Informe de cumplimiento normativo

Generado: 03/05/2026 21:23

Proyecto de cualificación QERDS y TSA bajo eIDAS

KPIs globales

Total requisitos	274	Cumplimiento global	0.0 %
Cumplen (C)	0	Cumplen parcial (CP)	0
No cumplen (NC)	274	No aplica (NA)	0
Gaps críticos	162	Evidencias validadas	0
Entregables aceptados	0	Total entregables	10

Cumplimiento por marco normativo

Marco	Total	C	CP	NC	NA	% Cumplimiento
eIDAS-910-2014	34	0	0	34	0	0.0 %
eIDAS-2-2024-1183	9	0	0	9	0	0.0 %
ETSI-EN-319-401	58	0	0	58	0	0.0 %
ETSI-EN-319-521	31	0	0	31	0	0.0 %
ETSI-EN-319-522	13	0	0	13	0	0.0 %
ETSI-EN-319-421	28	0	0	28	0	0.0 %
ETSI-EN-319-422	10	0	0	10	0	0.0 %
ETSI-TS-119-312	12	0	0	12	0	0.0 %
ETSI-EN-319-403	15	0	0	15	0	0.0 %
LEY-6-2020	20	0	0	20	0	0.0 %
ENS-ALTA	17	0	0	17	0	0.0 %
RGPD-LOPDGDD	12	0	0	12	0	0.0 %
ISO-IEC-27001	9	0	0	9	0	0.0 %
HSM-CERT	6	0	0	6	0	0.0 %

Preparación para auditoría CAR

Requisitos preparados: **0** de 274 · Preparación: **0.0 %** · Bloqueantes (criticidad Alta no listos): **162**

