yubico

LIBRO ELECTRÓNICO SOBRE EL CUMPLIMIENTO DEL DORA

YubiKey: clave para el cumplimiento de DORA

Autoridades Europeas de Supervisión (AES)/Supervisores principales:

eba European Banking Authority

eiopa European Insurance and Occupational Pensions Authority

ESMA European Securities and Markets Authority

El reglamento DORA se aprobó el 16 de enero de 2023 y está vigente desde el 17 de enero de 2025

Afecta aproximadamente a:

- 22 000 entidades financieras[1]
- 15 000 proveedores de servicios de TIC[2]

Las sanciones por incumplimiento pueden imponerse a:

- Entidades financieras
- Personas responsables
- Miembros del consejo de administración
- Proveedores terceros esenciales de TIC (CTPP, por sus siglas en inglés)

En los últimos veinte años, casi una quinta parte de los ciberataques en todo el mundo se han dirigido al sector financiero[3]. Aunque es poco probable que el coste medio de un ciberataque (0,45 millones de euros) o de una filtración de datos (5,53 millones de euros) vaya a enviar a la quiebra a una organización, sí que puede amenazar a su solvencia y, en última instancia, a la estabilidad financiera global, ya que hay un mayor riesgo de sufrir pérdidas extremas (de hasta 2270 millones de euros).[4]

La interdependencia tecnológica, como la dependencia compartida de las tecnologías de la información y la comunicación (TIC) de terceros, aumenta aún más el riesgo sistémico de entidades, sectores y países. Por ejemplo, el 8 % de los incidentes cibernéticos que se produjeron a nivel mundial en el sector financiero en 2023 podrían atribuirse a ataques de día cero a MOVEit, lo que demuestra el gran impacto que tienen las filtraciones de terceros (la cadena de suministro).[5]

¿Qué es el DORA?

El Reglamento de Resiliencia Operativa Digital (DORA)[6] pretende gestionar el riesgo relacionado con las TIC en el sector financiero europeo y sus cadenas de suministro para que se pueda resistir y responder a los incidentes cibernéticos, así como recuperarse de ellos, de forma que se asegure la estabilidad financiera, aunque haya grandes interrupciones operativas.

DORA establece un marco integral que permite gestionar los riesgos internos y los de terceros. Se ha diseñado para reducir la complejidad normativa y armonizar y actualizar las normas de resiliencia operativa y de gestión de riesgos que hubiera en toda la legislación anterior de la Unión Europea.

¿Quién debe cumplir el DORA?

DORA engloba a casi todas las entidades financieras y a los proveedores terceros (TPP, por sus siglas en inglés) de TIC de los que dependen, incluidos los proveedores de servicios de nube, las organizaciones de gestion de datos y otros servicios de TIC. Esta legislación cubre a los TPP de TIC independientemente de su ubicación, es decir, no se limita a la instalaciones situadas en la Unión Europea.

A principios de 2025, algunos TPP de TIC se designarán como esenciales (CTPP por sus siglas en inglés), que serán aquellos que desempeñen funciones críticas o importantes en diversas entidades financieras y que, en caso de fallo, podrían tener un impacto sistémico en la estabilidad, la continuidad o la calidad de los servicios financieros.[7] Las AES supervisarán de forma directa a los CTPP y les exigirán que establezcan una filial dentro de la UE y asuman el coste de la supervisión, que será proporcional a la facturación.

Entidades financieras[8]

Entidades de crédito	Entidades de pago	Proveedores de servicios de información sobre cuentas	Entidades de dinero electrónico	Empresas de inversión
Proveedores de servicios de criptoactivos	Depositarios centrales de valores	Contrapartes centrales	Centros de negociación	Registros de operaciones
Gestores de fondos de inversión alternativos	Sociedades gestoras	Proveedores de servicios de notificación de datos	Empresas de seguros y reaseguros	Intermediarios de seguros, reaseguros y seguros auxiliares
Entidades de pensiones de jubilación	Agencias de calificación crediticia	Administradores de índices de referencia cruciales	Proveedores de servicios de financiación participativa	Registros de titulizaciones

Ejemplos de TPP de TIC[9]

Directos o indirectos (subcontratistas)

Servicios de software y aplicaciones (software comercial o desarrollo personalizado)	Servicios de infraestructura de red (sin contar los servicios de telecomunicaciones)
Centros de datos	Consultorías de TIC y servicios de TIC gestionados
Servicios de seguridad de la información y ciberseguridad	Proveedores de cloud computing
Servicios de datos y de análisis de los mismos (incluyendo la entrada, el almacenamiento y el tratamiento de datos)	Otros[10]

¿Cuál es la sanción por incumplimiento?

