INFORME DE AKAMAI

Reglamento sobre la resiliencia operativa digital

Preparación de las instituciones financieras para cumplir la norma DORA con Akamai

El Reglamento sobre la Resiliencia Operativa Digital (DORA) es una nueva pieza importante de la legislación europea que establece normas más estrictas para las entidades financieras reguladas, al exigir un marco de resiliencia operativa digital mejorado que cubra no solo a tales entidades, sino también a sus proveedores externos de tecnologías de la información y la comunicación (TIC). DORA entrará en vigor el 17 de enero de 2025.

Ámbito de aplicación de DORA

DORA se aplica a entidades financieras de todo el mundo que operan en los mercados de la UE. El ámbito incluye entidades tradicionales como bancos, gestoras de inversiones y entidades de crédito, así como entidades no tradicionales como proveedores de servicios de criptoactivos y plataformas de financiación colectiva.

Además, DORA impone ciertas obligaciones a entidades que no son financieras y que generalmente están exentas de cumplir la normativa al respecto. Por ejemplo, los proveedores de servicios externos que suministran sistemas y servicios de TIC a empresas financieras, como los proveedores de servicios en la nube y los centros de datos, deben cumplir ciertos requisitos de DORA. Además, DORA afecta a empresas que proporcionan servicios de información de terceros críticos, como servicios de calificación crediticia y proveedores de análisis de datos. Los proveedores externos de TIC designados como críticos por las Autoridades Europeas de Supervisión (AES) estarán sujetos a la evaluación por parte de un supervisor principal designado por las AES.

Akamai respaldará los objetivos de las autoridades financieras y proporcionará asistencia como tercero crítico y como proveedor, y ayudará a cumplir los regímenes marco a los que nuestros clientes están sujetos. Cooperaremos para proporcionar asistencia con las consultas y ayudar a comprender los medios por los que proporcionamos resiliencia operativa.

Los 5 pilares de DORA

El enfoque integral de DORA se basa en cinco pilares fundamentales, cada uno de ellos adaptado para abordar distintas facetas de la resiliencia operativa digital.

Gestión de riesgos	Notificación de incidentes	Pruebas de resiliencia operativa digital	Riesgos de TIC de terceros	Intercambio de información e inteligencia

Gestión de riesgos

- Visibilidad completa del rendimiento del servicio mediante Akamai Control Center (ACC) y sus paneles de gestión de análisis de seguridad integrados, supervisión de SLA e información sobre la documentación, incluidas las políticas y los informes.
- Las evaluaciones contractuales de gestión de riesgos de terceros que se llevan a cabo anualmente en Akamai permiten obtener información sobre la seguridad de la empresa y evaluar los riesgos asociados con el servicio.
- Los productos Zero Trust y de segmentación de Akamai ayudan a los clientes a minimizar y aliviar los riesgos relacionados con el ransomware y las amenazas de elevación de acceso interno.
- La auditoría continua de la seguridad de Akamai mediante marcos de seguridad según los sectores y las regiones como SOC 2, ISO 27001 o la Oficina Federal de Seguridad de la Información (BSI) alemana permiten mejorar la evaluación del estado de riesgo de la empresa.

Notificación de incidentes

- Cobertura ininterrumpida con sistema de notificación para todos los incidentes que afectan al cliente dentro de los plazos previstos.
- Cobertura mundial, con expertos en seguridad y servicios de atención al cliente disponibles en varios centros de operaciones ubicados en las principales regiones geográficas.
- Provisión de información sobre incidentes a través de akamaistatus.com, servicio comunitario y ACC.

Akamai

Pruebas de resiliencia operativa digital

- Modelo de resiliencia de vanguardia probado para resistir los mayores ataques DDoS observados en el sector de las TIC.
- Pruebas trimestrales de la infraestructura y pruebas semestrales del nivel de preparación del personal para la recuperación en caso de desastres.
- Aprendizaje continuo e implementación de mejoras año tras año para garantizar que el régimen de pruebas de penetración interno y orientado al cumplimiento normativo se ajuste al marco TIBER-UE para evaluar el modelo de resiliencia existente.

Riesgos de TIC de terceros

- Akamai evalúa a todos sus proveedores y terceros antes de incorporarlos y utilizar sus servicios y plataformas. Cada proveedor y producto se somete a comprobaciones específicas relacionadas con la seguridad de su servicio, la forma en que procesa la información, el cumplimiento de la ley de privacidad y si el estado financiero de la empresa supone algún riesgo para Akamai.
- El equipo dedicado de gestión de riesgos de terceros (TPRM) garantiza que los proveedores cumplan contractualmente con las normas de contratación de proveedores de Akamai. Cada proveedor crítico está sujeto a un control anual de conformidad con las obligaciones contractuales, y se establecen planes de salida en caso de que haya una infracción del cumplimiento.

Intercambio de información e inteligencia

- El grupo de inteligencia sobre seguridad de Akamai lleva a cabo investigaciones continuas sobre las amenazas emergentes dirigidas a los proveedores de TIC y a los clientes de Akamai. Se utiliza una sofisticada red de señuelos e inteligencia reunidos fuera del Edge globalmente distribuido de Akamai para identificar indicadores de riesgo (IOC), que posteriormente se comparten a través de diferentes canales de comunicación.
- Akamai participa en la comunidad de intercambio de inteligencia de FS-ISAC, y aporta muestras y casos prácticos de inteligencia "Green" (verde) y "Amber" (ámbar) de TLP.

"Las entidades financieras contarán con un marco de gestión del riesgo relacionado con las TIC sólido, completo y bien documentado como parte de su sistema global de gestión de riesgos, que les permita hacer frente al riesgo relacionado con las TIC de forma rápida, eficiente y exhaustiva y asegurar un alto nivel de resiliencia operativa digital". (Artículo 6)

El marco de resiliencia operativa requiere una atención continua para proteger los activos de TIC e información de la organización. Esto incluye la protección continua del software, los equipos físicos y los datos. Así, prevé actualizaciones periódicas, al menos una vez al año, en caso de incidentes importantes relacionados con las TIC, las directivas de supervisión o la información procedente de los procesos de prueba o las auditorías.

Cómo ayuda Akamai

Akamai se alinea con los objetivos de las autoridades de un sistema financiero europeo sólido y valora el diálogo continuo. Cumplimos diligentemente con las normativas y ayudaremos a los clientes a comprender nuestro enfoque con los terceros críticos, al tiempo que mejoramos su resiliencia operativa.

Con Akamai, las instituciones financieras pueden gestionar de forma eficaz los desafíos relacionados con el cumplimiento, incluida la ambigüedad y la incertidumbre en materia de normativas, ya sea DORA o normativas futuras, mediante medidas de seguridad integrales que abarcan desde las cargas de trabajo de las aplicaciones y las API hasta la infraestructura de aplicaciones. La seguridad se convierte en un componente vital del conjunto de herramientas normativas, lo que facilita un cambio sostenible y eficaz y, lo que es más importante, fomenta la confianza de los clientes en las instituciones financieras y en el mercado financiero en general.

Obtenga más información sobre DORA.