KINGSTON IRONKEY™

Directiva SRI2

Este flyer ofrece información sobre la Directiva SRI2, en qué consiste, cómo afectará a las empresas y qué pueden hacer estas para cumplir con esta nueva directiva.

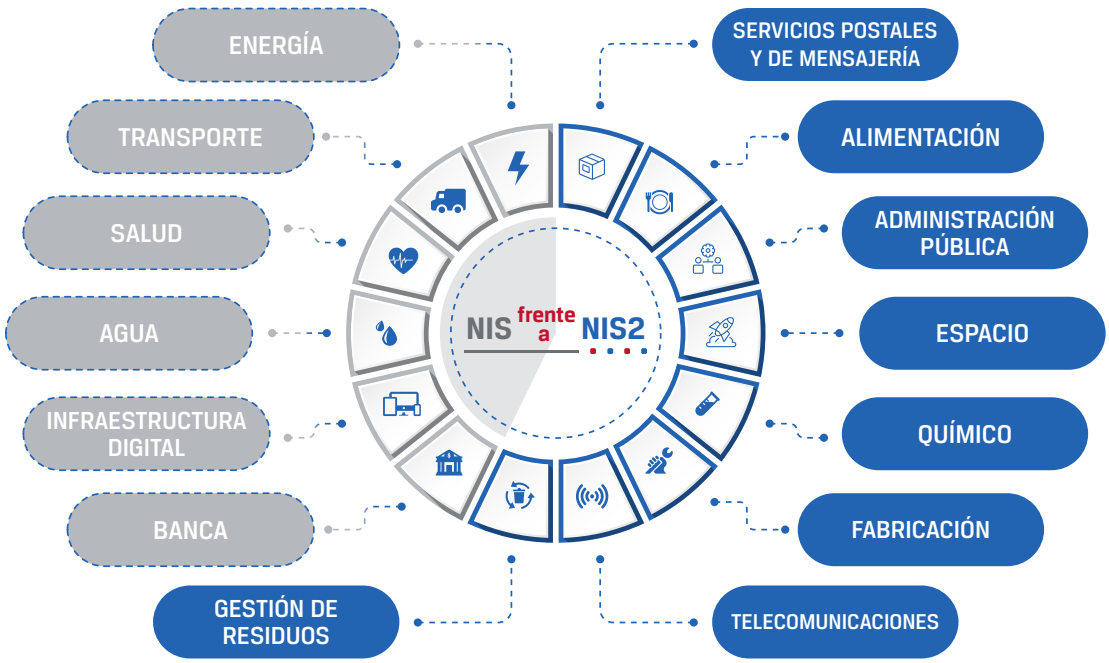
¿En qué consiste?

- La SRI2 (Directiva relativa a las medidas para un elevado nivel común de ciberseguridad en toda la Unión) es una Directiva más amplia de la UE que mejora la Directiva SRI original. La SRI2 tiene como objetivo fortalecer la ciberseguridad de las infraestructuras críticas en toda la UE garantizando una mayor resiliencia y protección contra las filtraciones de datos y las interrupciones causadas por entidades o agentes maliciosos.
- Esta directiva entró en vigor el 17 de octubre de 2024.

Principales diferencias entre la SRI y la SRI2

La Unión Europea ha implantado la Directiva SRI2 como una importante actualización de la Directiva SRI (Directiva sobre la seguridad de las redes y sistemas de información de toda la Unión) original de 2016, con un mayor alcance que abarca infraestructuras más críticas y proveedores de servicios esenciales.

- **Requisitos de seguridad:** la SRI2 exige medidas más estrictas, como la gestión de riesgos, evaluaciones de seguridad periódicas, estrategias de respuesta ante incidentes y el uso de cifrado y controles de acceso para la protección de datos.
- **Notificación de incidentes:** la Directiva SRI original exigía que las entidades notificaran incidentes importantes sin demoras indebidas. Con la SRI2, los incidentes deben notificarse dentro de las 24 horas posteriores a la detección, lo que permitirá responder con mayor rapidez ante los ataques y las interrupciones.
- **Seguridad de la cadena de suministro:** la SRI2 enfatiza que las empresas también serán responsables de sus proveedores y prestadores de servicios.



¿A quiénes afectará?

El alcance ampliado de la SRI2 implica que se verá afectada una variedad más amplia de sectores. Entre estos, se encuentran los sectores de la energía, el transporte, la banca, las infraestructuras de los mercados financieros, la sanidad, el suministro y distribución de agua potable, la infraestructura digital y los Gobiernos, así como el sector aeroespacial. Si su organización opera en la UE o con cualquier entidad de la UE, estará sujeta a estos reglamentos y a cualquier sanción por incumplimiento.

Por qué sus clientes deberían preocuparse por la SRI2?