Si a un CTPP se le notifica una infracción, DORA permite que el supervisor le imponga una sanción diaria (que puede durar hasta 6 meses) con un importe equivalente al 1 % de la facturación diaria media a nivel mundial del año fiscal anterior hasta que se ajuste al reglamento.

Si es una entidad financiera quien lo infringe, las autoridades competentes de cada Estado miembro definirán sanciones administrativas o penales "proporcionadas y disuasorias", y las aplicarán. Estas sanciones pueden aplicarse a entidades financieras, las personas jurídicas responsables de la infracción o a los miembros del consejo directivo.

Requisitos del DORA

DORA establece requisitos para que las entidades financieras protejan las redes y los sistemas de información y fomenten la resiliencia. Para lograrlo, establece requisitos en estos cinco pilares:

Gestión del riesgo relacionado con las TIC	**Notificación de incidentes relacionados con las TIC**	**Pruebas de resiliencia operativa digital**	**Intercambio de información e inteligencia**	**Riesgo de TIC de terceros TPP | CTPP**
Estrategias, políticas y herramientas para proteger los datos y los activos de TIC	Gestión y notificación de incidentes relacionados con las TIC	Pruebas periódicas proporcionadas en función del tamaño y la importancia de la entidad	Acuerdos de intercambio de información adoptados	Mitigación del riesgo de terceros mediante cláusulas contractuales y seguimiento

Si bien las entidades financieras exigirán, a través de cláusulas contractuales, que sus proveedores de servicios de TIC lleven a cabo iniciativas similares de gestión del riesgo para cumplir con el DORA, son estas las que asumen en última instancia la responsabilidad de aprobar, gestionar y controlar el uso de los servicios de TIC, una medida diseñada para "fortalecer la rendición de cuentas" sobre el riesgo relacionado con las TIC de terceros.[11]

Requisitos de autenticación del DORA

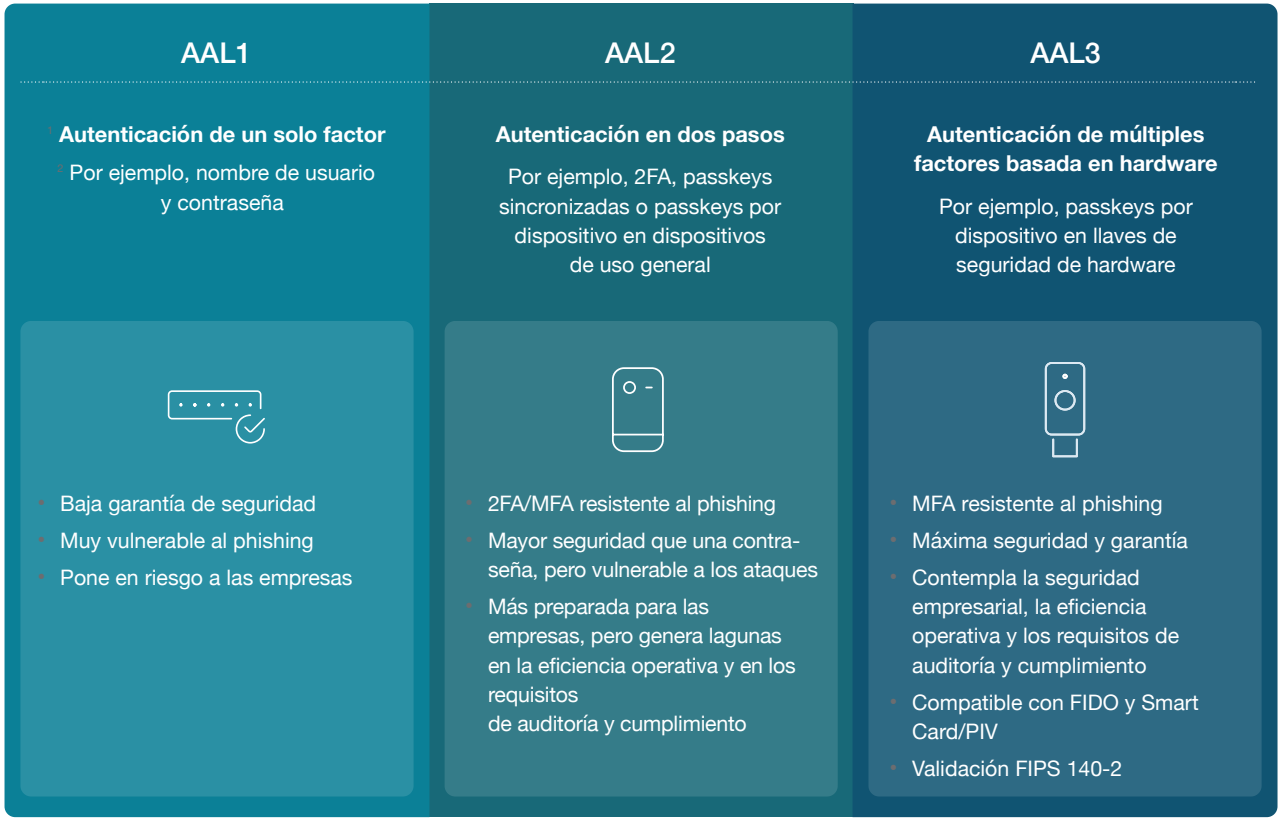
Como parte del marco de gestión del riesgo, las entidades cubiertas por el reglamento deben establecer "políticas y protocolos para mecanismos de autenticación fuerte, basados en estándares pertinentes" y promover "medidas de protección de las claves criptográficas".[12]

