Sophos
Directiva NIS2

Álvaro Fernández
Director Comercial Sophos Iberia

SOPHOS

Agenda

El **contexto**

El **propósito** de la NIS 2

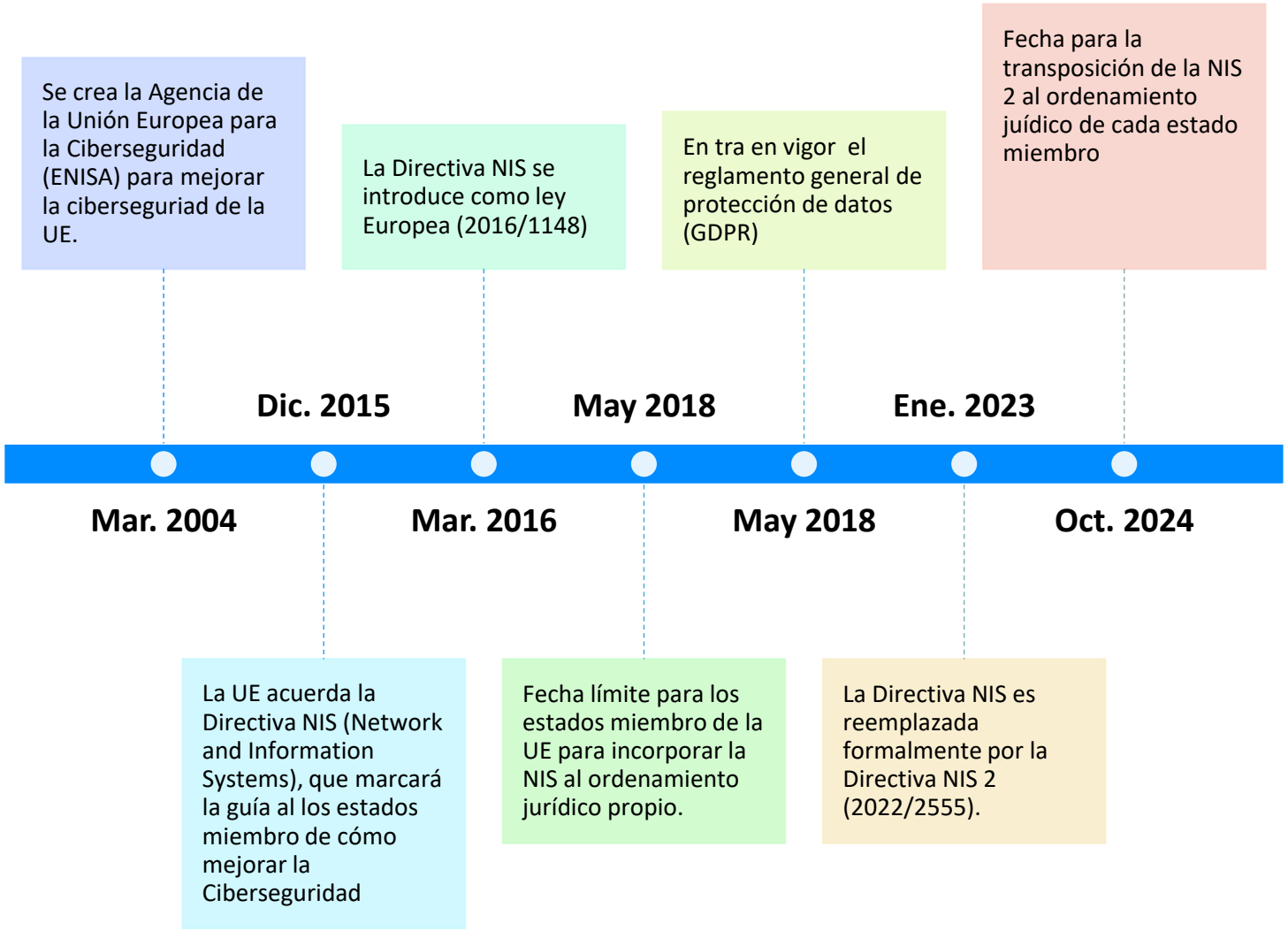
Medidas Clave de la legislación

Impacto de los cambios

Acciones que hay que tomar

Cómo ayuda **Sophos y Conclusiones**

Contexto 1 – Inicitativas Clave de la Unión Europea



Contexto 2 – Las Amenazas

Mayor dependencia de la tecnología por parte de la sociedad, debido a la transformación digital que fue acelerada por el COVID.

