logalty

LOGALTY PRUEBA POR INTERPOSICION SL

Firmado digitalmente por LOGALTY PRUEBA POR INTERPOSICION SL
Fecha: 2024.07.22 12:03:38 +02'00'

logalty Prueba Electrónica Efectiva

Declaración de Prácticas de Confianza

Servicio de sellado de tiempo electrónico

Versión 2.4

eIDAS | QCert for ESig | QCert for ESeal | QWAC | QTimestamp | QeRDS | eDelivery

INFORMACIÓN GENERAL

Líder	Área de servicios de confianza
Tipo	**Política** Normativa Plan Procedimiento Guía Reporte de Auditoría
Distribución	**Público** Restringido Confidencial Uso Interno Confidencial
Fecha	22/07/2024
Descripción	Declaración de Prácticas de Confianza Servicio de sellado de tiempo electrónico
Aprobado	CRS
Estado	Iniciado Borrador en curso Borrador para comentarios Borrador final para aprobación Aprobado **Publicado** Retirado

1 INTRODUCCIÓN 14

1.1 PRESENTACIÓN 14
1.2 NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN 14
1.2.1 IDENTIFICADORES DE CERTIFICADOS 14
1.3 PARTICIPANTES EN LOS SERVICIOS DE CERTIFICACIÓN 14
1.3.1 PRESTADOR DE SERVICIOS DE CERTIFICACIÓN 14
1.3.1.1 Logalty CA ROOT 03 15
1.3.1.2 Logalty Qualified CA G2 16
1.3.1.3 Logalty CA G2 16
1.3.2 REGISTRADORES / AUTORIDAD DE REGISTRO 17
1.3.3 ENTIDADES FINALES 17
1.3.3.1 Suscriptores del servicio de certificación 17
1.3.3.2 Creadores de sellos 18
1.3.4 PARTES USUARIAS 18
1.3.5 OTROS PARTICIPANTES 18
1.4 USO DE LOS CERTIFICADOS 18
1.4.1 USOS PERMITIDOS PARA LOS CERTIFICADOS 18
1.4.1.1 Certificado cualificado de Sello electrónico de TSA/TSU 19
1.4.2 LÍMITES Y PROHIBICIONES DE USO DE LOS CERTIFICADOS 20
1.4.3 EMISIÓN DE CERTIFICADOS DE PRUEBAS 21
1.5 ADMINISTRACIÓN DE LA DECLARACIÓN DE PRÁCTICAS DE CONFIANZA 21
1.5.1 ORGANIZACIÓN QUE ADMINISTRA EL DOCUMENTO 21
1.5.2 DATOS DE CONTACTO DE LA ORGANIZACIÓN 22
1.5.3 PROCEDIMIENTOS DE GESTIÓN DEL DOCUMENTO 22
1.5.3.1 Revisión del documento 23
1.5.4 APROBACIÓN DEL DOCUMENTO 23
1.6 DEFINICIONES Y ACRÓNIMOS 23
1.6.1 DEFINICIONES 24
1.6.2 ACRÓNIMOS 26

2 PUBLICACIÓN DE INFORMACIÓN Y DEPÓSITO DE CERTIFICADOS 28

2.1 DEPÓSITO(S) DE CERTIFICADOS 28
2.2 PUBLICACIÓN DE INFORMACIÓN DEL PRESTADOR DE SERVICIOS DE CERTIFICACIÓN 28
2.2.1 TÉRMINOS Y CONDICIONES 28
2.3 FRECUENCIA DE PUBLICACIÓN 29
2.4 CONTROL DE ACCESO 29

3 IDENTIFICACIÓN Y AUTENTICACIÓN 29

3.1 REGISTRO DE NOMBRES 29
3.1.1 TIPOS DE NOMBRES 29
3.1.2 SIGNIFICADO DE LOS NOMBRES 30
3.1.3 EMPLEO DE ANÓNIMOS Y SEUDÓNIMOS 30
3.1.4 INTERPRETACIÓN DE FORMATOS DE NOMBRES 30

3.1.5 UNICIDAD DE LOS NOMBRES 31
3.1.6 RESOLUCIÓN DE CONFLICTOS RELATIVOS A NOMBRES 31
3.1.7 AUTENTICACIÓN DE LA IDENTIDAD DE UNA PERSONA FÍSICA 32
3.2 VALIDACIÓN INICIAL DE LA IDENTIDAD 32
3.2.1 PRUEBA DE POSESIÓN DE CLAVE PRIVADA 32
3.2.2 AUTENTICACIÓN DE LA IDENTIDAD DE UNA ORGANIZACIÓN, EMPRESA O ENTIDAD MEDIANTE REPRESENTANTE 32
3.2.2.1 Identidad 32
3.2.3 AUTENTICACIÓN DE LA IDENTIDAD DE UNA PERSONA FÍSICA 34
3.2.4 INFORMACIÓN DE SUSCRIPTOR NO VERIFICADA 34
3.2.5 AUTENTICACIÓN DE LAS AUTORIDADES DE REGISTRO 34
3.2.6 CRITERIOS DE INTEROPERACIÓN 34
3.3 IDENTIFICACIÓN Y AUTENTICACIÓN DE SOLICITUDES DE RENOVACIÓN 34
3.4 IDENTIFICACIÓN Y AUTENTICACIÓN DE LA SOLICITUD DE REVOCACIÓN 35

4 REQUISITOS DE OPERACIÓN DEL CICLO DE VIDA DE LOS CERTIFICADOS 35

4.1 SOLICITUD DE CERTIFICADO 35
4.1.1 LEGITIMACIÓN PARA SOLICITAR LA EMISIÓN 35
4.1.2 PROCEDIMIENTO DE ALTA Y RESPONSABILIDADES 36
4.2 PROCESAMIENTO DE LA SOLICITUD DE CERTIFICADO 36
4.2.1 EJECUCIÓN DE LAS FUNCIONES DE IDENTIFICACIÓN Y AUTENTICACIÓN 36
4.2.2 APROBACIÓN O RECHAZO DE LA SOLICITUD 37
4.2.3 PLAZO PARA RESOLVER LA SOLICITUD 37
4.3 EMISIÓN DEL CERTIFICADO 37
4.3.1 ACCIONES DE LOGALTY DURANTE EL PROCESO DE EMISIÓN 37
4.3.2 NOTIFICACIÓN DE LA EMISIÓN AL SUSCRIPTOR 38
4.4 ACEPTACIÓN DEL CERTIFICADO 38
4.4.1 PROCEDIMIENTO DE LA ACEPTACIÓN 38
4.4.1.1 Conducta que constituye aceptación del certificado 40
4.4.2 PUBLICACIÓN DEL CERTIFICADO 40
4.4.3 NOTIFICACIÓN DE LA EMISIÓN A TERCEROS 40
4.5 USO DEL PAR DE CLAVES Y DEL CERTIFICADO 40
4.5.1 USO POR EL SUSCRIPTOR 40
4.5.1.1 Obligaciones del suscriptor del certificado 40
4.5.1.2 Responsabilidad civil del suscriptor del certificado 41
4.5.2 USO POR EL TERCERO QUE CONFÍA EN CERTIFICADOS 42
4.5.2.1 Obligaciones del tercero que confía en certificados 42
4.5.2.2 Responsabilidad civil del tercero que confía en certificados 43
4.6 RENOVACIÓN DE CERTIFICADOS SIN CAMBIO DE CLAVES 43
4.7 RENOVACIÓN DE CERTIFICADOS CON CAMBIO DE CLAVES 43
4.8 MODIFICACIÓN DE CERTIFICADOS 43
4.9 REVOCACIÓN DE CERTIFICADOS 43
4.9.1 CAUSAS DE REVOCACIÓN DE CERTIFICADOS 43
4.9.2 LEGITIMACIÓN PARA SOLICITAR LA REVOCACIÓN 45
4.9.3 PROCEDIMIENTOS DE SOLICITUD DE REVOCACIÓN 45
4.9.3.1 En general 45
4.9.4 PLAZO TEMPORAL DE SOLICITUD DE REVOCACIÓN 46
4.9.5 PLAZO TEMPORAL DE PROCESAMIENTO DE LA SOLICITUD 46
4.9.6 OBLIGACIÓN DE CONSULTA DE INFORMACIÓN DE REVOCACIÓN DE CERTIFICADOS 46

4.9.7 Frecuencia de emisión de listas de revocación de certificados (LRCs) 47
4.9.8 Plazo máximo de publicación de LRCs 47
4.9.9 Disponibilidad de servicios de comprobación en línea de estado de certificados 47
4.9.10 Obligación de consulta de servicios de comprobación de estado de certificados 48
4.9.11 Requisitos especiales en caso de compromiso de la clave privada 48
4.9.12 Causas de suspensión de certificados 49
4.9.13 Solicitud de suspensión 49
4.9.14 Procedimientos para la petición de suspensión 49
4.9.15 Período máximo de suspensión 49
4.10 Servicios de comprobación de estado de certificados 49
4.10.1 Características operativas de los servicios 49
4.10.2 Disponibilidad de los servicios 49
4.10.3 Características opcionales 50
4.11 Finalización de la suscripción 50
4.12 Depósito y recuperación de claves 50
4.12.1 Política y prácticas de depósito y recuperación de claves 50
4.12.2 Política y prácticas de encapsulado y recuperación de claves de sesión 50

5 CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES 50

5.1 Controles de seguridad física 50
5.1.1 Localización y construcción de las instalaciones 51
5.1.2 Acceso físico 52
5.1.3 Electricidad y aire acondicionado 53
5.1.4 Exposición al agua 53
5.1.5 Prevención y protección de incendios 53
5.1.6 Almacenamiento de soportes 53
5.1.7 Tratamiento de residuos 54
5.1.8 Copia de respaldo fuera de las instalaciones 54
5.2 Controles de procedimientos 54
5.2.1 Funciones fiables 54
5.2.2 Número de personas por tarea 56
5.2.3 Identificación y autenticación para cada función 56
5.2.4 Roles que requieren separación de tareas 56
5.3 Controles de personal 56
5.3.1 Requisitos de historial, calificaciones, experiencia y autorización 56
5.3.2 Procedimientos de investigación de historial 57
5.3.3 Requisitos de formación 58
5.3.4 Requisitos y frecuencia de actualización formativa 58
5.3.5 Secuencia y frecuencia de rotación laboral 59
5.3.6 Sanciones para acciones no autorizadas 59
5.3.7 Requisitos de contratación de profesionales 59
5.3.8 Suministro de documentación al personal 60
5.4 Procedimientos de auditoría de seguridad 60
5.4.1 Tipos de eventos registrados 60
5.4.2 Frecuencia de tratamiento de registros de auditoría 62
5.4.3 Período de conservación de registros de auditoría 62
5.4.4 Protección de los registros de auditoría 62
5.4.5 Procedimientos de copia de respaldo 63

5.4.6 Localización del sistema de acumulación de registros de auditoría 63
5.4.7 Notificación del evento de auditoría al causante del evento 63
5.4.8 Análisis de vulnerabilidades 63
5.5 Archivos de informaciones 64
5.5.1 Tipos de registros archivados 64
5.5.2 Período de conservación de registros 65
5.5.3 Protección del archivo 65
5.5.4 Procedimientos de copia de respaldo 66
5.5.5 Requisitos de sellado de fecha y hora 66
5.5.6 Localización del sistema de archivo 66
5.5.7 Procedimientos de obtención y verificación de información de archivo 66
5.6 Renovación de claves 66
5.7 Compromiso de claves y recuperación de desastre 67
5.7.1 Procedimientos de gestión de incidencias y compromisos 67
5.7.2 Corrupción de recursos, aplicaciones o datos 67
5.7.3 Compromiso de la clave privada de la entidad 67
5.7.4 Continuidad del negocio después de un desastre 68
5.8 Terminación del servicio 69

6 CONTROLES DE SEGURIDAD TÉCNICA 70

6.1 Generación e instalación del par de claves 70
6.1.1 Generación del par de claves 70
6.1.1.1 Generación del par de claves del firmante 71
6.1.2 Envío de la clave privada al firmante 71
6.1.3 Envío de la clave pública al emisor del certificado 71
6.1.4 Distribución de la clave pública del prestador de servicios de certificación 72
6.1.5 Tamaños de claves 72
6.1.6 Generación de parámetros de clave pública 72
6.1.7 Comprobación de calidad de parámetros de clave pública 72
6.1.8 Propósitos de uso de claves 72
6.2 Protección de la clave privada y controles de los módulos criptográficos 73
6.2.1 Estándares de módulos criptográficos 73
6.2.2 Control por más de una persona (n de m) sobre la clave privada 73
6.2.3 Depósito de la clave privada 73
6.2.4 Copia de respaldo de la clave privada 74
6.2.5 Archivo de la clave privada 74
6.2.6 Introducción de la clave privada en el módulo criptográfico 74
6.2.7 Almacenamiento de la clave privada en el módulo criptográfico 74
6.2.8 Método de activación de la clave privada 74
6.2.9 Método de desactivación de la clave privada 75
6.2.10 Método de destrucción de la clave privada 75
6.2.11 Clasificación de módulos criptográficos 75
6.3 Otros aspectos de gestión del par de claves 75
6.3.1 Archivo de la clave pública 75
6.3.2 Períodos de utilización de las claves pública y privada 76
6.4 Datos de activación 76
6.4.1 Generación e instalación de datos de activación 76
6.4.2 Protección de datos de activación 76

6.5 CONTROLES DE SEGURIDAD INFORMÁTICA 76
6.5.1 REQUISITOS TÉCNICOS ESPECÍFICOS DE SEGURIDAD INFORMÁTICA 77
6.5.2 EVALUACIÓN DEL NIVEL DE SEGURIDAD INFORMÁTICA 78
6.6 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA 78
6.6.1 CONTROLES DE DESARROLLO DE SISTEMAS 78
6.6.2 CONTROLES DE GESTIÓN DE SEGURIDAD 78
6.6.2.1 Clasificación y gestión de información y bienes 78
6.6.2.2 Operaciones de gestión 79
6.6.2.3 Tratamiento de los soportes y seguridad 79
6.6.2.4 Planificación del sistema 79
6.6.2.5 Reportes de incidencias y respuesta 79
6.6.2.6 Procedimientos operacionales y responsabilidades 80
6.6.2.7 Gestión del sistema de acceso 80
6.6.2.8 Generación del certificado 80
6.6.2.9 Gestión de la revocación 81
6.6.2.10 Estado de la revocación 81
6.6.2.11 Gestión del ciclo de vida del hardware criptográfico 81
6.7 CONTROLES DE SEGURIDAD DE RED 82
6.8 FUENTES DE TIEMPO 82

7 PERFILES DE CERTIFICADOS, CRL Y OCSP 82

7.1 PERFIL DE CERTIFICADO 82
7.1.1 NÚMERO DE VERSIÓN 82
7.1.2 EXTENSIONES DEL CERTIFICADO 82
7.1.3 IDENTIFICADORES DE OBJETO (OID) DE LOS ALGORITMOS 83
7.1.4 FORMATO DE NOMBRES 83
7.1.5 RESTRICCIÓN DE LOS NOMBRES 83
7.1.6 IDENTIFICADOR DE OBJETO (OID) DE LOS TIPOS DE CERTIFICADOS 84
7.1.7 USO DE LA EXTENSIÓN "POLICY CONSTRAINTS" 84
7.1.8 SINTAXIS Y SEMÁNTICA DE LOS CALIFICADORES DE POLÍTICA 84
7.1.9 TRATAMIENTO SEMÁNTICO PARA LA EXTENSIÓN CRÍTICA "CERTIFICATE POLICY" 84
7.2 PERFIL DE LA LISTA DE REVOCACIÓN DE CERTIFICADOS 84
7.3 PERFIL DE OCSP 84

