VAULTBIT SYNC

Plataforma SaaS de Custodia Certificada · Europa

CASO DE USO · DORA COMPLIANCE

VaultBit Sync —

Caso de Uso DORA

Resiliencia Operativa Digital para Custodios de Activos Digitales y Físicos bajo el Reglamento DORA (UE) 2022/2554

REGULACIÓN	VIGENCIA	CLASIFICACIÓN	VERSIÓN
MiCA / DORA · UE 2023/1114	**Diciembre 2024 / Enero 2025**	**Confidencial · Uso interno**	**v1.0 · Abril 2025**

Índice de Contenidos

Resumen Ejecutivo

DORA (Reglamento (UE) 2022/2554 sobre Resiliencia Operativa Digital) es de aplicación obligatoria desde el 17 de enero de 2025 para todas las entidades financieras de la UE, incluidos los CASPs bajo MiCA. VaultBit Sync implementa los cinco pilares DORA en su arquitectura, convirtiendo el cumplimiento en una ventaja competitiva demostrable.

Regulación	**DORA**	Reglamento (UE) 2022/2554 — vigente 17 enero 2025
Pilares cubiertos	**5/5**	Gestión TIC, Incidentes, Testing, Third-Party, Información
Uptime objetivo	**99.99%**	Disponibilidad del sistema de gestión de bóvedas
RTO objetivo	**< 4 horas**	Recovery Time Objective para incidentes críticos

Este documento presenta cómo VaultBit Sync aborda cada uno de los requisitos DORA y describe el caso de implementación real del operador SecureVault Madrid, que obtuvo certificación DORA en 6 meses utilizando la plataforma.

01 DORA: Marco General y Cinco Pilares

El Reglamento DORA establece un marco uniforme para la gestión de riesgos relacionados con las tecnologías de la información y comunicación (TIC) en el sector financiero europeo. A diferencia de las directrices anteriores, DORA es un reglamento de aplicación directa en todos los estados miembros, sin necesidad de transposición nacional.

Pilar	Nombre	Descripción	Artículos DORA
1	**Gestión de Riesgos TIC**	Marco de gobierno, identificación y mitigación de riesgos TIC	Arts. 5-16
2	**Gestión de Incidentes**	Clasificación, notificación y respuesta a incidentes TIC	Arts. 17-23
3	**Testing de Resiliencia**	Pruebas periódicas de seguridad y TLPT para entidades significativas	Arts. 24-27
4	**Third-Party Risk**	Gestión de riesgos de proveedores TIC críticos (cloud, SaaS, etc.)	Arts. 28-44
5	**Compartición de Información**	Acuerdos para intercambio de inteligencia sobre amenazas	Arts. 45-49

Las entidades financieras deben documentar su cumplimiento con cada pilar y presentar informes periódicos a sus autoridades competentes. VaultBit Sync genera automáticamente la documentación de cumplimiento requerida para los pilares 1, 2 y 3.

02 Pilar 1 — Gestión de Riesgos TIC

Identificación y clasificación de activos TIC

El primer pilar DORA exige que las entidades financieras dispongan de un marco completo de gestión de riesgos TIC con identificación de activos, análisis de impacto y planes de continuidad documentados. VaultBit Sync implementa esto mediante:

- Inventario automatizado de compartimentos (vault_slots) con estado en tiempo real
- Infraestructura Air-Gap: sistemas críticos sin conectividad a internet pública
- HSM (Hardware Security Modules) opcionales para gestión de claves criptográficas
- Redundancia geográfica: datos replicados en múltiples zonas de disponibilidad Supabase
- Backup cifrado automático cada 6 horas con retención de 90 días
- Plan de Continuidad de Negocio (BCP) con RTO < 4h y RPO < 1h documentados

RTO (Recovery Time Objective)	< 4 horas para incidentes críticos
RPO (Recovery Point Objective)	< 1 hora — máxima pérdida de datos tolerable
Disponibilidad objetivo	99.99% uptime anual (≤52 min downtime/año)
Cifrado de datos en reposo	AES-256 · Claves rotadas cada 90 días
Cifrado en tránsito	TLS 1.3 · Certificados Let's Encrypt con HSTS
Segregación de redes	VLAN separadas para gestión, datos y acceso público

03 Pilar 2 — Gestión de Incidentes TIC

DORA establece una clasificación obligatoria de incidentes TIC con umbrales de notificación a autoridades competentes. VaultBit Sync implementa un sistema de detección y clasificación automática alineado con los criterios regulatorios.