Gran incremento de los ciberataques, especialmente de Ransomware.

Aumento de los atques a la cadena de suministro en un mundo interconectado.

Contexto estratégico debido a la Guerra en Ukrania

La aceptación de, si bien la Directiva NIS original ha mejorado la coherencia, los estándares de ciberseguridad y resiliencia en toda la UE todavía varían ampliamente y existe una visión **inconsistente** en toda la UE sobre las amenazas cibernéticas.

El propósito de la NIS 2

La UE quiere asegurarse de que sus ciudadanos y sus economías estén protegidos del creciente riesgo de las amenazas cibernéticas

La directvia NIS 2 busca mejorar la postura de Seguridad de forma común en los diferentes estados miembro

Por lo tanto, la NIS2 se basa en los requisitos de la Directiva NIS original. La intención sigue siendo proteger las infraestructuras y organizaciones críticas dentro de la UE y elevar la postura de ciberseguridad de los diferentes Estados miembros

Eliminar las diferencias en materia de ciberseguridada de los diferentes Estados miembros

NIS 2 – Puntos Clave

La NIS2 exige que los Estados miembros adopten una serie de medidas adicionales, entre ellas:

- Mayor resiliencia cibernética entre los proveedores de servicios esenciales
- Endurecer los estándares y las sanciones de ciberseguridad para mejorar la resiliencia
- Mayor capacidad para anticipar y responder a los ciberataques
- Respuesta mejorada ante incidentes en toda la UE

Mayor resiliencia cibernética entre los proveedores de servicios esenciales

Afecta a más sectores de actividad que la NIS1

Hay dos categorías de organización: esencial e importante.

Las organizaciones que son subcontratistas y proveedores de servicios que brindan soporte están específicamente cubiertas.

Se aplica independientemente del tamaño cuando una entidad es el único proveedor en un Estado miembro de un servicio que es crítico y cuya interrupción tendría un impacto significativo.

Se espera que el NIS 2 se aplique a una amplia gama de empresas que prestan sus servicios o llevan a cabo sus actividades en la UE, incluso si no tienen su sede en un Estado miembro..

NIS 2 Sectores de actividad afectados

Alta criticidad (detallados en el anexo I) y otros sectores críticos (anexo II), tanto del sector público como del sector privado que se consideren medianas o grandes empresas (según la Recomendación 2003/361/CE una mediana empresa ocupa entre 50 y 250 empleados, tiene un volumen de negocios que no excede los 50M €

- **Sectores de alta criticidad** (detalladas en el Anexo I de la Directiva):
  - Energía
  - Transporte
  - Banca
  - Infraestructuras de los mercados financieros
  - Sector Sanitario
  - Agua Potable
  - Aguas residuales
  - Infraestructura digital
  - Gestión de servicios TIC a empresas
  - Administración pública
  - Espacio

- **Otros Sectores críticos** (Anexo II de la Directiva):
  - Servicios postales
  - Gestión de residuos
  - Fabricación, producción y distribución de sustancias y mezclas químicas
  - Producción, transformación y distribución de alimentos
  - Fabricación
  - Proveedores de Servicios Digitales
  - Investigación

Endurecer los estándares y las sanciones de ciberseguridad para mejorar la resiliencia (1)

- La directiva NIS original otorgaba a las organizaciones flexibilidad para cumplir con las regulaciones. Sin embargo, esta flexibilidad llevó a que algunas organizaciones no tomaran las medidas necesarias para protegerse a sí mismas y a sus clientes de las amenazas cibernéticas.
- La NIS2 refuerza los requisitos de seguridad e introduce sanciones para las organizaciones que no cumplan con la directiva. La intención es tener una aplicación y sanciones armonizadas.
- Gran parte de los detalles relevantes sobre lo que se requiere se encuentran en el artículo 21 de la Directiva.

