INFORME DE AKAMAI

Cumplimiento de DORA: Pilar por pilar

Con la Ley de Resiliencia Operativa Digital (DORA) ya vigente, las entidades financieras y los proveedores de servicios externos de TIC (tecnologías de la información y las comunicaciones) que operan en la UE tienen que seguir nuevas reglas. Aunque los nuevos requisitos ya estén en vigor, tanto su amplitud como su complejidad obligan a muchas instituciones financieras a seguir trabajando para lograr el pleno cumplimiento de esta ley en los próximos meses y años.

Consideraciones clave sobre el cumplimiento de DORA

En este artículo se describen consideraciones clave para facilitar el cumplimiento de DORA. Aunque no constituyen una lista cerrada, pretendemos que sirva de ayuda para destacar aquellas acciones que permitan a las entidades financieras cumplir esta normativa antes.

Trabajar con el objetivo en mente de cumplir la ley DORA puede ayudar a las organizaciones a mitigar mejor los riesgos, a proteger los datos clave, a ser más resilientes frente a las amenazas en constante evolución y a poder disfrutar de una mayor visibilidad de las redes, los sistemas y los procesos.

Aunque la experiencia hasta cumplir la ley DORA puede resultar compleja y costosa, también ofrece la oportunidad de crear un marco de seguridad unificado e integral que ayude a la organización a prepararse a conseguir sus objetivos futuros.

Acción	Dónde radica su importancia	Soluciones
PILAR 1: Gestión de riesgos de TIC		
Restringir el movimiento lateral por carga de trabajo.	Contiene incidentes, protege los flujos de datos esenciales y minimiza el tiempo de inactividad y el posible impacto en la empresa.	Microsegmentación con políticas específicas de las cargas de trabajo, inspección del tráfico este-oeste a través de firewalls internos, control de acceso basado en identidades (IBAC), acceso de red Zero Trust (ZTNA), redes definidas por software (SDN), gestión de acceso privilegiado (PAM), y detección y respuesta en los terminales (EDR)
Limitar el acceso de los usuarios a las aplicaciones necesarias en función de los roles y la identidad.	Proporciona un enfoque específico y metódico para proteger los activos esenciales mediante el control de quién puede acceder a qué. Evita el acceso no autorizado y le proporciona un control detallado de los usuarios y del acceso al sistema.	Control de acceso basado en roles (RBAC), gestión de acceso e identidades (IAM), acceso de red Zero Trust (ZTNA), inicio de sesión único (SSO), autenticación multifactorial (MFA) y gestión de acceso privilegiado (PAM)
Eliminar el acceso mediante ID y contraseña, sustituyéndolo por MFA.	Protege contra el robo de credenciales.	Autenticación multifactorial, inicio de sesión único (SSO), autenticación sin contraseña (p. ej., biométrica, claves FIDO2), políticas de acceso condicional que exigen MFA, gestión de acceso privilegiado (PAM) con MFA para un acceso con medidas de control reforzadas y soluciones de MFA basadas en tokens de hardware o de notificación móvil

Acción	Dónde radica su importancia	Soluciones
Garantizar la visibilidad de todos los activos de TIC, desde servidores y redes hasta aplicaciones.	Una gestión de riesgos eficaz comienza con la capacidad de identificar y controlar vulnerabilidades concretas en todos los activos en cualquier momento. El control y la visibilidad son fundamentales.	Base de datos de gestión de la configuración (CMDB), gestión de activos de TI (ITAM), gestión de eventos e información de seguridad (SIEM), detección y respuesta de red (NDR), detección y respuesta en los terminales (EDR), supervisión del rendimiento de las aplicaciones (APM), gestión de la estrategia de seguridad de la nube (CSPM), gestión de la seguridad de las aplicaciones (ASPM) y gestión de la estrategia de seguridad de los datos (DSPM)
Transmisión de datos segura.	Los datos privados, incluida la información de identificación personal (PII), los registros financieros y los datos transaccionales deben tratarse de forma confidencial.	Protocolos de cifrado sólidos, VPN, TLS, protocolos de transferencia segura de archivos, cifrado de terminales, PKI y otros
PILAR 2: Gestión e informes de incidentes relacionados con las TIC		
Límites de los segmentos.	Acelera los procesos de detección, respuesta y recuperación al contener y aislar los incidentes de forma rápida.	Microsegmentación, segmentación de red, firewalls de última generación, listas de control de acceso (ACL), redes definidas por software (SDN) y acceso de red Zero Trust
Posibilitar el aislamiento de segmentos comprometidos sin interrumpir las operaciones a un nivel más general.	Garantiza una respuesta rápida a los incidentes.	Microsegmentación, redes definidas por software (SDN), detección y respuesta en los terminales (EDR), control de acceso a la red (NAC), acceso de red Zero Trust (ZTNA) y LAN virtuales (VLAN)
Restringir el acceso a información confidencial y a aplicaciones esenciales.	Reduce la probabilidad de que se produzca una amenaza.	Control de acceso basado en roles (RBAC), autenticación multifactorial (MFA), acceso de red Zero Trust (ZTNA), gestión de acceso e identidades (IAM), gestión de acceso privilegiado (PAM), y red y microsegmentación
Usar detección y respuesta a amenazas en tiempo real.	Una respuesta rápida a los incidentes de TIC resulta esencial para limitar su impacto. La información detallada sobre amenazas y la información de registro también pueden ser útiles para la elaboración de informes.	Gestión de eventos e información de seguridad (SIEM), detección y respuesta en los terminales (EDR), detección y respuesta extendidas (XDR), sistemas de detección y prevención de intrusiones (IDPS), fuentes e integración de inteligencia sobre amenazas, orquestación, automatización y respuesta de seguridad (SOAR), análisis del comportamiento y servicios de detección de anomalías, engaño y de búsqueda de amenazas