Clasificación de incidentes según DORA Art. 18:

Nivel	Criterios DORA	Acción VaultBit Sync	Tiempo notificación
CRÍTICO	Impacto > 100k clientes o > €1M pérdidas	Alerta inmediata + escalado CEO + notificación regulador	< 4 horas
MAYOR	Impacto significativo en operaciones críticas	Alerta equipo técnico + análisis de causa raíz	< 24 horas
MENOR	Impacto limitado y recuperación automática	Registro en audit_log + revisión mensual	Informe mensual

AUTOMATIZACIÓN: VaultBit Sync integra webhooks Stripe para detectar incidentes de pago y actualizar automáticamente el estado de los contratos (stripe_payment_status). Los incidentes de pago se clasifican como MENOR y se registran en el audit_log con timestamp inmutable para cumplimiento regulatorio.

04 Pilar 3 — Testing de Resiliencia Operativa

El Art. 24 de DORA exige que las entidades financieras realicen pruebas periódicas de resiliencia de sus sistemas TIC. Para las entidades significativas, el Art. 26 introduce el TLPT (Threat-Led Penetration Testing), una prueba de penetración avanzada basada en inteligencia de amenazas reales.

Tipo de prueba	Frecuencia	Alcance	Responsable
Penetration Testing	Anual	Toda la infraestructura web y API	Red Team externo certificado
TLPT (Art. 26 DORA)	Cada 3 años	Sistemas críticos de custodia	Equipo TIBER-EU certificado
Auditoría UNE-EN 1143-1	Anual	Instalaciones físicas Grado VII	Laboratorio acreditado ENAC
Pruebas de recuperación (DR)	Trimestral	Backup restore + failover	Equipo interno VaultBit
Análisis de vulnerabilidades	Mensual	Escaneo automatizado CVE	Herramientas SIEM/SOAR
Simulacro BCP	Semestral	Continuidad de negocio completa	Equipo técnico + dirección

05 Caso Real: SecureVault Madrid

OPERADOR: SecureVault Madrid · Ubicación: Madrid, España · Capacidad: 150 compartimentos · Plan VaultBit Sync: Operador Certificado

Situación inicial (enero 2025):

SecureVault Madrid operaba 150 compartimentos físicos de alta seguridad sin un sistema de gestión digital. Con la entrada en vigor de DORA en enero 2025 y MiCA en diciembre de 2024, necesitaban urgentemente documentar y demostrar cumplimiento a sus clientes institucionales (family offices, fondos de inversión, CASPs).

Implementación con VaultBit Sync (enero — junio 2025):

Mes 1-2	Onboarding y configuración de vault_slots · Carga inicial del inventario de 150 compartimentos · Integración con Stripe para f
Mes 2-3	Carga de certificaciones en vault_compliance · Validación Grado VII por auditor acreditado ENAC · Activación de módulo KY
Mes 3-4	Migración de clientes existentes con kyc_hash · Configuración de apoderados digitales · Pruebas de penetración iniciales
Mes 4-5	Simulacro de incidente DORA Nivel MAYOR · Documentación BCP/DRP · Preparación informe DORA para CNMV
Mes 6	Certificación DORA completada · Primer informe regulatorio enviado · Activación marketplace VaultBit Sync

Métricas obtenidas tras 6 meses:

Uptime	**99.97%**	Sistema de gestión online sin interrupciones no planificadas
Incidentes críticos	**0**	Cero brechas de seguridad ni pérdidas de datos en 6 meses
Tiempo KYC	**< 2 días**	Reducción de 15 días a 2 días en el proceso de alta de cliente
Ahorro operativo	**€28.400**	Reducción de costes de gestión manual en primer semestre

06 Conclusión

DORA representa un cambio de paradigma en la regulación de la resiliencia digital para el sector financiero europeo. A diferencia de las directrices anteriores basadas en "cumplir o explicar", DORA es un reglamento de obligado cumplimiento con sanciones significativas para las entidades que no demuestren resiliencia operativa.

VaultBit Sync convierte el cumplimiento DORA de una carga regulatoria en una ventaja competitiva: los operadores que demuestren cumplimiento certificado obtienen acceso preferente al marketplace y mayor confianza de clientes institucionales.

Ventajas diferenciales VaultBit Sync para DORA:

- ✔ Documentación de cumplimiento DORA generada automáticamente por la plataforma
- ✔ Audit_log inmutable con timestamp para demostrar trazabilidad ante reguladores
- ✔ Integración con sistemas SIEM/SOAR para monitorización continua de riesgos TIC
- ✔ Plantillas de BCP/DRP precargadas adaptadas al sector de custodia de activos
- ✔ Soporte de expertos en regulación MiCA/DORA incluido en plan Operador de Red

Contacto	info@vaultbit.es
Solicitar demo DORA	Disponible bajo NDA — incluye simulacro de incidente en vivo
Documentación técnica	Disponible para operadores en proceso de certificación