Endurecer los estándares y las sanciones de ciberseguridad para mejorar la resiliencia (2)

- El **artículo 21** de la Directiva detalla las medidas necesarias, entre ellas:

  - **"Higiene cibernética"** básica, que abarca prácticas básicas como la gestión de contraseñas, la protección de los administradores de sistemas, las actualizaciones de software y la realización de copias de seguridad.
  - Gestión de vulnerabilidades
  - Formación en ciberseguridad
  - Seguridad de la **cadena de suministro**
  - Estándares de **cifrado** y criptografía
  - **Gestión de activos**
  - Control de acceso y seguridad de confianza cero **(ZTNA)**
  - Proceso de **análisis de riesgos** que identifica las medidas que deben adoptarse
  - **Gestión y notificación de incidentes**

Endurecer los estándares y las sanciones de ciberseguridad para mejorar la resiliencia (4)

- Las sanciones incluyen la necesidad de responder a las órdenes derivadas de la implementación de auditorías de seguridad que midan el cumplimiento de la Directiva NIS 2.
- Se estima que las empresas actualmente cubiertas por la Directiva NIS necesitarán **aumentar los presupuestos de TIC hasta en un 12%** para cumplir con la NIS2. Para aquellas que se adhieran a ella recientemente, la estimación es de hasta un 22%. Sin embargo, en la Directiva se reconoce que los costes deben ser proporcionados.
- Las sanciones pueden incluir **multas administrativas de hasta 10 millones de euros o el 2%** de la facturación mundial de la organización.
- **La alta dirección de las entidades críticas**

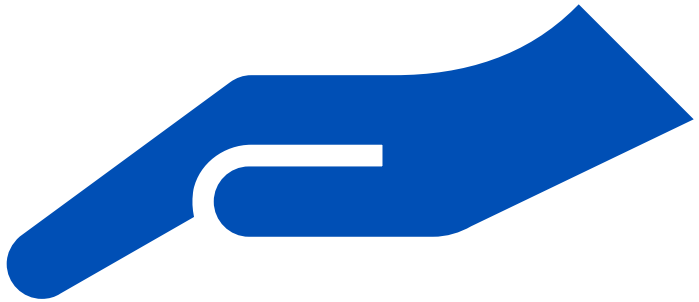
Endurecer los estándares y las sanciones de ciberseguridad para mejorar la resiliencia (5)

- Los miembros de los órganos de dirección están obligados a tener conocimientos prácticos suficientes en ciberseguridad:
  - Formarse y demostrar conocimientos en ciberseguridad.
  - Articular formaciones en ciberseguridad para su plantilla:
    - Conocimientos y destrezas suficientes.
    - Capacidades de detección de riesgos.
    - Evaluar prácticas de gestión del riesgo.
  - Aprobar medidas para la gestión de riesgos.
  - Supervisar la puesta en práctica de las medidas.
  - Responder personalmente por el incumplimiento.

Mayor capacidad para anticipar y responder a los ciberataques

- La Directiva reconoce que, para poder mejorar su respuesta a los ciberataques, es necesario mejorar la coordinación y la comunicación.

- Esto se aplica tanto entre los Estados miembros como entre los gobiernos y entre las entidades del sector público y privado. Por lo tanto, se hace hincapié en la presentación de informes de forma ágil y oportuna.