Detalle por requisito

Código	Marco	Cláusula	Nivel	Crit.	Responsable
REQ-EIDAS-13	eIDAS-910-2014	Art. 13 – Responsabilidad y carga de la prueba	NC	Alta	
REQ-EIDAS-14	eIDAS-910-2014	Art. 14 – Aspectos internacionales	UE	Baja	
REQ-EIDAS-15	eIDAS-910-2014	Art. 15 – Accesibilidad para personas con discapacidad	NC	Baja	
REQ-EIDAS-17	eIDAS-910-2014	Art. 17 – Canal formal con el organismo de supervisión	NC	Alta	
REQ-EIDAS-19-1	eIDAS-910-2014	Art. 19.1 – Medidas técnicas y organizativas adecuadas	NC	Alta	
REQ-EIDAS-19-2	eIDAS-910-2014	Art. 19.2 – Notificación de violaciones de seguridad en 24h	NC	Alta	
REQ-EIDAS-20-1	eIDAS-910-2014	Art. 20.1 – Auditoría bienal por CAB y entrega del CAR	NC	Alta	
REQ-EIDAS-20-2	eIDAS-910-2014	Art. 20.2 – Auditorías ad-hoc del supervisor	NC	Media	
REQ-EIDAS-21-1	eIDAS-910-2014	Art. 21.1 – Notificación previa al inicio del servicio cualificado	NC	Alta	
REQ-EIDAS-21-2	eIDAS-910-2014	Art. 21.2 – Verificación por el supervisor (≤3 meses)	NC	Alta	
REQ-EIDAS-22	eIDAS-910-2014	Art. 22 – Inclusión en la Trusted List (TSL)	NC	Alta	
REQ-EIDAS-23	eIDAS-910-2014	Art. 23 – Uso de la etiqueta de confianza UE	NC	Baja	
REQ-EIDAS-24-1A	eIDAS-910-2014	Art. 24.1.a – Verificación de identidad de los clientes	NC	Alta	
REQ-EIDAS-24-1B	eIDAS-910-2014	Art. 24.1.b – Personal cualificado y competente	NC	Media	
REQ-EIDAS-24-1C	eIDAS-910-2014	Art. 24.1.c – Recursos financieros suficientes / seguro	NC	Alta	
REQ-EIDAS-24-1D	eIDAS-910-2014	Art. 24.1.d – Información precontractual a los clientes	NC	Media	
REQ-EIDAS-24-1E	eIDAS-910-2014	Art. 24.1.e – Sistemas y productos fiables y certificados	NC	Alta	
REQ-EIDAS-24-1F	eIDAS-910-2014	Art. 24.1.f – Sistemas de almacenamiento robustos	NC	Alta	
REQ-EIDAS-24-1G	eIDAS-910-2014	Art. 24.1.g – Medidas contra falsificación y robo	NC	Alta	
REQ-EIDAS-24-1H	eIDAS-910-2014	Art. 24.1.h – Registro y conservación de información	NC	Alta	
REQ-EIDAS-24-1I	eIDAS-910-2014	Art. 24.1.i – Plan de cese del TSP	NC	Alta	
REQ-EIDAS-24-1J	eIDAS-910-2014	Art. 24.1.j – Tratamiento de datos personales conforme RGPD	NC	Media	
REQ-EIDAS-24-2	eIDAS-910-2014	Art. 24.2 – Verificación remota de identidad por medios equivalentes	NC	Alta	
REQ-EIDAS-41	eIDAS-910-2014	Art. 41 – Presunción legal del sello cualificado de tiempo	NC	Alta	
REQ-EIDAS-42-1	eIDAS-910-2014	Art. 42.1 – Requisitos técnicos del sello cualificado de tiempo	NC	Alta	
REQ-EIDAS-42-2	eIDAS-910-2014	Art. 42.2 – Reconocimiento mutuo del sello de tiempo	NC	Alta	
REQ-EIDAS-43-1	eIDAS-910-2014	Art. 43.1 – Cuatro presunciones del servicio QERDS	UE	Alta	
REQ-EIDAS-43-2	eIDAS-910-2014	Art. 43.2 – Distinción clara entre servicio cualificado y no cualificado	NC	Media	
REQ-EIDAS-44-1A	eIDAS-910-2014	Art. 44.1.a – Cualificación del prestador QERDS	NC	Alta	
REQ-EIDAS-44-1B	eIDAS-910-2014	Art. 44.1.b – Identificación del emisor nivel sustancial/alto	NC	Alta	
REQ-EIDAS-44-1C	eIDAS-910-2014	Art. 44.1.c – Identificación del destinatario nivel sustancial/alto antes de la entrega	NC	Alta	
REQ-EIDAS-44-1D	eIDAS-910-2014	Art. 44.1.d – Protección de integridad con firma/sello cualificado	NC	Alta	
REQ-EIDAS-44-1E	eIDAS-910-2014	Art. 44.1.e – Sello cualificado de tiempo en todos los hitos	NC	Alta	
REQ-EIDAS-44-2	eIDAS-910-2014	Art. 44.2 – Interoperabilidad técnica entre QERDS de la UE	NC	Media	
REQ-EIDAS2-ARCHIVO	eIDAS-2-2024-1183	Servicio cualificado de archivo electrónico (fuera del alcance)	NC	Baja	
REQ-EIDAS2-ATTREG	eIDAS-2-2024-1183	Atestaciones electrónicas de atributos (fuera del alcance actual)	NC	Baja	
REQ-EIDAS2-AUDITEID	eIDAS-2-2024-1183	Auditorías de ciberseguridad adicionales bajo eIDAS 2	NC	Media	
REQ-EIDAS2-CYBERDA	eIDAS-2-2024-1183	Alineación con NIS2: los TSP cualificados como entidades esenciales	NC	Alta	
REQ-EIDAS2-IMPLACTS	eIDAS-2-2024-1183	Sistema de seguimiento de Reglamentos de ejecución eIDAS 2	NC	Media	
REQ-EIDAS2-INCIDEA	eIDAS-2-2024-1183	Plazos de notificación de incidentes reforzados: 24h/72h/1 mes	NC	Alta	
REQ-EIDAS2-INTEROPA	eIDAS-2-2024-1183	Interoperabilidad transfronteriza reforzada bajo eIDAS 2	NC	Media	
REQ-EIDAS2-VULN	eIDAS-2-2024-1183	Notificación de vulnerabilidades graves al supervisor	NC	Media	
REQ-EIDAS2-WALLET	eIDAS-2-2024-1183	EUDI Wallet: análisis de impacto futuro (fuera del alcance actual)	NC	Baja	

