Ficha técnica

DORA: cómo te ayuda Specops a cumplir la normativa

DORA: resumen rápido

¿Qué es DORA? La Ley de Resiliencia Operativa Digital (Reglamento (UE) 2022/2554) es un marco normativo obligatorio de la UE en materia de ciberseguridad.

¿Qué cubre DORA? Se centra en la gestión del riesgo TIC, el control de identidades y accesos, la detección y notificación de incidentes, las pruebas de resiliencia operativa, la gestión del riesgo de terceros y el intercambio de información sobre ciberamenazas.

¿A quién aplica DORA? A bancos, aseguradoras, empresas de inversión, entidades de pago y de dinero electrónico, proveedores de servicios de criptoactivos y proveedores terceros críticos de servicios TIC que operan en el sector financiero de la UE o prestan servicios a este.

¿Es lo mismo que la NIS2? No. NIS2 aplica de forma amplia a sectores críticos; DORA se centra específicamente en los servicios financieros y prevalece sobre NIS2 para las entidades financieras incluidas en su ámbito. Ambos comparten objetivos en torno a la resiliencia cibernética, pero DORA fija un nivel más alto y más prescriptivo para el sector financiero.

¿Hay multas por incumplimiento? Sí. Las entidades financieras pueden enfrentarse a multas de hasta el 2 % del volumen de negocio anual total a escala mundial, o de hasta el 1 % del volumen de negocio medio diario mundial. Las personas responsables de fallos de cumplimiento pueden enfrentarse a sanciones de hasta 1 millón de euros.

¿Por qué elegir Specops para la DORA?

Requisito	Cómo ayuda Specops al cumplimiento
Visibilidad de las contraseñas ***Artículo 8 de DORA: Identificación*** Las entidades financieras deben identificar y evaluar los riesgos TIC, incluidas las vulnerabilidades ligadas a las credenciales de usuario y a los derechos de acceso en todo su entorno.	**Specops Password Auditor** (herramienta gratuita) Ejecuta un análisis de solo lectura de tu entorno de Active Directory para detectar contraseñas comprometidas, en blanco, obsoletas y sin caducidad. Genera informes de cumplimiento exportables.
Credenciales comprometidas ***Artículo 9(4)(d) de DORA: Protección y prevención*** Las entidades financieras deben implantar políticas y protocolos para mecanismos de autenticación robusta, incluidos controles que garanticen que las credenciales utilizadas para acceder a sistemas TIC no sean débiles ni estén comprometidas.	**Specops Password Policy con protección contra contraseñas filtradas** La mayoría de las herramientas solo bloquean contraseñas comprometidas al cambiarlas o restablecerlas. Specops analiza continuamente tu Active Directory y bloquea contraseñas comparándolas con nuestra base de datos, en constante crecimiento, de más de 6.000 millones de contraseñas comprometidas.

Requisito	Cómo ayuda Specops al cumplimiento
Autenticación multifactorial (MFA) sólida ***Artículo 9(4)(d) de DORA: Protección y prevención*** Las entidades financieras deben implantar políticas y protocolos para mecanismos de autenticación robusta, especialmente para el acceso remoto a la red, el acceso privilegiado y el acceso a sistemas que soportan funciones críticas.	**Specops Secure Access** Añade MFA resistente al phishing para el inicio de sesión en Windows, RDP y VPN. Incluye compatibilidad con SSO para aplicaciones SaaS mediante OIDC y SAML, y se integra con plataformas SIEM, SOC y de analítica.
Verificación en el service desk ***Artículo 9, apartado 4, letras c) y d), de la DORA: Protección y prevención*** Los controles de derechos de acceso y la autenticación robusta también deben extenderse a los procesos operativos, incluido el service desk, donde los fallos en la verificación de identidad suponen un riesgo TIC directo.	**Specops Secure Service Desk** Los agentes verifican la identidad del usuario mediante MFA (más de 20 métodos) antes de realizar cualquier acción sobre la cuenta. Incluye un registro de auditoría completo de cada interacción. Se integra con plataformas ITSM, así como con plataformas SIEM, SOC y de analítica.
Verificación de alta fiabilidad ***Artículo 9, apartado 4, letras c) y d), de la DORA: Protección y prevención*** Los requisitos de autenticación robusta también aplican a la verificación de identidad para acceder a sistemas TIC, incluidas acciones de alto riesgo como la recuperación de cuentas y la restitución de accesos privilegiados.	**Specops Verified ID** Escanea documentos oficiales de identidad y realiza una comprobación biométrica de prueba de vida para una verificación de máxima garantía.
Restablecimientos de contraseña seguros ***Artículo 9, apartado 4, letras c) y d), del Reglamento DORA: Protección y prevención*** Los controles de acceso y los requisitos de autenticación robusta aplican a todo el ciclo de vida de la identidad, incluido el proceso de restablecimiento de contraseña, que no debe ser un eslabón más débil que la autenticación principal.	**Specops uReset** Restablecimiento de contraseñas de autoservicio protegido con MFA. Los usuarios pueden actualizar de forma segura las credenciales locales en caché desde cualquier ubicación, dispositivo o navegador, tanto dentro como fuera de la VPN. Se integra con plataformas SIEM, SOC y de analítica.

Contacta con tu representante de Specops o visita este enlace para reservar una llamada de valoración

Reservar ahora