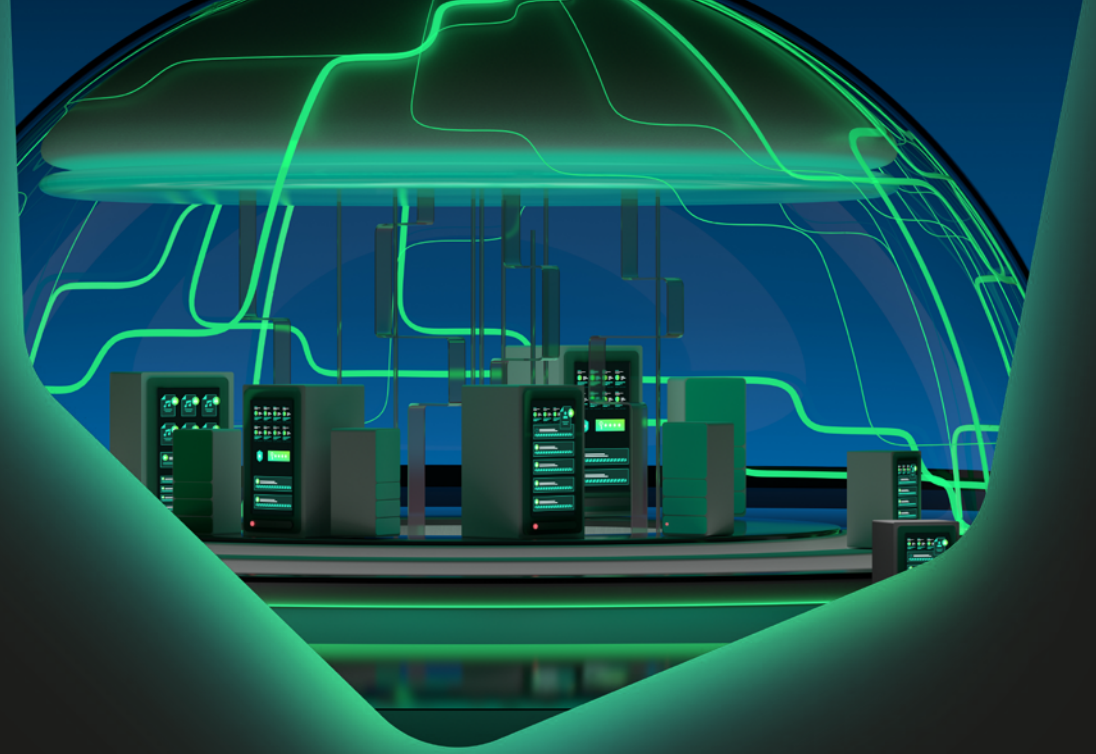
kaspersky

Mapa de soluciones NIS 2



¿De qué trata la Directiva NIS 2?

La Directiva NIS 2[1] entró en vigor el 16 de enero de 2023, y los Estados miembros debían incorporarla antes del 17 de octubre de 2024, aunque su adopción aún varía entre países. Además de otros objetivos, la Directiva NIS 2 exige a los principales operadores de industrias clave que adopten medidas de seguridad y notifiquen los incidentes.

¿A quién se aplica la NIS 2?

Una entidad entra en el ámbito de aplicación de la Directiva si opera en uno de los sectores y tipos de servicios enumerados en los anexos de la Directiva y si tiene un determinado tamaño. Para conocer todos los detalles, excepciones y matices, consulta los artículos 2 y 3 y los anexos I y II de la Directiva[2]. La Directiva NIS 2 establece dos categorías para las entidades incluidas en su ámbito de aplicación: entidades esenciales y entidades importantes. Ambas categorías deben cumplir los mismos requisitos. La diferenciación radica en las medidas de supervisión y las sanciones.

Sectores que se regularán

Sectores de alta criticidad
(Entidades esenciales*)

- Energía
- Agua potable
- Empresas de transporte
- Infraestructura digital
- Bancos
- Aguas residuales
- Infraestructura del mercado financiero
- Gestión de servicios TIC (B2B)
- Salud
- Administración pública
- Espacio

Otros sectores críticos
(Entidades importantes*)

- Servicios postales y de mensajería
- Producción y distribución de alimentos
- Residuos Operaciones y mantenimiento
- Industria
- Fabricación y distribución de productos químicos
- Investigación
- Proveedores digitales

¿Cuáles son los requisitos de ciberseguridad de NIS 2?

De conformidad con el apartado 1 del artículo 21 de la Directiva, los Estados miembros velarán por que las entidades esenciales e importantes adopten medidas técnicas, operativas y organizativas adecuadas y proporcionadas para gestionar los riesgos que se plantean para la seguridad de las redes y sistemas de información que dichas entidades utilizan para sus operaciones o para la prestación de sus servicios, así como para prevenir o reducir al mínimo el impacto de los incidentes en los destinatarios de sus servicios y en otros servicios.

Como proveedor de ciberseguridad, Kaspersky aprovecha toda su experiencia para ayudar a las organizaciones a crear ciberdefensas sólidas y cumplir con la NIS 2. Podemos ayudarte con nuestras soluciones y servicios líderes.

---

[1]Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, del 14 de diciembre de 2022, relativa a medidas para un nivel común elevado de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972, y por la que se deroga la Directiva (UE) 2016/1148 (Directiva NIS 2); https://eur-lex.europa.eu/eli/dir/2022/2555

[2]https://eur-lex.europa.eu/eli/dir/2022/2555

Requisito de la NIS2	Solución de Kaspersky	Ventajas	Información
Capítulo IV, Art. 20, Gobernanza			
2. Los Estados miembros velarán por que los miembros de los órganos de dirección de las entidades esenciales e importantes estén obligados a seguir una formación, y alentarán a las entidades esenciales e importantes a ofrecer periódicamente una formación similar a sus empleados, con el fin de que adquieran conocimientos y competencias suficientes que les permitan identificar los riesgos y evaluar las prácticas de gestión de los riesgos de ciberseguridad y su impacto en los servicios prestados por la entidad.	**Concienciación con Kaspersky Security Awareness**	**Kaspersky Security Awareness**: un nuevo enfoque para dominar las competencias de seguridad informática; Kaspersky Security Awareness es una solución eficaz y de eficacia probada con un largo historial internacional de éxitos. Utilizada por empresas de todos los tamaños para formar a más de un millón de empleados en más de 75 países, la solución abarca más de 25 años de conocimientos en ciberseguridad de Kaspersky con una amplia experiencia en formación de adultos. Estas soluciones de formación interesantes y eficaces aumentan la concienciación de ciberseguridad de tu personal para que todos desempeñen su labor en la ciberseguridad general de tu organización. Como los cambios de comportamiento sostenibles llevan tiempo, nuestro enfoque implica la creación de un ciclo de aprendizaje continuo con múltiples componentes	https://www.kaspersky.es/enterprise-security/security-awareness
	Kaspersky Formación para expertos	**Kaspersky xTraining** es la respuesta a un panorama de ciberamenazas en constante evolución. Aportamos conocimientos actualizados sobre estrategias eficaces de detección y mitigación de amenazas a partir de experiencias exhaustivas y conocidas del Kaspersky Global Research & Analysis Team (GReAT)	https://xtraining.kaspersky.com/
	Formación ICS	**Kaspersky ICS CERT** es un proyecto global establecido en 2016 para coordinar los esfuerzos de los proveedores de sistemas de automatización industrial y los propietarios y operadores de instalaciones industriales. El equipo cuenta con más de 30 expertos en investigación de amenazas y vulnerabilidades de ICS, respuesta a incidentes y análisis de seguridad. Brindamos formación en los aspectos básicos de la ciberseguridad industrial y las habilidades prácticas para investigar incidentes de ciberseguridad y llevar a cabo investigaciones de vulnerabilidades. Nuestros programas se basan en la experiencia práctica y en casos reales. El equipo de Kaspersky ICS CERT imparte cursos de formación para diferentes operadores del sector ICS, desde operadores de campo hasta el nivel C, incluidos los profesionales de la ciberseguridad dedicados al TO.	https://ics-cert.kaspersky.com/media/services/Kaspersky-Industrial-Cybersecurity-training-program-En.pdf
Capítulo IV, Art. 21, Medidas de gestión de riesgos de ciberseguridad			
1. Los Estados miembros velarán por que las entidades esenciales e importantes adopten medidas técnicas, operativas y organizativas adecuadas y proporcionadas para gestionar los riesgos que se plantean para la seguridad de las redes y sistemas de información que dichas entidades utilizan para sus operaciones o para la prestación de sus servicios, así como para prevenir o reducir al mínimo el impacto de los incidentes en los destinatarios de sus servicios y en otros servicios.	**Kaspersky Next**	**Kaspersky Next** es la solución de Kaspersky para proteger tu infraestructura contra ransomware, malware y amenazas evasivas y complejas. Cuenta con funcionalidad de EDR en todos los niveles, adaptada a tus necesidades y recursos. Nuestras tecnologías EDR y XDR se basan en la galardonada protección de endpoints y en controles de nivel empresarial. Obtén una novedosa eficiencia con la automatización de tareas simples y complejas junto con una respuesta guiada para impulsar tu eficacia y minimizar los recursos que necesitas para administrar tu ciberseguridad. Las opciones en la nube y en las instalaciones se adaptan a tus requisitos específicos y, llegado el momento, controlan toda tu infraestructura con XDR abierto integral.	
	Kaspersky MDR	**Kaspersky Managed Detection and Response** ofrece una detección, priorización, investigación y respuesta continuas, totalmente gestionadas y adaptadas individualmente. Como resultado, permite obtener todos los beneficios principales de tener su propio centro de operaciones de seguridad sin tener que establecer uno realmente. El objetivo principal del servicio de MDR es detectar amenazas en cada etapa de un ciberataque, tanto antes del riesgo real como después de que los actores maliciosos hayan penetrado en la infraestructura corporativa. Los analistas de SOC investigan las alertas y notifican al cliente acerca de la actividad maliciosa, y brindan respuestas y asesoramiento basados en herramientas, todo ello mediante una supervisión de la seguridad ininterrumpida potenciada por la búsqueda automatizada de amenazas, la investigación de incidentes y las respuestas guiadas y gestionadas	https://www.kaspersky.es/enterprise-security/managed-detection-and-response
	Kaspersky XDR	**Kaspersky XDR** es una plataforma abierta, una herramienta universal para crear un ecosistema unificado de productos de ciberseguridad. La plataforma actúa como una solución Anti APT todo en uno impulsada por Kaspersky Threat Intelligence que monitoriza todos los posibles puntos de entrada de ciberdelincuentes, correlacionando la información y orquestando todos los componentes de protección de la infraestructura. Kaspersky XDR incluye una amplia variedad de integraciones listas para usarse con Kaspersky y productos de terceros	https://www.kaspersky.es/enterprise-security/xdr