Las normas técnicas de regulación (NTR) se han diseñado para complementar al DORA y cumplen con los estándares internacionales sobre gestión del riesgo relacionado con las TIC, como la Directiva relativa a la seguridad de las redes y la información (SRI), ahora la SRI 2, y el Marco de Ciberseguridad del NIST.[13] Estos estándares dejan aún más claro si cabe que los métodos de autenticación deben ser proporcionales al riesgo e ir en consonancia con las principales prácticas de acceso remoto, acceso privilegiado y acceso a funciones esenciales o importantes.[14]

Cómo identificar el riesgo relacionado con la autenticación

Para cumplir con los requisitos de autenticación basada en el riesgo del DORA, las entidades cubiertas deben seleccionar un autenticador en función de su solidez, haciendo referencia al estándar mundial del NIST[15] o al eIDAS.[16] Estas directrices establecen que **no todos los tipos de autenticación de múltiples factores (MFA) son iguales**, lo que se representa a través de los niveles de garantía de autenticación/niveles de garantía (AAL/LoA).

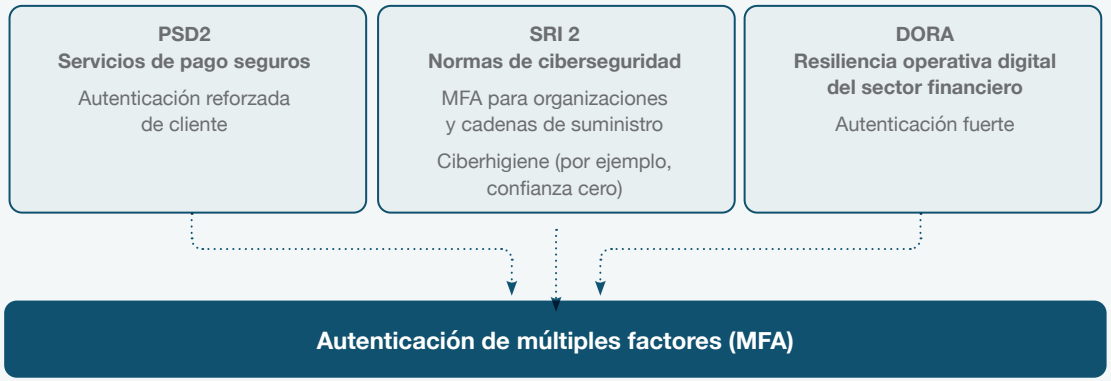
Si bien cualquier forma de MFA es mejor que solo usar una contraseña (AAL1/LoA bajo), los métodos tradicionales de MFA (AAL2/LoA sustancial), como los SMS, la autenticación móvil y los códigos de un solo uso (OTP), tienen una tasa de penetración de ataques de entre el 10 y el 24 %[17], mientras que un autenticador basado en hardware a prueba de phishing (AAL3/LoA alto) ofrece una mayor seguridad, ya que reduce la amenaza de poner en riesgo las cuentas.[18]