Código	Marco	Cláusula	Nivel	Crit.	Responsable
REQ-401-5-RA1	ETSI-EN-319-401	§5 Risk Assessment	NC	Alta	
REQ-401-5-RA2	ETSI-EN-319-401	§5 Risk Assessment	NC	Media	
REQ-401-5-RA3	ETSI-EN-319-401	§5 Risk Assessment	NC	Alta	
REQ-401-6.1-A	ETSI-EN-319-401	§6.1 Internal organization – Entidad legal	NC	Baja	
REQ-401-6.1-B	ETSI-EN-319-401	§6.1 Internal organization – Roles y responsabilidades	NC	Alta	
REQ-401-6.1-C	ETSI-EN-319-401	§6.1 Internal organization – Segregación de funciones	NC	Alta	
REQ-401-6.1-D	ETSI-EN-319-401	§6.1 Internal organization – Compromiso de dirección	NC	Media	
REQ-401-6.10-A	ETSI-EN-319-401	§6.10 Collection of evidence – Logs	NC	Alta	
REQ-401-6.10-B	ETSI-EN-319-401	§6.10 Collection of evidence – Integridad	NC	Alta	
REQ-401-6.10-C	ETSI-EN-319-401	§6.10 Collection of evidence – Sincronización temporal	NC	Alta	
REQ-401-6.11-A	ETSI-EN-319-401	§6.11 Business continuity – Plan	NC	Alta	
REQ-401-6.11-B	ETSI-EN-319-401	§6.11 Business continuity – Pruebas	NC	Alta	
REQ-401-6.11-C	ETSI-EN-319-401	§6.11 Business continuity – DR	NC	Alta	
REQ-401-6.12-A	ETSI-EN-319-401	§6.12 Termination plan – Documento	NC	Alta	
REQ-401-6.12-B	ETSI-EN-319-401	§6.12 Termination plan – Custodia de evidencias	NC	Alta	
REQ-401-6.12-C	ETSI-EN-319-401	§6.12 Termination plan – Recursos financieros	NC	Alta	
REQ-401-6.13-A	ETSI-EN-319-401	§6.13 Compliance – Identificación de requisitos	NC	Media	
REQ-401-6.13-B	ETSI-EN-319-401	§6.13 Compliance – Auditoría externa	NC	Alta	
REQ-401-6.13-C	ETSI-EN-319-401	§6.13 Compliance – Auditoría interna	NC	Media	
REQ-401-6.13-D	ETSI-EN-319-401	§6.13 Compliance – Acciones correctoras	NC	Media	
REQ-401-6.2-A	ETSI-EN-319-401	§6.2 Human resources – Verificación	NC	Media	
REQ-401-6.2-B	ETSI-EN-319-401	§6.2 Human resources – Cualificación	NC	Media	
REQ-401-6.2-C	ETSI-EN-319-401	§6.2 Human resources – Formación	NC	Media	
REQ-401-6.2-D	ETSI-EN-319-401	§6.2 Human resources – Confidencialidad	NC	Baja	
REQ-401-6.2-E	ETSI-EN-319-401	§6.2 Human resources – Sanciones	NC	Baja	
REQ-401-6.3-A	ETSI-EN-319-401	§6.3 Asset management – Inventario	NC	Media	
REQ-401-6.3-B	ETSI-EN-319-401	§6.3 Asset management – Clasificación	NC	Media	
REQ-401-6.3-C	ETSI-EN-319-401	§6.3 Asset management – Soportes	NC	Media	
REQ-401-6.4-A	ETSI-EN-319-401	§6.4 Access control – Política	NC	Media	
REQ-401-6.4-B	ETSI-EN-319-401	§6.4 Access control – Identificación y autenticación	NC	Alta	MFA
REQ-401-6.4-C	ETSI-EN-319-401	§6.4 Access control – Gestión de privilegios	NC	Media	
REQ-401-6.4-D	ETSI-EN-319-401	§6.4 Access control – Registro de accesos	NC	Alta	
REQ-401-6.5-A	ETSI-EN-319-401	§6.5 Cryptographic controls – Política	NC	Alta	
REQ-401-6.5-B	ETSI-EN-319-401	§6.5 Cryptographic controls – Ciclo de vida de claves	NC	Alta	
REQ-401-6.5-C	ETSI-EN-319-401	§6.5 Cryptographic controls – HSM	NC	Alta	
REQ-401-6.5-D	ETSI-EN-319-401	§6.5 Cryptographic controls – Doble control	NC	Alta	
REQ-401-6.6-A	ETSI-EN-319-401	§6.6 Physical security – Perímetro	NC	Baja	
REQ-401-6.6-B	ETSI-EN-319-401	§6.6 Physical security – Controles de acceso físico	NC	Baja	
REQ-401-6.6-C	ETSI-EN-319-401	§6.6 Physical security – Protecciones ambientales	NC	Baja	
REQ-401-6.7-A	ETSI-EN-319-401	§6.7 Operations – Procedimientos documentados	NC	Media	
REQ-401-6.7-B	ETSI-EN-319-401	§6.7 Operations – Gestión del cambio	NC	Media	
REQ-401-6.7-C	ETSI-EN-319-401	§6.7 Operations – Gestión de capacidad	NC	Media	
REQ-401-6.7-D	ETSI-EN-319-401	§6.7 Operations – Protección frente a malware	NC	Media	
REQ-401-6.7-E	ETSI-EN-319-401	§6.7 Operations – Backup y restauración	NC	Alta	