Kaspersky comprende las necesidades de los diferentes sectores y tamaños de empresa y **protege a más de 220 000 empresas de todo el mundo** contra las ciberamenazas. La fiable ciberprotección todo en uno de Kaspersky cubre múltiples dimensiones de protección. **¡Protégete ya!**

Requisito de la NIS2	Solución de Kaspersky	Ventajas	Información
Capítulo IV, Art. 21, Medidas de gestión de riesgos de ciberseguridad			
1. Los Estados miembros velarán por que las entidades esenciales e importantes adopten medidas técnicas, operativas y organizativas adecuadas y proporcionadas para gestionar los riesgos que se plantean para la seguridad de las redes y sistemas de información que dichas entidades utilizan para sus operaciones o para la prestación de sus servicios, así como para prevenir o reducir al mínimo el impacto de los incidentes en los destinatarios de sus servicios y en otros servicios.	**Kaspersky Industrial Cybersecurity**	**Kaspersky Industrial Cybersecurity (KICS)** es una plataforma de detección y respuesta extendidas (XDR) para organizaciones industriales, diseñada y certificada especialmente para proteger a equipos, activos y redes de TO críticos de ciberamenazas. La plataforma incluye tecnologías integradas que protegen los componentes de automatización industrial y sistemas de control en cada nivel. KICS for Nodes es un software de protección, detección y respuesta de endpoints con funciones de auditoría de cumplimiento y sensores de endpoints. KICS for Networks está diseñado para el análisis, la detección y la respuesta del tráfico de red de TO. La función de administración centralizada al nivel del sitio, esencial para la escalabilidad de las operaciones de seguridad de TO a un alto volumen de infraestructuras industriales de gran tamaño, diversas y distribuidas geográficamente, está integrada en la plataforma. La integración constante entre los componentes de la plataforma brinda una visibilidad total de múltiples redes de TO y sistemas de automatización distribuidos geográficamente y ofrece una mejor experiencia del cliente, conocimiento de la situación y flexibilidad de despliegue. Con detección y respuesta extendidas, la plataforma de KICS permite la convergencia TI/TO y proporciona numerosos beneficios para proveedores únicos	https://www.kaspersky.es/enterprise-security/industrial-cybersecurity
	Kaspersky Container Security	**La solución de Kaspersky Container Security (KCS)** protege cada etapa del ciclo de vida de una aplicación contenerizada, desde el desarrollo hasta la operación. Protege los procesos comerciales de la organización, de acuerdo con los estándares y las regulaciones de seguridad, y admite la implementación de un enfoque DevSecOps. Kaspersky Container Security brinda una protección integral frente a las últimas ciberamenazas y automatiza tus auditorías de cumplimiento, liberando los recursos del equipo de seguridad de la información para ocuparse de otras tareas y reduciendo el plazo de lanzamiento. Kaspersky Container Security se ha desarrollado de manera específica para los entornos contenedorizados, a fin de garantizar la protección en los diferentes niveles, desde la imagen del contenedor hasta el sistema operativo host.	https://www.kaspersky.es/enterprise-security/container-security
	Kaspersky Threat Intelligence	**Threat Intelligence** de Kaspersky te proporciona acceso a la inteligencia que necesitas para mitigar ciberamenazas de la mano de nuestro equipo líder de investigadores y analistas. Gracias a nuestros conocimientos, experiencia e inteligencia avanzada de todos los aspectos relativos a la ciberseguridad, en Kaspersky nos hemos convertido en el partner de confianza de las fuerzas del orden y los organismos gubernamentales más importantes del mundo, entre las que se incluyen la Interpol e importantes equipos CERT. Kaspersky Threat Intelligence te ofrece acceso inmediato a inteligencia de amenazas táctica, operativa y estratégica. Kaspersky Threat Intelligence te permite identificar y prevenir proactivamente las amenazas, te mantiene informado sobre las últimas amenazas y vulnerabilidades y te permite tomar medidas proactivas para proteger tus sistemas antes de que se produzca un ataque.	https://www.kaspersky.es/enterprise-security/threat-intelligence
	Kaspersky Web Traffic Security	**Kaspersky Web Traffic Security** (en lo sucesivo también denominado "la aplicación" o "KWTS") es una solución diseñada para proteger el tráfico HTTP, HTTPS y FTP que pasa a través de un servidor proxy. La aplicación protege a los usuarios de una red corporativa cuando acceden a recursos web. Por ejemplo, elimina el malware y otras amenazas del flujo de datos que entra en la red corporativa a través de los protocolos HTTP(S) y FTP, bloquea los sitios web infectados y de phishing y controla el acceso a los recursos web en función de las categorías de recursos web y los tipos de contenido.	https://www.kaspersky.es/enterprise-security/internet-gateway