8 AUDITORÍA DE CONFORMIDAD 84

8.1 FRECUENCIA DE LA AUDITORÍA DE CONFORMIDAD 85
8.2 IDENTIFICACIÓN Y CUALIFICACIÓN DEL AUDITOR 85
8.3 RELACIÓN DEL AUDITOR CON LA ENTIDAD AUDITADA 86
8.4 LISTADO DE ELEMENTOS OBJETO DE AUDITORÍA 86
8.5 ACCIONES QUE EMPRENDER COMO RESULTADO DE UNA FALTA DE CONFORMIDAD 87
8.6 TRATAMIENTO DE LOS INFORMES DE AUDITORÍA 87

9 REQUISITOS COMERCIALES Y LEGALES 87

9.1 TARIFAS 87

9.1.1 TARIFA DE EMISIÓN O RENOVACIÓN DE CERTIFICADOS 87
9.1.2 TARIFA DE ACCESO A CERTIFICADOS 88
9.1.3 TARIFA DE ACCESO A INFORMACIÓN DE ESTADO DE CERTIFICADO 88
9.1.4 TARIFAS DE OTROS SERVICIOS 88
9.1.5 POLÍTICA DE REINTEGRO 88
9.2 RESPONSABILIDAD FINANCIERA 88
9.2.1 COBERTURA DE SEGURO 88
9.2.2 OTROS ACTIVOS 89
9.2.3 COBERTURA DE SEGURO PARA SUSCRIPTORES Y TERCEROS QUE CONFÍAN EN CERTIFICADOS 89
9.3 CONFIDENCIALIDAD DE LA INFORMACIÓN 89
9.3.1 INFORMACIONES CONFIDENCIALES 89
9.3.2 INFORMACIONES NO CONFIDENCIALES 90
9.3.3 DIVULGACIÓN DE INFORMACIÓN DE REVOCACIÓN 91
9.3.4 DIVULGACIÓN LEGAL DE INFORMACIÓN 91
9.3.5 DIVULGACIÓN DE INFORMACIÓN POR PETICIÓN DE SU TITULAR 91
9.3.6 OTRAS CIRCUNSTANCIAS DE DIVULGACIÓN DE INFORMACIÓN 91
9.4 PROTECCIÓN DE LA INFORMACIÓN PERSONAL 91
9.5 DERECHOS DE PROPIEDAD INTELECTUAL 92
9.5.1 PROPIEDAD DE LOS CERTIFICADOS E INFORMACIÓN DE REVOCACIÓN 93
9.5.2 PROPIEDAD DE LA DECLARACIÓN DE PRÁCTICAS DE CONFIANZA 93
9.5.3 PROPIEDAD DE LA INFORMACIÓN RELATIVA A NOMBRES 93
9.5.4 PROPIEDAD DE CLAVES 93
9.6 OBLIGACIONES Y RESPONSABILIDAD CIVIL 94
9.6.1 OBLIGACIONES DE LA ENTIDAD DE CERTIFICACIÓN DE LOGALTY 94
9.6.2 GARANTÍAS OFRECIDAS A SUSCRIPTORES Y TERCEROS QUE CONFÍAN EN CERTIFICADOS 95
9.7 EXENCIÓN DE GARANTÍA 96
9.8 LIMITACIONES DE RESPONSABILIDAD 97
9.8.1 RESPONSABILIDADES DE LA AUTORIDAD DE CERTIFICACIÓN 97
9.8.2 RESPONSABILIDADES DE LA AUTORIDAD DE REGISTRO 98
9.8.3 RESPONSABILIDADES DEL SUSCRIPTOR 98
9.8.4 DELIMITACIÓN DE RESPONSABILIDADES 98
9.8.5 CLÁUSULA DE INDEMNIDAD DE SUSCRIPTOR 100
9.8.6 CLÁUSULA DE INDEMNIDAD DE TERCERO QUE CONFÍA EN EL CERTIFICADO 100
9.8.7 CASO FORTUITO Y FUERZA MAYOR 101
9.9 INDEMNIZACIONES 101
9.9.1 ALCANCE DE LA COBERTURA 101
9.9.2 LIMITACIONES DE PÉRDIDAS 101
9.10 PERÍODO DE VALIDEZ 101
9.10.1 PLAZO 101
9.10.2 SUSTITUCIÓN Y DEROGACIÓN DE LA DPC 102
9.10.3 EFECTOS DE LA FINALIZACIÓN 102
9.11 NOTIFICACIONES INDIVIDUALES Y COMUNICACIONES CON LOS PARTICIPANTES 102
9.12 ENMIENDAS 102
9.12.1 PROCEDIMIENTO PARA LOS CAMBIOS 102
9.12.1.1 Elementos que pueden cambiar sin necesidad de notificación 102
9.12.1.2 Cambios con notificación 102
9.12.1.3 Mecanismo de notificación 103
9.12.2 PERIODO Y PROCEDIMIENTO DE NOTIFICACIÓN 103
9.12.3 CIRCUNSTANCIAS EN LAS QUE EL OID DEBE SER CAMBIADO 103

9.13 RECLAMACIONES Y RESOLUCIÓN DE CONFLICTOS 104
9.14 NORMATIVA APLICABLE 104
9.15 CUMPLIMIENTO DE LA NORMATIVA APLICABLE 104
9.16 OTRAS DISPOSICIONES 105
9.16.1 CLÁUSULAS DE DIVISIBILIDAD, SUPERVIVENCIA, ACUERDO ÍNTEGRO Y NOTIFICACIÓN 105
9.17 OTRAS PROVISIONES 105

CONTROL DE VERSIONES

VERSIÓN	PARTES CAMBIADAS	DESCRIPCIÓN CAMBIO	AUTOR	FECHA
1.0	Todo	Creación del documento	ASTREA/DG	03/04/2018
1.1		Revisión RGPD Revisión después CAR 2018	ASTREA	22/10/2018
1.2	1.5	Cambio denominación social	DG	23/10/2018
1.3	1.6	Cambio ubicación apartados de definiciones y acrónimos para adecuación a RFC 3647	ASTREA	02/04/2019
		Incorporación referencias LOPGDD	ASTREA	03/04/2019
	1.2.1; 1.4.1.9; 1.4.1.11; 3.2.2; 4.3.2.2; 4.8.1; 4.8.2; 4.8.3.2; 9.6.1	Inclusión tipos de certificados para servicios PSD2	ASTREA	08/04/2019
1.4	1.2.1; 1.3.1; 1.4.1	Inclusión nuevos tipos de certificados con política OVCP	ASTREA-AC	08/05/2019
	3.5; 4.8	Se elimina el contenido de los apartados sobre suspensión de certificados	ASTREA-AC	08/05/2019
	Todo	Revisión para adecuación a RFC3647	ASTREA-AC	15/05/2019
	4.2	Creación subapartado para la validación de los registros CAA	ASTREA-AC	15/05/2019
	1.3	Prioridad de las Baseline Requirements	ASTREA-AC	15/05/2019
	1.4.1.1.11	Cambio OIDs para cert SSL PSD2	ASTREA-AC	21/05/2019
	3.2.4	Adaptación de aspectos en la validación de certificados de autenticación web	ASTREA-AC	22/05/2019
	2.2	Inclusión referencia a los Términos y condiciones	ASTREA-FA	23/05/2019

	8	Se amplía información sobre los servicios auditados y las normas usadas	ASTREA-AC	23/05/2019
	6.1.1	Modificación durabilidad de los certificados de entidad final	ASTREA-AC	23/05/2019
	1.3.3.1	Se incluye la excepción para emitir certificados al propio TSP	ASTREA-AC	23/05/2019
	1.4.1	Se incluye certificado de autenticación web con EV para PSD2	ASTREA-AC	04/06/2019
1.5	5.7.3	Resolución en caso de compromiso de la clave privada de la CA.	ASTREA	10/07/2019
	4.9.6	Revisión	ASTREA	10/07/2019
	1.2.1 1.4.1.9	Cambio por error en OID	ASTREA-AC	3/10/2019
		Cambio de plantilla	ASTREA-AC	17/02/2020
	1.5	Cambio denominación empresa	ASTREA-AC	20/02/2020
		Revisión diversos aspectos legales	ASTREA-FA	08/06/2020
	3.4; 4.4.1; 6.1.2; 6.2.7.2;	Modificación de la denominación de la plataforma de gestión de certificados	ASTREA-AC	09/06/2020
	3.2.7	Control del dominio	ASTREA-AC	29/06/2020
	4.9.11	Detalle adicional para alineación con el plan de cese del servicio	NA	30/06/2020
	4.11 y 6.2.7.2	Mejora de redacción. Eliminación de la emisión de oficio	NA	30/06/2020
	1.3.1.4	Detalle adicional sobre la plataforma y sus certificaciones	NA	30/06/2020
	5.4.8	Modificación del texto sobre gestión de vulnerabilidades	CO	30/06/2020
	5.7.3	Se incluye referencia a la actuación en caso de compromiso de la clave privada de la CA	CO	30/06/2020
	5.7.4	Se incluye referencia al SGCN	CO	30/06/2020

	5.8	Se modifica el texto del plan de cese de los servicios	CO	30/06/2020
1.6	3.2.2, 3.2.4	Modificación en el método de verificación del control del dominio.	ASTREA-AC	27/10/2020
	6.3.2	Indicación del periodo máximo de vigencia de los certificados de autenticación web	ASTREA-AC	27/10/2020
	1.2.1, 1.4.1	Inclusión de nuevos certificados de PF representante	ASTREA-AC	27/10/2020
	1.3.1.2	Modificación del certificado de la CA	ASTREA-AC	27/10/2020
	1.2.1, 1.4.1.10, 1.4.1.11	Se eliminan las referencias a CABforum como sus OIDs	ASTREA-AC	27/10/2020
	3.2.4, 3.3, 3.4, 4.8, 4.9.3.1	Modificaciones diversas	ASTREA-AC	12/11/2020
1.7	1.3.1, 1.3.2, 3.1.7.1, 4.9.3.2, 5.3.2, 5.7.3, 9.2.1, 9.2.3, 9.4, 9.8.1, 9.14, 9.15	Adaptación a Ley 6/2020	ASTREA-FA	09/04/2021
2.0	4.9.7, 6.1.7	Cambios menores o error formato	ASTREA-AC	29/03/2022
	3.2.3.1	Legitimación notarial de las solicitudes	ASTREA-AC	29/03/2022
	3.2.3, 3.2.3.1, 3.2.3.3, 9.4	Inclusión de la video-identificación	ASTREA-AC	28/04/2022
	6.1.6, 7.1.4	Indicación respecto al tamaño de ciertos campos del certificado	ASTREA-AC	29/04/2022
	1.3.3.1	Revisión	ASTREA-AC	10/05/2022
	1.5.3.1	Revisión del apartado	CO	13/05/2022
	9.4	Ampliación del apartado	ASTREA-FA	16/05/2022
2.1	4.5.3	Revisión	ASTREA-AC	26/05/2022
2.2	1.2.1 / 1.3 / 1.4.1 / 3.1 / 3.2.2 / 3.2.3 / 3.2.4 / 4.1.2 / 4.5.1 / 5.2.1 / 6.1.1 / 7.1.3 / 9.2	Eliminación de tipos de certificados y otras revisiones menores.	ASTREA-AC	08/05/2023
2.3	1.2.1 / 6.1.3 / 5.8	Revisión	ASTREA-AC	16/05/2023
	6.2.4 / 6.8	Ampliación tras auditoría	ASTREA-AC	19/06/2023

2.4		Eliminación de algunos servicios de confianza.	ASTREA-AC	14/02/2024

1 Introducción

1.1 Presentación

Este documento declara las prácticas de confianza de los servicios de sellado de tiempo electrónico de la Autoridad de Certificación de LOGALTY.

Los tipos de certificados que se emiten son los siguientes:

- De Servicio de sellado de tiempo electrónico, para la expedición de sellos de tiempo electrónico

1.2 Nombre del documento e identificación

Este documento es la "Declaración de Prácticas de Confianza de LOGALTY para los servicios de sellado de tiempo electrónico".

1.2.1 Identificadores de certificados

Logalty ha asignado a cada política de certificado un identificador de objeto (OID), para su identificación por las aplicaciones.

OID	Tipos de certificados CUALIFICADOS
1.3.6.1.4.1.30210.1.5.1	De Sello electrónico de TSA

En caso de contradicción entre esta Declaración de Prácticas de Confianza y otros documentos de prácticas y procedimientos, prevalecerá lo establecido en esta Declaración de Prácticas.

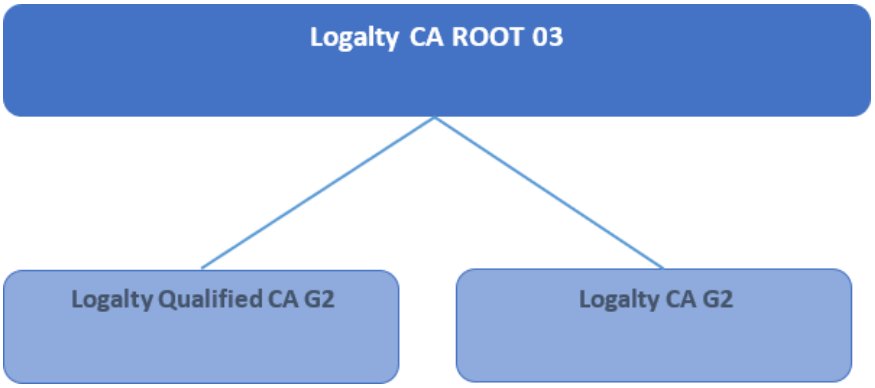
1.3 Participantes en los servicios de certificación

1.3.1 Prestador de servicios de certificación

LOGALTY es un prestador de servicios de confianza, que actúa de acuerdo con lo dispuesto en el Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la

identificación electrónica y los servicios de confianza para la transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE, la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, y las normas técnicas del ETSI aplicables a los prestadores en general (ETSI EN 319 401), a los prestadores que expiden sellos de tiempo (ETSI EN 319 421), al objeto de facilitar el cumplimiento de los requisitos legales y el reconocimiento internacional de sus servicios.

Para la prestación de los servicios de certificación, LOGALTY ha establecido la siguiente jerarquía de entidades de certificación



1.3.1.1 Logalty CA ROOT 03

Se trata de la entidad de certificación raíz de la jerarquía que emite certificados a otras entidades de certificación, y cuyo certificado de clave pública ha sido autofirmado.

Datos de identificación:

CN:	Logalty CA ROOT 03
Huella digital:	5b39539340c50a9cb6f8bcf66a3e262c5f122f60
Válido desde:	6 de junio de 2018 12:17:11
Válido hasta:	6 de junio de 2043 12:17:11
Longitud de clave RSA:	4096 bits

1.3.1.2 Logalty Qualified CA G2

Se trata de la entidad de certificación dentro de la jerarquía que emite los certificados cualificados a las entidades finales, y cuyo certificado de clave pública ha sido firmado digitalmente por la Logalty CA ROOT 03.