Código	Marco	Cláusula	Nivel	Crit.	Responsable
REQ-401-6.7-F	ETSI-EN-319-401	§6.7 Operations – Gestión de vulnerabilidades	NC	Alta	
REQ-401-6.8-A	ETSI-EN-319-401	§6.8 Network security – Segmentación	NC	Alta	
REQ-401-6.8-B	ETSI-EN-319-401	§6.8 Network security – Cifrado en tránsito	NC	Alta	
REQ-401-6.8-C	ETSI-EN-319-401	§6.8 Network security – Detección de intrusiones	NC	Alta	
REQ-401-6.9-A	ETSI-EN-319-401	§6.9 Incident management – Procedimiento	NC	Alta	
REQ-401-6.9-B	ETSI-EN-319-401	§6.9 Incident management – Notificación al supervisor	NC	Alta	
REQ-401-6.9-C	ETSI-EN-319-401	§6.9 Incident management – Lecciones aprendidas	NC	Media	
REQ-401-7-A	ETSI-EN-319-401	§7 TSPS – Existencia	NC	Alta	
REQ-401-7-B	ETSI-EN-319-401	§7 TSPS – Términos y condiciones	NC	Media	
REQ-401-7-C	ETSI-EN-319-401	§7 TSPS – Información a partes confiantes	NC	Media	
REQ-401-7-D	ETSI-EN-319-401	§7 TSPS – Política de servicio	NC	Alta	
REQ-401-SUB-A	ETSI-EN-319-401	§6 Subcontratación de funciones	NC	Alta	
REQ-401-SUB-B	ETSI-EN-319-401	§6 Subcontratación – Cloud	NC	Alta	
REQ-401-VULN-A	ETSI-EN-319-401	§ Gestión de vulnerabilidades públicas	NC	Media	
REQ-521-6.1-A	ETSI-EN-319-521	§6 Risk assessment – ERDS	NC	Alta	
REQ-521-7.1-A	ETSI-EN-319-521	§7.1 ERDS Practice Statement	NC	Alta	
REQ-521-7.1-B	ETSI-EN-319-521	§7.1 ERDS Disclosure Statement	NC	Media	
REQ-521-7.1-C	ETSI-EN-319-521	§7.1 Términos y condiciones del ERDS	NC	Media	
REQ-521-7.10-A	ETSI-EN-319-521	§7.10 Archivo de registros operativos del ERDS	NC	Media	
REQ-521-7.11-A	ETSI-EN-319-521	§7.11 Procedimiento de quejas y reclamaciones	NC	Media	
REQ-521-7.11-B	ETSI-EN-319-521	§7.11 Atención al cliente con SLA definido	NC	Media	
REQ-521-7.2-A	ETSI-EN-319-521	§7.2 Identificación del emisor – ERDS general	NC	Alta	
REQ-521-7.2-B	ETSI-EN-319-521	§7.2 Identificación cualificada del emisor – QERDS	NC	Alta	
REQ-521-7.3-A	ETSI-EN-319-521	§7.3 Identificación del destinatario – ERDS general	NC	Alta	
REQ-521-7.3-B	ETSI-EN-319-521	§7.3 Identificación cualificada del destinatario – QERDS	NC	Alta	
REQ-521-7.3-C	ETSI-EN-319-521	§7.3 Trato no discriminatorio de destinatarios	NC	Media	
REQ-521-7.4-A	ETSI-EN-319-521	§7.4 Integridad del contenido transmitido	NC	Alta	
REQ-521-7.4-B	ETSI-EN-319-521	§7.4 Confidencialidad del contenido	NC	Media	
REQ-521-7.4-C	ETSI-EN-319-521	§7.4 Detección de modificaciones verificable por terceros	NC	Alta	
REQ-521-7.5-A	ETSI-EN-319-521	§7.5 Catálogo de evidencias del servicio	NC	Alta	
REQ-521-7.5-B	ETSI-EN-319-521	§7.5 Firma cualificada de evidencias – QERDS	NC	Alta	
REQ-521-7.5-C	ETSI-EN-319-521	§7.5 Sellado de tiempo cualificado de evidencias	NC	Alta	
REQ-521-7.5-D	ETSI-EN-319-521	§7.5 Estructura semántica conforme EN 319 522-2	NC	Media	
REQ-521-7.5-E	ETSI-EN-319-521	§7.5 Formato técnico conforme EN 319 522-3	NC	Media	
REQ-521-7.6-A	ETSI-EN-319-521	§7.6 Validación de evidencias por terceros	NC	Media	
REQ-521-7.7-A	ETSI-EN-319-521	§7.7 Sellado de tiempo en todos los hitos del flujo	NC	Alta	
REQ-521-7.8-A	ETSI-EN-319-521	§7.8 Preservación a largo plazo de evidencias (LTV/LTA)	NC	Alta	
REQ-521-7.8-B	ETSI-EN-319-521	§7.8 Verificación periódica de integridad del archivo	NC	Alta	
REQ-521-7.9-A	ETSI-EN-319-521	§7.9 Plan de terminación específico ERDS	NC	Alta	
REQ-521-ACCEPT-A	ETSI-EN-319-521	Registro de aceptación expresa o tácita por el destinatario	NC	Alta	
REQ-521-FRAUD-A	ETSI-EN-319-521	Detección y prevención de fraude y suplantación de identidad	NC	Alta	
REQ-521-IMPL-A	ETSI-EN-319-521	Seguimiento de Reglamentos de Ejecución QERDS	NC	Alta	
REQ-521-INTEROP-A	ETSI-EN-319-521	eIDAS art. 44.2 – Interoperabilidad QERDS	NC	Media	
REQ-521-LEVELS-A	ETSI-EN-319-521	Declaración de niveles de servicio ERDS	NC	Media	