Requisito de la NIS2	Solución de Kaspersky	Ventajas	Información
Capítulo IV, Art. 21, Medidas de gestión de riesgos de ciberseguridad			
1. Los Estados miembros velarán por que las entidades esenciales e importantes adopten medidas técnicas, operativas y organizativas adecuadas y proporcionadas para gestionar los riesgos que se plantean para la seguridad de las redes y sistemas de información que dichas entidades utilizan para sus operaciones o para la prestación de sus servicios, así como para prevenir o reducir al mínimo el impacto de los incidentes en los destinatarios de sus servicios y en otros servicios.	**Kaspersky Seguridad de correo**	**Las aplicaciones de Kaspersky Security for Mail Server** te ayudan a crear resiliencia frente a los ataques basados en correo electrónico mediante: la identificación y el filtrado del correo sospechoso o no deseado en la pasarela. La mayoría de los ataques de correo sólo comienzan a activarse en el endpoint: Kaspersky Security for Mail Server se propone detenerlos mucho antes de que lleguen tan lejos. Nuestra galardonada protección fortalece su resiliencia al detectar e interceptar ataques, justo en el inicio de la cadena de ataques, antes de que puedan penetrar su perímetro de seguridad y avanzar hacia sus dispositivos y usuarios. Procesamiento rápido y preciso de los correos electrónicos legítimos: La importante función del correo electrónico en las comunicaciones corporativas requiere que el procesamiento de la seguridad sea rápido, ágil y preciso, sin suponer un obstáculo para las comunicaciones legítimas. Kaspersky Security for Mail Server ofrece las tecnologías de protección más efectivas de la industria contra cualquier tipo de amenaza, desde los correos spam y de phishing hasta ataques al correo corporativo (BEC) y el ransomware, sin prácticamente falsos positivos, al tiempo que permite que los correos legítimos circulen sin ningún tipo de interrupción. Proteger el correo electrónico más allá de la pasarela: Kaspersky Security for Mail Server detecta contenido malicioso o no deseado no solamente en la puerta de enlace, sino también en los buzones de correo individuales de Microsoft Exchange Server o Microsoft Exchange Online. Los ataques de phishing retrasados diseñados para evadir las contramedidas en la puerta de enlace, los mensajes BEC generados después de la apropiación de cuentas y los escenarios de amenazas internas que nunca necesitan pasar a través de la puerta de enlace: todos estos pueden identificarse y erradicarse, lo que hace que la protección del buzón del servidor sea imprescindible.	https://www.kaspersky.es/enterprise-security/mail-server-security
2. Las medidas mencionadas en el párrafo 1 se basarán en un enfoque que contemple todos los riesgos y que tenga por objeto proteger las redes y los sistemas de información, así como el entorno físico de dichos sistemas, frente a los incidentes, e incluirán, como mínimo, lo siguiente: a) políticas de análisis de riesgos y seguridad de los sistemas de información;	**Kaspersky Incident Response**	**Incident response**: obtiene una imagen detallada del incidente. El servicio cubre la investigación de incidentes y el ciclo de respuesta completos, desde la respuesta temprana a los incidentes y la recopilación de pruebas hasta la identificación de rastros adicionales de piratería informática y la preparación de un plan de mitigación.	https://www.kaspersky.es/enterprise-security/incident-response
	Kaspersky Next	**Kaspersky Next** es la solución de Kaspersky para proteger tu infraestructura contra ransomware, malware y amenazas evasivas y complejas. Cuenta con funcionalidad de EDR en todos los niveles, adaptada a tus necesidades y recursos. Nuestras tecnologías EDR y XDR se basan en la galardonada protección de endpoints y en controles de nivel empresarial. Obtén una novedosa eficiencia con la automatización de tareas simples y complejas junto con una respuesta guiada para impulsar tu eficacia y minimizar los recursos que necesitas para administrar tu ciberseguridad. Las opciones en la nube y en las instalaciones se adaptan a tus requisitos específicos y, llegado el momento, controlan toda tu infraestructura con XDR abierto integral.	
	Kaspersky Industrial Cybersecurity	**Kaspersky Industrial Cybersecurity (KICS)** es una plataforma de detección y respuesta extendidas (XDR) para organizaciones industriales, diseñada y certificada especialmente para proteger a equipos, activos y redes de TO críticos de ciberamenazas. La plataforma incluye tecnologías integradas que protegen los componentes de automatización industrial y sistemas de control en cada nivel. KICS for Nodes es un software de protección, detección y respuesta de endpoints con funciones de auditoría de cumplimiento y sensores de endpoints. KICS for Networks está diseñado para el análisis, la detección y la respuesta del tráfico de red de TO. La función de administración centralizada al nivel del sitio, esencial para la escalabilidad de las operaciones de seguridad de TO a un alto volumen de infraestructuras industriales de gran tamaño, diversas y distribuidas geográficamente, está integrada en la plataforma. La integración constante entre los componentes de la plataforma brinda una visibilidad total de múltiples redes de TO y sistemas de automatización distribuidos geográficamente y ofrece una mejor experiencia del cliente, conocimiento de la situación y flexibilidad de despliegue. Con detección y respuesta extendidas, la plataforma de KICS permite la convergencia TI/TO y proporciona numerosos beneficios para proveedores únicos	https://www.kaspersky.es/enterprise-security/industrial-cybersecurity
	Evaluación de vulnerabilidades de Kaspersky	Este servicio proporciona información sobre vulnerabilidades existentes y las consecuencias de su explotación, evalúa la eficacia de la aplicación de las medidas de seguridad implementadas y le permite planificar acciones futuras para corregir las deficiencias detectadas y mejorar la seguridad. Realizar evaluaciones de seguridad con regularidad te permite comprender claramente el estado de tu ciberseguridad y garantiza el cumplimiento de las buenas prácticas del sector.	https://www.kaspersky.es/enterprise-security/cybersecurity-services

Kaspersky comprende las necesidades de los diferentes sectores y tamaños de empresa y **protege a más de 220 000 empresas de todo el mundo** contra las ciberamenazas. La fiable ciberprotección todo en uno de Kaspersky cubre múltiples dimensiones de protección. **¡Protégete ya!**

Requisito de la NIS2	Solución de Kaspersky	Ventajas	Información
Capítulo IV, Art. 21, Medidas de gestión de riesgos de ciberseguridad			
2. Las medidas mencionadas en el párrafo 1 se basarán en un enfoque que contemple todos los riesgos y que tenga por objeto proteger las redes y los sistemas de información, así como el entorno físico de dichos sistemas, frente a los incidentes, e incluirán, como mínimo, lo siguiente: a) políticas de análisis de riesgos y seguridad de los sistemas de información;	**Kaspersky Digital Footprint Intelligence**	**Kaspersky Digital Footprint Intelligence** es un servicio integral de protección contra riesgos digitales que ayuda a los clientes a supervisar sus activos digitales y detectar amenazas desde la red superficial, profunda y oscura. Con alertas en tiempo real, Kaspersky Digital Footprint intelligence permite a las organizaciones responder de manera rápida y eficaz contra las amenazas potenciales. Los informes analíticos integran estos datos con la información exhaustiva de nuestros expertos, que proporciona datos sobre los riesgos de ciberseguridad y recomendaciones sobre cómo mitigarlos.	https://dfi.kaspersky.com/es
	Kaspersky APT, Crimeware, informes ICS	Con los **informes de inteligencia**, los clientes de Kaspersky se beneficiarán de un acceso constante y exclusivo a análisis y perspectivas, incluidos datos técnicos exhaustivos (en una amplia gama de formatos) sobre actores APT dirigidos a tu industria y geografía, conocerán y contrarrestarán adecuadamente el software delictivo y las ciberamenazas que afectan a las organizaciones industriales (incluidas las amenazas que nunca se harán públicas). Los informes contienen un resumen de información inmediata y relevante que ilustra cada detalle del ataque, además de ofrecer una descripción técnica detallada con las normas YARA e IoC pertinentes, ofreciendo a los investigadores de seguridad, analistas de malware, ingenieros de seguridad, analistas de redes de seguridad e investigadores de APT, datos aplicables que permiten una respuesta precisa y rápida a las amenazas.	https://www.kaspersky.es/enterprise-security/threat-intelligence
	Fuentes de datos de amenazas de vulnerabilidades de Kaspersky	Al integrar **fuentes de inteligencia sobre amenazas** actualizadas que contienen información sobre IP, URL y hash de archivos sospechosos y maliciosos en los sistemas de seguridad existentes, como los sistemas SIEM, SOAR y las plataformas de inteligencia de amenazas, los equipos de seguridad pueden automatizar el proceso de evaluación inicial y proporcionar a los especialistas pertinentes el contexto necesario para identificar inmediatamente las alertas que requieren un análisis en profundidad, o que necesitan ser escaladas a los equipos de respuesta a incidentes para una mayor investigación y respuesta. Las fuentes de datos proceden de fuentes altamente fiables y heterogéneas, como Kaspersky Security Network y nuestras propias arañas web, nuestro servicio de supervisión de botnets (seguimiento ininterrumpido de botnets y de sus actividades y objetivos), trampas de spam, partners y equipos de investigación.	https://www.kaspersky.es/enterprise-security/threat-intelligence
	KUMA	**Kaspersky Unified Monitoring and Analysis Platform (KUMA)** es una solución SIEM avanzada para la gestión de datos y eventos de seguridad. KUMA analiza los eventos de seguridad de la información en tiempo real, lo que aumenta significativamente el conocimiento de la situación. KUMA recibe eventos de seguridad de varias fuentes, incluyendo productos Kaspersky, sistemas operativos, aplicaciones de terceros y herramientas de seguridad. Correlaciona estos eventos entre sí y con fuentes de inteligencia de amenazas con el fin de identificar actividades sospechosas en la infraestructura de la red corporativa y proporciona notificaciones oportunas de incidentes de seguridad. Mediante la recolección de registros de todos los controles de seguridad y la correlación de los datos resultantes en tiempo real, KUMA agrega toda la información necesaria para investigar y responder a los incidentes.	https://support.kaspersky.com/help/KUMA/1.6/en-US/217694.htm
	Kaspersky Container Security	**La solución de Kaspersky Container Security (KCS)** protege cada etapa del ciclo de vida de una aplicación contenerizada, desde el desarrollo hasta la operación. Protege los procesos comerciales de la organización, de acuerdo con los estándares y las regulaciones de seguridad, y admite la implementación de un enfoque DevSecOps. Kaspersky Container Security brinda una protección integral frente a las últimas ciberamenazas y automatiza tus auditorías de cumplimiento, liberando los recursos del equipo de seguridad de la información para ocuparse de otras tareas y reduciendo el plazo de lanzamiento. Kaspersky Container Security se ha desarrollado de manera específica para los entornos contenedorizados, a fin de garantizar la protección en los diferentes niveles, desde la imagen del contenedor hasta el sistema operativo host.	https://www.kaspersky.es/enterprise-security/container-security