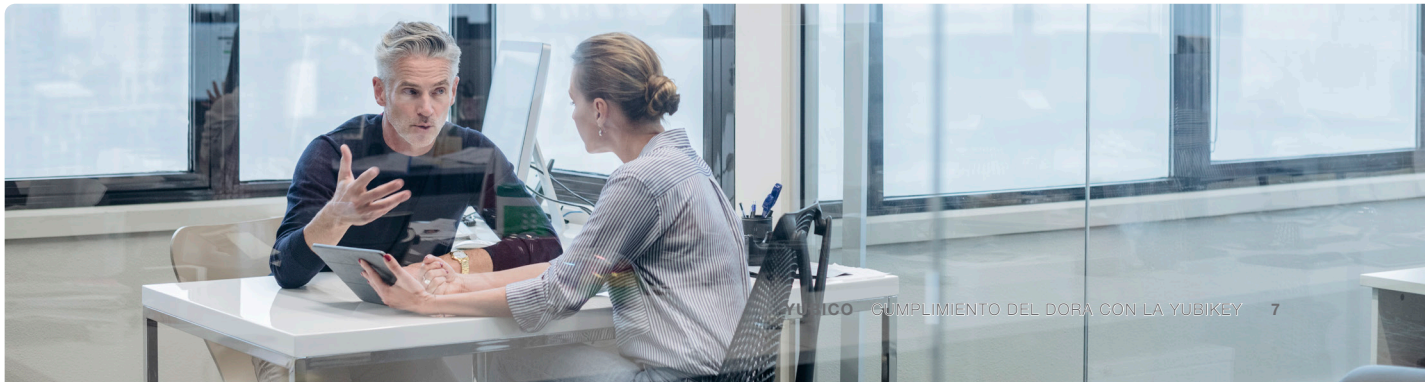
Consulte más información en nuestra guía sobre la SRI 2
Leer la guía

¿Cómo afecta la SRI 2 al DORA?

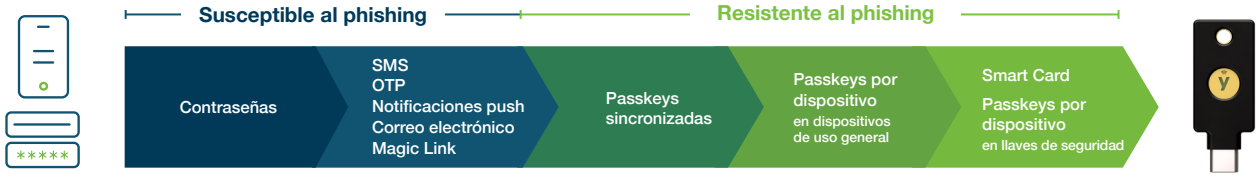
El DORA forma parte de una tríada de normativas concebidas para fortalecer las protecciones digitales y salvaguardar las infraestructuras digitales esenciales, la primera de las cuales fue la Directiva de Servicios de Pago (PSD por sus siglas en inglés), dirigida a proteger a los consumidores y actualizada con la PSD2, seguida ahora del DORA y la SRI 2, centradas en las organizaciones y sus cadenas de suministro. Las tres regulaciones abordan el riesgo con la necesidad de una autenticación fuerte. Dado que el DORA se diseñó para complementar la SRI 2, las organizaciones financieras, reconocidas como entidades esenciales, deberían adherirse a los requisitos más amplios de la SRI 2, como la implementación de una MFA fuerte (AAL3/LoA alto) y los principios de confianza cero.



Es esencial destacar que, mientras que los requisitos del DORA tienen prioridad sobre la SRI 2 en los aspectos en los que coinciden, las estipulaciones de la SRI 2 siguen aplicándose en otras áreas.[19] Esto significa que los requisitos de MFA más específicos de la SRI 2, junto con las prácticas de ciberhigiene como la confianza cero, indican que las entidades cubiertas deberán a empezar a usar únicamente una MFA resistente al phishing de nivel AAL2 o superior.



Cumplimiento rápido del DORA con la YubiKey



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 a prueba de 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, 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.

- Acceso privilegiado
- Restricciones para móviles
- Estaciones de trabajo compartidas
- Teletra-bajadores
- Personal de oficina
- Acceso de terceros
- Clientes finales

Garantice el cumplimiento de los requisitos del DORA implementando la YubiKey hoy mismo. Para que la cadena de suministro de sus TPP de TIC sea más segura, exija la implementación global de una MFA resistente al phishing para sus propios usuarios y sistemas.