Acción	Dónde radica su importancia	Soluciones
Plantearse la posibilidad de poner en marcha una búsqueda avanzada de amenazas con corrección.	Detecta riesgos de forma proactiva.	Servicios de búsqueda de amenazas y proveedores de servicios de seguridad gestionados (MSSP)
PILAR 3: Pruebas de resiliencia operativa digital		
Simular un fallo en las partes segmentadas de la red.	Proporciona una vista en tiempo real de la resiliencia operativa.	Integración con una herramienta de modelado para mostrar la resiliencia de la ruta completa y los puntos de cumplimiento Herramientas de ingeniería del caos, entornos de simulación de redes y de prueba, redes definidas por software (SDN), ejercicios de equipos rojos/equipos azules, pruebas de recuperación ante desastres y failover, y entornos de laboratorio de seguridad
Realizar pruebas de estrés y simulaciones de ataques de forma periódica.	Destaca las deficiencias de las redes, las aplicaciones y los sistemas esenciales. Le permite realizar los ajustes necesarios rápidamente y crear estrategias de respuesta adaptables, lo que aumenta su capacidad para mitigar las amenazas a medida que evolucionen.	Guía de respuesta ante ransomware y ejercicios teóricos para equipos rojos, azules y morados Pruebas periódicas de penetración, simulación de ataques y vulneraciones, herramientas de análisis de vulnerabilidades y evaluaciones de la estrategia, simulación de ataques distribuidos de denegación de servicio (DDoS) y de ataques automatizados
Utilizar ZTNA y MFA para las pruebas de resiliencia.	Al mantener políticas de acceso estrictas durante interrupciones o incidentes simulados, obtiene una imagen real de su estado de seguridad.	Acceso de red Zero Trust (ZTNA), autenticación multifactorial (MFA), gestión de acceso e identidades (IAM), gestión de eventos e información de seguridad (SIEM) y microsegmentación
Controlar el acceso a aplicaciones y recursos clave con mucha presión.	Mejora la fiabilidad y la preparación de sus defensas.	Acceso de red Zero Trust (ZTNA), autenticación multifactorial (MFA), control de acceso basado en roles (RBAC), gestión de acceso privilegiado (PAM), gestión de acceso e identidades (IAM), red y microsegmentación, balanceadores de carga, y protección de API y aplicaciones web (WAAP)
Probar la preparación para un ataque distribuido de denegación de servicio (DDoS).	Ayuda a detectar vulnerabilidades y a optimizar las estrategias de resiliencia.	Simulación y pruebas de DDoS, protección contra ataques DDoS basados en la nube, firewalls de aplicaciones web (WAF), centros de barrido de tráfico, herramientas de análisis del comportamiento de la red y de detección de anomalías, guías de respuesta a incidentes, ejercicios teóricos y ejercicios de equipos rojos