Datos de identificación:

CN:	Logalty Qualified CA G2
Huella digital:	0141dc0253de6a83e6a5ea5d6d2254fa9d4a4fdb
Válido desde:	4 de septiembre de 2020 14:07:18
Válido hasta:	4 de septiembre de 2033 14:07:18
Longitud de clave RSA:	4096 bits

1.3.1.3 Logalty CA G2

Se trata de la entidad de certificación dentro de la jerarquía que emite los certificados no cualificados a las entidades finales, y cuyo certificado de clave pública ha sido firmado digitalmente por la Logalty CA ROOT 03.

Datos de identificación:

CN:	Logalty CA G2
Huella digital:	1f785827bb035a6d878731febf726a2f122b2801
Válido desde:	6 de junio de 2018 13:02:54
Válido hasta:	6 de junio de 2031 13:02:54
Longitud de clave RSA:	4096 bits

1.3.2 Registradores / Autoridad de Registro

En general, el prestador del servicio de certificación actúa como verificador de la identidad de los solicitantes y personas identificadas en los certificados.

Las funciones de registro de los suscriptores se realizan por delegación y de acuerdo con las instrucciones del prestador de servicios de certificación, en los términos del artículo 24.1 del Reglamento (UE) 910/2014, y del artículo 7 de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, y bajo la plena responsabilidad del prestador de servicios de confianza frente a terceros.

1.3.3 Entidades finales

Las entidades finales son las personas y organizaciones destinatarias de los servicios de emisión, gestión y uso de certificados digitales, para los usos de sellado de tiempo.

Serán entidades finales de los servicios de certificación de Logalty las siguientes:

- Suscriptores del servicio de certificación.
- Creadores de sellos.
- Partes que confían.

1.3.3.1 Suscriptores del servicio de certificación

Los suscriptores del servicio de certificación son:

- las empresas, entidades u organizaciones que los adquieren a LOGALTY para su uso en su ámbito corporativo empresarial u organizativo, y se encuentran identificados en los certificados,

En general y para evitar cualquier conflicto de intereses, el suscriptor y el prestador de servicios de

confianza serán entidades separadas. No obstante, lo anterior, se declara como excepción el caso de la emisión de certificados para la propia LOGALTY. Cuando se produce esta emisión para la misma LOGALTY la expedición del certificado seguirá un procedimiento, validando que la petición sea exclusivamente interna, solo para servicios o responsables de LOGALTY y que dichas expediciones estén adecuadamente autorizadas.

1.3.3.2 Creadores de sellos

Son las personas jurídicas que disponen de certificados y crean sellos de tiempo electrónicos a partir del uso de los citados certificados.

1.3.4 Partes usuarias

Las partes usuarias son las personas y las organizaciones que precisan confiar en los sellos de tiempo electrónicos.

Como paso previo a confiar en los certificados, las partes usuarias deben verificarse, como se establece en esta declaración de prácticas de confianza y, en su caso, en las correspondientes instrucciones disponibles en la página web de LOGALTY (https://www.logalty.com/certificateauthority/)

1.3.5 Otros participantes

La Autoridad de Certificación de LOGALTY es la Autoridad de Sellado de Tiempo electrónico cuando ofrece el servicio de confianza de creación de sellos de tiempo electrónicos.

1.4 Uso de los certificados

Esta sección lista las aplicaciones para las que puede emplearse cada tipo de certificado, establece limitaciones a ciertas aplicaciones y prohíbe ciertas aplicaciones de los certificados.

1.4.1 Usos permitidos para los certificados

Se deben tener en cuenta los usos permitidos indicados en los diversos campos de los perfiles de certificados, disponibles en el web de LOGALTY (https://www.logalty.com/certificateauthority)

1.4.1.1 Certificado cualificado de Sello electrónico de TSA/TSU

Este certificado dispone de los siguientes OID:

En la jerarquía de certificación de Logalty	1.3.6.1.4.1.30210.1.5.1
De acuerdo con la política QCP-l	0.4.0.194112.1.1

Los certificados de sello electrónico de TSA/TSU son certificados cualificados de acuerdo con el artículo 38 y el Anexo III del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 421 y ETSI EN 319 422.

Este certificado permite a Unidades de Sellado de Tiempo o TSU emitir los sellos de tiempo cuando reciben una solicitud bajo las especificaciones de la RFC3161.

Las claves se generan en soporte de un dispositivo seguro HSM. La información de usos en el perfil de certificado indica lo siguiente:

- El campo “key usage” tiene activadas, y por tanto nos permite realizar, las siguientes funciones:
    - Content Commitment
- El campo “extend key usage” tiene activada la función:
    - TimeStamping
- En el campo “Qualified Certificate Statements” aparece la siguiente declaración:
    - QcCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.

- El campo “User Notice” describe el uso de este certificado.

1.4.2 Límites y prohibiciones de uso de los certificados

Los certificados se deben emplear para su función propia y finalidad establecida, sin que puedan utilizarse para otras funciones o con otras finalidades.

Del mismo modo, los certificados deben emplearse únicamente de acuerdo con la ley aplicable, especialmente teniendo en cuenta las restricciones de importación y exportación existentes en cada momento.

Excepto cuando se prevea expresamente en un procedimiento de LOGALTY, los certificados no pueden emplearse para firmar peticiones de emisión, renovación, suspensión o revocación de certificados, ni para firmar certificados de clave pública de ningún tipo, ni firmar listas de revocación de certificados (LRC), sin perjuicio de lo indicado en el artículo 24.1.c) del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

Los certificados no se han diseñado, no se pueden destinar y no se autoriza su uso o reventa como equipos de control de situaciones peligrosas o para usos que requieren actuaciones a prueba de fallos, como el funcionamiento de instalaciones nucleares, sistemas de navegación o comunicaciones aéreas, o sistemas de control de armamento, donde un fallo pudiera directamente conllevar la muerte, lesiones personales o daños medioambientales severos.

Se deben tener en cuenta los límites indicados en los diversos campos de los perfiles de certificados, visibles en el web de Logalty (https://www.logalty.com/certificateauthority/)

El empleo de los certificados digitales en operaciones que contravengan esta DPC, los documentos jurídicos vinculantes de cada certificado, o los contratos con las entidades de registro o con los firmantes, los creadores de sellos y/o los suscriptores, tendrá la consideración de uso indebido a los efectos legales oportunos, eximiéndose por tanto LOGALTY, hasta donde permita la legislación vigente, de cualquier responsabilidad por este uso indebido de los certificados que realice el firmante o cualquier tercero.

LOGALTY no revisa los datos sobre los que se puede aplicar el uso pretendido de un certificado. Por lo tanto, no es posible por parte de LOGALTY emitir valoración alguna sobre dicho contenido, asumiendo por tanto el suscriptor, el firmante o la persona responsable del uso de los datos de creación de sello,

cualquier responsabilidad dimanante del contenido aparejado al uso de un certificado. Todo ello sin perjuicio del régimen aplicable a los servicios de la sociedad de la información, cuando sea legalmente procedente.

Asimismo, le será imputable al suscriptor, al firmante o a la persona responsable del uso de los datos de creación de sello, cualquier responsabilidad que pudiese derivarse de la utilización del mismo fuera de los límites y condiciones de uso recogidas en esta DPC, los documentos jurídicos vinculantes con cada certificado, o los contratos o convenios con las entidades de registro o con sus suscriptores, así como de cualquier otro uso indebido del mismo derivado de este apartado o que pueda ser interpretado como tal en función de la legislación vigente.

1.4.3 Emisión de certificados de pruebas

LOGALTY emite certificados de pruebas para su revisión en procesos de inspección o notificación por el Supervisor y en procesos de evaluación en auditorías de conformidad. Estos certificados emitidos bajo la jerarquía en producción de LOGALTY incluye datos ficticios que son:

Certificados de Sello Electrónico	
Campo O	Organization Prueba
SerialNumber	B00000000
Locality	Alcobendas
OU	Operaciones

Para poder disponer de estos certificados se debe enviar un correo electrónico a la dirección info.ca@logalty.com

1.5 Administración de la Declaración de Prácticas de Confianza

1.5.1 Organización que administra el documento

Logalty Trust Services

Logalty Prueba por Interposición SL

Calle de Cantabria 2 (Ed. Amura)

28108 Alcobendas, Madrid

España

Phone: +34 902 78 99 74

Email: info.ca@logalty.com

1.5.2 Datos de contacto de la organización

Logalty Prueba por Interposición SL

Calle de Cantabria 2 (Ed. Amura)

28108 Alcobendas, Madrid

Phone: +34 915 145 800

Fax: +34 917 913 085

Email: logalty@logalty.com

Identificación Registro	Registro Mercantil de Madrid
Tomo	22055
Folio	60
Hoja	M-393315
CIF	B-84492891

1.5.3 Procedimientos de gestión del documento

El sistema documental y de organización de LOGALTY garantiza, mediante la existencia y la aplicación de los correspondientes procedimientos, el correcto mantenimiento de este documento y de las

especificaciones de servicio relacionados con el mismo.

1.5.3.1 Revisión del documento

Logalty revisa esta DPC una vez al año como mínimo, siguiendo el **procedimiento de gestión documental en su última versión en vigor**, el cual establece el procedimiento general de gestión documental que determinará el ciclo de vida de los instrumentos del Sistema Integrado de Gestión de la Seguridad y Continuidad, y aquellos pertenecientes a los servicios de confianza a lo largo de todas sus fases.

Dicho procedimiento establece que los cambios en las prácticas de confianza del Servicio de Certificación y Sellado de Tiempo Electrónico supondrán un cambio de versión que deberá ser aprobado por el Comité de Continuidad Riesgos y Seguridad (CRS). La descripción de los cambios se incluirá en el apartado "control de versiones" de la sección "Información General" en el inicio de este documento.

Los cambios menores que no supongan un cambio de versión serán aprobados por el gerente de servicios de identidad e informados al CRS.

Las nuevas versiones de esta DPC, una vez aprobadas, serán publicadas en la web y notificadas, si procede, al supervisor.

El gerente de servicios de identidad y confianza será el responsable de identificar y comunicar al CRS los cambios en las prácticas de confianza.

1.5.4 Aprobación del documento

Las modificaciones futuras de esta Declaración de Prácticas de Confianza, de la Política de Seguridad y de los Textos de Divulgación (PDS) son aprobadas por el Comité de Continuidad, Riesgos y de Seguridad de la Información, el cuál de forma adicional se responsabilizará de su correcta implementación.

LOGALTY comunica de forma permanente los cambios que se produzcan en sus obligaciones publicando nuevas versiones de su documentación jurídica en su web

https://www.logalty.com/certificateauthority.

1.6 Definiciones y acrónimos

1.6.1 Definiciones

Autoridad de Certificación	Es la entidad responsable de la emisión y gestión de los certificados digitales.
Autoridad de Registro	Entidad responsable de la gestión de las solicitudes, identificación y registro de los solicitantes de un certificado. Puede formar parte de la Autoridad de Certificación o ser ajena.
Certificado	Archivo que asocia la clave pública con algunos datos identificativos del Sujeto/Firmante y es firmada por la AC.
Clave pública	Valor matemático conocido públicamente y usado para la verificación de una firma digital o el cifrado de datos.

Clave privada	Valor matemático conocido únicamente por el Sujeto/Firmante y usado para la creación de una firma digital o el descifrado de datos. La clave privada de la AC será usada para la firma de certificados y firma de CRL's. La clave privada del servicio TSA será usada para la firma de los sellos de tiempo.
DPC	Conjunto de prácticas adoptadas por una Autoridad de Certificación para la emisión de certificados en conformidad con una política de certificación concreta.
CRL	Archivo que contiene una lista de los certificados que han sido revocados en un periodo de tiempo determinado y que es firmada por la AC.
Datos de Activación	Datos privados, como PIN's o contraseñas empleadas para la activación de la clave privada
DCCF	Dispositivo Cualificado de creación de firma. Elemento software o hardware, convenientemente certificado, empleado por el Sujeto/Firmante para la generación de firmas electrónicas, de manera que se realicen las operaciones criptográficas dentro del dispositivo y se garantice su control únicamente por el Sujeto/Firmante.

Firma digital	El resultado de la transformación de un mensaje, o cualquier tipo de dato, por la aplicación de la clave privada en conjunción con unos algoritmos conocidos, garantizando de esta manera: a) que los datos no han sido modificados (integridad) b) que la persona que firma los datos es quien dice ser (identificación) c) que la persona que firma los datos no puede negar haberlo hecho (no repudio en origen)
OID	Identificador numérico único registrado bajo la estandarización ISO y referido a un objeto o clase de objeto determinado.
Par de claves	Conjunto formado por la clave pública y privada, ambas relacionadas entre sí matemáticamente.
PKI	Conjunto de elementos hardware, software, recursos humanos, procedimientos, etc., que componen un sistema basado en la creación y gestión de certificados de clave pública.
Solicitante	En el contexto de este documento, el solicitante será una persona física apoderada con un poder especial para realizar determinados trámites en nombre y representación de una persona jurídica, o de sí misma para certificados individuales.

Suscriptor	En el contexto de este documento la persona jurídica propietaria del certificado (a nivel corporativo) o la persona física en certificados individuales.
Parte Usuaria	En el contexto de este documento, persona que voluntariamente confía en el certificado digital y lo utiliza como medio de acreditación de la autenticidad e integridad del documento firmado
Emisor	Aquella persona física o jurídica que pone a disposición de Logalty la documentación respecto de la cual Logalty presta sus servicios de Contratación online, Notificación certificada, Comunicación certificada o Grabación de Llamadas.
Receptor	Aquella persona jurídica o física a quien va destinada la documentación respecto de la cual Logalty presta sus servicios de Contratación online, Notificación certificada, Comunicación certificada o Grabación de Llamadas.

1.6.2 Acrónimos

AC (o también CA)	Certificate Authority Autoridad de Certificación
AR (o también RA)	Registration Authority Autoridad de Registro
CPD	Centro de Proceso de Datos
DPC (o también CPS)	Certification Practice Statement. Declaración de Prácticas de Certificación
CRL (o también LRC)	Certificate Revocation List. Lista de certificados revocados
DN	Distinguished Name. Nombre distintivo dentro del certificado digital
DNI	Documento Nacional de Identidad
ETSI EN	European Telecommunications Standards Institute – European Standard.
FIPS	Federal Information Processing Standard Publication
HSM	Hardware Security Module Módulo de seguridad en Hardware
IETF	Internet Engineering Task Force
NIF	Número de Identificación Fiscal
NTP	Network Time Protocol Protocolo de tiempo en red.
OCSP	On-line Certificate Status Protocol. Protocolo de acceso al estado de los certificados
OID	Object Identifier. Identificador de objeto
PDS	PKI Disclosure Statements Texto de Divulgación de PKI.
PIN	Personal Identification Number. Número de identificación personal

PKI	Public Key Infrastructure. Infraestructura de clave pública
QSCD *(o también DCCF)*	Qualified Electronic Signature/Seal Creation Device. Dispositivo cualificado de creación de firma/sellos
QCP	Qualified Certificate Policy Política de certificados cualificados
QCP-l	Policy for EU qualified certificate issued to a legal person Política de certificados cualificados para personas jurídicas.
QCP-l-qscd	Policy for EU qualified certificate issued to a legal person where the private key and the related certificate reside on a QSCD Política de certificados cualificados para personas jurídicas con dispositivo cualificado de firma/sello
RFC	Request for Comments Documento RFC
RSA	Rivest-Shimar-Adleman. Tipo de algoritmo de cifrado
SHA	Secure Hash Algorithm. Algoritmo seguro de Hash
SSL	Secure Sockets Layer. Protocolo diseñado por Netscape y convertido en estándar de la red, permite la transmisión de información cifrada entre un navegador de Internet y un servidor.
TCP/IP	Transmission Control. Protocol/Internet Protocol. Sistema de protocolos, definidos en el marco de la IEFT.
TSA	Time Stamping Authority Autoridad de Sellado de Tiempo Electrónico
TSU	Time Stamping Unit Unidad de Sellado de Tiempo.
UTC	Coordinated Universal Time Tiempo universal coordinado
VPN	Virtual Private Network. Red privada virtual

2 Publicación de información y depósito de certificados

2.1 Depósito(s) de certificados

LOGALTY dispone de un Depósito de certificados, en el que se publican las informaciones relativas a los servicios de certificación.