Respuesta mejorada ante incidentes en toda la UE

- Con la Directiva NIS original, las organizaciones solo debían informar los incidentes que tuvieran un impacto significativo en sus operaciones. Como resultado de este elemento discrecional, muchas organizaciones no informaron los incidentes.
- Según la NIS2, existe la obligación de **informar los incidentes cibernéticos, independientemente del impacto**. El objetivo de este cambio es garantizar que las autoridades nacionales pertinentes puedan rastrear las amenazas.
- Existen requisitos obligatorios para el momento de informar los incidentes al Centro Nacional de Seguridad Cibernética (CSIRT) pertinente. Los incidentes significativos deben informarse dentro de las 24 horas posteriores a los informes de actualización.
- Los estados deben tener un plan de respuesta a incidentes y haber establecido un Equipo Nacional de Respuesta a Incidentes de Seguridad Informática (CSIRT).

Respuesta mejorada ante incidentes en toda la UE

- Antes de 24 h.: alerta temprana.
- Antes de 72 h.: notificación de incidente.
- Antes de 1 mes: informe final (+ intermedio + posterior)

¿Qué significa todo esto?

- Más organizaciones se verán afectadas y se les exigirá que cumplan con la Directiva NIS 2. Deberán introducir nuevos sistemas y prácticas de ciberseguridad, lo que podría tener importantes implicaciones financieras.

- Las organizaciones que ya están cubiertas por la NIS pueden tener que ajustar su postura de ciberseguridad para cumplir con las nuevas normas obligatorias y mejoradas, lo que también tendrá implicaciones financieras.
- AAPP > ENS ALTO

Lo que debes hacer – Acciones clave

- **Comprenda** qué Estado miembro (o Estados) tiene jurisdicción sobre su empresa a efectos de la NIS 2 e identifique qué medidas de gestión de riesgos de ciberseguridad debe implementar para cumplir con la normativa**.**
- **Identifique, evalúe y aborde sus riesgos cibernéticos.**
- **Trabaje con las medidas establecidas en el artículo 21** y compárelas con un marco de seguridad adecuado, como la norma ISO 27001.
- **Concéntrese en los riesgos de su cadena de suministro,** en particular en lo que respecta al software.
- **Comprenda cuánto costará "tomar medidas técnicas, operativas y organizativas adecuadas y proporcionadas para gestionar los riesgos".**
- **Formalice un plan de respuesta a incidentes** y comprenda sus requisitos de presentación de informes.
- Obtenga la **aprobación formal de la alta dirección.**

¿Cómo puede ayudar Sophos?

SOPHOS

White Paper

SOPHOS

La Directiva SRI 2

Requisitos, efectos y datos clave

Este monográfico se ha redactado en colaboración con el abogado Dr. David Bomhard de Noerr Partnerschaftsgesellschaft mbB.

En respuesta a la creciente amenaza de los ciberataques y la consiguiente necesidad de incrementar las defensas (incluidas las defensas técnicas) contra tales incidentes, el Consejo de la Unión Europea y el Parlamento Europeo han adoptado la Directiva sobre la seguridad de las redes y sistemas de información 2.0 (Directiva (UE) 2022/2555, «Directiva SRI 2»). Esta Directiva dispone unos requisitos de seguridad TI revisados y más amplios para todos los Estados miembros de la UE. Uno de los propósitos más importantes de esta legislación sobre seguridad TI en la UE es contribuir «al funcionamiento eficaz de su economía y su sociedad» (véase el considerando 1 de la Directiva SRI 2).