Código	Marco	Cláusula	Nivel	Crit.	Responsable
REQ-521-NOPICK-A	ETSI-EN-319-521	Gestión de no-recogida y expiración de plazo	NC	Media	
REQ-522-1-A	ETSI-EN-319-522	EN 319 522-1 – Arquitectura mapeada al modelo	NC	Media	del estándar
REQ-522-1-B	ETSI-EN-319-522	EN 319 522-1 – Roles del servicio identificados	NC	Media	
REQ-522-1-C	ETSI-EN-319-522	EN 319 522-1 – Modelo de prestación declarado	NC	Media	
REQ-522-1-D	ETSI-EN-319-522	EN 319 522-1 – Capability Document publicado	NC	Media	
REQ-522-2-A	ETSI-EN-319-522	EN 319 522-2 – Contenido semántico de cada tipo	NC	Media	de evidencia
REQ-522-2-B	ETSI-EN-319-522	EN 319 522-2 – Identificadores únicos (Message-ID,	NC	Media	Evidence-ID)
REQ-522-2-C	ETSI-EN-319-522	EN 319 522-2 – Marcas temporales semánticas	NC	Alta	completas
REQ-522-3-A	ETSI-EN-319-522	EN 319 522-3 – Evidencias en formato estándar	NC	Media	(XML/ASN.1)
REQ-522-3-B	ETSI-EN-319-522	EN 319 522-3 – Firmas de evidencias con perfiles	NC	Alta	AdES (XAdES, CAdES, PAdES)
REQ-522-3-C	ETSI-EN-319-522	EN 319 522-3 – Empaquetado estándar de conjuntos	NC	Media	de evidencias
REQ-522-4-A	ETSI-EN-319-522	EN 319 522-4 – Common Service Interface para	NC	Media	interoperabilidad
REQ-522-4-B	ETSI-EN-319-522	EN 319 522-4 – Binding REST conforme al estándar	NC	Media	
REQ-522-4-C	ETSI-EN-319-522	EN 319 522-4 – Binding REM para email certificado	NC	Baja	europeo
REQ-421-6-RA	ETSI-EN-319-421	§6 Risk assessment específico TSA	SC	Alta	
REQ-421-7.1-A	ETSI-EN-319-421	§7.1 TSA Practice Statement (TSPS)	NC	Alta	
REQ-421-7.1-B	ETSI-EN-319-421	§7.1 Time-Stamping Policy	NC	Alta	
REQ-421-7.1-C	ETSI-EN-319-421	§7.1 OID de la política en los tokens	NC	Alta	
REQ-421-7.1-D	ETSI-EN-319-421	§7.1 Disclosure Statement de la TSA	NC	Media	
REQ-421-7.2-A	ETSI-EN-319-421	§7.2 Generación de claves de la TSU	NC	Alta	
REQ-421-7.2-B	ETSI-EN-319-421	§7.2 Protección de la clave privada TSU en HSM	NC	Alta	certificado
REQ-421-7.2-C	ETSI-EN-319-421	§7.2 Certificado de la TSU emitido por CA cualificada	NC	Alta	
REQ-421-7.2-D	ETSI-EN-319-421	§7.2 Periodo de validez de la clave TSU y rotación	NC	Alta	
REQ-421-7.2-E	ETSI-EN-319-421	§7.2 Rekeying de la TSU sin interrupción del servicio	NC	Alta	
REQ-421-7.2-F	ETSI-EN-319-421	§7.2 Destrucción irreversible de la clave TSU al final del ciclo	NC	Alta	
REQ-421-7.2-G	ETSI-EN-319-421	§7.2 Plan de respuesta ante compromiso de clave TSU	NC	Alta	
REQ-421-7.3-A	ETSI-EN-319-421	§7.3 Emisión de tokens conforme EN 319 422 y RFC 3161	NC	Alta	
REQ-421-7.3-B	ETSI-EN-319-421	§7.3 Sincronización del reloj TSU con UTC (precisión ≤1 s)	NC	Alta	
REQ-421-7.3-C	ETSI-EN-319-421	§7.3 Parada automática ante desviación fuera de tolerancia	NC	Alta	
REQ-421-7.3-D	ETSI-EN-319-421	§7.3 Algoritmos de hash y firma en tokens conforme TS 119 312	NC	Alta	
REQ-421-7.3-E	ETSI-EN-319-421	§7.3 Re-firma de tokens para preservación a largo plazo	NC	Media	
REQ-421-7.4-A	ETSI-EN-319-421	§7.4 Calibración periódica del reloj TSU	NC	Alta	
REQ-421-7.5-A	ETSI-EN-319-421	§7.5 Endpoint de la TSA conforme RFC 3161	NC	Alta	
REQ-421-7.6-A	ETSI-EN-319-421	§7.6 SLA de disponibilidad declarado y medido	NC	Alta	
REQ-421-7.6-B	ETSI-EN-319-421	§7.6 Plan de continuidad específico TSA	NC	Alta	
REQ-421-7.6-C	ETSI-EN-319-421	§7.6 Registro de eventos de la TSA	SC	Alta	
REQ-421-7.7-A	ETSI-EN-319-421	§7.7 Roles específicos de la TSA con segregación	NC	Alta	
REQ-421-8-A	ETSI-EN-319-421	§8 Plan de terminación específico TSA	NC	Alta	
REQ-421-DECIDE	ETSI-EN-319-421	Decisión arquitectónica: TSA propia vs. externa	NC	Alta	
REQ-421-EXT-A	ETSI-EN-319-421	TSA externa – Verificación de cualificación en la OTL	NC	Alta	
REQ-421-EXT-B	ETSI-EN-319-421	TSA externa – Contrato con cláusulas específicas eIDAS	NC	Alta	
REQ-421-EXT-C	ETSI-EN-319-421	TSA externa – TSA secundaria como backup	NC	Alta	
REQ-422-A	ETSI-EN-319-422	§5 Perfil de la petición de sellado (TSA request)	NC	Alta	
REQ-422-B	ETSI-EN-319-422	§6 Perfil del token de sellado (TST Info)	NC	Alta	

