La Directiva SRI 2

La Directiva relativa a la seguridad de las redes y sistemas de información (SRI) de la UE fue la primera disposición legislativa sobre ciberseguridad a nivel comunitario y entró en vigor en 2016. Sin embargo, para paliar las limitaciones identificadas en el marco actual y responder a las crecientes amenazas a la ciberseguridad en la UE a raíz de la digitalización y la COVID-19, la Comisión Europea ha sustituido la Directiva SRI por la Directiva SRI 2, que introduce medidas de supervisión más estrictas para las autoridades nacionales y requisitos de ejecución más rigurosos, y pretende armonizar los regímenes de sanciones de los Estados miembros. La Directiva SRI 2 entró en vigor el 16 de enero de 2023, y los Estados miembros disponen de 21 meses, hasta el 17 de octubre de 2024, para transponerla a la legislación nacional.

La Directiva SRI 2 pretende reforzar los requisitos de seguridad en la UE ampliando su ámbito de aplicación a más sectores y entidades, contemplando medidas como el análisis de riesgos y las políticas de seguridad de los sistemas de información, la gestión de incidentes y la seguridad de la cadena de suministro, y simplificando las obligaciones de notificación, entre otras. En caso de incumplimiento, la SRI 2 exige a los Estados miembros que impongan multas importantes: 10 millones EUR o el 2 % del volumen de negocios mundial (el importe que sea más elevado) para las entidades esenciales y 7 millones EUR o el 1,4 % del volumen de negocios mundial (el importe que sea más elevado) para las entidades importantes. La SRI 2 impone obligaciones directas a los órganos de dirección para que apliquen y supervisen el cumplimiento de la legislación por parte de su organización. El incumplimiento podría dar lugar a la imposición de una prohibición temporal de ejercer responsabilidades de gestión al personal directivo de la entidad, incluidos los más altos cargos ejecutivos.

En este documento se describe cómo las soluciones de Sophos ofrecen herramientas eficaces para ayudar a las organizaciones a dar respuesta al Capítulo IV de la Directiva SRI 2, **Medidas para la gestión de riesgos de ciberseguridad y obligaciones de notificación** y, en última instancia, ayudarles a cumplir la Directiva SRI 2.

Las especificaciones y descripciones están sujetas a cambios sin previo aviso. Sophos renuncia a todas las garantías con respecto a esta información. El uso de productos de Sophos por sí solo no garantiza el cumplimiento de la ley. La información que figura en este documento no constituye asesoramiento jurídico. Los clientes son los únicos responsables del cumplimiento de todas las leyes y reglamentos y deben consultar a su propia asesoría jurídica para obtener asistencia en relación con dicho cumplimiento.

Directiva SRI 2 – Capítulo IV: Medidas para la gestión de riesgos de ciberseguridad y obligaciones de notificación

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.