Dicho servicio se encuentra disponible durante las 24 horas de los 7 días de la semana y, en caso de fallo del sistema fuera de control de LOGALTY, ésta realizará sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo en el plazo establecido en la sección 5.8.4 de esta Declaración de Prácticas de Confianza.

2.2 Publicación de información del prestador de servicios de certificación

LOGALTY publica las siguientes informaciones, en su Depósito:

- Los certificados emitidos, en su caso, cuando se haya obtenido consentimiento.
- Las listas de certificados revocados y otras informaciones de estado de revocación de los certificados. La Declaración de Prácticas de Confianza.
- Los textos de divulgación (PKI Disclosure Statements - PDS), como mínimo en lengua española e inglesa.

2.2.1 Términos y condiciones

LOGALTY informa a las partes que confían en los servicios de certificación digital a través de los textos de divulgación (PDS), y regula la concreta prestación del servicio a los usuarios y suscriptores, mediante la documentación contractual de los términos y condiciones.

Dicha información, y los términos y condiciones, se suministra por medios electrónicos durante el proceso de contratación, y de solicitud y emisión del certificado, y su aceptación es obligatoria y previa a la emisión del certificado. Asimismo, la aceptación expresa de los términos y condiciones y la PDS queda incluida en la hoja de solicitud del certificado, la cual es firmada por medios electrónicos.

2.3 Frecuencia de publicación

La información del prestador de servicios de certificación, incluyendo las PDS y la Declaración de Prácticas de Confianza, se publica en cuanto se encuentra disponible.

Los cambios en la Declaración de Prácticas de Confianza se rigen por lo establecido en la sección 1.5 de este documento.

La información de estado de revocación de certificados se publica de acuerdo con lo establecido en las secciones 4.8.7 y 4.8.8 de esta Declaración de Prácticas de Confianza.

2.4 Control de acceso

LOGALTY no limita el acceso de lectura a las informaciones establecidas en la sección 1, pero establece controles para impedir que personas no autorizadas puedan añadir, modificar o borrar registros del Depósito, para proteger la integridad y autenticidad de la información, especialmente la información de estado de revocación.

LOGALTY emplea sistemas fiables para el Depósito, de modo tal que:

- Únicamente personas autorizadas pueden hacer anotaciones y modificaciones en los datos almacenados.
- Puede comprobarse la autenticidad de la información.
- Los certificados sólo estarán disponibles para consulta si la persona física identificada en el certificado ha prestado su consentimiento.
- Puede detectarse cualquier cambio técnico que afecte a los requisitos de seguridad.

3 Identificación y autenticación

3.1 Registro de nombres

3.1.1 Tipos de nombres

Todos los certificados contienen un nombre diferenciado X.501 en el campo *Subject*, incluyendo un componente *Common Name* (CN=), relativo a la identidad de la unidad de tiempo electrónico (TSU).

De acuerdo con el apartado 4.2.1 de la ETSI EN 319 412-3 al respecto de los certificados emitidos a personas jurídicas, se indica que, en caso de incluirse, el tamaño de los campos `organizationName`, `organizationalUnitName` y `commonName` puede ser más largo que el límite establecido en la IETF RFC 5280.

3.1.1.1 Certificados de sello electrónico

Country [C]	"ES"
Organization (O)	Nombre oficial de la Entidad u Organización suscriptora del certificado
organizationIdentifier	NIF de la entidad u Organización a la que está vinculado este sello (en formato ETSI EN 319412-1)
Serial Number	NIF de la entidad u Organización
Locality	Localidad de la organización
Common Name	Nombre de la plataforma donde reside el sello de TSU

3.1.2 Significado de los nombres

Los nombres contenidos en los campos SubjectName y SubjectAlternativeName de los certificados son comprensibles en lenguaje natural, de acuerdo con lo establecido en la sección anterior.

3.1.3 Empleo de anónimos y seudónimos

En ningún caso se pueden utilizar seudónimos para identificar a una persona jurídica.

En ningún caso se emiten certificados anónimos.

3.1.4 Interpretación de formatos de nombres

Los formatos de nombres se interpretarán de acuerdo con la legislación del país de establecimiento del suscriptor, en sus propios términos.

El campo “país” será el del país en el que se realice el contrato con el subscriptor.

3.1.5 Unicidad de los nombres

Los nombres de los suscriptores de certificados serán únicos, para cada política de certificado de LOGALTY.

No se podrá asignar un nombre de suscriptor que ya haya sido empleado, a un suscriptor diferente, situación que, en principio no se debe producir, gracias a la presencia del número del NIF, o equivalente, en el esquema de nombres.

3.1.6 Resolución de conflictos relativos a nombres

Los solicitantes de certificados no incluirán nombres en las solicitudes que puedan suponer infracción, por el futuro suscriptor, de derechos de terceros.

LOGALTY no estará obligada a determinar previamente que un solicitante de certificados tiene derechos de propiedad industrial, de marca o de dominio sobre el nombre que aparece en una solicitud de certificado, sino que en principio procederá a certificar.

Asimismo, no actuará como árbitro o mediador, ni de ningún otro modo deberá resolver disputa alguna concerniente a la propiedad de nombres de personas u organizaciones, nombres de dominio, marcas o nombres comerciales.

Sin embargo, en caso de recibir una notificación relativa a un conflicto de nombres, conforme a la legislación del país del suscriptor, podrá emprender las acciones pertinentes orientadas a revocar el certificado.

En todo caso, el prestador de servicios de certificación se reserva el derecho de rechazar una solicitud de certificado debido a conflicto de nombres.

Para cuantas dudas o divergencias puedan surgir en la interpretación y/o cumplimiento de este contrato, las Partes, con renuncia expresa a cualquier otro fuero que pudiera corresponderles, pactan sumisión a los Juzgados y Tribunales de Madrid capital.

3.1.7 Autenticación de la identidad de una persona física

No aplica.

3.2 Validación inicial de la identidad

La identidad de los suscriptores de certificados resulta fijada en el momento de la firma del contrato entre LOGALTY y dichos suscriptores corporativos, momento en el cual se verifica al suscriptor mediante su documento nacional de identidad o similar y, dependiendo del certificado, los poderes de actuación de la persona representante, y resto de documentación necesaria. Para esta verificación, se podrá emplear documentación pública o notarial, y/o la consulta directa a los registros públicos correspondientes.

3.2.1 Prueba de posesión de clave privada

La posesión de la clave privada se demuestra en virtud del procedimiento fiable de entrega y aceptación del certificado por el suscriptor por el suscriptor corporativo.

3.2.2 Autenticación de la identidad de una organización, empresa o entidad mediante representante

3.2.2.1 Identidad

Las personas físicas con capacidad de actuar en nombre de las personas públicas o privadas suscriptoras, podrán actuar como representantes de estas, siempre y cuando exista una situación previa de representación legal o voluntaria entre la persona física y la persona pública o privada, que exige su reconocimiento por LOGALTY, la cual se realizará mediante el siguiente procedimiento presencial:

- El representante del suscriptor se reunirá presencialmente con un representante autorizado de LOGALTY, el cual pondrá a su disposición un formulario de autenticación. Alternativamente, el representante del suscriptor podrá obtener el formulario de la página web de LOGALTY para su cumplimentación previa.

- El representante cumplimentará el formulario, con las siguientes informaciones y a la que acompañará los siguientes documentos:
    - Sus datos de identificación como representante:
        - Nombre y apellidos.
        - Lugar y fecha de nacimiento.
        - Documento: DNI o NIF del representante.
    - Los datos de identificación del suscriptor al que representa:
        - Denominación o razón social.
        - Toda información de registro existente, incluyendo los datos relativos a la constitución y personalidad jurídica y a la extensión y vigencia de las facultades de representación del solicitante.
        - Documento: NIF de la persona pública o privada.
        - Documento: Documentos públicos que sirvan para acreditar los extremos citados de manera fehaciente y su inscripción en el correspondiente registro público si así resulta exigible. La citada comprobación podrá realizarse, asimismo, mediante consulta en el registro público en el que estén inscritos los documentos de constitución y de apoderamiento, pudiendo emplear los medios telemáticos facilitados por los citados registros públicos.
    - Los datos relativos a la representación o la capacidad de actuación que ostenta:
        - La vigencia de la representación o la capacidad de actuación (fecha de inicio y fin).
        - La indicación de Representación o capacidad total. Esta comprobación se podrá realizar mediante consulta telemática al registro público donde conste inscrita la representación.
- Cumplimentado y firmado el formulario, se firmará y entregará a LOGALTY junto con la documentación justificativa indicada.
- El personal de LOGALTY comprobará la identidad del representante mediante la

presentación del DNI o NIF, el contenido de la representación con la documentación.

- Alternativamente, de acuerdo con lo establecido en el artículo 24.1.d) del Reglamento (UE) 910/2014, y en el artículo 7.1 de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, se podrá legitimar notarialmente la firma del formulario, y hacerse llegar a LOGALTY por correo postal certificado, en cuyo caso los pasos 4 a 5 anteriores no serán precisos.
- LOGALTY comprueba la existencia de la entidad solicitante de un certificado de autenticación web mediante el acceso al Registro Mercantil.

3.2.3 Autenticación de la identidad de una persona física

No aplica. Logalty no expide certificados a personas física.

3.2.4 Información de suscriptor no verificada

LOGALTY no incluye ninguna información de suscriptor no verificada en los certificados.

3.2.5 Autenticación de las Autoridades de Registro

Es preciso que exista y se incluya en la solicitud una autorización para dicha expedición del certificado creada por un representante legal de la persona jurídica o entidad sin personalidad jurídica o con poder de representación suficiente del creador de sellos.

LOGALTY consultará al Registro Mercantil para comprobar que la entidad solicitante está constituida, que dispone de personalidad jurídica, sus datos actuales, así como el nombramiento y vigencia de la persona física autorizada.

Esta validación podrá realizarse por medios electrónicos. En caso de que el solicitante aporte documentación en papel se podrá escanear por el operador y firmarla con un sello electrónico.

3.2.6 Criterios de interoperación

LOGALTY se reserva el derecho de proporcionar servicios de interoperación con otros prestadores. Dichos servicios se establecerán por contrato.

3.3 Identificación y autenticación de solicitudes de renovación

Logalty no realiza renovaciones de certificados.

Antes de la caducidad del certificado se avisa al suscriptor para la emisión de un nuevo certificado, usando para ello las indicaciones del apartado 3.2 de esta DPC.

3.4 Identificación y autenticación de la solicitud de revocación

LOGALTY o una Entidad de Registro autentica las peticiones e informes relativos a la revocación de un certificado, comprobando que provienen de una persona autorizada.

Los métodos aceptables para dicha comprobación son los siguientes:

- El envío de una solicitud de revocación por parte del suscriptor por medio de la plataforma electrónica existente, de gestión del ciclo de vida de los certificados.
- El envío de una solicitud de revocación por parte del suscriptor firmada electrónicamente.
- El uso de información que sólo conoce la persona responsable del certificado, y que le permite revocar de forma automática su certificado.
- La personación física en una oficina de la empresa, entidad u Organización suscriptora.
- Otros medios de comunicación, como el envío de la solicitud de revocación firmada manuscritamente junto a una fotocopia de su documento oficial de identificación, por medio de envío postal. Logalty realiza las comprobaciones pertinentes para asegurarse de la veracidad de la solicitud.

Ampliación del procedimiento en el documento: LGT_revocacionCERT.

4 Requisitos de operación del ciclo de vida de los certificados

4.1 Solicitud de certificado

4.1.1 Legitimación para solicitar la emisión

El suscriptor del certificado debe firmar un contrato de prestación de servicios de certificación con LOGALTY.

Igualmente, con anterioridad a la emisión y entrega de un certificado, existe una previa solicitud de certificados formalizada en documento específico u hoja de solicitud de certificados en formato electrónico por medio de la plataforma electrónica existente.

En el caso de existir una relación previa entre el suscriptor y LOGALTY el solicitante podrá realizar la solicitud, que se instrumenta jurídicamente mediante una hoja de solicitud de certificados firmada por dicho solicitante en nombre de la persona jurídica subscriptora.

4.1.2 Procedimiento de alta y responsabilidades

LOGALTY puede recibir solicitudes de certificados en nombre de personas jurídicas.

Las solicitudes se instrumentan mediante un documento cumplimentado por el solicitante en nombre de la persona jurídica. Estas solicitudes se tramitan mediante la plataforma electrónica existente. La solicitud, además, podrá ser realizada por un operador autorizado por el suscriptor (o responsable de certificación), que haya sido designado por el suscriptor en el contrato entre dicho suscriptor y LOGALTY.

La solicitud deberá acompañarse de toda la documentación justificativa de la identidad y resto de datos necesarios de la persona jurídica suscriptora, de acuerdo con lo establecido en la sección 3.2.3. También se deberá acompañar otros datos, como una dirección de correo electrónico o postal que permitan contactar con la persona jurídica suscriptora.

4.2 Procesamiento de la solicitud de certificado

4.2.1 Ejecución de las funciones de identificación y autenticación

Una vez recibida una petición de certificado, LOGALTY se asegura de que las solicitudes de certificado sean completas, precisas y estén debidamente autorizadas, antes de procesarlas.

En caso afirmativo, LOGALTY verifica la información proporcionada, verificando el cumplimiento de lo indicado en la sección 3.2 de esta Declaración de Prácticas de Certificación.

En relación con los certificados cualificados, la documentación justificativa de la aprobación de la

solicitud debe ser conservada y debidamente registrada y **con garantías de seguridad e integridad durante el plazo de 15 años desde la extinción del certificado** o la finalización del servicio prestado, incluso en caso de pérdida anticipada de vigencia por revocación. Esta documentación podrá ser conservada de forma segura por medio de la plataforma electrónica existente.

4.2.2 Aprobación o rechazo de la solicitud

Cuando se verifique la corrección de los datos correspondientes a la solicitud, LOGALTY aprobará la solicitud del certificado y procederá a su emisión y entrega.

Si de la verificación resulta la certeza que la información no es correcta, o se sospecha la incorrecta, o la misma puede afectar a la reputación de la Entidad de Certificación o de los suscriptores, LOGALTY denegará la petición, o suspenderá su aprobación hasta que realice las comprobaciones complementarias que considere oportunas. Si dichas comprobaciones no permiten la certeza de la corrección de la información a verificar, LOGALTY podrá denegará la solicitud definitivamente.

LOGALTY notifica al solicitante la aprobación o denegación de la solicitud.

LOGALTY podrá automatizar los procedimientos de verificación de la corrección de la información que será contenida en los certificados, y de aprobación de las solicitudes, por medio de la plataforma electrónica existente.