Código	Marco	Cláusula	Nivel	Crit.	Responsable
REQ-422-C	ETSI-EN-319-422	§6 Algoritmos de hash en tokens	NC	SHA-256 mínimo	Alta
REQ-422-D	ETSI-EN-319-422	§6 Algoritmo de firma del token: RSA	NC	RSA-3072+ o ECDSA P-256+	Alta
REQ-422-E	ETSI-EN-319-422	§6 Campo policy (OID) en cada token	NC		Alta
REQ-422-F	ETSI-EN-319-422	§6 Campo accuracy: precisión del reloj declarada	NC		Media
REQ-422-G	ETSI-EN-319-422	§6 SerialNumber único e impredecible	NC		Alta
REQ-422-H	ETSI-EN-319-422	§6 Token encapsulado en CMS SignedData	NC	conforme al perfil	Alta
REQ-422-I	ETSI-EN-319-422	§6 Estrategia de validación a largo plazo (LTV)	NC		Media
REQ-422-J	ETSI-EN-319-422	RFC 3161 §3.4 – HTTP/HTTPS binding con Content-Types correctos	NC		Media
REQ-312-AES	ETSI-TS-119-312	Cifrado simétrico: AES-128/256 en modo autenticado (GCM/CCM)	NC		Media
REQ-312-DEPRECATION	ETSI-TS-119-312	Eliminación de algoritmos deprecados en todos los componentes	NC		Alta
REQ-312-ECDSA	ETSI-TS-119-312	ECDSA: curvas aceptables (P-256, P-384, P-521, Brainpool)	NC		Media
REQ-312-HASH	ETSI-TS-119-312	Algoritmos de hash: SHA-256 mínimo en toda la cadena	NC		Alta
REQ-312-INTEROP	ETSI-TS-119-312	Interoperabilidad criptográfica con herramientas de estándar	NC		Media
REQ-312-PERIOD	ETSI-TS-119-312	Periodos de validez de claves conforme tabla ETSI TS 119 312	NC		Alta
REQ-312-PQ	ETSI-TS-119-312	Preparación post-cuántica: evaluación de impacto	NC		Baja
REQ-312-RNG	ETSI-TS-119-312	Generación de aleatoriedad: CSPRNG validado o TRNG hardware	NC		Alta
REQ-312-RSA	ETSI-TS-119-312	RSA: longitud mínima de clave 3072 bits	NC		Alta
REQ-312-RSAPSS	ETSI-TS-119-312	RSA-PSS preferido sobre PKCS#1 v1.5 para nuevos despliegues	NC		Media
REQ-312-TLS	ETSI-TS-119-312	TLS 1.2/1.3 con suites seguras; SSL/TLS 1.0/1.1 desactivados	SC		Alta
REQ-312-TRANSITION	ETSI-TS-119-312	Plan de transición criptográfica (crypto-agility)	NC		Media
REQ-403-AUD-A	ETSI-EN-319-403	Auditoría in situ: acceso al personal, sistemas y operaciones	NC		Alta
REQ-403-AUD-B	ETSI-EN-319-403	Cobertura completa de cláusulas aplicables	NC		Alta
REQ-403-AUD-C	ETSI-EN-319-403	Verificación técnica de la implementación criptográfica	NC		Alta
REQ-403-CAB-A	ETSI-EN-319-403	Selección del CAB: acreditado por ENAC con alcance adecuado	NC		Alta
REQ-403-CAB-B	ETSI-EN-319-403	Independencia y competencia del equipo auditor	NC		Alta
REQ-403-CAR-A	ETSI-EN-319-403	Emisión del CAR: documento formal firmado por el CAB	NC		Alta
REQ-403-CAR-B	ETSI-EN-319-403	Vigencia del CAR: renovación bienal planificada	NC		Media
REQ-403-CONFIDENTIAL	ETSI-EN-319-403	NDA específico con el CAB para proteger información sensible	NC		Alta
REQ-403-COST-A	ETSI-EN-319-403	Provisión presupuestaria recurrente para auditorías bienales	NC		Media
REQ-403-FIND-A	ETSI-EN-319-403	Clasificación y gestión de hallazgos de la auditoría	NC		Alta
REQ-403-FIND-B	ETSI-EN-319-403	Cierre de todas las NC mayores antes del CAR positivo	NC		Alta
REQ-403-INCID-A	ETSI-EN-319-403	Disposición para auditorías ad-hoc del supervisor	NC		Media
REQ-403-PREP-A	ETSI-EN-319-403	Preparación: paquete documental previo a la auditoría	NC		Alta
REQ-403-PREP-B	ETSI-EN-319-403	Pre-auditoría interna o asistida antes de la auditoría CAR	NC		Media
REQ-403-SUPER-A	ETSI-EN-319-403	Entrega del CAR al supervisor en ≤ 3 días hábiles	NC		Alta
REQ-L6-10-1	LEY-6-2020	Art. 10.1 – SGSI apropiado y retención mínima de 5 años	NC		Media
REQ-L6-10-2	LEY-6-2020	Art. 10.2 – Información precontractual al usuario	NC		Media
REQ-L6-11-1	LEY-6-2020	Art. 11.1 – Solvencia técnica y financiera del PSC	NC		Alta
REQ-L6-11-2	LEY-6-2020	Art. 11.2 – Seguro de responsabilidad civil mínimo 1.500.000 €	NC		Alta
REQ-L6-12-1	LEY-6-2020	Art. 12.1 – Notificación previa al cese del servicio cualificado	NC		Alta
REQ-L6-12-2	LEY-6-2020	Art. 12.2 – Notificación de cambios sustanciales al servicio	NC		Media
REQ-L6-13-1	LEY-6-2020	Art. 13.1 – Notificación del cese con 2 meses de antelación	NC		Alta
REQ-L6-13-2	LEY-6-2020	Art. 13.2 – Custodia post-cese mínimo 15 años (servicio cualificado)	NC		Alta
REQ-L6-15	LEY-6-2020	Art. 15 – Auditoría por CAB acreditado por ENAC	NC		Alta

