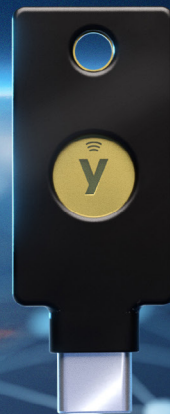




DIRECTIVA SRI2

# Prepárese para la Directiva NIS2 con la YubiKey





## ¿Qué es la Directiva NIS 2?

La Directiva sobre la seguridad de las redes y sistemas de información (NIS) se introdujo en 2016 como marco legal para las normas de ciberseguridad en toda la UE. La Directiva NIS 2 es una actualización y supone una ampliación del ámbito de aplicación que entró en vigor en enero de 2023.<sup>1</sup>

La NIS 2 introduce nuevos requisitos de seguridad y medidas de supervisión, y abarca a un mayor número de entidades de una gama más amplia de sectores, así como a sus socios en la cadena de producción. Los Estados miembros tienen hasta el 17 de octubre de 2024 para transponer las medidas de la Directiva NIS 2 a sus respectivas legislaciones nacionales. La aplicación de las nuevas medidas de seguridad comienza el 18 de octubre de 2024, lo que genera requisitos normativos inmediatos para las empresas que operan o llevan a cabo actividades en la UE.<sup>2</sup>



## ¿Quién debe cumplir la Directiva NIS 2?

La NIS 2 afecta a todos los proveedores, organizaciones y empresas que prestan servicios esenciales o importantes, una distinción que repercute en el nivel de supervisión y en las posibles sanciones por incumplimiento. La NIS 2 amplía el ámbito de aplicación de la Directiva NIS para obligar a más organizaciones a reforzar sus prácticas de ciberseguridad en función de su importancia para la sociedad.



Hasta que los Estados miembros creen listas indicando quiénes deben cumplir la directiva, las organizaciones deben asumir que la SRI2 se aplicará en su caso si se cumplen los siguientes criterios:





## La SRI2 introduce requisitos más estrictos

La primera Directiva SRI exigía a los proveedores de servicios esenciales y digitales que adoptaran medidas técnicas y organizativas adecuadas y proporcionadas al riesgo, teniendo en cuenta la seguridad de los sistemas y las instalaciones, la gestión de incidentes, la gestión de la continuidad de las operaciones, la supervisión, la auditoría y las pruebas, así como el cumplimiento de las normas internacionales. Este amplio mandato dio lugar a importantes lagunas en la forma en la que los Estados miembros establecieron sus requisitos.

Para reforzar la ciberseguridad general en toda la UE, la SRI2 ahora exige unas obligaciones técnicas, operativas y organizativas mínimas tanto en las organizaciones como en sus cadenas de suministro:

### 10 elementos para todas las entidades sujetas a la normativa



**Directiva SRI**

**Añadido a SRI2**

\* o autenticación continua y, si procede, comunicaciones seguras

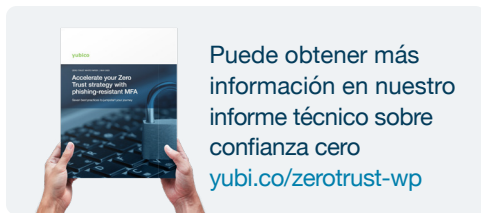
La SRI2 también incluye un marco para los requisitos de notificación de incidentes y para las actividades de supervisión y cumplimiento (por ejemplo, auditorías) por parte de los Estados miembros, con diferenciación entre entidades esenciales e importantes. Además, para reforzar el cumplimiento de las medidas de seguridad, la SRI2 impone sanciones de hasta 7 millones de euros para las entidades importantes o 10 millones de euros para las esenciales, o del 1,4 % o 2 % de los ingresos anuales, respectivamente. Por lo tanto, es fundamental que todas las entidades sujetas a la normativa apliquen medidas para reducir el riesgo de incidentes peligrosos, incluida la adopción de controles sólidos de acceso y de gestión de identidades.

## No todos los tipos de MFA son iguales

Al implementar la MFA para cumplir con la SRI2, las organizaciones deben seleccionar un autenticador en función de su nivel de seguridad, tomando como referencia la norma global del NIST<sup>3</sup> o el Reglamento eIDAS<sup>4</sup>. Estas directrices establecen que **no todos los tipos de MFA son iguales**, lo que se representa a través de los niveles de garantía de autenticación/niveles de garantía (AAL/LoA). Si bien cualquier forma de MFA es mejor que una contraseña sola (AAL1/LoA bajo), los métodos tradicionales de MFA (AAL2/LoA sustancial), como los SMS, la autenticación móvil y los códigos de un solo uso (OTP), tienen una tasa de penetración de ataques del 10-24 %<sup>5</sup>, mientras que un autenticador basado en hardware a prueba de phishing (AAL3/LoA alto) ofrece una mayor seguridad, ya que cumple los requisitos de la SRI2 y reduce la amenaza de poner en riesgo las cuentas.<sup>6</sup>