White Paper

B. Productos de Sophos para operadores de entidades esenciales e importantes

REQUISITOS DE LA DIRECTIVA SRI 2	SOLUCIÓN DE SOPHOS	CÓMO CONTRIBUYE
Capítulo IV, Artículo 20, Gobernanza		
2. Los Estados miembros garantizarán que los miembros de los órganos de dirección de las entidades esenciales e importantes deban asistir a formaciones y alentarán a estas entidades para que ofrezcan formaciones similares a sus empleados periódicamente al objeto de adquirir conocimientos y destrezas suficientes que les permitan detectar riesgos y evaluar las prácticas de gestión de riesgos de ciberseguridad y su repercusión en los servicios proporcionados por la entidad.	**Formación y certificaciones de Sophos**	Cursos de formación y certificaciones que ayuden a Partners y clientes a sacar el máximo partido de los despliegues de seguridad de Sophos; acceso a los conocimientos y experiencias más recientes en materia de prácticas recomendadas de seguridad.
	Sophos Phish Threat	Ofrece ciberataques de phishing simulados y formación de concienciación en materia de seguridad para los usuarios finales de la organización. Los cursos abarcan una amplia gama de temas, desde lecciones generales sobre phishing y ciberseguridad hasta prevención de pérdida de datos, protección de contraseñas y mucho más.
Capítulo IV, Artículo 21, Medidas para la gestión de riesgos de ciberseguridad		
2. Los Estados miembros velarán por que las entidades esenciales e importantes tomen las medidas técnicas, operativas y de organización adecuadas y proporcionadas para gestionar los riesgos que se planteen para la seguridad de los sistemas de redes y de información... basado en a) las políticas de seguridad de los sistemas de información y análisis de riesgos;	**Sophos Intercept X** **Sophos Intercept X for Server**	Integra tecnología innovadora como Deep Learning, antiexploits y antiadversarios en la detección de tráfico malicioso, y la aúna con información sobre amenazas en tiempo real para ayudar a prevenir, detectar y remediar las amenazas de forma sencilla en todos los dispositivos y plataformas.
	Sophos Firewall	Se sirve de la tecnología de Machine Learning líder del sector de Sophos (con el respaldo de SophosLabs Intelix) para identificar al instante el ransomware y las amenazas desconocidas más recientes antes de que entren en la red. Ofrece protección avanzada frente al malware web dirigido y descargas automáticas (drive-by) más recientes, filtrado de URL/sitios maliciosos, filtrado de aplicaciones web y filtrado basado en la nube para protección sin conexión.
	Sophos Cloud Optix	Supervisa de forma continua los estándares de configuración, detecta desviaciones de los mismos e impide, detecta y corrige automáticamente cambios accidentales o maliciosos en la configuración de recursos.
	Función de Seguridad Sincronizada en productos de Sophos	Comparte la telemetría y el estado de seguridad, lo que permite un aislamiento, una detección y una remediación coordinados del malware en todos los servidores, endpoints y firewalls, deteniendo así los ataques avanzados.
	Sophos Managed Detection and Response (MDR)	La detección y respuesta a amenazas 24/7 identifica y neutraliza los ciberataques avanzados que la tecnología por sí sola no puede detener.
2. b) la gestión de incidentes;	**Sophos Managed Detection and Response (MDR)**	Supervisa continuamente las señales procedentes de todo el entorno de seguridad, incluidas las tecnologías de protección para redes, correo electrónico, firewalls, identidad, endpoints y nube, lo que nos permite detectar y responder con rapidez y precisión a posibles incidentes de ciberseguridad. Se incluye de serie un servicio integral de respuesta a incidentes a cargo de expertos con cobertura 24/7. Incluye informes y análisis de causa raíz exhaustivos. Nuestro tiempo medio de detección, investigación y respuesta es de solo 38 minutos.
	Servicio Sophos Rapid Response	Servicio prestado por un equipo de expertos en respuesta a incidentes que ofrece una asistencia rápida a la hora de identificar y neutralizar amenazas activas contra una organización.
	Seguridad Sincronizada en productos de Sophos	Comparte la telemetría y el estado de seguridad, lo que permite un aislamiento, una detección y una remediación coordinados del malware en todos los servidores, endpoints y firewalls.

ASSESSMENT Cumplimiento NIS2 Próximamente

NIS2 Directive Compliance Assessment

The NIS2 Directive is a European Union law that aims to strengthen cybersecurity measures for essential services and digital service providers. It mandates organizations to implement robust security measures to protect against cyberattacks and ensure business continuity.

Our NIS2 Directive assessment is designed to help you evaluate your organization's compliance level. It covers key areas such as risk assessment, incident response, supply chain security, and more. By completing this assessment, you will receive a comprehensive report outlining your strengths and weaknesses.