Código	Marco	Cláusula	Nivel	Crit.	Responsable
REQ-L6-19	LEY-6-2020	Art. 19 – Procedimiento de identificación remota conforme normativa	NC	Alta	
REQ-L6-21	LEY-6-2020	Art. 21 – Cooperación con inspecciones del supervisor	NC	Media	
REQ-L6-23	LEY-6-2020	Art. 23 – Infracciones muy graves (sanción hasta 1.500.000 €)	NC	Alta	
REQ-L6-24	LEY-6-2020	Art. 24 – Infracciones graves (sanción 30.001 a 500.000 €)	NC	Alta	
REQ-L6-25	LEY-6-2020	Art. 25 – Infracciones leves (sanción hasta 30.000 €)	NC	Baja	
REQ-L6-3	LEY-6-2020	Art. 3 – Régimen jurídico integrado eIDAS + Ley 6/2020	NC	Baja	
REQ-L6-7-1	LEY-6-2020	Art. 7.1 – Vídeo-identificación conforme a normativa española	NC	Alta	
REQ-L6-7-2	LEY-6-2020	Art. 7.2 – Métodos alternativos de identificación equivalentes	NC	Media	
REQ-L6-9	LEY-6-2020	Art. 9 – Responsabilidad del prestador	NC	Media	
REQ-L6-DA	LEY-6-2020	Disposición Adicional – Coordinación con AAPP autonómicas y locales	NC	Baja	
REQ-L6-DT	LEY-6-2020	Disposiciones Transitorias – Adaptación de servicios pre-existentes	NC	Baja	
REQ-ENS-AUDIT	ENS-ALTA	Certificación ENS ALTA bienal por entidad certificadora habilitada	NC	Alta	
REQ-ENS-mp.com	ENS-ALTA	mp.com.* Comunicaciones cifradas y redes segmentadas	NC	Alta	
REQ-ENS-mp.info	ENS-ALTA	mp.info.* Controles sobre la información del servicio cualificado	NC	Alta	
REQ-ENS-mp.s	ENS-ALTA	mp.s.* Protección DDoS, WAF y alta disponibilidad del servicio	NC	Alta	
REQ-ENS-op.acc	ENS-ALTA	op.acc.1-7 Control de acceso con MFA (obligatorio en ALTA)	NC	Alta	
REQ-ENS-op.cont	ENS-ALTA	op.cont.1-4 BCP/DRP con pruebas anuales reales (no solo de mesa)	NC	Alta	
REQ-ENS-op.exp.10	ENS-ALTA	op.exp.10 Protección de registros frente a alteración	NC	Alta	
REQ-ENS-op.exp.11	ENS-ALTA	op.exp.11 Gestión segura del ciclo de vida de claves criptográficas	NC	Alta	
REQ-ENS-op.exp.7	ENS-ALTA	op.exp.7 Gestión de incidentes adaptada a plazos eIDAS (24h)	NC	Alta	
REQ-ENS-op.exp.8	ENS-ALTA	op.exp.8 Logs de actividad en SIEM con retención e integridad	NC	Alta	
REQ-ENS-op.ext	ENS-ALTA	op.ext.* Gestión de proveedores externos críticos	NC	Alta	
REQ-ENS-op.mon	ENS-ALTA	op.mon.1-3 Monitorización 24/7 con SIEM/IDS/IPS	NC	Alta	
REQ-ENS-op.pl.1	ENS-ALTA	op.pl.1 Análisis de riesgos con metodología reconocida	NC	Alta	
REQ-ENS-op.pl.2	ENS-ALTA	op.pl.2 Arquitectura de seguridad documentada	NC	Media	
REQ-ENS-op.pl.5	ENS-ALTA	op.pl.5 Uso preferente de componentes certificados	NC	Alta	
REQ-ENS-org.1	ENS-ALTA	org.1 Política de seguridad aprobada y comunicada	NC	Baja	
REQ-ENS-org.2	ENS-ALTA	org.2 Normativa de seguridad: cuerpo normativo vinculante	NC	Baja	
REQ-GDPR-12-22	RGPD-LOPDGDD	Arts. 12-22 RGPD – Derechos de los interesados	NC	Media	
REQ-GDPR-13-14	RGPD-LOPDGDD	Arts. 13/14 RGPD – Información al interesado (política de privacidad)	NC	Media	
REQ-GDPR-25	RGPD-LOPDGDD	Art. 25 RGPD – Privacidad desde el diseño y por defecto	NC	Media	
REQ-GDPR-28	RGPD-LOPDGDD	Art. 28 RGPD – Contratos de encargo con todos los subprocesadores	NC	Alta	
REQ-GDPR-30	RGPD-LOPDGDD	Art. 30 RGPD – Registro de actividades de tratamiento (RAT)	NC	Media	
REQ-GDPR-33	RGPD-LOPDGDD	Art. 33 RGPD – Notificación de violaciones a la AEPD en ≤72 horas	NC	Media	
REQ-GDPR-35	RGPD-LOPDGDD	Art. 35 RGPD – Evaluación de impacto en protección de datos (EIPD/DPIA)	NC	Media	
REQ-GDPR-37	RGPD-LOPDGDD	Art. 37 RGPD – Delegado de Protección de Datos (DPD) designado	NC	Baja	
REQ-GDPR-5	RGPD-LOPDGDD	Art. 5 RGPD – Siete principios del tratamiento	NC	Media	
REQ-GDPR-6	RGPD-LOPDGDD	Art. 6 RGPD – Base jurídica para cada tratamiento	NC	Media	
REQ-LOPDGDD-31	RGPD-LOPDGDD	LOPDGDD Art. 31 – Bloqueo de datos al finalizar la relación	NC	Media	
REQ-LOPDGDD-77	RGPD-LOPDGDD	LOPDGDD Art. 77 – Régimen sancionador especial para AAPP	NC	Baja	
REQ-ISO27K-10	ISO-IEC-27001	§10 Mejora continua y gestión de no conformidades	NC	Media	
REQ-ISO27K-4	ISO-IEC-27001	§4 Contexto de la organización y alcance del SGSI	NC	Media	
REQ-ISO27K-5	ISO-IEC-27001	§5 Liderazgo y compromiso de la alta dirección	NC	Baja	
REQ-ISO27K-6	ISO-IEC-27001	§6 Planificación: análisis de riesgos y objetivos del SGSI	NC	Media	