Acción	Dónde radica su importancia	Soluciones
PILAR 4: Gestión del riesgo de terceros		
Segmentar los entornos donde interactúan proveedores o aplicaciones de terceros.	Acelera los procesos de detección, respuesta y recuperación al contener y aislar los incidentes de forma rápida.	Microsegmentación con políticas basadas en identidades, LAN virtuales (VLAN), zonas desmilitarizadas (DMZ), firewall con controles de acceso detallados, acceso de red Zero Trust (ZTNA), control de acceso a la red (NAC) y puertas de enlace VPN dedicadas
Acceso seguro a Internet para todas las comunicaciones externas.	Garantiza que los terceros solo se conecten a través de accesos seguros y controlados.	Puertas de enlace web seguras (SWG), agentes de seguridad de acceso a la nube (CASB), seguridad DNS, firewalls de nueva generación con filtrado de URL (NGFW), comunicaciones cifradas (p. ej., HTTPS, TLS 1.2/1.3), puertas de enlace de seguridad de correo electrónico con cifrado, acceso de red Zero Trust (ZTNA)
Habilitar la supervisión continua en tiempo real del acceso de terceros.	Detecta y protege inmediatamente contra los riesgos procedentes de proveedores de TIC o de sus proveedores externos.	Microsegmentación, portal de análisis y reglas de protección de API y aplicaciones web (WAAP) personalizadas Gestión de eventos e información de seguridad (SIEM), gestión de acceso e identidades (IAM), gestión de acceso privilegiado (PAM), análisis del comportamiento de usuarios y entidades (UEBA), acceso de red Zero Trust (ZTNA), control de acceso a la red (NAC), y detección y respuesta en los terminales (EDR)
PILAR 5: Intercambio de información		
Segmentar los datos confidenciales y restringir el acceso únicamente a los usuarios autorizados.	Reduce la probabilidad de que se produzca una amenaza.	Clasificación y etiquetado de datos, microsegmentación con políticas que giran en torno a los datos, control de acceso basado en roles (RBAC), gestión de acceso e identidades (IAM), prevención de pérdida de datos (DLP) y gestión de acceso privilegiado (PAM)
Asegurarse de que la información se comparta tanto a nivel interno como externo a través de canales seguros.	Reduce el riesgo de que los datos confidenciales se puedan ver comprometida.	Cifrado integral (p. ej., TLS 1.2/1.3, S/MIME), protocolos de transferencia segura de archivos (p. ej., SFTP, FTPS), soluciones de correo electrónico cifrado, redes privadas virtuales (VPN), puertas de enlace web seguras (SWG) y prevención de pérdida de datos (DLP)

Acción	Dónde radica su importancia	Soluciones
Permitir un acceso seguro a las plataformas de comunicación.	Reduce el riesgo de que los datos confidenciales se puedan ver comprometida.	Autenticación multifactorial (MFA), gestión de acceso e identidades (IAM), inicio de sesión único (SSO), acceso de red Zero Trust (ZTNA), controles de seguridad de terminales, plataformas de comunicación cifradas y puertas de enlace web seguras (SWG)
Aplicar la verificación de identidad.	Refuerza la confianza en el proceso de intercambio de información al tiempo que protege la integridad de los datos.	Autenticación multifactorial (MFA), gestión de acceso e identidades (IAM), inicio de sesión único (SSO), gestión de acceso privilegiado (PAM), autenticación biométrica (por ejemplo, huella dactilar, reconocimiento facial), certificados digitales e infraestructura de clave pública (PKI) y servicios de directorio (por ejemplo, Active Directory, Microsoft Entra ID)
Compartir datos de forma segura más allá de las fronteras con otros miembros de la comunidad financiera sobre amenazas, vulnerabilidades y patrones de ataque emergentes.	Distribuye la inteligencia sobre amenazas en las distintas zonas geográficas, creando respuestas rápidas y estrategias de defensa colectiva.	Plataformas de inteligencia contra amenazas, canales de comunicación cifrados (p. ej., TLS, S/MIME, VPN), uso compartido de información y eventos (p. ej., FS-ISAC), clasificación de datos y controles de acceso, protocolos de transferencia segura de archivos (p. ej., SFTP, FTPS) y políticas de uso compartido de datos transfronterizas

Aviso: *La información proporcionada aquí se incluye solo con fines informativos generales. No debe interpretarse como un consejo legal y no supone ningún compromiso por parte de Akamai. Las leyes y normativas pueden variar, y las interpretaciones legales pueden cambiar con el tiempo. No se garantiza la exactitud, integridad o idoneidad de la información proporcionada. Si necesita consejo legal o tiene preguntas concretas en este sentido, consulte a un profesional del sector jurídico cualificado que le proporcionará asesoramiento específico sobre su situación y jurisdicción.*