4.2.3 Plazo para resolver la solicitud

LOGALTY atiende las solicitudes de certificados por orden de llegada, en un plazo razonable, pudiendo especificarse una garantía de plazo máximo en el contrato de emisión de certificados. Las solicitudes se mantienen activas hasta su aprobación o rechazo.

4.3 Emisión del certificado

4.3.1 Acciones de LOGALTY durante el proceso de emisión

Tras la aprobación de la solicitud de certificación se procede a la emisión del certificado de forma segura y se pone a disposición del titular para su aceptación, por medio de la plataforma electrónica existente.

Los procedimientos establecidos en esta sección también se aplican en caso de renovación de certificados, dado que la misma implica la emisión de un nuevo certificado.

Durante el proceso, LOGALTY:

- Protege la confidencialidad e integridad de los datos de registro de que dispone.
- Utiliza sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.
- Genera el par de claves, mediante un procedimiento de generación de certificados vinculado de forma segura con el procedimiento de generación de claves.
- Emplea un procedimiento de generación de certificados que vincula de forma segura el certificado con la información de registro, incluyendo la clave pública certificada.
- Se asegura de que el certificado es emitido por sistemas que utilicen protección contra falsificación y que garanticen la confidencialidad de las claves durante el proceso de generación de dichas claves.
- Incluye en el certificado las informaciones establecidas en el Reglamento (UE) 910/2014.
- Indica la fecha y la hora en que se expidió un certificado.

4.3.2 Notificación de la emisión al suscriptor

LOGALTY notifica la emisión del certificado la persona jurídica subscriptora.

4.4 Aceptación del certificado

4.4.1 Procedimiento de la aceptación

Durante este proceso, LOGALTY debe realizar las siguientes actuaciones:

- Cuando no se ha realizado con anterioridad, acreditar definitivamente la identidad de la persona física representante legal o apoderada suficiente solicitante del certificado de sello
- electrónico.

- Entregar a la persona física representante legal o apoderada suficiente:
    - Las condiciones generales de prestación de servicios de certificación electrónica que incluye aviso legal sobre protección de datos, incluidas en el texto de divulgación o PDS.
    - Las indicaciones exactas para la aceptación del certificado.
    - Información básica acerca del uso del certificado, incluyendo especialmente información acerca del prestador de servicios de certificación y de la Declaración de Prácticas de Confianza aplicable, así como sus obligaciones, facultades y responsabilidades.
    - Información acerca del certificado.
    - Reconocimiento, por parte del representante legal, de disponer de acceso al certificado.
    - Régimen de obligaciones del uso del certificado.
    - Responsabilidad del titular.
    - Método de imputación exclusiva al titular, de su clave privada y de sus datos de activación del certificado.
    - La fecha del acto de aceptación.
- Obtener la aceptación del certificado, por medio de firma, escrita o electrónica, o acto indicado en el apartado 4.4.2, de la persona representante del titular. En la opción de la firma electrónica de la aceptación, ésta se realiza por medio de los servicios de la plataforma electrónica existente y/o se puede firmar con una firma manuscrita capturada electrónicamente.

El suscriptor y/o Autoridad de Registro, en su caso, colabora en estos procesos, debiendo registrar documentalmente los anteriores actos y conserva los citados documentos originales (hojas de entrega y aceptación), remitiendo copia electrónica a LOGALTY, así como los originales cuando LOGALTY precise de acceso a los mismos.

Cuando esta documentación se guarde electrónicamente, o no se realice interviniendo el suscriptor y/o Autoridad de Registro, se utilizarán los servicios correspondientes a la plataforma electrónica existente.

4.4.1.1 Conducta que constituye aceptación del certificado

La aceptación del certificado por la persona física representante se produce con cualquiera de las dos opciones:

- Mediante la firma electrónica de una hoja de aceptación.
- Mediante el cambio del PIN del certificado.

4.4.2 Publicación del certificado

LOGALTY publica el certificado en el Depósito a que se refiere la sección 2, con los controles de seguridad pertinentes y siempre que LOGALTY disponga de la autorización de la persona física representante.

4.4.3 Notificación de la emisión a terceros

No aplica

4.5 Uso del par de claves y del certificado

4.5.1 Uso por el suscriptor

4.5.1.1 Obligaciones del suscriptor del certificado

LOGALTY obliga contractualmente al suscriptor a:

- Facilitar a la Entidad de Certificación información completa y adecuada, conforme a los requisitos de esta Declaración de Prácticas de Confianza, en especial en lo relativo al procedimiento de registro.
- Manifestar su consentimiento previo a la emisión y entrega de un certificado.

- Emplear el certificado de acuerdo con lo establecido en la sección 4.
- Comunicar a LOGALTY y a cualquier persona que el suscriptor crea que pueda confiar en el certificado, sin retrasos injustificables:
    - La pérdida, el robo o el compromiso potencial de su clave privada.
    - La pérdida de control sobre su clave privada, debido al compromiso de los datos de activación (por ejemplo, el código PIN) o por cualquier otra causa.
    - Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.
    - La pérdida, la alteración, el uso no autorizado, el robo o el compromiso, cuando exista, de la tarjeta.
- Trasladar a las personas físicas identificadas en el certificado el cumplimiento de las obligaciones específicas de los mismos, y establecer mecanismos para garantizar el efectivo cumplimiento de estas.
- No monitorizar, manipular o realizar actos de ingeniería inversa sobre la implantación técnica de los servicios de certificación de LOGALTY, sin permiso previo por escrito.
- No comprometer la seguridad de los servicios de certificación del prestador de servicios de certificación de LOGALTY, sin permiso previo por escrito.

4.5.1.2 Responsabilidad civil del suscriptor del certificado

LOGALTY obliga contractualmente al suscriptor a responsabilizarse de:

- Que todas las manifestaciones realizadas en la solicitud son correctas.
- Que todas las informaciones suministradas por el suscriptor contenidas en el certificado son correctas.
- Que el certificado se emplea exclusivamente para usos legales y autorizados, de acuerdo con la Declaración de Prácticas de Confianza.
- Que ninguna persona no autorizada ha tenido jamás acceso a la clave privada del certificado,

y que es el único responsable de los daños causados por su incumplimiento del deber de protección del control exclusivo de acceso a la clave privada.

- Que el suscriptor es una entidad final y no un prestador de servicios de certificación, y que no emplea la clave privada correspondiente a la clave pública listada en el certificado para firmar certificado alguno (o cualquier otro formato de clave pública certificada), ni Lista de Revocación de Certificados, ni título de prestador de servicios de certificación ni en ningún otro caso.

4.5.2 Uso por el tercero que confía en certificados

4.5.2.1 Obligaciones del tercero que confía en certificados

LOGALTY obliga al tercero que confía en certificados a:

- Asesorarse de forma independiente acerca del hecho de que el certificado es apropiado para el uso que se pretende.
- Verificar la validez o revocación de los certificados emitidos, para lo que empleará información sobre el estado de los certificados.
- Verificar todos los certificados de la jerarquía de certificados, antes de confiar en la firma digital o en alguno de los certificados de la jerarquía.
- Hay que reconocer que para considerarse certificado cualificado debe estar incluido en la Lista de Confianza nacional (Trusted List).
- Tener presente cualquier limitación en el uso del certificado, con independencia de que se encuentre en el propio certificado o en el contrato de tercero que confía en el certificado.
- Tener presente cualquier precaución establecida en un contrato o en otro instrumento, con independencia de su naturaleza jurídica.
- No monitorizar, manipular o realizar actos de ingeniería inversa sobre la implantación técnica de los servicios de certificación de LOGALTY, sin permiso previo por escrito.
- No comprometer la seguridad de los servicios de certificación de la LOGALTY, sin permiso previo por escrito.

4.5.2.2 Responsabilidad civil del tercero que confía en certificados

LOGALTY obliga al tercero a manifestar:

- Que dispone de suficiente información para tomar una decisión informada con el objeto de confiar en el certificado o no.
- Que es el único responsable de confiar o no en la información contenida en el certificado.
- Que será el único responsable si incumple sus obligaciones como tercero que confía en el certificado.

4.6 Renovación de certificados sin cambio de claves

Logalty no realiza renovación de certificados.

4.7 Renovación de certificados con cambio de claves

Logalty no realiza renovación de certificados.

4.8 Modificación de certificados

La modificación de certificados, excepto la modificación de la clave pública certificada será tratada como una nueva emisión de certificado, aplicándose lo descrito en las secciones 4, 4.2, 4.3 y 4.4.

4.9 Revocación de certificados

4.9.1 Causas de revocación de certificados

LOGALTY revoca un certificado cuando concurre alguna de las siguientes causas:

- Circunstancias que afectan a la información contenida en el certificado:
    - Modificación de alguno de los datos contenidos en el certificado, después de la

correspondiente emisión del certificado que incluye las modificaciones.

- Descubrimiento de que alguno de los datos contenidos en la solicitud de certificado es incorrecto.
- Descubrimiento de que alguno de los datos contenidos en el certificado es incorrecto.

- Circunstancias que afectan a la seguridad de la clave o del certificado:
  - Compromiso de la clave privada, de la infraestructura o de los sistemas del prestador de servicios de certificación que emitió el certificado, siempre que afecte a la fiabilidad de los certificados emitidos a partir de ese incidente.
  - Infracción, por LOGALTY, de los requisitos previstos en los procedimientos de gestión de certificados, establecidos en esta Declaración de Prácticas de Confianza.
  - Compromiso o sospecha de compromiso de la seguridad de la clave o del certificado emitido.
  - Acceso o utilización no autorizados, por un tercero, de la clave privada correspondiente a la clave pública contenida en el certificado.
  - El uso irregular del certificado por la persona física identificada en el certificado, o la falta de diligencia en la custodia de la clave privada.
- Circunstancias que afectan al suscriptor en el certificado:
  - Finalización de la relación jurídica de prestación de servicios entre LOGALTY y el suscriptor.
  - Modificación o extinción de la relación jurídica subyacente o causa que provocó la emisión del certificado a la persona física identificada en el certificado.
  - Infracción por el solicitante del certificado de los requisitos preestablecidos para la solicitud de este.
  - Infracción por el suscriptor, de sus obligaciones, responsabilidad y garantías, establecidas en el documento jurídico correspondiente.
  - La extinción de la persona jurídica suscriptora del certificado.
  - Solicitud del suscriptor de revocación del certificado, de acuerdo con lo establecido en la sección 4.

- Otras circunstancias:
    - La terminación del servicio de certificación de la Entidad de Certificación de LOGALTY, de acuerdo con lo establecido en la sección 9.
    - El uso del certificado que sea dañino y continuado para LOGALTY. En este caso, se considera que un uso es dañino en función de los siguientes criterios:
        - La naturaleza y el número de quejas recibidas.
        - La identidad de las entidades que presentan las quejas.
        - La legislación relevante vigente en cada momento.
        - La respuesta del suscriptor o de la persona identificada en el certificado a las quejas recibidas.

4.9.2 Legitimación para solicitar la revocación

Pueden solicitar la revocación de un certificado:

- El suscriptor del certificado, por medio del responsable del servicio de certificación.
- La Entidad de Certificación de LOGALTY.

4.9.3 Procedimientos de solicitud de revocación

4.9.3.1 En general

La entidad que precise revocar un certificado debe solicitarlo a LOGALTY.

La solicitud de revocación puede ser solicitada por medio de la plataforma electrónica existente, firmada electrónicamente por email (contacto indicado en el apartado 1.5.1), o acudiendo físicamente a una oficina de Logalty o del suscriptor.

La solicitud de revocación comprenderá la siguiente información:

- Fecha de solicitud de la revocación.

- Identidad del suscriptor.
- Razón detallada para la petición de revocación.
- Nombre y título de la persona que pide la revocación.
- Información de contacto de la persona que pide la revocación.

La solicitud debe ser autenticada, por LOGALTY, de acuerdo con los requisitos establecidos en la sección 3.4 de esta política, antes de proceder a la revocación.

LOGALTY podrá incluir cualquier otro requisito para la confirmación de las solicitudes de revocación.

El procedimiento de revocación se puede encontrar en el documento “LGT_revocacionCERT”.

La solicitud de revocación será procesada a su recepción, y se informará al suscriptor y, en su caso, a la persona física identificada en el certificado, acerca del cambio de estado del certificado revocado.

LOGALTY no reactiva el certificado una vez ha sido revocado.

Tanto el servicio de gestión de las revocaciones como el servicio de consulta son considerados servicios críticos y así constan en el Plan de contingencias y el plan de continuidad de negocio de LOGALTY.

4.9.4 Plazo temporal de solicitud de revocación

Las solicitudes de revocación se remitirán de forma inmediata en cuanto se tenga conocimiento de la causa de revocación, en horario de 24x7 y no será superior a las 24 horas.

4.9.5 Plazo temporal de procesamiento de la solicitud

La revocación se producirá inmediatamente cuando sea recibida, en horario de 24x7.

4.9.6 Obligación de consulta de información de revocación de certificados

Los terceros deben comprobar el estado de aquellos certificados en los cuales desean confiar.

Un método por el cual se verifica el estado de los certificados es consultando el servicio OCSP de la Entidad de Certificación de LOGALTY en la web siguiente:

http://ocsp1.logalty.es

El servicio OCSP incluye los certificados expirados en sus respuestas.

LOGALTY valida el estado de todos los certificados antes de la realización de una firma desde sus plataformas de creación de firma.

4.9.7 Frecuencia de emisión de listas de revocación de certificados (LRCs)

LOGALTY emite una LRC al menos cada 24 horas.

La LRC indica el momento programado de emisión de una nueva LRC, si bien se puede emitir una LRC antes del plazo indicado en la LRC anterior, para reflejar revocaciones.

La LRC mantiene obligatoriamente el certificado revocado o suspendido hasta que expira. Las LRCs no incluyen los certificados expirados en sus respuestas.

4.9.8 Plazo máximo de publicación de LRCs

Las LRCs se publican en el Depósito en un periodo inmediato razonable tras su generación, que en ningún caso no supera unos pocos minutos.

4.9.9 Disponibilidad de servicios de comprobación en línea de estado de certificados

De forma alternativa, los terceros que confían en certificados podrán consultar el Depósito de certificados de LOGALTY, que se encuentra disponible las 24 horas de los 7 días de la semana en el web: https://www.logalty.com/certificateauthority/

Para comprobar la última CRL emitida se debe descargar:

- Logalty Qualified CA G2
    - http://crl1.logalty.es/qualifiedLogaltySubCA02.crl
      http://crl2.logalty.es/qualifiedLogaltySubCA02.crl

En caso de fallo de los sistemas de comprobación de estado de certificados por causas fuera del control de LOGALTY, ésta deberá realizar sus mejores esfuerzos por asegurar que este servicio se mantenga inactivo el mínimo tiempo posible, que no podrá superar un día.

LOGALTY suministra información a los terceros que confían en certificados acerca del funcionamiento del servicio de información de estado de certificados.

Los servicios de comprobación de estado de los certificados son de uso gratuito.

LOGALTY mantiene disponible la información del estado de revocación pasado el período de validez del certificado, por medio del servicio OCSP. Esta disponibilidad se mantiene en caso de finalización de los servicios PKI por parte de LOGALTY, transfiriendo esta obligación a otro prestador.

4.9.10 Obligación de consulta de servicios de comprobación de estado de certificados

Resulta obligatorio consultar el estado de los certificados antes de confiar en los mismos.