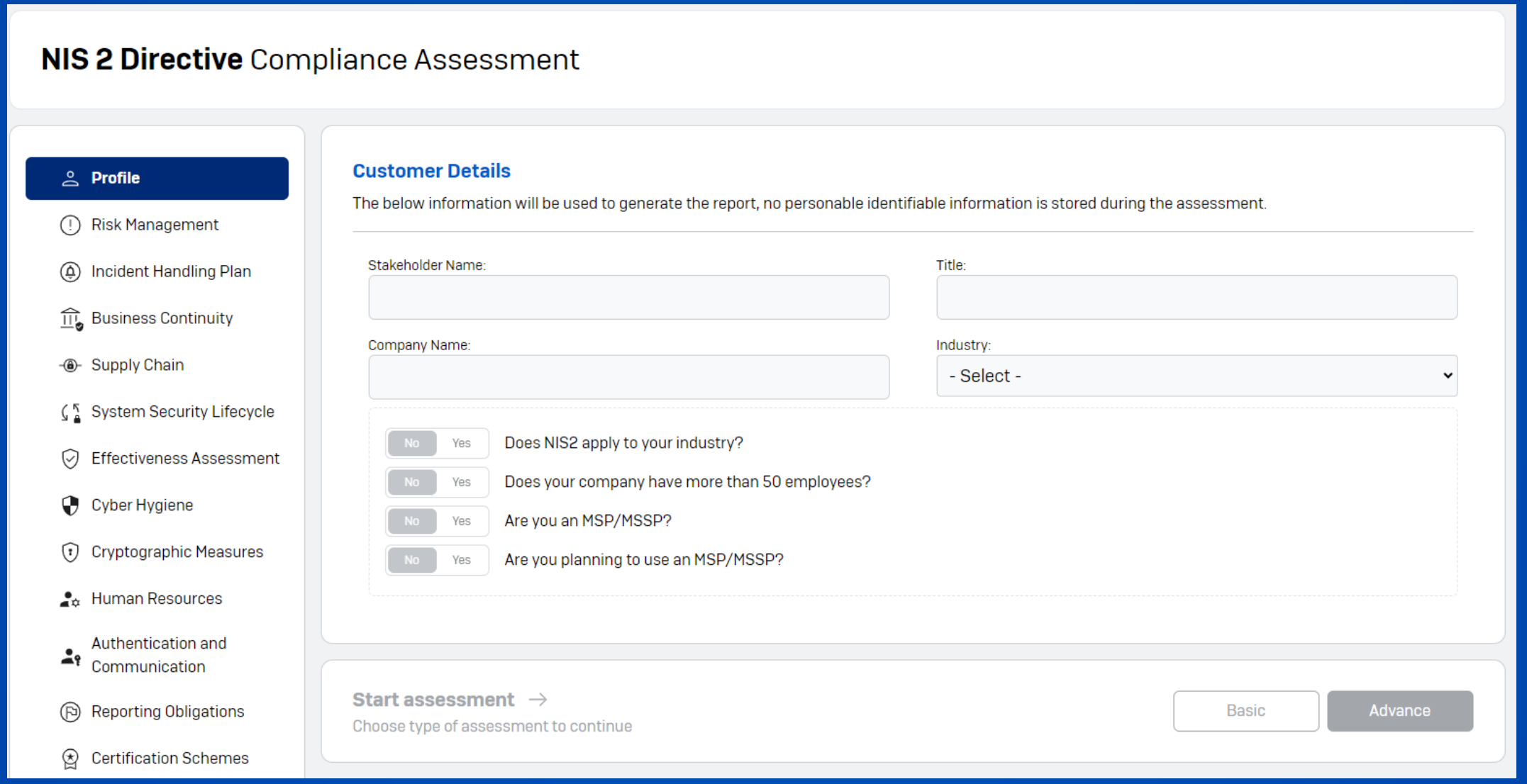
Why Take the Assessment?