Requisito de la NIS2	Solución de Kaspersky	Ventajas	Información
Capítulo IV, Art. 21, Medidas de gestión de riesgos de ciberseguridad			
2. b) gestión de incidentes;	**Kaspersky Incident Response**	**Incident response**: obtiene una imagen detallada del incidente. El servicio cubre la investigación de incidentes y el ciclo de respuesta completos, desde la respuesta temprana a los incidentes y la recopilación de pruebas hasta la identificación de rastros adicionales de piratería informática y la preparación de un plan de mitigación.	https://www.kaspersky.es/enterprise-security/incident-response
	EDR Optimum	La visibilidad limitada y la falta de recursos juegan a favor de los atacantes. **Kaspersky Endpoint Detection and Response (EDR) Optimum** ofrece detección avanzada, funciones de investigación simplificadas y respuesta automatizada en un paquete fácil de usar para proteger tu empresa de las amenazas más recientes.	https://www.kaspersky.es/enterprise-security/edr-security-software-solution
	EDR Expert	Los ciberataques son cada vez más sofisticados y capaces de evitar las medidas de seguridad existentes. **Kaspersky Endpoint Detection and Response (EDR) Expert** ofrece visibilidad completa de todos los endpoints en la red corporativa y defensas de nivel superior mediante la automatización de las tareas rutinarias de EDR. Además, hace que los analistas puedan detectar, priorizar, analizar y neutralizar amenazas complejas y ataques de tipo APT más fácilmente. Kaspersky EDR Expert utiliza un único agente que se puede gestionar tanto desde una única plataforma de gestión basada en la nube, como desde una consola offline en entornos de brecha física, para aprovechar las tecnologías de inteligencia sobre amenazas e incorporar estrategias de detección personalizables.	https://www.kaspersky.es/enterprise-security/endpoint-detection-response-edr
	Kaspersky XDR	**Kaspersky XDR** es una plataforma abierta, una herramienta universal para crear un ecosistema unificado de productos de ciberseguridad. La plataforma actúa como una solución Anti APT todo en uno impulsada por Kaspersky Threat Intelligence que monitoriza todos los posibles puntos de entrada de ciberdelincuentes, correlacionando la información y orquestando todos los componentes de protección de la infraestructura. Kaspersky XDR incluye una amplia variedad de integraciones listas para usarse con Kaspersky y productos de terceros	https://www.kaspersky.es/enterprise-security/xdr
	Kaspersky MDR	**Kaspersky Managed Detection and Response** ofrece una detección, priorización, investigación y respuesta continuas, totalmente gestionadas y adaptadas individualmente. Como resultado, permite obtener todos los beneficios principales de tener su propio centro de operaciones de seguridad sin tener que establecer uno realmente. El objetivo principal del servicio de MDR es detectar amenazas en cada etapa de un ciberataque, tanto antes del riesgo real como después de que los actores maliciosos hayan penetrado en la infraestructura corporativa. Los analistas de SOC investigan las alertas y notifican al cliente acerca de la actividad maliciosa, y brindan respuestas y asesoramiento basados en herramientas, todo ello mediante una supervisión de la seguridad ininterrumpida potenciada por la búsqueda automatizada de amenazas, la investigación de incidentes y las respuestas guiadas y gestionadas	https://www.kaspersky.es/enterprise-security/managed-detection-and-response
	Kaspersky Threat Lookup	**Kaspersky Threat Lookup** proporciona todos los conocimientos de Kaspersky sobre ciberamenazas y las relaciones entre ellas, reunidos en un único y potente servicio web. El objetivo es proporcionar a los equipos de seguridad tantos datos como sea posible para prevenir los ataques informáticos antes de que comprometan a la organización. La plataforma recupera la inteligencia de amenazas más reciente sobre URL, dominios, direcciones IP, hash de archivos, nombres de amenazas, datos estadísticos y de comportamiento, datos de WHOIS y DNS, atributos de archivos, datos de geolocalización, descarga de cadenas, marcas de tiempo, etc. El resultado es una visibilidad global de las amenazas nuevas y emergentes: esto te permite proteger mejor tu empresa, mejorando significativamente la calidad y la eficacia de las actividades de respuesta a incidentes.	https://www.kaspersky.es/enterprise-security/threat-intelligence
	Kaspersky Threat Analysis	Ante una posible amenaza cibernética, es esencial tomar una decisión a tiempo. Además de tecnologías de análisis de amenazas como el sandboxing, **Kaspersky Threat Analysis** ofrece tecnologías de atribución de vanguardia (un enfoque multicapa que proporciona un análisis eficaz de las amenazas, para que puedas tomar decisiones con pleno conocimiento de causa para defenderte de los ataques incluso antes de que se inicien). Varias herramientas de análisis de amenazas se combinan para permitirte a ti y a tu equipo analizar la situación desde todos los ángulos, teniendo una imagen completa del entorno de amenazas, y responder de manera rápida y efectiva.	https://www.kaspersky.es/enterprise-security/threat-intelligence

Requisito de la NIS2	Solución de Kaspersky	Ventajas	Información
Capítulo IV, Art. 21, Medidas de gestión de riesgos de ciberseguridad			
2. b) gestión de incidentes;	**Kaspersky Threat Data Feeds**	Mediante la integración en sistemas de seguridad existentes, como SIEM, SOAR y plataformas de inteligencia sobre amenazas, y **fuentes de inteligencia sobre amenazas** actualizadas que contienen información sobre IP, URL y hashes de archivos sospechosos y maliciosos, los equipos de seguridad pueden automatizar el proceso de evaluación inicial y proporcionar a los especialistas pertinentes el contexto que necesitan para identificar inmediatamente las alertas que requieren un análisis en profundidad, o que deben remitirse a los equipos de respuesta a incidentes para una mayor investigación y respuesta. Las fuentes de datos proceden de fuentes altamente fiables y heterogéneas, como Kaspersky Security Network y nuestras propias arañas web, nuestro servicio de supervisión de botnets (seguimiento ininterrumpido de botnets y de sus actividades y objetivos), trampas de spam, partners y equipos de investigación.	https://www.kaspersky.es/enterprise-security/threat-intelligence
	KUMA	**Kaspersky Unified Monitoring and Analysis Platform (KUMA)** es una solución SIEM avanzada para la gestión de datos y eventos de seguridad. KUMA analiza los eventos de seguridad de la información en tiempo real, lo que aumenta significativamente el conocimiento de la situación. KUMA recibe eventos de seguridad de varias fuentes, incluyendo productos Kaspersky, sistemas operativos, aplicaciones de terceros y herramientas de seguridad. Correlaciona estos eventos entre sí y con fuentes de inteligencia de amenazas con el fin de identificar actividades sospechosas en la infraestructura de la red corporativa y proporciona notificaciones oportunas de incidentes de seguridad. Mediante la recolección de registros de todos los controles de seguridad y la correlación de los datos resultantes en tiempo real, KUMA agrega toda la información necesaria para investigar y responder a los incidentes.	https://support.kaspersky.com/help/KUMA/1.6/en-US/217694.htm
	Kaspersky Container Security	**La solución de Kaspersky Container Security (KCS)** protege cada etapa del ciclo de vida de una aplicación contenerizada, desde el desarrollo hasta la operación. Protege los procesos comerciales de la organización, de acuerdo con los estándares y las regulaciones de seguridad, y admite la implementación de un enfoque DevSecOps. Kaspersky Container Security brinda una protección integral frente a las últimas ciberamenazas y automatiza tus auditorías de cumplimiento, liberando los recursos del equipo de seguridad de la información para ocuparse de otras tareas y reduciendo el plazo de lanzamiento. Kaspersky Container Security se ha desarrollado de manera específica para los entornos contenedorizados, a fin de garantizar la protección en los diferentes niveles, desde la imagen del contenedor hasta el sistema operativo host.	https://www.kaspersky.es/enterprise-security/container-security
2. c) continuidad del negocio, como gestión de copias de seguridad y recuperación de desastres, y gestión de crisis;	**Kaspersky Next**	**Kaspersky Next** es la solución de Kaspersky para proteger tu infraestructura contra ransomware, malware y amenazas evasivas y complejas. Cuenta con funcionalidad de EDR en todos los niveles, adaptada a tus necesidades y recursos. Nuestras tecnologías EDR y XDR se basan en la galardonada protección de endpoints y en controles de nivel empresarial. Obtén una novedosa eficiencia con la automatización de tareas simples y complejas junto con una respuesta guiada para impulsar tu eficacia y minimizar los recursos que necesitas para administrar tu ciberseguridad. Las opciones en la nube y en las instalaciones se adaptan a tus requisitos específicos y, llegado el momento, controlan toda tu infraestructura con XDR abierto integral.	
	Kaspersky MDR	**Kaspersky Managed Detection and Response** ofrece una detección, priorización, investigación y respuesta continuas, totalmente gestionadas y adaptadas individualmente. Como resultado, permite obtener todos los beneficios principales de tener su propio centro de operaciones de seguridad sin tener que establecer uno realmente. El objetivo principal del servicio de MDR es detectar amenazas en cada etapa de un ciberataque, tanto antes del riesgo real como después de que los actores maliciosos hayan penetrado en la infraestructura corporativa. Los analistas de SOC investigan las alertas y notifican al cliente acerca de la actividad maliciosa, y brindan respuestas y asesoramiento basados en herramientas, todo ello mediante una supervisión de la seguridad ininterrumpida potenciada por la búsqueda automatizada de amenazas, la investigación de incidentes y las respuestas guiadas y gestionadas	https://www.kaspersky.es/enterprise-security/managed-detection-and-response

