatizar la identificación y categorización de riesgos y vulnerabilidades en la superficie externa corporativa y la detección de la brecha que los ha causado. Esto facilita la priorización de respuestas y la asignación de recursos adecuados para abordar las vulnerabilidades más críticas en tiempo real. Al detectar brechas de seguridad de manera proactiva, las organizaciones pueden actuar antes de que se produzca un daño significativo, reduciendo el éxito y el impacto de los ataques y mejorando su capacidad de recuperación.

# DIRECTIVA NIS 2

## CUMPLIMIENTO DE LA NIS 2: VENTAJAS DE LA MONITORIZACIÓN DE LA SUPERFICIE EXTERNA

### ANÁLISIS DE TENDENCIAS Y PATRONES DE ATAQUE

La monitorización continua y automatizada de la superficie externa corporativa facilita datos objetivos para el análisis de tendencias y patrones de ataque a lo largo del tiempo. La identificación de actividades sospechosas y comportamientos anómalos son indicadores de amenazas en desarrollo o intentos de infiltración. Con esta información, las organizaciones pueden fortalecer sus defensas, corregir sus vulnerabilidades y mejorar su postura de seguridad general.

### EVOLUCIÓN PROACTIVA DE LA SEGURIDAD DE PROVEEDORES

La monitorización continua con IA de la superficie de ataque externa también permite una evaluación proactiva y no intrusiva del estado de Ciberseguridad de proveedores y terceros antes de que se conviertan en un eslabón débil en la cadena de suministro. Al analizar datos públicos y acceder a información relevante en tiempo real, se detectan vulnerabilidades y se evalúa el nivel de seguridad de los proveedores para determinar si cumplen con los requisitos de la Directiva NIS 2. Esto permite una respuesta rápida y coordinada para anular el riesgo de terceros, mitigar el impacto del posible incidente y evitar que se propague a lo largo de la cadena de suministro.

### ADAPTACIÓN A NUEVAS AMENAZAS

La IA es especialmente eficaz en la detección de amenazas emergentes y variantes de ataque sofisticadas. A través del aprendizaje automático y algoritmos de detección de anomalías, la IA puede identificar patrones de ataque cambiantes y nuevas tácticas utilizadas por los ciberdelincuentes. Esto permite a las organizaciones adaptar sus estrategias de seguridad y estar preparadas para enfrentar ciberamenazas en constante evolución.

kartos©

Capa de IA que permite el funcionamiento 100% automatizado sin intervención humana en ninguna parte del proceso.

**Funcionamiento continuo 365x24x7,** lo que permite detectar filtraciones de nueva información prácticamente en tiempo real.

**Herramienta estrictamente no intrusiva.** La investigación se realiza en Internet, la Deep Web y la DarkWeb y no se ataca el perímetro IT de las organizaciones, por lo que su funcionamiento y la información obtenida cumplen estrictamente con los límites impuestos por la legislación.

**Máxima sencillez de uso.** No requiere ninguna configuración compleja. Basta con introducir el dominio en la plataforma y funciona de manera autónoma, sin necesidad de configurar parámetros de búsqueda ni de cualquier otro criterio de localización de información.

Única plataforma que **analiza las conversaciones en redes sociales desde la perspectiva de detección de amenazas** y ataques, más allá de la relativa a reputación y branding.

**Monitorización automatizada, objetiva y continúa de los riesgos causados por las terceras partes** que pertenecen a la Superficie de Ataque Externa de la organización.

**Conoce más sobre nuestras licencias.**
**Prueba de forma gratuita nuestra herramienta.**
**Empieza a usar Kartos y a cumplir con la NIS 2**

hello@enthec.com

## 5 FUNCIONALIDADES
en una única plataforma

Kartos Corporate Watchbots es la plataforma para la **Gestión Continua de la Exposición a Amenazas (CTEM)** desarrollada por Enthec para extender el perímetro de seguridad controlado por las organizaciones. Kartos proporciona a las empresas toda la información que los ciberdelincuentes tienen sobre ellas para que mejoren su defensa contra varios tipos de ataques.

### GESTIÓN DE LA SUPERFICIE EXTERNA DE ATAQUE
Detección de activos corporativos e información sobre sistemas, servicios en la nube y aplicaciones que están disponibles y visibles en el dominio público para cualquier ciberdelincuente.

### PROTECCIÓN DEL RIESGO DIGITAL
Detección de información contextual sobre posibles agentes de ataques, sus tácticas y procesos para llevar a cabo actividades maliciosas. Eliminación de actividades maliciosas en nombre de la organización.

### TERCERAS PARTES
Gestión, valoración y control del riesgo de la cadena de valor durante todo el tiempo que dure la relación comercial, a través de datos objetivos obtenidos en tiempo real de forma automatizada, continua y no intrusiva.

### COMPLIANCE:
Control y gestión del cumplimiento legal corporativo y de terceros basado en datos objetivos obtenidos en tiempo real de forma automatizada y continua.

### SECURITY RATING SERVICES
Evaluación independiente de riesgos propios y de terceros, para una visualización amplia de la madurez en ciberseguridad de cualquier organización. Ampliación y ponderación de la información proporcionada por los métodos tradicionales de evaluación de riesgos por terceros.

## Análisis de 9 Categorías de Amenazas

- Red
- Salud de DNS / Phishing
- Gestión de Parches
- Reputación IP
- Seguridad Web
- Seguridad e-mail
- Filtración de Documentos
- Filtración de Credenciales
- Redes Sociales

#WeAlreadyKnow

@enthec

@enthecsolutions

@enthecsolutions