REQUISITOS DE LA DIRECTIVA SRI 2	SOLUCIÓN DE SOPHOS	CÓMO CONTRIBUYE
2. c) la continuidad de las actividades, como la gestión de copias de seguridad y la recuperación en caso de catástrofe, y la gestión de crisis;	**Sophos Managed Detection and Response (MDR)**	Garantiza el aspecto de seguridad de la información de la gestión de la continuidad del negocio al ofrecer detección y respuesta 24/7 a incidentes de seguridad en todo el entorno de TI, sirviéndose de la experiencia humana, la IA y tecnologías avanzadas.
	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. Incluye la reversión a los archivos originales tras un ataque de ransomware o de registro de arranque maestro. Aplica una corrección de nivel forense erradicando el código malicioso y eliminando cambios perniciosos que introduce el malware en las claves del registro.
	Sophos Cloud Optix	Supervisa las cuentas de AWS, Azure y GCP para los servicios de almacenamiento en la nube sin programaciones de copias de seguridad activadas y ofrece remediación guiada.
2. d) la seguridad de la cadena de suministro, incluidos los aspectos de seguridad relativos a las relaciones entre cada entidad y sus proveedores o prestadores de servicios directos;	**Sophos Intercept X with XDR**	Proporciona una defensa en profundidad contra amenazas que penetran a través de proveedores externos usando IA, prevención de exploits, protección comportamental, antiransomware y otras funciones. Además, la potente funcionalidad XDR le permite identificar automáticamente actividad sospechosa, priorizar los indicadores de amenazas y buscar rápidamente las posibles amenazas en endpoints y servidores.
	Sophos Managed Detection and Response (MDR)	Ofrece un servicio totalmente administrado de búsqueda y remediación de amenazas por parte de expertos. Los especialistas de Sophos buscan, validan y remedian de forma ininterrumpida y proactiva posibles amenazas e incidentes en la cadena de suministro en su nombre.
	Sophos ZTNA	Protege de los ataques a la cadena de suministro que dependen del acceso de los proveedores a sus sistemas mediante controles de acceso muy granulares. Esta solución implementada en la nube valida la identidad del usuario y el estado de seguridad y cumplimiento del dispositivo antes de conceder acceso a los recursos. Autentica las solicitudes de Partners de confianza, independientemente de su ubicación.
2. e) la seguridad en la adquisición, el desarrollo y el mantenimiento de sistemas de redes y de información, incluida la gestión y divulgación de las vulnerabilidades;	**Sophos Managed Detection and Response (MDR)**	Nuestros expertos en búsqueda de amenazas supervisan e investigan las alertas de toda la red, valiéndose de herramientas de protección para redes, firewalls, endpoints, el correo electrónico y la nube para identificar e investigar actividades sospechosas y proteger los datos personales dondequiera que estén. Sophos NDR genera señales procesables de alto nivel en toda la infraestructura de red para optimizar las ciberdefensas. Sophos MDR responde de forma proactiva a la divulgación de vulnerabilidades por parte del cliente. Tras la notificación, se inicia una investigación exhaustiva en busca de indicios de exploits. Si es necesario, Sophos MDR remediará el incidente y ofrecerá orientación sobre cómo reforzar el entorno contra futuros ataques. Se facilita un informe completo de autoría humana a raíz de la investigación de la divulgación.
2. f) las políticas y los procedimientos para evaluar la eficacia de las medidas para la gestión de riesgos de ciberseguridad;	**Sophos Managed Detection and Response (MDR)**	Investiga y evalúa los posibles riesgos de seguridad en todo el entorno 24/7, sirviéndose de la información sobre amenazas líder en el mundo de Sophos X-Ops para identificar los niveles de riesgo y priorizar la respuesta.
2. g) las prácticas básicas de ciberhigiene y formación en ciberseguridad;	**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.
2. h) las políticas y procedimientos relativos a la utilización de criptografía y, en su caso, de cifrado;	**Sophos Central Device Encryption**	Protege dispositivos y datos con cifrado completo de disco para Windows y macOS. Verifique el estado del cifrado de los dispositivos y demuestre que cumple las normativas.
	Sophos Email **Sophos Firewall**	Ofrece cifrado TLS y compatibilidad con SMTP/S junto con cifrado integral de portal basado en imposición y cifrado opcional de portal basado en extracción.
	Sophos Mobile	Impone el cifrado de dispositivos y monitoriza el cumplimiento en relación con la política de cifrado.