Requisito de la NIS2	Solución de Kaspersky	Ventajas	Información
Capítulo IV, Art. 21, Medidas de gestión de riesgos de ciberseguridad			
2. c) continuidad del negocio, como gestión de copias de seguridad y recuperación de desastres, y gestión de crisis;	**Kaspersky Incident Response**	**Incident response**: obtiene una imagen detallada del incidente. El servicio cubre la investigación de incidentes y el ciclo de respuesta completos, desde la respuesta temprana a los incidentes y la recopilación de pruebas hasta la identificación de rastros adicionales de piratería informática y la preparación de un plan de mitigación.	https://www.kaspersky.es/enterprise-security/incident-response
	Kaspersky Incident Response	Desde el momento en que se descubre un incidente de ciberseguridad, toda medida cuenta. La forma en que se administran las comunicaciones, externas e internas, es fundamental, especialmente cuando se trata de vectores de ataque desconocidos y amenazas persistentes avanzadas (APT). Cualquier empresa puede ser víctima de un ciberataque, por lo que es necesario que exista un equipo de crisis —idealmente formado por especialistas del departamento de seguridad de la información, la división de operaciones y las comunicaciones corporativas— preparado para minimizar los daños. Esto puede hacerse mediante acciones autorizadas, apropiadas, precisas y oportunas. Kaspersky ha desarrollado la mejor formación que capacita a la alta dirección, a la seguridad de la información y a los profesionales de la comunicación corporativa para gestionar las comunicaciones de crisis, incluyendo el desarrollo y la aplicación de los activos adecuados, mientras se está bajo el ataque de un ciberincidente desconocido o de una amenaza persistente avanzada (APT).	https://www.kaspersky.es/enterprise-security/incident-response
2. d) seguridad de la cadena de suministro, incluidos los aspectos de seguridad relativos a las relaciones entre cada entidad y sus proveedores directos o proveedores de servicios;	**SD-Wan**	**Kaspersky SD-WAN**está diseñada para desarrollar redes seguras y tolerantes a fallos con administración unificada, una característica esencial para las actuales empresas distribuidas. La solución te permite utilizar canales de comunicación diversos, optimizar conexiones de la nube, reforzar la seguridad, mejorar el rendimiento de las aplicaciones y agilizar la implementación de servicios nuevos.	https://www.kaspersky.es/enterprise-security/sd-wan
	Kaspersky Threat Intelligence	**Threat Intelligence** de Kaspersky te proporciona acceso a la inteligencia que necesitas para mitigar ciberamenazas de la mano de nuestro equipo líder de investigadores y analistas. Gracias a nuestros conocimientos, experiencia e inteligencia avanzada de todos los aspectos relativos a la ciberseguridad, en Kaspersky nos hemos convertido en el partner de confianza de las fuerzas del orden y los organismos gubernamentales más importantes del mundo, entre las que se incluyen la Interpol e importantes equipos CERT. Kaspersky Threat Intelligence te ofrece acceso inmediato a inteligencia de amenazas táctica, operativa y estratégica. Kaspersky Threat Intelligence te permite identificar y prevenir proactivamente las amenazas, te mantiene informado sobre las últimas amenazas y vulnerabilidades y te permite tomar medidas proactivas para proteger tus sistemas antes de que se produzca un ataque.	https://www.kaspersky.es/enterprise-security/threat-intelligence
	Kaspersky MDR	**Kaspersky Managed Detection and Response** ofrece una detección, priorización, investigación y respuesta continuas, totalmente gestionadas y adaptadas individualmente. Como resultado, permite obtener todos los beneficios principales de tener su propio centro de operaciones de seguridad sin tener que establecer uno realmente. El objetivo principal del servicio de MDR es detectar amenazas en cada etapa de un ciberataque, tanto antes del riesgo real como después de que los actores maliciosos hayan penetrado en la infraestructura corporativa. Los analistas de SOC investigan las alertas y notifican al cliente acerca de la actividad maliciosa, y brindan respuestas y asesoramiento basados en herramientas, todo ello mediante una supervisión de la seguridad ininterrumpida potenciada por la búsqueda automatizada de amenazas, la investigación de incidentes y las respuestas guiadas y gestionadas	https://www.kaspersky.es/enterprise-security/managed-detection-and-response
	Scan Engine	**Kaspersky Scan Engine (KSE)** brinda una protección integral para portales y aplicaciones web, servidores proxy, sistemas de almacenamiento en red y puertas de enlace de correo. Se puede administrar e implementar fácilmente a través de ICAP y HTTP, como un servicio independiente, agrupación en clúster o contenedor Docker. KSE utiliza los últimos métodos de detección para encontrar y eliminar malware, como troyanos, amenazas de phishing, gusanos, rootkits, spyware y adware.	https://www.kaspersky.es/scan-engine

Requisito de la NIS2	Solución de Kaspersky	Ventajas	Información
Capítulo IV, Art. 21, Medidas de gestión de riesgos de ciberseguridad			
2. e) seguridad en la adquisición, desarrollo y mantenimiento de redes y sistemas de información, incluida la gestión y divulgación de vulnerabilidades;	**Evaluación de vulnerabilidades de Kaspersky**	Este servicio proporciona información sobre vulnerabilidades existentes y las consecuencias de su explotación, evalúa la eficacia de la aplicación de las medidas de seguridad implementadas y le permite planificar acciones futuras para corregir las deficiencias detectadas y mejorar la seguridad. Realizar evaluaciones de seguridad con regularidad te permite comprender claramente el estado de tu ciberseguridad y garantiza el cumplimiento de las buenas prácticas del sector.	https://www.kaspersky.es/enterprise-security/cybersecurity-services
	Fuentes de datos de amenazas de vulnerabilidades de Kaspersky	Al integrar **fuentes de inteligencia sobre amenazas** actualizadas que contienen información sobre IP, URL y hash de archivos sospechosos y maliciosos en los sistemas de seguridad existentes, como los sistemas SIEM, SOAR y las plataformas de inteligencia de amenazas, los equipos de seguridad pueden automatizar el proceso de evaluación inicial y proporcionar a los especialistas pertinentes el contexto necesario para identificar inmediatamente las alertas que requieren un análisis en profundidad, o que necesitan ser escaladas a los equipos de respuesta a incidentes para una mayor investigación y respuesta. Las fuentes de datos proceden de fuentes altamente fiables y heterogéneas, como Kaspersky Security Network y nuestras propias arañas web, nuestro servicio de supervisión de botnets (seguimiento ininterrumpido de botnets y de sus actividades y objetivos), trampas de spam, partners y equipos de investigación.	https://www.kaspersky.es/enterprise-security/threat-intelligence
	Kaspersky Next	**Kaspersky Next** es la solución de Kaspersky para proteger tu infraestructura contra ransomware, malware y amenazas evasivas y complejas. Cuenta con funcionalidad de EDR en todos los niveles, adaptada a tus necesidades y recursos. Nuestras tecnologías EDR y XDR se basan en la galardonada protección de endpoints y en controles de nivel empresarial. Obtén una novedosa eficiencia con la automatización de tareas simples y complejas junto con una respuesta guiada para impulsar tu eficacia y minimizar los recursos que necesitas para administrar tu ciberseguridad. Las opciones en la nube y en las instalaciones se adaptan a tus requisitos específicos y, llegado el momento, controlan toda tu infraestructura con XDR abierto integral.	
	Kaspersky Industrial Cybersecurity	**Kaspersky Industrial CyberSecurity (KICS)** es una plataforma de detección y respuesta extendidas (XDR) para organizaciones industriales, diseñada y certificada especialmente para proteger a equipos, activos y redes de TO críticos de ciberamenazas. La plataforma incluye tecnologías integradas que protegen los componentes de automatización industrial y sistemas de control en cada nivel. KICS for Nodes es un software de protección, detección y respuesta de endpoints con funciones de auditoría de cumplimiento y sensores de endpoints. KICS for Networks está diseñado para el análisis, la detección y la respuesta del tráfico de red de TO. La función de administración centralizada al nivel del sitio, esencial para la escalabilidad de las operaciones de seguridad de TO a un alto volumen de infraestructuras industriales de gran tamaño, diversas y distribuidas geográficamente, está integrada en la plataforma. La integración constante entre los componentes de la plataforma brinda una visibilidad total de múltiples redes de TO y sistemas de automatización distribuidos geográficamente y ofrece una mejor experiencia del cliente, conocimiento de la situación y flexibilidad de despliegue. Con detección y respuesta extendidas, la plataforma de KICS permite la convergencia TI/TO y proporciona numerosos beneficios para proveedores únicos	https://www.kaspersky.es/enterprise-security/industrial-cybersecurity
	Kaspersky Digital Footprint Intelligence	**Kaspersky Digital Footprint Intelligence** es un servicio integral de protección contra riesgos digitales que ayuda a los clientes a supervisar sus activos digitales y detectar amenazas desde la red superficial, profunda y oscura. Con alertas en tiempo real, Kaspersky Digital Footprint intelligence permite a las organizaciones responder de manera rápida y eficaz contra las amenazas potenciales. Los informes analíticos integran estos datos con la información exhaustiva de nuestros expertos, que proporciona datos sobre los riesgos de ciberseguridad y recomendaciones sobre cómo mitigarlos.	https://dfi.kaspersky.com/es