- «Se espera que los costes de la ciberdelincuencia alcancen los 10,5 billones de dólares anuales para 2025, frente a los 3 billones de dólares de 20151. Este aumento viene provocado por ciberataques cada vez más sofisticados, casos de ransomware y filtraciones de datos, y la frecuencia y la gravedad de los ataques aumentan cada año» —Cybersecurity Ventures
- El Informe sobre Riesgos Globales de 20232 del Foro Económico Mundial destaca que las ciberamenazas se encuentran entre los principales riesgos globales.

Con el objetivo de combatir las crecientes amenazas, la Unión Europea ha introducido esta nueva Directiva, mientras que las autoridades nacionales han aumentado sus poderes de supervisión. El incumplimiento de esta normativa puede dar lugar a sanciones de hasta 10 millones de euros o el 2 % de la facturación anual global de la empresa, el valor que sea más alto.

¿Cómo pueden ayudar las soluciones cifradas de Kingston IronKey a las empresas para cumplir la SRI2?

Las soluciones USB y SSD cifradas por hardware de Kingston IronKey ofrecen una protección de datos avanzada que puede ayudar a las empresas a cumplir con los requisitos de la directiva:

- **Protección de datos:** cumple los requisitos de cifrado y control de acceso de la SRI2.
- **Cumplimiento normativo:** ayuda a las empresas a cumplir con los estándares de la SRI2 y a demostrar dicho cumplimiento.
- **Respuesta ante incidentes:** facilita la recuperación y restauración rápida de los servicios en caso de ataque o filtración.
- **Seguridad de la cadena de suministro:** mitiga los riesgos gracias al almacenamiento portátil seguro.

Conclusión

A medida que la ciberdelincuencia alcanza niveles sin precedentes, la implantación de la Directiva SRI2 representa un paso importante para mejorar la ciberseguridad de las infraestructuras críticas en toda la UE. Las empresas deben tomar medidas proactivas para cumplir con la SRI2 y proteger los datos confidenciales. Los dispositivos de Kingston IronKey utilizan cifrado por hardware para ofrecer un medio escalable y de confianza para cumplir con la legislación y salvaguardar la información crítica, lo que ayuda a las empresas a navegar el complejo panorama actual de la ciberseguridad.

Preguntas para los revendedores a sus clientes/usuarios finales

- ¿Conoce la Directiva SRI2, que entró en vigor el 17 de octubre de 2024?
- ¿Qué estrategia va a implantar para cumplir con la SRI2?
- ¿Conoce las consecuencias a las que puede enfrentarse si no cumple con la SRI2? Las multas podrían alcanzar el 2 % de la facturación anual global.
- ¿Hace copias de seguridad de sus datos confidenciales de forma segura a través de hardware cifrado?

Descripción destacada	IronKey Vault Privacy 50 Series	IronKey Vault Privacy 80 ES	IronKey Keypad 200 Series	IronKey D500S	IronKey S1000
Nivel de seguridad	Empresarial general	Empresarial general	Grado militar	Grado militar/primera categoría	Grado militar/primera categoría
Capacidades[4]	8-512GB	480-7,680GB	16-256GB USB-A 8-512GB USB-C	8-512GB	8-128GB
Modo de cifrado de hardware AES de 256 bits	XTS	XTS	XTS	XTS	Criptochip en el dispositivo + XTS
Validación FIPS[5]	FIPS 197	FIPS 197	FIPS 140-3 de nivel 3 (pendiente)	FIPS 140-3 de nivel 3 (pendiente)	FIPS 140-2 de nivel 3

Si desea obtener más información sobre cómo Kingston puede ayudarle a encontrar la solución adecuada para sus clientes, escanee el código QR y complete nuestro formulario Pregunte a un experto.

www.kingston.com

1. www.esentire.com/cybersecurity-fundamentals-defined/glossary/cybersecurity-ventures-report-on-cybercrime
2. www.weforum.org/publications/global-risks-report-2023
3. USB Tipo-C® y USB-C® son marcas comerciales registradas de USB Implementers Forum.
4. Parte del espacio especificado de los dispositivos de almacenamiento Flash se emplea para el formateo y para otras funciones, por lo cual no estará disponible para el almacenamiento de datos. Para obtener más información, consulte la Guía de memorias Flash de Kingston en kingston.com/flashguide.
5. Normas federales estadounidenses para el procesamiento de la información (FIPS, por sus siglas in inglés), publicación 140-2: «Security Requirements for Cryptographic Modules». Para obtener más información, consulte http://csrc.nist.gov/publications/PubsFIPS.html

© 2025 Kingston Technology Europe Co LLP y Kingston Digital Europe Co LLP, Kingston Court, Brooklands Close, Sunbury-on-Thames, Middlesex, TW16 7EP, Reino Unido. Tel: +44 (0) 1932 738888 Fax: +44 (0) 1932 785469
Reservados todos los derechos. Todos los nombres de empresas y marcas registradas son propiedad de sus respectivos dueños.