4.9.11 Requisitos especiales en caso de compromiso de la clave privada

El compromiso de la clave privada de LOGALTY es notificado a todos los participantes en los servicios de certificación, en la medida de lo posible, mediante la publicación de este hecho en la página web de LOGALTY, así como, si se considera necesario, en otros medios de comunicación, incluso en papel. En caso de compromiso de la clave privada, LOGALTY ejecuta las acciones previstas en el plan de cese del servicio, conforme al escenario de cese no programado.

En caso de compromiso, se procederá a la revocación inmediata de todos los certificados de entidad final, se emitirá una última CRL sin fecha de renovación, que será publicada, y el servicio OCSP, que permanecerá activo, devolverá para todos los certificados que los mismos han sido revocados por

compromiso de clave. Esta información de estado se mantendrá accesible durante el plazo de quince años desde la revocación o la expiración de los certificados, según proceda.

4.9.12 Causas de suspensión de certificados

LOGALTY no realiza suspensión de certificados.

4.9.13 Solicitud de suspensión

LOGALTY no realiza suspensión de certificados.

4.9.14 Procedimientos para la petición de suspensión

LOGALTY no realiza suspensión de certificados.

4.9.15 Período máximo de suspensión

LOGALTY no realiza suspensión de certificados.

4.10 Servicios de comprobación de estado de certificados

4.10.1 Características operativas de los servicios

Los servicios de comprobación de estado de certificados se prestan mediante una interfaz de consulta web, en la web https://www.logalty.com/certificateauthority/.

4.10.2 Disponibilidad de los servicios

Los servicios de comprobación de estado de certificados se encuentran disponibles las 24 horas del día, los 7 días de la semana, durante todo el año, con excepción de las paradas programadas.

4.10.3 Características opcionales

Sin estipulación.

4.11 Finalización de la suscripción

En la modalidad de servicio corporativo, la suscripción dura tanto tiempo como el contrato de servicio, que al menos cubre la duración de todos los certificados corporativos expedidos en ejecución de este.

4.12 Depósito y recuperación de claves

4.12.1 Política y prácticas de depósito y recuperación de claves

LOGALTY no presta servicios de depósito y recuperación de claves.

4.12.2 Política y prácticas de encapsulado y recuperación de claves de sesión

Sin estipulación.

5 Controles de seguridad física, de gestión y de operaciones

5.1 Controles de seguridad física

LOGALTY ha establecido controles de seguridad física y ambiental para proteger los recursos de las instalaciones donde se encuentran los sistemas, los propios sistemas y los equipamientos empleados para las operaciones de registro y aprobación de las solicitudes, generación técnica de los certificados y la gestión del hardware criptográfico.

En concreto, la política de seguridad física y ambiental aplicable a los servicios de generación de certificados, de dispositivos criptográficos y de gestión de revocación ha establecido prescripciones para las siguientes contingencias:

- Controles de acceso físico.
- Protección frente a desastres naturales.

- Medidas de protección frente a incendios.
- Fallo de los sistemas de apoyo (energía electrónica, telecomunicaciones, etc.)
- Derrumbamiento de la estructura.
- Protección antirrobos.
- Salida no autorizada de equipamientos, informaciones, soportes y aplicaciones relativos a componentes empleados para los servicios del prestador de servicios de certificación.

Estas medidas resultan aplicables a las instalaciones donde se producen los certificados bajo la plena responsabilidad de LOGALTY, que la presta desde sus instalaciones de alta seguridad, tanto principales como, en su caso, de operación en contingencia, que son debidamente auditadas de forma periódica.

Las instalaciones cuentan con sistemas de mantenimiento preventivo y correctivo con asistencia 24h-365 días al año con asistencia en las 24 horas siguientes al aviso.

5.1.1 Localización y construcción de las instalaciones

La protección física se logra mediante la creación de perímetros de seguridad claramente definidos en torno a los servicios. La calidad y solidez de los materiales de construcción de las instalaciones garantiza unos adecuados niveles de protección frente a intrusiones por la fuerza bruta y ubicada en una zona de bajo riesgo de desastres y permite un rápido acceso.

La sala donde se realizan las operaciones criptográficas en el Centro de Proceso de Datos:

- Cuenta con redundancia en sus infraestructuras.
- Cuenta con varias fuentes alternativas de electricidad y refrigeración en caso de emergencia.
- Las operaciones de mantenimiento no requieren que el Centro esté offline en ningún momento.

LOGALTY dispone de instalaciones que protegen físicamente la prestación de los servicios de aprobación de solicitudes de certificados y de gestión de revocación del compromiso causado por acceso no autorizado a los sistemas o a los datos, así como a la divulgación de los mismos.

5.1.2 Acceso físico

LOGALTY dispone de tres niveles de seguridad física (Entrada del Edificio donde se ubica el CPD, acceso a la sala del CPD y acceso al RAC) para la protección del servicio de generación de certificados, debiendo accederse desde los niveles inferiores a los niveles superiores.

El acceso físico a las dependencias de la LOGALTY donde se llevan a cabo procesos de certificación está limitado y protegido mediante una combinación de medidas físicas y procedimentales. Así:

- Está limitado a personal expresamente autorizado, con identificación en el momento del acceso y registro de este, incluyendo filmación por circuito cerrado de televisión y su archivo.
- El acceso a las salas se realiza con lectores de tarjeta de identificación y gestionado por un sistema informático que mantiene un log de entradas y salidas automático.
- Para el acceso al rack donde se ubican los procesos criptográficos es necesario la autorización previa de LOGALTY a los administradores del servicio de hospedaje que disponen de la llave para abrir la jaula.

En cuanto al acceso a las salas de acceso restringido (como la que alberga el CPD), existe un listado con las personas autorizadas a pedir acceso a las personas de las que dependen directamente de ellos (ya sean empleados o externos). Este listado se revisa con una periodicidad máxima de 6 meses.

Cualquier intervención de un tercero en el CPD requiere que el área de RIM&DATA CENTRE SHARED SERVICES de Fujitsu conozca previamente el detalle de la intervención y se haya planificado la visita.

Para la planificación de la misma es necesaria la apertura de una solicitud de acceso al CPD en el que se debe detallar:

- Personal que accede a la sala y rol
    - Identificar elementos a los que es necesario acceder (elemento o rack completo en el caso de que sea dedicado)
    - Acciones que se van a realizar.

- Fecha de la visita
- Duración.

El registro de la solicitud se realizará de acuerdo con los procedimientos establecidos con cada cliente y registrados en la herramienta de gestión de la actividad que corresponda.

Una vez que la visita ha sido aprobada, se procederá a la petición de dos llaves necesarias para poder acceder al CPD y custodiadas por dos grupos diferentes de la compañía, con el objetivo de minimizar los riesgos de acceso indebido.

5.1.3 Electricidad y aire acondicionado

Las instalaciones de LOGALTY disponen de equipos estabilizadores de corriente y un sistema de alimentación eléctrica de equipos duplicado con un grupo electrógeno.

Las salas que albergan equipos informáticos cuentan con sistemas de control de temperatura con equipos de aire acondicionado.

5.1.4 Exposición al agua

Las instalaciones están ubicadas en una zona de bajo riesgo de inundación.

Las salas donde se albergan equipos informáticos disponen de un sistema de detección de humedad.

5.1.5 Prevención y protección de incendios

Las instalaciones y activos de LOGALTY cuentan con sistemas automáticos de detección y extinción de incendios.

5.1.6 Almacenamiento de soportes

Únicamente el personal autorizado tiene acceso a los medios de almacenamiento.

La información de más alto nivel de clasificación se guarda en una caja de seguridad fuera de las

instalaciones del Centro de Proceso de Datos.

5.1.7 Tratamiento de residuos

La eliminación de soportes, tanto papel como magnéticos, se realizan mediante mecanismos que garanticen la imposibilidad de recuperación de la información.

En el caso de soportes magnéticos, se procede al formateo, borrado permanente, o destrucción física del soporte, de acuerdo con los estándares de nuestro proveedor Fujitsu.

En el caso de documentación en papel, mediante trituradoras o en papeleras dispuestas al efecto para posteriormente ser destruidos, bajo control.

5.1.8 Copia de respaldo fuera de las instalaciones

No se realizan copias de respaldo fuera de las instalaciones, ya que las copias de respaldo de cada centro de proceso de datos se almacenan en el otro centro de proceso de datos, de forma cruzada, generando así la redundancia necesaria.

5.2 Controles de procedimientos

LOGALTY garantiza que sus sistemas se operan de forma segura, para lo cual ha establecido e implantado procedimientos para las funciones que afectan a la provisión de sus servicios.

El personal al servicio de LOGALTY ejecuta los procedimientos administrativos y de gestión de acuerdo con la política de seguridad.

5.2.1 Funciones fiables

LOGALTY ha identificado, de acuerdo con su política de seguridad, las siguientes funciones o roles con la condición de fiables:

- **Auditor Interno**: Responsable del cumplimiento de los procedimientos operativos. Se trata de una persona externa al departamento de Sistemas de Información. Las tareas de Auditor interno

son incompatibles en el tiempo con las tareas de Certificación e incompatibles con Sistemas. Estas funciones estarán subordinadas a la Dirección de operaciones, reportando tanto a ésta como a la dirección técnica.

- **Gestor de Incidencias de Seguridad**: Responsable del seguimiento de las alertas de eventos de seguridad potencialmente críticos y de garantizar que los incidentes sean notificados con los procedimientos del TSP.
- **Administrador de Sistemas**: Responsable del funcionamiento correcto del hardware y software soporte de la plataforma de certificación
- **Administrador de CA**: Responsable de las acciones a ejecutar con el material criptográfico, o con la realización de alguna función que implique la activación de las claves privadas de las autoridades de certificación descritas en este documento, o de cualquiera de sus elementos.
- **Operador de CA**: responsable necesario conjuntamente con el Administrador de CA de la custodia de material de activación de las claves criptográficas, también responsable de las operaciones de backup y mantenimiento de la AC.
- **Administrador de Registro**: Persona responsable de aprobar las peticiones de certificados realizadas por el suscriptor.
- **Responsable de Seguridad**: Encargado de coordinar, controlar y hacer cumplir las medidas de seguridad definidas por las políticas de seguridad de LOGALTY. Debe encargarse de los aspectos relacionados con la seguridad de la información: lógica, física, redes, organizativa, etc.
- **Oficial de Registro**: Persona encargada junto al Administrador de Registro de la verificación y aprobación de las peticiones de certificados.
- **Oficial de Revocación**: Responsable de comprobar y aplicar los cambios en el estado de un certificado.

Las personas que ocupan los puestos anteriores se encuentran sometidas a procedimientos de investigación y control específicos. Estas personas realizan sus funciones basándose en el principio de menor privilegio.

5.2.2 Número de personas por tarea

LOGALTY garantiza al menos dos personas para realizar las tareas que se detallan en las Políticas de Certificación correspondientes, especialmente en la gestión del dispositivo de custodia de las claves de la Autoridad de Certificación raíz e intermedias.

5.2.3 Identificación y autenticación para cada función

Las personas asignadas para cada rol son identificadas por el auditor interno que se asegurará que cada persona realiza las operaciones para las que está asignado.

Cada persona solo controla los activos necesarios para su rol, asegurando así que ninguna persona accede a recursos no asignados.

El acceso a recursos se realiza dependiendo del activo mediante tarjetas criptográficas y códigos de activación.

5.2.4 Roles que requieren separación de tareas

Las siguientes tareas son realizadas, al menos, por dos personas:

- Emisión y revocación de certificados, y el acceso al depósito.
- Generación, emisión y destrucción de certificados de la Entidad de Certificación.
- Puesta en producción de la Entidad de Certificación.

5.3 Controles de personal

5.3.1 Requisitos de historial, calificaciones, experiencia y autorización

Todo el personal que realiza tareas calificadas como confiables lleva al menos un año trabajando en el centro de producción y tiene contratos laborales fijos.

Todo el personal está cualificado y ha sido instruido convenientemente para realizar las operaciones que le han sido asignadas.

El personal en puestos de confianza no tiene intereses personales que entran en conflicto con el

desarrollo de la función que tenga encomendada.

LOGALTY se asegura de que el personal de registro es confiable para realizar las tareas de registro. El Administrador de Registro ha realizado un curso de preparación para la realización de las tareas de validación de las peticiones.

En general, LOGALTY retirará de sus funciones de confianza a un empleado cuando se tenga conocimiento de la existencia de la comisión de algún hecho delictivo que pudiera afectar al desempeño de sus funciones.

LOGALTY no asignará un sitio confiable o de gestión a una persona que no sea idónea para el puesto. Por este motivo, previamente se realiza una investigación hasta donde permita la legislación aplicable, relativa a los siguientes aspectos:

- Estudios, incluyendo titulación alegada.
- Trabajos anteriores, hasta cinco años, incluyendo referencias profesionales y comprobación que realmente se realizó el trabajo alegado.

5.3.2 Procedimientos de investigación de historial

LOGALTY, antes de contratar a una persona o de que ésta acceda al puesto de trabajo, realiza las siguientes comprobaciones:

- Referencias de los trabajos de los últimos años
- Referencias profesionales
- Estudios, incluyendo titulación alegada.

LOGALTY realiza dichas comprobaciones con observancia estricta del REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD), y con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos (LOPDGDD).

La investigación se repetirá con una periodicidad suficiente.

Todas las comprobaciones se realizan hasta donde lo permite la legislación vigente aplicable. Los motivos que pueden dar lugar a rechazar al candidato a un puesto fiable son los siguientes:

- Falsedades en la solicitud de trabajo, realizadas por el candidato.
- Referencias profesionales muy negativas o muy poco fiables en relación con el candidato.

En la solicitud para el puesto de trabajo se informa acerca de la necesidad de someterse a una investigación previa, advirtiéndole de que la negativa a someterse a la investigación implica el rechazo de la solicitud.

5.3.3 Requisitos de formación

LOGALTY forma al personal en puestos fiables y de gestión, hasta que alcanzan la cualificación necesaria, manteniendo archivo de dicha formación.

Los programas de formación son actualizados y mejorados de forma periódica. La formación incluye, al menos, los siguientes contenidos:

- Principios y mecanismos de seguridad de la jerarquía de certificación, así como el entorno de usuario de la persona a formar.
- Tareas que debe realizar la persona.
- Políticas y procedimientos de seguridad de LOGALTY. Uso y operación de maquinaria y aplicaciones instaladas.
- Gestión y tramitación de incidentes y compromisos de seguridad.
- Procedimientos de continuidad de negocio y emergencia.
- Procedimiento de gestión y de seguridad en relación con el tratamiento de los datos de carácter personal.

5.3.4 Requisitos y frecuencia de actualización formativa

LOGALTY actualiza la formación del personal de acuerdo con las necesidades, y con la frecuencia suficientes para cumplir sus funciones de forma competente y satisfactoria, especialmente cuando se realicen modificaciones sustanciales en las tareas de certificación.

5.3.5 Secuencia y frecuencia de rotación laboral

No aplicable.

5.3.6 Sanciones para acciones no autorizadas

LOGALTY dispone de un sistema sancionador, para depurar las responsabilidades derivadas de acciones no autorizadas, adecuado a la legislación laboral aplicable y, en especial, coordinado con el sistema sancionador del convenio colectivo que resulte de aplicación al personal.

Las acciones disciplinarias incluyen la suspensión y el despido de la persona responsable de la acción dañina, de forma proporcionada a la gravedad de la acción no autorizada.