REQUISITOS DE LA DIRECTIVA SRI 2	SOLUCIÓN DE SOPHOS	CÓMO CONTRIBUYE
2. i) la seguridad de los recursos humanos, las políticas de control de acceso y la gestión de activos;	**Sophos Managed Detection and Response (MDR)**	Los expertos en búsqueda de amenazas supervisan y correlacionan la actividad del sistema de información en todo el entorno de seguridad TI, identificando e investigando actividades sospechosas mediante la revisión periódica de los registros de actividad del sistema de información, como registros de auditoría, registros de acceso, informes de acceso e informes de seguimiento de incidentes de seguridad.
	Sophos Firewall	La concienciación de los usuarios en todas las áreas de nuestro firewall rige todas las políticas e informes de firewall, ofreciendo controles a nivel de usuario sobre aplicaciones, ancho de banda y otros recursos de red.
	Sophos Central	Mantiene actualizadas las listas de acceso y la información sobre los privilegios de los usuarios. Se han instaurado procedimientos para garantizar que los derechos de acceso se revoquen si las personas dejan de cumplir las condiciones para recibirlo (por ejemplo, porque cambian de puesto o abandonan la empresa).
	Sophos ZTNA	Permite una mayor seguridad y agilidad en entornos que cambian con rapidez, ya que acelera y facilita la inscripción o baja de usuarios y dispositivos. Valida continuamente la identidad del usuario, el estado de seguridad del dispositivo y el cumplimiento antes de conceder acceso a aplicaciones y datos.
	Sophos Cloud Optix	Administración de inventario en múltiples proveedores de servicios en la nube, con una supervisión continua de los recursos y una visualización completa de la topología de red y el tráfico.
2. j) el uso de soluciones de autenticación multifactorial o de autenticación continua, comunicaciones de voz, vídeo y texto seguras y sistemas seguros de comunicaciones de emergencia en la entidad, cuando proceda.	**Sophos Firewall**	Admite opciones flexibles de autenticación multifactorial, incluidos servicios de directorio para acceder a áreas clave del sistema.
	Sophos ZTNA	Valida continuamente la identidad del usuario, el estado de seguridad del dispositivo y el cumplimiento antes de conceder acceso a aplicaciones y datos.
	Sophos Central	Protege las cuentas con privilegios y de administrador con autenticación avanzada de doble factor.
	Sophos Cloud Optix	Supervisa las cuentas de AWS/Azure/GCP para detectar accesos de usuarios raíz e IAM con la MFA deshabilitada para que pueda gestionar y garantizar el cumplimiento.
Capítulo IV, Artículo 23, Obligaciones de notificación		
4. Los Estados miembros velarán por que, a los efectos de la notificación con arreglo al apartado 1, las entidades afectadas presenten al CSIRT o, en su caso, a la autoridad competente: d) un informe final, a más tardar un mes después de presentar la notificación del incidente contemplada en la letra b), en el que se recojan los siguientes elementos: ***(i) una descripción detallada del incidente, incluyendo su gravedad e impacto;***	**Sophos Managed Detection and Response (MDR)**	Tras la notificación, se inicia una investigación exhaustiva en busca de indicios de exploits. Si es necesario, Sophos MDR remediará el incidente y ofrecerá orientación sobre cómo reforzar el entorno contra futuros ataques. Se facilita un informe completo de autoría humana a raíz de la investigación de la divulgación.
4. Los Estados miembros velarán por que, a los efectos de la notificación con arreglo al apartado 1, las entidades afectadas presenten al CSIRT o, en su caso, a la autoridad competente: d) un informe final, a más tardar un mes después de presentar la notificación del incidente contemplada en la letra b), en el que se recojan los siguientes elementos: ***(ii) el tipo de amenaza o causa principal que probablemente haya desencadenado el incidente;***	**Sophos Managed Detection and Response (MDR)**	Sophos MDR investiga y evalúa los posibles riesgos de seguridad en todo el entorno 24/7, sirviéndose de la información sobre amenazas líder en el mundo de Sophos X-Ops. El análisis completo de la causa raíz realizado por Sophos MDR permite reforzar el entorno y actualizar los planes y estrategias de respuesta para incorporar lo aprendido.
	Sophos XDR	Va más allá del endpoint y se sirve de extensas fuentes de datos de la red, el correo electrónico, la nube y dispositivos móviles para darle una visión aún más amplia de su postura de ciberseguridad, con la capacidad de profundizar en detalles granulares en caso necesario. Gracias a los datos que cada producto aporta a Sophos Data Lake, podrá responder rápidamente a preguntas críticas para el negocio, correlacionar eventos de distintas fuentes de datos y tomar medidas aún más informadas. Por ejemplo, puede contrastar los datos con la información de la red para obtener una visión más amplia de un incidente o de lo que ha sucedido con los dispositivos que han quedado fuera de servicio en un ataque.

Ventas en España
Teléfono: (+34) 913 756 756
Correo electrónico: comercialES@sophos.com

Ventas en América Latina
Correo electrónico: Latamsales@sophos.com

2023-03-15 RC-ES (PS)

SOPHOS