AAL1	AAL2	AAL3
<p><b>Autenticación de un solo factor</b></p> <p>Por ejemplo, nombre de usuario y contraseña</p>	<p><b>Autenticación en dos pasos</b></p> <p>Por ejemplo, 2FA, passkeys sincronizadas o passkeys por dispositivo en dispositivos de uso general</p>	<p><b>Autenticación de múltiples factores basada en hardware</b></p> <p>Por ejemplo, passkeys por dispositivo en llaves de seguridad de hardware</p>
		
<ul style="list-style-type: none"><li>• Baja garantía de seguridad</li><li>• Muy vulnerable al phishing</li><li>• Pone en riesgo a las empresas</li></ul>	<ul style="list-style-type: none"><li>• 2FA/MFA resistente al phishing</li><li>• Mayor seguridad que una contraseña, pero vulnerable a los ataques</li><li>• Más preparada para las empresas, pero genera lagunas en la eficiencia operativa y en los requisitos de auditoría y cumplimiento</li></ul>	<ul style="list-style-type: none"><li>• MFA resistente al phishing</li><li>• Máxima seguridad y garantía</li><li>• Aborda la seguridad empresarial, la eficiencia operativa y los requisitos de auditoría y cumplimiento</li><li>• Compatible con FIDO y Smart Card/PIV</li><li>• Validación FIPS 140-2</li></ul>



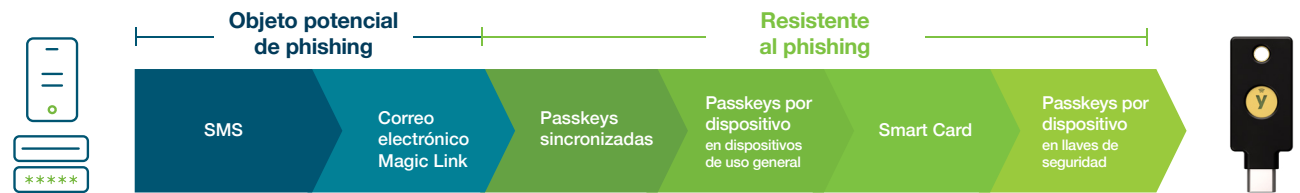


## Confianza cero como práctica de higiene cibernética

Aunque la SRI2 no indica explícitamente las medidas tecnológicas exactas que deben aplicarse, se hace referencia a la confianza cero como una práctica de higiene cibernética para todas las entidades esenciales e importantes. Una estrategia de confianza cero, basada en el concepto de nunca confiar y siempre verificar, traslada los controles de seguridad desde el perímetro tradicional de la red hacia un método basado en la identidad. Para ello, se implementan sólidas políticas de autenticación y control de acceso granular, además de cifrado y gestión de claves.

El modelo de madurez de confianza cero (ZTMM),<sup>7</sup> desarrollado por la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) de EE. UU., ofrece un marco para la transición de un punto de partida tradicional a una confianza cero inicial, avanzada y óptima. En cada etapa, el ZTMM exige que se adopten formas más sólidas de MFA para avanzar hacia el uso exclusivo de MFA resistente al phishing, que emplea verificación criptográfica entre dispositivos o entre un dispositivo y un dominio, haciendo que el proceso de autenticación sea inmune a los intentos de ataque o subversión.

## Cumplimiento rápido de la SRI2 con la YubiKey



### La familia YubiKey

La YubiKey está disponible en varios formatos para equipos de escritorio, portátiles y dispositivos móviles.

La **YubiKey** es una llave de seguridad de hardware diseñada para crear organizaciones de usuarios resistentes al phishing. Como raíz de confianza de hardware, la YubiKey ofrece una autenticación resistente al phishing con la máxima garantía. Fabricada y programada en Suecia por la empresa sueca Yubico, la YubiKey cuenta con las certificaciones FIPS y FIDO.

Gracias a su compatibilidad con los protocolos Smart Card/PIV y FIDO2 (Passkey), así como con FIDO U2F, OTP/TOTP y OpenPGP, la YubiKey se adapta a su situación en materia de ciberseguridad y es adecuada para una gran variedad de contextos empresariales.



Garantice el cumplimiento de los requisitos de la SRI2 sobre la MFA implementando la YubiKey hoy mismo. Para obtener una mayor seguridad en la cadena de suministro, exija que todos los proveedores implementen una MFA resistente al phishing para sus propios usuarios y sistemas.