Contacto
yubi.co/contacto

Más información
yubi.co/finance

Fuentes

[1] PwC, *DORA and its impact on UK financial entities and ICT service providers* [DORA y su impacto en las entidades financieras británicas y los proveedores de servicios de TIC], (consultado el 7 de octubre de 2024)

[2] Comité Mixto de las Autoridades Europeas de Supervisión, *ESAs Report on the landscape of ICT third-party providers in the EU* [Informe de las AES sobre el ecosistema de los proveedores terceros de TIC en la UE], (18 de septiembre de 2023)

[3] Fondo Monetario Internacional, *Informe sobre la estabilidad financiera mundial*, (abril de 2024)

[4] *Ibid*; Verizon, *2024 Data Breach Investigations Report* [Informe sobre investigaciones de filtraciones de datos de 2024], (1 de mayo de 2024)

[5] Verizon, *2024 Data Breach Investigations Report* [Informe sobre investigaciones de filtraciones de datos de 2024], (1 de mayo de 2024)

[6] Diario Oficial de la Unión Europea, REGLAMENTO (UE) 2022/2554, (14 de diciembre de 2022)

[7] Comité Mixto de las Autoridades Europeas de Supervisión, JS SC DOR-23-54, (26 de mayo de 2023)

[8] Diario Oficial de la Unión Europea, REGLAMENTO (UE) 2022/2554, (14 de diciembre de 2022)

[9] Comité Mixto de las Autoridades Europeas de Supervisión, *ESAs Report on the landscape of ICT third-party providers in the EU* [Informe de las AES sobre el ecosistema de los proveedores terceros de TIC en la UE], (18 de septiembre de 2023)

[10] El DORA define otros servicios de TIC de la siguiente forma: "los servicios digitales y de datos prestados a través de los sistemas de TIC a uno o varios usuarios internos o externos de forma continua, incluidos el hardware como servicio y los servicios de hardware que incluyen la prestación de asistencia técnica a través de actualizaciones de software o firmware por parte del proveedor de hardware y excluidos los servicios telefónicos analógicos tradicionales". Diario Oficial de la Unión Europea, REGLAMENTO (UE) 2022/2554, (14 de diciembre de 2022)

[11] Comité Mixto de las Autoridades Europeas de Supervisión, JC 2023 84, (17 de enero de 2024)

[12] Diario Oficial de la Unión Europea, REGLAMENTO (UE) 2022/2554, (14 de diciembre de 2022)

[13] Comité Mixto de las Autoridades Europeas de Supervisión, JC 2023 86, (17 de enero de 2024)

[14] *Ibid*.

[15] NIST, NIST SP 800-63-4 Digital Identity Guidelines [Guía actualizada de identidad digital SP 800-63-4], (diciembre de 2022)

[16] Comisión Europea, eIDAS Levels of Assurance (LoA) [Niveles de garantía (LoA) del eIDAS], (2014)

[17] Kurt Thomas y Angelika Moscicki, *New research: how effective is basic account hygiene at preventing hijacking* [Nueva investigación sobre la eficacia de la higiene básica de cuentas para prevenir secuestros], (17 de mayo de 2019)

[18] Oficina de la Unión Europea, Reglamento de Ejecución (UE) 2015/1502 de la Comisión, (septiembre de 2015)

[19] Diario Oficial de la Unión Europea, Directrices de la Comisión sobre la aplicación del artículo 4, apartado 1, y (2) de la Directiva (UE) 2022/2555 (Directiva SRI 2), (18 de septiembre de 2023)

yubico

Acerca de Yubico

Yubico (Nasdaq Stockholm: YUBICO), la inventora de la YubiKey, ofrece el estándar de referencia para la autenticación de múltiples factores (MFA) resistente al phishing. Esta autenticación detiene al instante la apropiación de cuentas y hace que el inicio de sesión seguro sea sencillo y esté disponible para todos. Desde su fundación en 2007, la empresa ha sido líder en el establecimiento de estándares globales para el acceso seguro a ordenadores, dispositivos móviles, servidores, navegadores y cuentas de Internet. Yubico es creadora y colaboradora principal de los estándares de autenticación abiertos FIDO2, 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.

Las soluciones de Yubico permiten iniciar sesión sin contraseña a través de la forma más segura de tecnología de passkey. Las YubiKeys funcionan desde el primer momento en cientos de aplicaciones y servicios para consumidores y empresas, lo que proporciona un alto nivel de seguridad de manera rápida y sencilla.

En el marco de su objetivo por hacer que Internet sea un lugar más seguro para todos, Yubico dona YubiKeys a organizaciones que ayudan a personas desfavorecidas a través de la iniciativa solidaria “Secure it Forward”. La empresa tiene sus sedes en Estocolmo y Santa Clara, California. Si desea obtener más información sobre Yubico, visite www.yubico.com.

© 2025 Yubico