Requisito de la NIS2	Solución de Kaspersky	Ventajas	Información
Capítulo IV, Art. 21, Medidas de gestión de riesgos de ciberseguridad			
2. e) seguridad en la adquisición, desarrollo y mantenimiento de redes y sistemas de información, incluida la gestión y divulgación de vulnerabilidades;	**Kaspersky MDR**	**Kaspersky Managed Detection and Response** ofrece una detección, priorización, investigación y respuesta continuas, totalmente gestionadas y adaptadas individualmente. Como resultado, permite obtener todos los beneficios principales de tener su propio centro de operaciones de seguridad sin tener que establecer uno realmente. El objetivo principal del servicio de MDR es detectar amenazas en cada etapa de un ciberataque, tanto antes del riesgo real como después de que los actores maliciosos hayan penetrado en la infraestructura corporativa. Los analistas de SOC investigan las alertas y notifican al cliente acerca de la actividad maliciosa, y brindan respuestas y asesoramiento basados en herramientas, todo ello mediante una supervisión de la seguridad ininterrumpida potenciada por la búsqueda automatizada de amenazas, la investigación de incidentes y las respuestas guiadas y gestionadas	https://www.kaspersky.es/enterprise-security/managed-detection-and-response
2. f) políticas y procedimientos para evaluar la eficacia de las medidas de gestión de riesgos de ciberseguridad;	**Kaspersky Digital Footprint Intelligence**	**Kaspersky Digital Footprint Intelligence** es un servicio integral de protección contra riesgos digitales que ayuda a los clientes a supervisar sus activos digitales y detectar amenazas desde la red superficial, profunda y oscura. Con alertas en tiempo real, Kaspersky Digital Footprint intelligence permite a las organizaciones responder de manera rápida y eficaz contra las amenazas potenciales. Los informes analíticos integran estos datos con la información exhaustiva de nuestros expertos, que proporciona datos sobre los riesgos de ciberseguridad y recomendaciones sobre cómo mitigarlos.	https://dfi.kaspersky.com/es
	Evaluación de vulnerabilidades de Kaspersky	Este servicio proporciona información sobre vulnerabilidades existentes y las consecuencias de su explotación, evalúa la eficacia de la aplicación de las medidas de seguridad implementadas y le permite planificar acciones futuras para corregir las deficiencias detectadas y mejorar la seguridad. Realizar evaluaciones de seguridad con regularidad te permite comprender claramente el estado de tu ciberseguridad y garantiza el cumplimiento de las buenas prácticas del sector.	https://www.kaspersky.es/enterprise-security/cybersecurity-services
	Kaspersky Next	**Kaspersky Next** es la solución de Kaspersky para proteger tu infraestructura contra ransomware, malware y amenazas evasivas y complejas. Cuenta con funcionalidad de EDR en todos los niveles, adaptada a tus necesidades y recursos. Nuestras tecnologías EDR y XDR se basan en la galardonada protección de endpoints y en controles de nivel empresarial. Obtén una novedosa eficiencia con la automatización de tareas simples y complejas junto con una respuesta guiada para impulsar tu eficacia y minimizar los recursos que necesitas para administrar tu ciberseguridad. Las opciones en la nube y en las instalaciones se adaptan a tus requisitos específicos y, llegado el momento, controlan toda tu infraestructura con XDR abierto integral.	
	Fuentes de datos de amenazas de vulnerabilidades de Kaspersky	Al integrar fuentes de inteligencia sobre amenazas actualizadas que contienen información sobre IP, URL y hash de archivos sospechosos y maliciosos en los sistemas de seguridad existentes, como los sistemas SIEM, SOAR y las plataformas de inteligencia de amenazas, los equipos de seguridad pueden automatizar el proceso de evaluación inicial y proporcionar a los especialistas pertinentes el contexto necesario para identificar inmediatamente las alertas que requieren un análisis en profundidad, o que necesitan ser escaladas a los equipos de respuesta a incidentes para una mayor investigación y respuesta. Las fuentes de datos proceden de fuentes altamente fiables y heterogéneas, como Kaspersky Security Network y nuestras propias arañas web, nuestro servicio de supervisión de botnets (seguimiento ininterrumpido de botnets y de sus actividades y objetivos), trampas de spam, partners y equipos de investigación.	https://www.kaspersky.es/enterprise-security/threat-intelligence