Código	Marco	Cláusula	Nivel	Crit.	Responsable
REQ-ISO27K-8	ISO-IEC-27001	§8 Operación: ejecución del plan y gestión de cambios	NC	Media	
REQ-ISO27K-9	ISO-IEC-27001	§9 Evaluación: auditoría interna y revisión por la dirección	NC	Media	
REQ-ISO27K-A5	ISO-IEC-27001	Anexo A §5 – Controles organizativos implementados	NC	Alta	
REQ-ISO27K-A8	ISO-IEC-27001	Anexo A §8 – Controles tecnológicos implementados	NC	Alta	
REQ-ISO27K-CERT	ISO-IEC-27001	Certificación ISO 27001 vigente con alcance que cubra QERDS/TSA	NC	Baja	
REQ-HSM-2016-650	HSM-CERT	Listado QSCD conforme Reglamento (UE) 2016/650	NC	Alta	
REQ-HSM-CC	HSM-CERT	Common Criteria EAL4+ con Protection Profile aplicable	NC	Alta	
REQ-HSM-CONFIG	HSM-CERT	Operación del HSM en modo certificado (FIPS mode activado)	NC	Alta	
REQ-HSM-FIPS	HSM-CERT	FIPS 140-2 Nivel 3 / FIPS 140-3 como certificación mínima del HSM	NC	Alta	
REQ-HSM-FIRMWARE	HSM-CERT	Gestión del firmware del HSM dentro del alcance certificado	NC	Alta	
REQ-HSM-LIFECYCLE	HSM-CERT	Mantenimiento de las certificaciones del HSM durante el servicio	NC	Alta	