5.3.7 Requisitos de contratación de profesionales

Los empleados contratados para realizar tareas confiables firman con anterioridad las cláusulas de confidencialidad y los requerimientos operacionales empleados por LOGALTY. Cualquier acción que comprometa la seguridad de los procesos aceptados podrían, una vez evaluados, dar lugar al cese del contrato laboral.

En el caso de que todos o parte de los servicios de certificación sean operados por un tercero, los controles y previsiones realizadas en esta sección, o en otras partes de la DPC, serán aplicados y cumplidos por el tercero que realice las funciones de operación de los servicios de certificación, no obstante, lo cual, la entidad de certificación será responsable en todo caso de la efectiva ejecución. Estos aspectos quedan concretados en el instrumento jurídico utilizado para acordar la prestación de los servicios de certificación por tercero distinto a LOGALTY.

5.3.8 Suministro de documentación al personal

El prestador de servicios de certificación suministrará la documentación que estrictamente precise su personal en cada momento, al objeto de realizar su trabajo de forma competente y satisfactoria.

5.4 Procedimientos de auditoría de seguridad

LOGALTY está sujeta a las validaciones cada dos años por medio de auditorías LOPD. Además, dispone de una auditoría anual de revisión de seguridad con el objetivo de identificar y analizar las vulnerabilidades potencialmente explotables.

5.4.1 Tipos de eventos registrados

LOGALTY produce y guarda registro, al menos, de los siguientes eventos relacionados con la seguridad de la entidad:

- Encendido y apagado del sistema.
- Intentos de creación, borrado, establecimiento de contraseñas o cambio de privilegios.
- Intentos de inicio y fin de sesión.
- Intentos de accesos no autorizados al sistema de la AC a través de la red.
- Intentos de accesos no autorizados al sistema de archivos.
- Acceso físico a los logs.
- Cambios en la configuración y mantenimiento del sistema.
- Registros de las aplicaciones de la AC.
- Encendido y apagado de la aplicación de la AC.
- Cambios en los detalles de la AC y/o sus claves.
- Cambios en la creación de políticas de certificados.
- Generación de claves propias.
- Creación y revocación de certificados.

- Registros de la destrucción de los medios que contienen las claves, datos de activación.
- Eventos relacionados con el ciclo de vida del módulo criptográfico, como recepción, uso y desinstalación de este.
- Las actividades de los cortafuegos y enrutadores
- La ceremonia de generación de claves y las bases de datos de gestión de claves.
- Registros de acceso físico.
- Cambios en el personal.
- Informes de compromisos y discrepancias.
- Registros de la destrucción de material que contenga información de claves, datos de activación o información personal del suscriptor, en caso de certificados individuales, o de la persona física identificada en el certificado, en caso de certificados de organización.
- Posesión de datos de activación, para operaciones con la clave privada de la Entidad de Certificación.
- Informes completos de los intentos de intrusión física en las infraestructuras que dan soporte a la emisión y gestión de certificados.

Las entradas del registro incluyen los siguientes elementos:

- Fecha y hora de la entrada.
- Número de serie o secuencia de la entrada, en los registros automáticos.
- Identidad de la entidad que entra el registro.
- Tipo de entrada.

Quedan registrados todos los sucesos relacionados con la preparación de los dispositivos cualificados de creación de firmas que son usados por los firmantes o custodios.

5.4.2 Frecuencia de tratamiento de registros de auditoría

LOGALTY revisa sus logs cuando se produce una alerta del sistema motivada por la existencia de algún incidente.

El procesamiento de los registros de auditoría consiste en una revisión de los registros que incluye la verificación de que éstos no han sido manipulados, una breve inspección de todas las entradas de registro y una investigación más profunda de cualquier alerta o irregularidad en los registros. Las acciones realizadas a partir de la revisión de auditoría están documentadas.

LOGALTY mantiene un sistema que permite garantizar:

- Espacio suficiente para el almacenamiento de logs
- Que los ficheros de logs no se reescriben.
- Que la información que se guarda incluye como mínimo: tipo de evento, fecha y hora, usuario que ejecuta el evento y resultado de la operación.
- Los ficheros de logs se guardarán en ficheros estructurados susceptibles de incorporar en una BBDD para su posterior exploración.

5.4.3 Período de conservación de registros de auditoría

LOGALTY almacena la información de los logs al menos durante 15 años.

5.4.4 Protección de los registros de auditoría

Los logs de los sistemas:

- Están protegidos de manipulación, borrado o eliminación mediante la firma de los ficheros que los contienen.
- Son almacenados en dispositivos ignífugos.
- Se protege su disponibilidad mediante el almacén en instalaciones externas al centro donde se ubica la AC.

El acceso a los ficheros de logs está reservado sólo a las personas autorizadas. Asimismo, los dispositivos son manejados en todo momento por personal autorizado.

Existe un procedimiento interno donde se detallan los procesos de gestión de los dispositivos que contienen datos de logs de auditoría.

5.4.5 Procedimientos de copia de respaldo

LOGALTY dispone de un procedimiento adecuado de backup de manera que, en caso de pérdida o destrucción de archivos relevantes, estén disponibles en un periodo corto de tiempo las correspondientes copias de backup de los logs.

LOGALTY tiene implementado un procedimiento de backup seguro de los logs de auditoría, realizando semanalmente una copia de todos los logs.

5.4.6 Localización del sistema de acumulación de registros de auditoría

La información de la auditoría de eventos es recogida automáticamente por el sistema operativo, las comunicaciones de red y por el software de gestión de certificados, además de por los datos manualmente generados, que serán almacenados por el personal debidamente autorizado. Todo ello compone el sistema de acumulación de registros de auditoría.

5.4.7 Notificación del evento de auditoría al causante del evento

Cuando el sistema de acumulación de registros de auditoría registra un evento, no es preciso enviar una notificación al individuo, organización, dispositivo o aplicación que causó el evento.

5.4.8 Análisis de vulnerabilidades

Toda la infraestructura es objeto de una evaluación de vulnerabilidades al menos cada tres meses (con pruebas de penetración al menos una vez al año) y siempre que una parte crítica de la infraestructura

se vea afectada. Esta evaluación es llevada a cabo por proveedores externos con personal cualificado, y cubre los siguientes elementos:

- SAST o pruebas de caja blanca: se detectan vulnerabilidades en el código fuente a lo largo de su ciclo de vida y antes de pasar a producción.
- DAST o pruebas de caja gris y negra: análisis de vulnerabilidades sobre el software en producción.
- Pentesting: sobre las URLs externas, redes y sistemas de información.
- Análisis de vulnerabilidades de los sistemas de información y parcheo.

Las vulnerabilidades detectadas se tratarán según los procedimientos existentes, los cuales incluyen clasificación, categorización, identificación y aplicación de parches. Serán priorizadas en función de su criticidad, estableciéndose un plazo máximo de resolución de 48 horas para las categorizadas como críticas.

5.5 Archivos de informaciones

5.5.1 Tipos de registros archivados

LOGALTY garantiza que toda la información relativa a los certificados se conserva durante un período de tiempo apropiado, según lo establecido en la sección 5.7.1 de esta política.

Los siguientes documentos implicados en el ciclo de vida del certificado son almacenados por LOGALTY (o por las entidades de registro):

- Todos los datos de auditoría de sistema (PKI, TSA y OCSP).
- Todos los datos relativos a los certificados, incluyendo los contratos con los firmantes y los datos relativos a su identificación y su ubicación
- Solicitudes de emisión y revocación de certificados, incluidos todos los informes relativos al proceso de revocación.
- Todas aquellas elecciones específicas que el firmante o el suscriptor disponga durante el acuerdo de suscripción .

- Tipo de documento presentado en la solicitud del certificado.
- Identidad de la Entidad de Registro que acepta la solicitud de certificado.
- Número de identificación único proporcionado por el documento anterior.
- Todos los certificados emitidos o publicados.
- CRLs emitidas o registros del estado de los certificados generados.
- El historial de claves generadas.
- Las comunicaciones entre los elementos de la PKI.
- Políticas y Prácticas de Certificación
- Todos los datos de auditoría identificados en la sección 4
- Información de solicitudes de certificación.
- Documentación aportada para justificar las solicitudes de certificación.
- Información del ciclo de vida del certificado.

LOGALTY es responsable del correcto archivo de todo este material.

5.5.2 Período de conservación de registros

LOGALTY archiva los registros especificados anteriormente durante 15 años.

5.5.3 Protección del archivo

LOGALTY protege el archivo de forma que sólo personas debidamente autorizadas puedan obtener acceso al mismo. El archivo está protegido contra visualización, modificación, borrado o cualquier otra manipulación mediante su almacenamiento en un sistema fiable.

LOGALTY asegura la correcta protección de los archivos mediante la asignación de personal cualificado para su tratamiento y el almacenamiento en cajas de seguridad ignífugas e instalaciones externas.

5.5.4 Procedimientos de copia de respaldo

LOGALTY como mínimo realiza copias de respaldo incrementales diarias de todos sus documentos electrónicos y realiza copias de respaldo completas semanalmente para casos de recuperación de datos.

Además, LOGALTY (o las organizaciones que realizan la función de registro) guarda copia de los documentos en papel en un lugar seguro diferente de las instalaciones de la propia Entidad de certificación.

5.5.5 Requisitos de sellado de fecha y hora

Los registros están fechados con una fuente fiable vía NTP con conexión a Fujitsu.

Los servidores de LOGALTY están conectados a una dos ips para la sincronización horaria, siendo uno de ellos el servidor hora.roa.es oficial de Stratum 1. La hora empleada para registrar los sucesos del registro de auditoría deberá ser sincronizada con la UTC, como mínimo, una vez al día.

No es necesario que esta información se encuentre firmada digitalmente.

5.5.6 Localización del sistema de archivo

LOGALTY dispone de un sistema centralizado de recogida de información de la actividad de los equipos implicados en el servicio de gestión de certificados.

5.5.7 Procedimientos de obtención y verificación de información de archivo

LOGALTY dispone de un procedimiento donde se describe el proceso para verificar que la información archivada es correcta y accesible.

5.6 Renovación de claves

Con anterioridad a que el uso de la clave privada de la AC caduque, será realizado un cambio de claves. La antigua AC y su clave privada solo se usarán para la firma de CRLs mientras existan certificados activos emitidos por dicha AC. Se generará una nueva AC con una clave privada nueva y un nuevo DN.

El cambio de claves del suscriptor es realizado mediante la realización de un nuevo proceso de emisión.

5.7 Compromiso de claves y recuperación de desastre

5.7.1 Procedimientos de gestión de incidencias y compromisos

Son almacenadas copias de seguridad de la siguiente información, que se ponen a disposición en caso de compromiso o desastre: datos técnicos de solicitud de certificados, datos de auditoría y registros de base de datos de todos los certificados emitidos.

Las copias de seguridad de las claves privadas de LOGALTY son generadas y mantenidas de acuerdo con lo establecido en la sección 6.2.4

5.7.2 Corrupción de recursos, aplicaciones o datos

Cuando acontezca un evento de corrupción de recursos, aplicaciones o datos, se comunicará la incidencia a seguridad, y se iniciarán los procedimientos de gestión oportunos, que contemplan escalado, investigación y respuesta al incidente. Si resulta necesario, se iniciarán los procedimientos de compromiso de claves o de recuperación de desastres de LOGALTY.

5.7.3 Compromiso de la clave privada de la entidad

En caso de sospecha o conocimiento del compromiso de LOGALTY, se activarán los procedimientos de compromiso de claves, documentados como parte de los planes de contingencia de la organización: Tratamiento del compromiso de clave privada de la CA. Dicho procedimiento contempla:

- Notificación de la incidencia al órgano de supervisión.
- Emisión inmediata de una CRL nueva y publicarla.
- Recomendación a los usuarios de los servicios de certificación que incorporen sellos de tiempo de archivo a todas las firmas o sellos, por defecto.
- Sin perjuicio de lo anterior, se procede a las actuaciones referidas a la información de revocación previstas para el cese de la autoridad de certificación, antes de la revocación del

certificado de la CA Subordinada.

- Advertencia a todos los suscriptores, de forma individualizada, y a las terceras partes interesadas, mediante publicación en la página web de Logalty y, posiblemente, a través de algún medio de comunicación pública.

5.7.4 Continuidad del negocio después de un desastre

LOGALTY dispone de un sistema de gestión de la continuidad del negocio certificado ISO 22301, que reúne el conjunto de procedimientos de respuesta a los eventos disruptivos que puedan poner en peligro la continuidad del servicio. Dichos procedimientos dotan de un marco organizado para la toma de las decisiones necesarias a ser tomadas inmediatamente después de ocurrido un siniestro total o parcial que genera interrupción en las infraestructuras, comunicaciones, sistemas, instalaciones o el personal que presta el servicio. Cubren actividades y aspectos para todas las fases, dotando de instrumentos y pautas para:

- Notificación del daño
- Evaluación inicial del daño e impacto asociado.
- Declaración de desastre.
- Actividades de recuperación de los servicios.
- Actividades de restauración y vuelta a la normalidad.

Este Plan define asimismo los equipos de trabajo, su composición y sus interdependencias, en función del rol que tendrán en todo el proceso de respuesta y contención de un desastre. Estos equipos incorporan personal del proveedor de TI, el cual tendrá un papel esencial en las actividades de contención del desastre.

Las actividades del plan de recuperación ante desastres se diseñan acorde a los parámetros de continuidad (RTO, RPO) definidos para los servicios.

Adicionalmente a lo anterior, se establecen procedimientos de entrenamiento, prueba y mantenimiento de este plan. Todo el personal de Logalty y del proveedor implicado, se entrena en el proceso de

recuperación del Plan de Contingencia. Esto es particularmente importante dado que los procedimientos son significativamente diferentes de las operaciones normales y se requiere un desempeño excelente para garantizar la restauración de los equipos y sistemas.

Como mínimo una vez al año, o cuando haya cambios significativos, se llevarán a cabo pruebas exhaustivas de los procedimientos del plan.

Para garantizar de forma proactiva la continuidad del servicio, Logalty cuenta con una estructura redundada en dos CPD's en configuración activo-activo, lo que permite un nivel de redundancia adecuado para garantizar los niveles de servicio. En caso de producirse un desastre que llegase a inhabilitar uno de ellos, el otro CPD puede asumir la carga de forma completa incluso bajo condiciones de alta carga de demanda.

Ambos CPD's se encuentran ubicados en áreas dedicadas de dos prestadores de servicios de alojamiento con nivel de disponibilidad equivalente a Tier III, así como en posesión de las principales certificaciones de gestión de la seguridad y del servicio (ISO 27001, ISO 20000). Las áreas dedicadas a los servicios de Logalty cuentan con los mayores niveles de seguridad, tanto ambiental como de control de acceso.

De forma adicional, Logalty mantiene una lista actualizada del personal que sustenta las funciones críticas, así como el mínimo número de personas que tienen que estar disponibles para garantizar su continuidad, ha determinado los backups existentes para los perfiles críticos y adoptado las medidas necesarias para garantizar que estos perfiles pueden asumir este rol, a través de sesiones de transferencia de conocimiento, traspaso de procedimientos operativos, custodia distribuida de credenciales con control dual para identificadores con alto nivel de privilegio, entre otros.

Existen oficinas en Madrid y Barcelona que permiten realojar a los perfiles clave en caso de que las instalaciones principales desde las que se prestan los servicios no estuvieran disponibles. Asimismo, existen mecanismos de teletrabajo que permiten acceder a los sistemas productivos de forma remota.

