kaspersky preparados para el futuro

La Directiva NIS 2 de la UE: Nuevas obligaciones y cómo prepararse para cumplirlas



¿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. En España, el Consejo de Ministros aprobó el anteproyecto de ley el 14 de enero de 2025, pero sigue pendiente su aprobación definitiva. 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.

¿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.

Estas medidas 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:

- Políticas de análisis de riesgos y seguridad de los sistemas de información;
- Gestión de incidentes;
- Continuidad del negocio, como gestión de copias de seguridad y recuperación de desastres, y gestión de crisis;
- 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;
- Seguridad en la adquisición, desarrollo y mantenimiento de redes y sistemas de información, incluida la gestión y divulgación de vulnerabilidades;
- Políticas y procedimientos para evaluar la eficacia de las medidas de gestión de riesgos de ciberseguridad;
- Prácticas básicas de higiene digital y formación en ciberseguridad;
- Políticas y procedimientos relativos al uso de criptografía y, en su caso, cifrado;
- Seguridad de los recursos humanos, políticas de control de acceso y gestión de activos; uso de soluciones de autenticación multifactor o autenticación continua, comunicaciones de voz, vídeo y texto seguras y sistemas de comunicación de emergencia seguros dentro de la entidad, cuando proceda.

[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



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!

¿Cuáles son las sanciones por incumplimiento?

Las autoridades competentes pueden imponer multas administrativas significativas por incumplimiento de las obligaciones derivadas de la legislación nacional de adopción de la Directiva NIS 2. Estas multas pueden ascender a un máximo de hasta 10 millones de euros o el 2 % del volumen de negocios anual mundial del grupo de empresas en el caso de empresas o entidades esenciales, o hasta 7 millones de euros o el 1,4 % del volumen de negocios anual mundial del grupo en el caso de empresas importantes u otras entidades.

¿Cómo deben empezar a prepararse las empresas? Recomendaciones

Las empresas y otras entidades deben empezar a prepararse ya:

- Evaluando si estarás sujeto a las obligaciones de ciberseguridad de la Directiva NIS 2 y en qué medida.
- Consulta la adaptación de la Directiva SRI a la legislación nacional de tu Estado miembro.
- Sigue la información y las recomendaciones de tus autoridades nacionales de ciberseguridad[3]
- Evalúa y sigue desarrollando las medidas técnicas, operativas y organizativas para gestionar los riesgos que plantea la seguridad de los sistemas de red y de información.

¿Cómo pueden ayudar a tu empresa las soluciones y servicios de Kaspersky?

Como proveedor de ciberseguridad, Kaspersky aprovecha toda su experiencia para ayudar a las organizaciones a crear ciberdefensas sólidas. Podemos ayudarte con las siguientes soluciones y servicios:

Endpoint Detection and Response (EDR) es una solución técnica que proporciona información detallada sobre lo que ocurre en tus endpoints. Con Kaspersky Endpoint Detection & Response (EDR) Optimum puedes analizar proactivamente tu red de servidores y clientes en busca de Indicadores de Compromiso (IoC) específicos. Tu departamento de TI o un proveedor de servicios externo adquieren un conocimiento profundo de los ciberataques inminentes y pueden tomar medidas inmediatas en caso necesario. En caso de incidente, recibirás datos importantes para el análisis de la causa raíz.

Managed Detection and Response (MDR) te permite subcontratar tu ciberprotección a nuestros expertos. Los cazadores de amenazas de Kaspersky supervisan los datos de telemetría de tus sistemas informáticos y detectan inmediatamente cualquier actividad sospechosa. Este servicio ininterrumpido lo prestan especialistas ubicados en varios Centros de Operaciones de Seguridad (SOC) de todo el mundo.

Concienciación: Kaspersky ha desarrollado un concepto global eficaz para desarrollar la experiencia en ciberseguridad dentro de la empresa. El espectro abarca desde la formación general para sensibilizar y motivar a su equipo, hasta la formación especializada para el personal del servicio de asistencia y la formación en línea para directivos. Nuestra plataforma interactiva de formación en línea, KASAP, ofrece a tu equipo una formación práctica sobre concienciación en materia de seguridad que puede integrarse fácilmente en la rutina diaria de trabajo. Los participantes pueden trabajar de forma flexible a través de los módulos de aprendizaje en línea y repetirlos en cualquier momento.

Inteligencia sobre amenazas (TI): el liderazgo en el sector (TI), proporciona a las organizaciones una visión de 360 grados del panorama de las amenazas. Les da acceso a la completa base de datos de amenazas de Kaspersky y al conocimiento experto del entorno de TI y TO. Esto les permite detectar a tiempo ataques inminentes, reforzar las medidas de seguridad y endurecer sus sistemas.

Respuesta a incidentes (IR): En caso de incidente de seguridad, las organizaciones bien preparadas tienen la ventaja de poder responder con mayor rapidez y eficacia. Kaspersky ofrece una gama de servicios de respuesta a incidentes para ayudar a las organizaciones a prepararse para una emergencia. Por ejemplo, Kaspersky Tabletop Exercise (TTX) es un ejercicio guiado que te permite revisar tus procesos y planes de respuesta a incidentes. Identificarás las lagunas de tu plan de emergencia, aclararás las funciones y responsabilidades del equipo y mejorarás la coordinación entre departamentos.

Ciberseguridad industrial: Kaspersky Industrial Cybersecurity (KICS) es una solución industrial probada y certificada que responde a las necesidades específicas de ciberseguridad de las empresas industriales y los operadores de infraestructuras críticas. KICS ya protege a más de 1000 clientes industriales de gama alta en todo el mundo.

[3] Véanse, por ejemplo, las recomendaciones de NCSC Irlanda: https://www.ncsc.gov.ie/pdfs/NCSC_NIS2_Guide.pdf ; el ANSSI francés: https://www.ssi.gouv.fr/directive-nis-2/; o CCBBélgica: https://ccb.belgium.be/en/nis-2-directive-what-does-it-mean-my-organization#_Toc128118851

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

kaspersky.es

2024 AO Kaspersky Lab. Las marcas comerciales y marcas de servicios registradas pertenecen a sus respectivos propietarios.