Requisito de la NIS2	Solución de Kaspersky	Ventajas	Información
Capítulo IV, Art. 21, Medidas de gestión de riesgos de ciberseguridad			
2. f) políticas y procedimientos para evaluar la eficacia de las medidas de gestión de riesgos de ciberseguridad;	**Kaspersky Industrial Cybersecurity**	**Kaspersky Industrial Cybersecurity (KICS)** es una plataforma de detección y respuesta extendidas (XDR) para organizaciones industriales, diseñada y certificada especialmente para proteger a equipos, activos y redes de TO críticos de ciberamenazas. La plataforma incluye tecnologías integradas que protegen los componentes de automatización industrial y sistemas de control en cada nivel. KICS for Nodes es un software de protección, detección y respuesta de endpoints con funciones de auditoría de cumplimiento y sensores de endpoints. KICS for Networks está diseñado para el análisis, la detección y la respuesta del tráfico de red de TO. La función de administración centralizada al nivel del sitio, esencial para la escalabilidad de las operaciones de seguridad de TO a un alto volumen de infraestructuras industriales de gran tamaño, diversas y distribuidas geográficamente, está integrada en la plataforma. La integración constante entre los componentes de la plataforma brinda una visibilidad total de múltiples redes de TO y sistemas de automatización distribuidos geográficamente y ofrece una mejor experiencia del cliente, conocimiento de la situación y flexibilidad de despliegue. Con detección y respuesta extendidas, la plataforma de KICS permite la convergencia TI/TO y proporciona numerosos beneficios para proveedores únicos	https://www.kaspersky.es/enterprise-security/industrial-cybersecurity
	Kaspersky MDR	**Kaspersky Managed Detection and Response** ofrece una detección, priorización, investigación y respuesta continuas, totalmente gestionadas y adaptadas individualmente. Como resultado, permite obtener todos los beneficios principales de tener su propio centro de operaciones de seguridad sin tener que establecer uno realmente. El objetivo principal del servicio de MDR es detectar amenazas en cada etapa de un ciberataque, tanto antes del riesgo real como después de que los actores maliciosos hayan penetrado en la infraestructura corporativa. Los analistas de SOC investigan las alertas y notifican al cliente acerca de la actividad maliciosa, y brindan respuestas y asesoramiento basados en herramientas, todo ello mediante una supervisión de la seguridad ininterrumpida potenciada por la búsqueda automatizada de amenazas, la investigación de incidentes y las respuestas guiadas y gestionadas	https://www.kaspersky.es/enterprise-security/managed-detection-and-response
2. g) prácticas básicas de higiene cibernética y formación en ciberseguridad;	**Concienciación con Kaspersky Security Awareness**	**Kaspersky Security Awareness**: un nuevo enfoque para dominar las competencias de seguridad informática; Kaspersky Security Awareness es una solución eficaz y de eficacia probada con un largo historial internacional de éxitos. Utilizada por empresas de todos los tamaños para formar a más de un millón de empleados en más de 75 países, la solución abarca más de 25 años de conocimientos en ciberseguridad de Kaspersky con una amplia experiencia en formación de adultos. Estas soluciones de formación interesantes y eficaces aumentan la concienciación de ciberseguridad de tu personal para que todos desempeñen su labor en la ciberseguridad general de tu organización. Como los cambios de comportamiento sostenibles llevan tiempo, nuestro enfoque implica la creación de un ciclo de aprendizaje continuo con múltiples componentes	https://www.kaspersky.es/enterprise-security/security-awareness
	Kaspersky Formación para expertos	**Kaspersky xTraining** es la respuesta a un panorama de ciberamenazas en constante evolución. Aportamos conocimientos actualizados sobre estrategias eficaces de detección y mitigación de amenazas a partir de experiencias exhaustivas y conocidas del Kaspersky Global Research & Analysis Team (GReAT)	https://xtraining.kaspersky.com/
	Formación ICS	**Kaspersky ICS CERT** es un proyecto global establecido en 2016 para coordinar los esfuerzos de los proveedores de sistemas de automatización industrial y los propietarios y operadores de instalaciones industriales. El equipo cuenta con más de 30 expertos en investigación de amenazas y vulnerabilidades de ICS, respuesta a incidentes y análisis de seguridad. Brindamos formación en los aspectos básicos de la ciberseguridad industrial y las habilidades prácticas para investigar incidentes de ciberseguridad y llevar a cabo investigaciones de vulnerabilidades. Nuestros programas se basan en la experiencia práctica y en casos reales. El equipo de Kaspersky ICS CERT imparte cursos de formación para diferentes operadores del sector ICS, desde operadores de campo hasta el nivel C, incluidos los profesionales de la ciberseguridad dedicados al TO.	https://ics-cert.kaspersky.com/media/services/Kaspersky-Industrial-Cybersecurity-training-program-En.pdf

Requisito de la NIS2	Solución de Kaspersky	Ventajas	Información
Capítulo IV, Art. 21, Medidas de gestión de riesgos de ciberseguridad			
2. h) políticas y procedimientos relativos al uso de criptografía y, en su caso, cifrado;	**Kaspersky Next**	**Kaspersky Next** es la solución de Kaspersky para proteger tu infraestructura contra ransomware, malware y amenazas evasivas y complejas. Cuenta con funcionalidad de EDR en todos los niveles, adaptada a tus necesidades y recursos. Nuestras tecnologías EDR y XDR se basan en la galardonada protección de endpoints y en controles de nivel empresarial. Obtén una novedosa eficiencia con la automatización de tareas simples y complejas junto con una respuesta guiada para impulsar tu eficacia y minimizar los recursos que necesitas para administrar tu ciberseguridad. Las opciones en la nube y en las instalaciones se adaptan a tus requisitos específicos y, llegado el momento, controlan toda tu infraestructura con XDR abierto integral.	
2. i) seguridad de los recursos humanos, políticas de control de acceso y gestión de activos;	**Kaspersky MDR**	**Kaspersky Managed Detection and Response** ofrece una detección, priorización, investigación y respuesta continuas, totalmente gestionadas y adaptadas individualmente. Como resultado, permite obtener todos los beneficios principales de tener su propio centro de operaciones de seguridad sin tener que establecer uno realmente. El objetivo principal del servicio de MDR es detectar amenazas en cada etapa de un ciberataque, tanto antes del riesgo real como después de que los actores maliciosos hayan penetrado en la infraestructura corporativa. Los analistas de SOC investigan las alertas y notifican al cliente acerca de la actividad maliciosa, y brindan respuestas y asesoramiento basados en herramientas, todo ello mediante una supervisión de la seguridad ininterrumpida potenciada por la búsqueda automatizada de amenazas, la investigación de incidentes y las respuestas guiadas y gestionadas	https://www.kaspersky.es/enterprise-security/managed-detection-and-response
	Kaspersky Digital Footprint Intelligence	**Kaspersky Digital Footprint Intelligence** es un servicio integral de protección contra riesgos digitales que ayuda a los clientes a supervisar sus activos digitales y detectar amenazas desde la red superficial, profunda y oscura. Con alertas en tiempo real, Kaspersky Digital Footprint intelligence permite a las organizaciones responder de manera rápida y eficaz contra las amenazas potenciales. Los informes analíticos integran estos datos con la información exhaustiva de nuestros expertos, que proporciona datos sobre los riesgos de ciberseguridad y recomendaciones sobre cómo mitigarlos.	https://dfi.kaspersky.com/es
2. j) el uso de soluciones de autenticación multifactor o autenticación continua, comunicaciones de voz, video y texto seguras y sistemas de comunicación de emergencia seguros dentro de la entidad, cuando proceda.	**Kaspersky Next**	**Las plataformas de gestión de soluciones Kaspersky Next** incluyen la configuración de autenticación de doble factor como herramienta de control de acceso seguro.	
	Kaspersky Threat Intelligence	El portal de **inteligencia sobre amenazas** proporciona acceso a la plataforma web y acceso a través de Open API	https://www.kaspersky.es/enterprise-security/threat-intelligence

Requisito de la NIS2	Solución de Kaspersky	Ventajas	Información
Capítulo IV, Art. 23, Requisitos de información			
4. d) Los Estados miembros velarán por que, a efectos de la notificación prevista en el apartado 1, las entidades de que se trate se sometan al CSIRT o, en su caso, a la autoridad competente: (a) sin demoras indebidas y, en cualquier caso, en el plazo de 24 horas a partir del momento en que se tenga conocimiento del incidente significativo, una alerta rápida, en la que, cuando proceda, se indicará si se sospecha que el incidente significativo ha sido causado por actos ilícitos o dolosos o podría tener repercusiones transfronterizas; (b) sin demoras indebidas y, en cualquier caso, en el plazo de 72 horas a partir del momento en que se tenga conocimiento del incidente significativo, una notificación del incidente, en la que, cuando proceda, se actualizará la información a que se refiere la letra a) y se indicará una evaluación inicial del incidente significativo, incluida su gravedad e impacto, así como, cuando se disponga de ellos, los indicadores de compromiso; (c) a petición de un CSIRT o, en su caso, de la autoridad competente, un informe intermedio sobre las actualizaciones de situación pertinentes; (d) un informe final, a más tardar un mes después de la presentación de la notificación del incidente con arreglo a la letra b), que incluya lo siguiente: (i) una descripción detallada del incidente, incluida su gravedad e impacto; (ii) el tipo de amenaza o causa principal que probablemente haya desencadenado el incidente;	**Kaspersky Incident Response**	**Incident response**: obtiene una imagen detallada del incidente. El servicio cubre la investigación de incidentes y el ciclo de respuesta completos, desde la respuesta temprana a los incidentes y la recopilación de pruebas hasta la identificación de rastros adicionales de piratería informática y la preparación de un plan de mitigación.	https://www.kaspersky.es/enterprise-security/incident-response
	Kaspersky APT, Crimeware, informes ICS	Con los informes de inteligencia, los clientes de Kaspersky se beneficiarán de un acceso constante y exclusivo a análisis y perspectivas, incluidos datos técnicos exhaustivos (en una amplia gama de formatos) sobre actores APT dirigidos a tu industria y geografía, conocerán y contrarrestarán adecuadamente el software delictivo y las ciberamenazas que afectan a las organizaciones industriales (incluidas las amenazas que nunca se harán públicas). Los informes contienen un resumen de información inmediata y relevante que ilustra cada detalle del ataque, además de ofrecer una descripción técnica detallada con las normas YARA e IoC pertinentes, ofreciendo a los investigadores de seguridad, analistas de malware, ingenieros de seguridad, analistas de redes de seguridad e investigadores de APT, datos aplicables que permiten una respuesta precisa y rápida a las amenazas.	https://www.kaspersky.es/enterprise-security/threat-intelligence
	Kaspersky Threat Lookup	**Kaspersky Threat Lookup** proporciona todos los conocimientos de Kaspersky sobre ciberamenazas y las relaciones entre ellas, reunidos en un único y potente servicio web. El objetivo es proporcionar a los equipos de seguridad tantos datos como sea posible para prevenir los ataques informáticos antes de que comprometan a la organización. La plataforma recupera la inteligencia de amenazas más reciente sobre URL, dominios, direcciones IP, hash de archivos, nombres de amenazas, datos estadísticos y de comportamiento, datos de WHOIS y DNS, atributos de archivos, datos de geolocalización, descarga de cadenas, marcas de tiempo, etc. El resultado es una visibilidad global de las amenazas nuevas y emergentes: esto te permite proteger mejor tu empresa, mejorando significativamente la calidad y la eficacia de las actividades de respuesta a incidentes.	https://www.kaspersky.es/enterprise-security/threat-intelligence
	Kaspersky Threat Analysis	Ante una posible amenaza cibernética, es esencial tomar una decisión a tiempo. Además de tecnologías de análisis de amenazas como el sandboxing, **Kaspersky Threat Analysis** ofrece tecnologías de atribución de vanguardia (un enfoque multicapa que proporciona un análisis eficaz de las amenazas, para que puedas tomar decisiones con pleno conocimiento de causa para defenderte de los ataques incluso antes de que se inicien). Varias herramientas de análisis de amenazas se combinan para permitirte a ti y a tu equipo analizar la situación desde todos los ángulos, teniendo una imagen completa del entorno de amenazas, y responder de manera rápida y efectiva.	https://www.kaspersky.es/enterprise-security/threat-intelligence
	Kaspersky MDR	**Kaspersky Managed Detection and Response** ofrece una detección, priorización, investigación y respuesta continuas, totalmente gestionadas y adaptadas individualmente. Como resultado, permite obtener todos los beneficios principales de tener su propio centro de operaciones de seguridad sin tener que establecer uno realmente. El objetivo principal del servicio de MDR es detectar amenazas en cada etapa de un ciberataque, tanto antes del riesgo real como después de que los actores maliciosos hayan penetrado en la infraestructura corporativa. Los analistas de SOC investigan las alertas y notifican al cliente acerca de la actividad maliciosa, y brindan respuestas y asesoramiento basados en herramientas, todo ello mediante una supervisión de la seguridad ininterrumpida potenciada por la búsqueda automatizada de amenazas, la investigación de incidentes y las respuestas guiadas y gestionadas	https://www.kaspersky.es/enterprise-security/managed-detection-and-response