Assessing your organization's compliance with the NIS2 Directive is crucial for several reasons:

- **Identify gaps:** Pinpoint areas where your cybersecurity posture needs improvement.
- **Mitigate risks:** Reduce the likelihood of cyberattacks and their potential impact.
- **Demonstrate compliance:** Prove to regulators and stakeholders that you are committed to cybersecurity.
- **Gain competitive advantage:** Show customers and partners that you prioritize data protection.

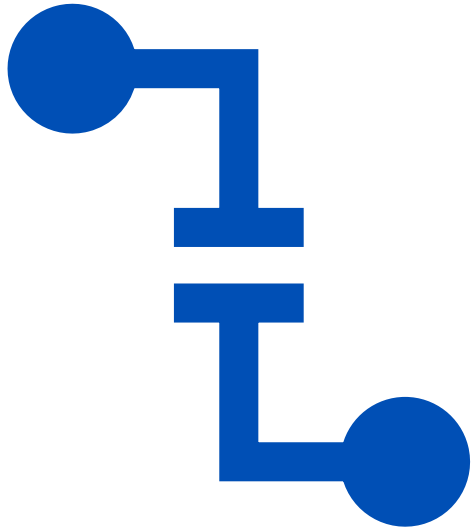
Start your assessment

Autoanálisis Cumplimiento NIS2



SOPHOS

¿Cómo puede ayudar Sophos? (2)



- El **artículo 21** de la Directiva detalla las medidas necesarias, entre ellas:

  - **"Higiene cibernética"** básica, que abarca prácticas básicas como la gestión de contraseñas, la protección de los administradores de sistemas, las actualizaciones de software y la realización de copias de seguridad.
  - Gestión de vulnerabilidades
  - Seguridad de la **cadena de suministro**
  - Estándares de **cifrado** y criptografía
  - **Gestión de activos**
  - Control de acceso y seguridad de confianza cero **(ZTNA)**
  - Proceso de **análisis de riesgos** que identifica las medidas que deben adoptarse
  - **Gestión y notificación de incidentes**

Sophos Central

SecOps

- MDR
- XDR
- IR Services
- Managed Risk
- Threat Intel
- Orchestration and Automation

Endpoint Security

- Endpoint Protection
- EDR
- Server/Workload Protection
- Mobile
- Encryption

Network Security

- Firewall
- NDR
- ZTNA
- SD-WAN
- Switch
- Wireless

Cloud Security

- Cloud Native Security
- Cloud Workload Protection
- Cloud Series Firewall

Email Security

- Email
- User Awareness Training

Sophos MDR: Industry-Leading Openness and Flexibility

Sophos MDR

Compatible with your environment
We can use our tools, another vendor's tools or any combination of the two

Compatible with your needs
Whether you need full-scale incident response or assistance making more accurate decisions

Compatible with your business
Our team has deep experience hunting threats targeting organizations in every industry

Sophos

- XDR Sophos XDR
- Fw Sophos Firewall
- Cld Sophos Cloud
- NDR Sophos NDR
- Em Sophos Email
- Ep Sophos Endpoint

Endpoint

Microsoft, CROWDSTRIKE, SentinelOne, TREND MICRO, Symantec (A Division of Broadcom), Trellix, Malwarebytes, BlackBerry CYLANCE

Firewall

paloalto NETWORKS, FORTINET, CHECK POINT, CISCO, SONICWALL

Cloud SaaS

aws, Azure, Google Cloud, orca security

Email

Microsoft 365, mimecast, proofpoint

Identity

Microsoft [Azure IDP, ATA], okta, DUO, ManageEngine

Network

DARKTRACE, THINKST CANARY, Skyhigh Security

Conclusiones

Conclusiones

- NIS 2 es un reconocimiento del alcance de las amenazas y de la importancia de su trabajo de ciberseguridad.
- Su implementación planteará desafíos en materia de cumplimiento y ciberseguridad.
- Es una oportunidad para abordar los principales riesgos de ciberseguridad.
- Abordar el objetivo clave de la Directiva es de vital importancia.
- Sophos tiene recursos gratuitos, así como productos y servicios que pueden ayudarle a tener éxito.

SOPHOS

Cybersecurity delivered.