

Facilitando el cumplimiento de DORA y las medidas de seguridad de la información con Prot-On



Nuestra solución Prot-On garantiza la protección y el control de acceso a los documentos.

La importancia del Reglamento de Resiliencia Operativa Digital (DORA)

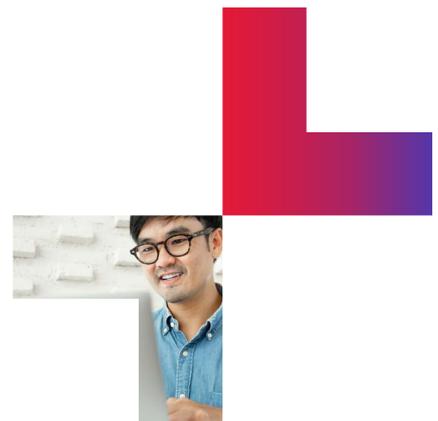
La Comisión Europea ha publicado el Reglamento de Resiliencia Operativa Digital (DORA) con el objetivo de mejorar la resiliencia operativa del sector financiero en la UE. Este reglamento se estructura sobre tres principios clave:

- **Gestión de riesgos informáticos y de ciberseguridad:** el reglamento obligará a estas entidades a establecer políticas y procedimientos que salvaguarden sus sistemas y datos de las ciberamenazas.
- **Gestión de la continuidad de la actividad:** las instituciones financieras estarán obligadas a desarrollar planes integrales de continuidad de negocio, asegurando su capacidad para prestar servicios a los clientes durante las interrupciones operativas.
- **Supervisión y vigilancia:** a través de este marco, las autoridades de supervisión y vigilancia controlarán y evaluarán la resistencia operativa de las entidades financieras. El incumplimiento de la normativa puede suponer multas de hasta 10 millones de euros o el 5% de su volumen de negocio total anual.

El Reglamento DORA entrará en vigor el **17 de enero de 2025**.



Se aplicará al conjunto de entidades financieras que operen en la UE, incluidos bancos, empresas de inversión, plataformas de negociación, entidades de contrapartida central y otras infraestructuras de los mercados financieros.



En CGI contamos con un amplio conocimiento y expertise global en Ciberseguridad

+40

años de experiencia

+1.700

profesionales especializados

+400

clientes en 40 países

+10M

activos digitales industriales securizados

+40

grandes referencias en Control de Acceso y Gestión de Identidad (IAM)

Requisitos para el cumplimiento de DORA

Las entidades financieras deben tomar las medidas oportunas para gestionar el riesgo y mejorar la resiliencia operativa frente a posibles incidentes mediante:

- Gestión de riesgos TIC.
- Gestión, clasificación y notificación de incidentes relacionados con las TIC.
- Pruebas de resiliencia operativa digital.
- Gestión de riesgos de terceros en las TIC.
- Intercambio de información e inteligencia.

Consulte los requisitos de DORA en https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

Prot-On asegura la gestión y protección de los datos

A través de nuestra solución facilitamos el uso de la encriptación y otras medidas de gestión y protección de datos exigidas por el Reglamento DORA:

- **Establecimiento de políticas destinadas a garantizar el mantenimiento de altos niveles de disponibilidad, autenticidad, integridad y confidencialidad de los datos**, según se recoge en los artículos 5 y 6 de este reglamento. Prot-On protege los datos confidenciales de accesos no autorizados, garantizando el control total de los datos con independencia de cómo se compartan dentro y fuera de la organización.

Además, permite **funciones avanzadas de seguridad para el cumplimiento de dichas políticas**, como los derechos de acceso granular, las fechas de caducidad, la revocación remota del acceso a documentos para cualquier usuario/grupo de usuarios y el acceso controlado.

- **Adopción de medidas de protección de claves criptográficas** por las que se encriptan los datos sobre la base de los resultados de los procesos aprobados de clasificación de datos y evaluación de riesgos de las TIC, dentro del artículo 9 del reglamento. Prot-On garantiza que los datos confidenciales estén cifrados y a salvo de accesos no autorizados.
- **Ayuda en la gestión de seguridad con la cadena de suministro** al permitir proteger y controlar los datos, independientemente de si la cuenta de correo es Office365 o no, y pudiendo integrar la gestión de identidad de usuarios con cualquier IdP (AD, LDAP...).
- **Facilita la gobernanza de la seguridad de los datos** mediante funciones integradas de clasificación manual (por usuario) y automática (expresiones regulares y patrones de IA).
- **Integra de forma nativa el uso de soluciones multifactor MFA** para acceso a la plataforma y acceso a los documentos.

En CGI ayudamos a nuestros clientes a identificar los riesgos de ciberseguridad, garantizar su protección y operar con confianza.

Prot-On

Es una solución IRM (Information Rights Management) para el cifrado y la gestión segura del intercambio de información, cuyas principales funcionalidades son:

- Protección de los archivos.
- Control de acceso a la información.
- Trazabilidad sobre la actividad de los documentos.
- Clasificación automática de archivos y textos.

Para más información:

Visite: cgi.com/spain/es/ciberseguridad

Envíe un email a: jose-manuel.kiernandiaz@cgi.com