Kaspersky comprende las necesidades de los diferentes sectores y tamaños de empresa y **protege a más de 220 000 empresas de todo el mundo** contra las ciberamenazas. La fiable ciberprotección todo en uno de Kaspersky cubre múltiples dimensiones de protección. **¡Protégete ya!**

kaspersky.es

Requisito de la NIS2	Solución de Kaspersky	Ventajas	Información
Capítulo IV, Art. 23, Requisitos de información			
4. d) Los Estados miembros velarán por que, a efectos de la notificación prevista en el apartado 1, las entidades de que se trate se sometan al CSIRT o, en su caso, a la autoridad competente: (a) sin demoras indebidas y, en cualquier caso, en el plazo de 24 horas a partir del momento en que se tenga conocimiento del incidente significativo, una alerta rápida, en la que, cuando proceda, se indicará si se sospecha que el incidente significativo ha sido causado por actos ilícitos o dolosos o podría tener repercusiones transfronterizas; (b) sin demoras indebidas y, en cualquier caso, en el plazo de 72 horas a partir del momento en que se tenga conocimiento del incidente significativo, una notificación del incidente, en la que, cuando proceda, se actualizará la información a que se refiere la letra a) y se indicará una evaluación inicial del incidente significativo, incluida su gravedad e impacto, así como, cuando se disponga de ellos, los indicadores de compromiso; (c) a petición de un CSIRT o, en su caso, de la autoridad competente, un informe intermedio sobre las actualizaciones de situación pertinentes; (d) un informe final, a más tardar un mes después de la presentación de la notificación del incidente con arreglo a la letra b), que incluya lo siguiente: (i) una descripción detallada del incidente, incluida su gravedad e impacto; (ii) el tipo de amenaza o causa principal que probablemente haya desencadenado el incidente;	**EDR Optimum**	La visibilidad limitada y la falta de recursos juegan a favor de los atacantes. **Kaspersky Endpoint Detection and Response (EDR) Optimum** ofrece detección avanzada, funciones de investigación simplificadas y respuesta automatizada en un paquete fácil de usar para proteger tu empresa de las amenazas más recientes.	https://www.kaspersky.es/enterprise-security/edr-security-software-solution
	EDR Expert	Los ciberataques son cada vez más sofisticados y capaces de evitar las medidas de seguridad existentes. **Kaspersky Endpoint Detection and Response (EDR) Expert** ofrece visibilidad completa de todos los endpoints en la red corporativa y defensas de nivel superior mediante la automatización de las tareas rutinarias de EDR. Además, hace que los analistas puedan detectar, priorizar, analizar y neutralizar amenazas complejas y ataques de tipo APT más fácilmente. Kaspersky EDR Expert utiliza un único agente que se puede gestionar tanto desde una única plataforma de gestión basada en la nube, como desde una consola offline en entornos de brecha física, para aprovechar las tecnologías de inteligencia sobre amenazas e incorporar estrategias de detección personalizables.	https://www.kaspersky.es/enterprise-security/endpoint-detection-response-edr
	Kaspersky XDR	**Kaspersky XDR** es una plataforma abierta, una herramienta universal para crear un ecosistema unificado de productos de ciberseguridad. La plataforma actúa como una solución Anti APT todo en uno impulsada por Kaspersky Threat Intelligence que monitoriza todos los posibles puntos de entrada de ciberdelincuentes, correlacionando la información y orquestando todos los componentes de protección de la infraestructura. Kaspersky XDR incluye una amplia variedad de integraciones listas para usarse con Kaspersky y productos de terceros	https://www.kaspersky.es/enterprise-security/xdr
	Kaspersky Industrial Cybersecurity	**Kaspersky Industrial CyberSecurity (KICS)** es una plataforma de detección y respuesta extendidas (XDR) para organizaciones industriales, diseñada y certificada especialmente para proteger a equipos, activos y redes de TO críticos de ciberamenazas. La plataforma incluye tecnologías integradas que protegen los componentes de automatización industrial y sistemas de control en cada nivel. KICS for Nodes es un software de protección, detección y respuesta de endpoints con funciones de auditoría de cumplimiento y sensores de endpoints. KICS for Networks está diseñado para el análisis, la detección y la respuesta del tráfico de red de TO. La función de administración centralizada al nivel del sitio, esencial para la escalabilidad de las operaciones de seguridad de TO a un alto volumen de infraestructuras industriales de gran tamaño, diversas y distribuidas geográficamente, está integrada en la plataforma. La integración constante entre los componentes de la plataforma brinda una visibilidad total de múltiples redes de TO y sistemas de automatización distribuidos geográficamente y ofrece una mejor experiencia del cliente, conocimiento de la situación y flexibilidad de despliegue. Con detección y respuesta extendidas, la plataforma de KICS permite la convergencia TI/TO y proporciona numerosos beneficios para proveedores únicos	https://www.kaspersky.es/enterprise-security/industrial-cybersecurity
	Kaspersky Container Security	**La solución de Kaspersky Container Security (KCS)** protege cada etapa del ciclo de vida de una aplicación contenerizada, desde el desarrollo hasta la operación. Protege los procesos comerciales de la organización, de acuerdo con los estándares y las regulaciones de seguridad, y admite la implementación de un enfoque DevSecOps. Kaspersky Container Security brinda una protección integral frente a las últimas ciberamenazas y automatiza tus auditorías de cumplimiento, liberando los recursos del equipo de seguridad de la información para ocuparse de otras tareas y reduciendo el plazo de lanzamiento. Kaspersky Container Security se ha desarrollado de manera específica para los entornos contenedorizados, a fin de garantizar la protección en los diferentes niveles, desde la imagen del contenedor hasta el sistema operativo host.	https://www.kaspersky.es/enterprise-security/container-security

Noticias sobre ciberamenazas: securelist.com
Kaspersky Blog: kaspersky.co.uk/blog
Ciberseguridad para grandes empresas: kaspersky.com/small-to-medium-business-security
Ciberseguridad para medianas empresas: kaspersky.es/enterprise-security

2025 AO Kaspersky Lab.
Las marcas comerciales y marcas de servicios registradas pertenecen a sus respectivos propietarios.

Kaspersky comprende las necesidades de los diferentes sectores y tamaños de empresa y **protege a más de 220 000 empresas de todo el mundo** contra las ciberamenazas. La fiable ciberprotección todo en uno de Kaspersky cubre múltiples dimensiones de protección. **¡Protégete ya!**

kaspersky.es