## El impacto económico total de las YubiKeys<sup>7</sup>:



### Máxima seguridad

Reduzca el riesgo un **99,9 %**



### Alta rentabilidad

Obtenga un retorno de la inversión del **203 %**



### Más rapidez

Disminuya el tiempo de autenticación más de **4 veces**



### Durabilidad

Índice de protección IP68, resistente al aplastamiento, sin baterías ni piezas móviles



### YubiHSM 2 y YubiHSM 2 FIPS

Protección criptográfica revolucionaria para servidores, aplicaciones y dispositivos informáticos.

## Cómo ayuda la YubiKey a abordar los retos de autenticación para infraestructuras clave

Muchas entidades esenciales e importantes sujetas a la SRI2 dependen de equipos de producción tradicionales, estaciones de trabajo compartidas y entornos con restricciones para móviles. La YubiKey es una opción ideal para organizaciones con infraestructuras clave complejas, ya que ofrece la flexibilidad necesaria para navegar entre dispositivos y cientos de productos, servicios y aplicaciones, incluidas las principales plataformas de gestión de acceso e identidades (IAM), soluciones de gestión de acceso privilegiado (PAM) y servicios en la nube, sin que los datos confidenciales se compartan entre los servicios. La YubiKey no requiere hardware adicional, software, alimentación externa, baterías ni conexión de red. La autenticación segura es sencilla: conecte la YubiKey a un puerto USB y toque el botón o toque mediante NFC.

## Cumpla los requisitos de cifrado y criptografía de la SRI2 con el YubiHSM 2

El **YubiHSM 2** se ha diseñado específicamente para permitir el cumplimiento, almacenar y generar claves criptográficas, proteger datos confidenciales y realizar operaciones criptográficas, con el fin de satisfacer los requisitos de cifrado estipulados en la SRI2 para su organización y los socios de la cadena de suministro y, por tanto, proteger toda la lista de materiales del software (SBOM). El YubiHSM 2, el módulo de seguridad de hardware (HSM) más pequeño del mundo, compatible con interfaces comunes como PKCS11 y Microsoft CNG, es ideal para:



### PKI

Proteja su infraestructura de claves públicas con seguridad confiando la generación y la protección de sus claves privadas de CA raíz y CA emisora al YubiHSM 2.



### Firma de código

Proteja la integridad de sus aplicaciones frente a interferencias de terceros generando y almacenando su clave privada de firma de código en el YubiHSM 2.



### Cifrado de bases de datos

Proteja la información de acceso no autorizado mediante el cifrado de la información confidencial y el almacenamiento seguro de claves de cifrado dentro en el YubiHSM 2.



### IoT

Aumente la seguridad de sus dispositivos IoT y soluciones autónomas con la potencia compacta del YubiHSM 2, que garantiza la integridad y la confidencialidad de sus operaciones.



### Defensa

Garantice la integridad de las comunicaciones y los datos intercambiados entre equipos terrestres, aéreos y marítimos con la resistente seguridad del YubiHSM 2, extraíble sobre el terreno.



**Contacto**  
[yubi.co/contacto](https://yubi.co/contacto)



**Más información**  
[yubi.co/yk5](https://yubi.co/yk5)

## Fuentes

<sup>1</sup> Diario Oficial de la Unión Europea, [Directiva \(UE\) 2016/1148](#), (14 de diciembre de 2022)

<sup>2</sup> Parlamento Europeo, [Directiva SRI2](#), (febrero de 2023)

<sup>3</sup> NIST, [NIST SP 800-63-4 Digital Identity Guidelines](#), (diciembre de 2022)

<sup>4</sup> Comisión Europea, [eIDAS Levels of Assurance \(LoA\)](#), (2014)

<sup>5</sup> Kurt Thomas y Angelika Moscicki, [New research: how effective is basic account hygiene at preventing hijacking](#), (17 de mayo de 2019)

<sup>6</sup> Oficina de la Unión Europea, [Reglamento de Ejecución \(UE\) 2015/1502 de la Comisión](#), (septiembre de 2015)

<sup>7</sup> Forrester, [The Total Economic Impact of Yubico YubiKeys](#), (septiembre de 2022)



## Acerca de Yubico

Yubico (Nasdaq Stockholm: YUBICO) es la inventora de la YubiKey, una llave de seguridad de hardware que representa el estándar de referencia para la autenticación de múltiples factores (MFA) resistente al phishing. Yubico pone a disposición de empresas y usuarios su experiencia en implementación y su flexibilidad operativa, ya que las YubiKeys funcionan en cientos de aplicaciones y servicios para consumidores y empresas.

Yubico es creadora y colaboradora principal de los estándares de autenticación abiertos FIDO2/passkey, WebAuthn y FIDO Universal 2nd Factor (U2F), y es pionera en ofrecer autenticación sin contraseña basada en hardware mediante passkeys de máxima garantía para clientes de más de 160 países. Si desea obtener más información, visite: [www.yubico.com](http://www.yubico.com).