5.8 Terminación del servicio

En caso de cese de los servicios, Logalty sigue siendo responsable de mantener accesible durante un período de tiempo, toda la información pertinente referente a los datos expedidos y recibidos como parte de la prestación de sus servicios de confianza, en particular al objeto de que sirvan de prueba en

los procedimientos legales y para garantizar la continuidad del servicio. Para dar satisfacción a esta responsabilidad, Logalty ha desarrollado un plan de cese que ordena las medidas a tomar en caso del cese de la empresa como prestadora de servicios de confianza, y también en caso de cierre de alguno de los servicios de confianza que presta. Este plan cubre:

- Provisión de fondos: Logalty aprovisionará la cantidad necesaria para cubrir los costes mediante una reserva voluntaria a efectos de contingencia de cierre.
- Informará a todos Firmantes/Suscriptores, Terceros que confían y otras AC's con los cuales tenga acuerdos u otro tipo de relación del cese con una anticipación mínima de 6 meses.
- Revocará toda autorización a entidades subcontratadas para actuar en nombre de la AC en el procedimiento de emisión de certificados.
- En caso de cese de la figura jurídica, transferirá sus obligaciones relativas al mantenimiento de la información del registro y de los logs durante el periodo de tiempo indicado a los suscriptores y usuarios.
- Destruirá o deshabilitará para su uso las claves privadas de la AC.
- Comunicará al Organismo supervisor, con una antelación mínima de 2 meses, el cese de su actividad.

Comunicará, también al Organismo supervisor, la apertura de cualquier proceso concursal que se siga contra LOGALTY, así como cualquier otra circunstancia relevante que pueda impedir la continuación de la actividad.

6 Controles de seguridad técnica

LOGALTY emplea sistemas y productos fiables, protegidos contra toda alteración y que garantizan la seguridad técnica y criptográfica de los procesos de certificación a los que sirven de soporte.

6.1 Generación e instalación del par de claves

6.1.1 Generación del par de claves

El par de claves de la entidad de certificación intermedia "LOGALTY QUALIFIED CA G2" es creado por la

entidad de certificación raíz “LOGALTY CA ROOT 03” de acuerdo con los procedimientos de ceremonia de LOGALTY, dentro del perímetro de alta seguridad destinado a esta tarea.

Las actividades realizadas durante la ceremonia de generación de claves han sido registradas, fechadas y firmadas por todos los individuos participantes en la misma, con la presencia de un Auditor. Dichos registros son custodiados a efectos de auditoría y seguimiento durante un período apropiado determinado por LOGALTY.

Para la generación de la clave de las entidades de certificación raíz e intermedia se utilizan dispositivos con las certificaciones FIPS 140-2 nivel 3.

Entidad Raíz “LOGALTY CA ROOT 03”	**4.096 bits**	**25 años**
CA intermedia “Logalty Qualified CA G2”	4.096 bits	13 años
Certificados de entidad final	2.048 bits	Dentro de los valores establecidos por las normas y legislación vigente
Unidad de Sello de Tiempo	4.096 bits	5 años

Más información en la ubicación: https://www.logalty.com/certificateauthority/

6.1.1.1 Generación del par de claves del firmante

Las claves del firmante son creadas por él mismo mediante software o hardware autorizados por LOGALTY.

Las claves son generadas usando el algoritmo de clave pública RSA, con una longitud mínima de 2048 bits.

6.1.2 Envío de la clave privada al firmante

En la emisión de certificados de sellos electrónicos de TSU las claves se gestionan internamente en los equipos existentes.

6.1.3 Envío de la clave pública al emisor del certificado

No hay remisión de la clave pública al prestador de servicios de certificación.

6.1.4 Distribución de la clave pública del prestador de servicios de certificación

Las claves de LOGALTY son comunicadas a los terceros que confían en certificados, asegurando la integridad de la clave y autenticando su origen, mediante su publicación en el depósito .

El certificado de las CA raíz y subordinadas estarán a disposición de los usuarios en la página Web de LOGALTY.

6.1.5 Tamaños de claves

La longitud de las claves de la Entidad de Certificación raíz o subordinadas es de 4096 bits como mínimo.

Las claves de los certificados de TSU serán de 3072 bits como mínimo.

6.1.6 Generación de parámetros de clave pública

La clave pública de la CA Root, de la CA subordinadas y de los certificados de los suscriptores está codificada de acuerdo con RFC 5280.

6.1.7 Comprobación de calidad de parámetros de clave pública

Las CA emplean los siguientes parámetros criptográficos:

- Longitud del Módulo RSA = 4096.
- Funciones criptográficas de Resumen: SHA512WithRSA.

6.1.8 Propósitos de uso de claves

Los usos de las claves para los certificados de las CA son exclusivamente para la firma de certificados y de CRLs.

Los usos de las claves para los certificados de entidad final para sellos electrónicos son exclusivamente

para la firma digital y el no repudio.

Otros usos están prohibidos.

6.2 Protección de la clave privada y controles de los módulos criptográficos

6.2.1 Estándares de módulos criptográficos

En relación con los módulos que gestionan claves de LOGALTY y de los suscriptores de certificados de firma electrónica, se asegura el nivel exigido por los estándares indicados en las secciones anteriores.

Los módulos criptográficos se someten a los controles de ingeniería previstos en las normas indicadas a lo largo de esta sección.

Los algoritmos de generación de claves empleados se aceptan comúnmente para el uso de la clave a que están destinados.

Todas las operaciones criptográficas de LOGALTY son realizadas en módulos con las certificaciones FIPS 140 level 3 y/o Common Criteria EAL 4+ alineado con las exigencias de CEN/TS 410 261.

6.2.2 Control por más de una persona (n de m) sobre la clave privada

Se requiere un control multi-persona para la activación de la clave privada de la AC. En el caso de esta DPC, en concreto existe una política de **2 de 3** personas para la activación de las claves.

Los dispositivos criptográficos se encuentran protegidos físicamente tal y como se determina en este documento.

Las instalaciones de la AC están provistas de sistemas de monitorización continua y alarmas para detectar, registrar y poder actuar de manera inmediata ante un intento de acceso a sus recursos no autorizado y / o irregular.

6.2.3 Depósito de la clave privada

LOGALTY no almacena copias de las claves privadas de los firmantes.

6.2.4 Copia de respaldo de la clave privada

LOGALTY realiza copia de backup de las claves privadas de las CA que hacen posible su recuperación en caso de desastre, de pérdida o deterioro de estas. Tanto la generación de la copia como la recuperación de ésta necesitan al menos de la participación de dos personas autorizadas según los roles de confianza.

Estos ficheros de recuperación se almacenan en armarios ignífugos. Las claves del suscriptor en software pueden ser almacenadas para su posible recuperación en caso de contingencia, en un dispositivo de almacenamiento externo separado de la clave de instalación.

Las claves del firmante en hardware no se pueden copiar ya que no pueden salir del dispositivo criptográfico.

6.2.5 Archivo de la clave privada

Las claves privadas de las AC son archivadas por un periodo de **10 años** después de la emisión del último certificado. Se almacenarán en archivos ignífugos seguros. Al menos será necesaria la colaboración de dos personas para recuperar la clave privada de las AC en el dispositivo criptográfico inicial.

6.2.6 Introducción de la clave privada en el módulo criptográfico

Las claves privadas se generan directamente en los módulos criptográficos de producción de LOGALTY.

6.2.7 Almacenamiento de la clave privada en el módulo criptográfico

Las claves privadas de la Entidad de Certificación se almacenan cifradas en los módulos criptográficos de producción de LOGALTY.

6.2.8 Método de activación de la clave privada

La clave privada de LOGALTY se activa mediante la ejecución del correspondiente procedimiento de inicio seguro del módulo criptográfico, por las personas indicadas en la sección 6.2.2.

Las claves de la AC se activan por un proceso de m de n (2 de 3)

La activación de las claves privadas de la AC Intermedia es gestionada con el mismo proceso de m de n que las claves de la AC.

6.2.9 Método de desactivación de la clave privada

Para la desactivación de la clave privada de LOGALTY se seguirán los pasos descritos en el manual del administrador del equipo criptográfico correspondiente, así como en el plan de cese.

6.2.10 Método de destrucción de la clave privada

Con anterioridad a la destrucción de las claves, se emitirá una revocación del certificado de las claves públicas asociadas a las mismas.

Se destruirán físicamente o reiniciarán a bajo nivel los dispositivos que tengan almacenada cualquier parte de las claves privadas de LOGALTY que deban ser objeto de destrucción. Para la eliminación se seguirán los pasos descritos en el manual del administrador del equipo criptográfico, así como en el plan de cese.

Finalmente se destruirán de forma segura las copias de seguridad.

6.2.11 Clasificación de módulos criptográficos

Ver la sección 6.2.1.

6.3 Otros aspectos de gestión del par de claves

6.3.1 Archivo de la clave pública

LOGALTY archiva sus claves públicas de forma rutinaria, de acuerdo con lo establecido en la sección 5.5

de este documento.

6.3.2 Períodos de utilización de las claves pública y privada

Los periodos de utilización de las claves son determinados por la duración del certificado, transcurrido el cual no pueden continuar utilizándose.

6.4 Datos de activación

6.4.1 Generación e instalación de datos de activación

Los datos de activación de los dispositivos que protegen las claves privadas de LOGALTY son generados de acuerdo con lo establecido en la sección 6.2.2 y los procedimientos de ceremonia de claves.

La creación y distribución de dichos dispositivos es registrada. Asimismo, LOGALTY genera de forma segura los datos de activación.

6.4.2 Protección de datos de activación

Los datos de activación de los dispositivos que protegen las claves privadas de las Autoridades de certificación raíz y subordinadas, son protegidos por los poseedores de las tarjetas de administradores de los módulos criptográficos, según consta en el documento de ceremonia de claves.

6.5 Controles de seguridad informática

LOGALTY emplea sistemas fiables para ofrecer sus servicios de certificación. LOGALTY ha realizado controles y auditorías informáticas a fin de establecer una gestión de sus activos informáticos adecuados con el nivel de seguridad requerido en la gestión de sistemas de certificación electrónica.

Respecto a la seguridad de la información, LOGALTY sigue el esquema de certificación sobre sistemas de gestión de la información ISO 27001.

Los equipos usados son inicialmente configurados con los perfiles de seguridad adecuados por parte del

personal de sistemas de LOGALTY, en los siguientes aspectos:

- Configuración de seguridad del sistema operativo.
- Configuración de seguridad de las aplicaciones.
- Dimensionamiento correcto del sistema.
- Configuración de Usuarios y permisos.
- Configuración de eventos de Log.
- Plan de backup y recuperación.
- Configuración de antivirus.
- Requerimientos de tráfico de red.

6.5.1 Requisitos técnicos específicos de seguridad informática

Cada servidor de LOGALTY incluye las siguientes funcionalidades:

- Control de acceso a los servicios de la SubCA y gestión de privilegios.
- Imposición de separación de tareas para la gestión de privilegios.
- Identificación y autenticación de roles asociados a identidades.
- Archivo del historial del suscriptor y la SubCA y datos de auditoría.
- Auditoría de eventos relativos a la seguridad.
- Autodiagnóstico de seguridad relacionado con los servicios de la SubCA.
- Mecanismos de recuperación de claves y del sistema de la SubCA.

Las funcionalidades expuestas son realizadas mediante una combinación de sistema operativo, software de PKI, protección física y procedimientos.

La verificación de la certificación de los dispositivos cualificados (QSCD) se realiza durante todo el período de validez del certificado. Si el QSCD perdiera su certificación como tal, LOGALTY avisará a los

usuarios de este hecho y ejecutará un plan de renovación de estos dispositivos.

6.5.2 Evaluación del nivel de seguridad informática

Las aplicaciones de autoridad de certificación y de registro empleadas por LOGALTY son fiables.

6.6 Controles de seguridad del ciclo de vida

6.6.1 Controles de desarrollo de sistemas

Las aplicaciones son desarrolladas e implementadas por LOGALTY de acuerdo con estándares de desarrollo y control de cambios.

Las aplicaciones disponen de métodos para la verificación de la integridad y autenticidad, así como de la corrección de la versión a emplear.

6.6.2 Controles de gestión de seguridad

LOGALTY desarrolla las actividades precisas para la formación y concienciación de los empleados en materia de seguridad. Los materiales empleados para la formación y los documentos descriptivos de los procesos son actualizados después de su aprobación para la gestión de la seguridad. En la realización de esta función dispone de un plan de formación anual. LOGALTY exige mediante contrato, las medidas de seguridad equivalentes a cualquier proveedor externo implicado en las labores de certificación.

6.6.2.1 Clasificación y gestión de información y bienes

LOGALTY mantiene un inventario de activos y documentación y un procedimiento para la gestión de este material para garantizar su uso.

La política de seguridad de LOGALTY detalla los procedimientos de gestión de la información donde se clasifica según su nivel de confidencialidad.

Los documentos están catalogados en tres niveles: SIN CLASIFICAR, USO INTERNO, y CONFIDENCIAL.

6.6.2.2 Operaciones de gestión

LOGALTY dispone de un procedimiento de gestión y respuesta de incidencias, mediante la implementación de un sistema de alertas y la generación de reportes periódicos (Logalty ProcIT- DSS02 Gestión de peticiones e incidencias v2r1).

En el documento de seguridad de LOGALTY se desarrolla en detalle el proceso de gestión de incidencias.

LOGALTY tiene documentado todo el procedimiento relativo a las funciones y responsabilidades del personal implicado en el control y manipulación de elementos contenidos en el proceso de certificación.

6.6.2.3 Tratamiento de los soportes y seguridad

Todos los soportes son tratados de forma segura de acuerdo con los requisitos de la clasificación de la información. Los soportes que contengan datos sensibles son destruidos de manera segura si no van a volver a ser requeridos.

6.6.2.4 Planificación del sistema

El departamento de Sistemas de LOGALTY mantiene un registro de las capacidades de los equipos. Juntamente con la aplicación de control de recursos de cada sistema se puede prever un posible redimensionamiento.

6.6.2.5 Reportes de incidencias y respuesta

LOGALTY dispone de un procedimiento para el seguimiento de incidencias y su resolución donde se registran las respuestas y una evaluación económica que supone la resolución de la incidencia.

6.6.2.6 Procedimientos operacionales y responsabilidades

LOGALTY define actividades, asignadas a personas con un rol de confianza, distintas de las personas encargadas de realizar las operaciones cotidianas que no tienen carácter de confidencialidad.

6.6.2.7 Gestión del sistema de acceso

LOGALTY realiza todos los esfuerzos que razonablemente están a su alcance para confirmar que el sistema de acceso está limitado a las personas autorizadas.

En particular:

- AC General
    - Se dispone de controles basados en firewalls, antivirus e IDS en alta disponibilidad.
    - Los datos sensibles son protegidos mediante técnicas criptográficas o controles de acceso con identificación fuerte.
    - LOGALTY dispone de un procedimiento documentado de gestión de altas y bajas de usuarios y política de acceso detallado en su política de seguridad.
    - LOGALTY dispone de procedimientos para asegurar que las operaciones se realizan respetando la política de roles.
    - Cada persona tiene asociado un rol para realizar las operaciones de certificación.
    - El personal de LOGALTY es responsable de sus actos mediante el compromiso de confidencialidad firmado con la empresa.

6.6.2.8 Generación del certificado

La autenticación para el proceso de emisión se realiza mediante un sistema m de n operadores para la activación de la clave privada de LOGALTY.

6.6.2.9 Gestión de la revocación

La revocación se realizará mediante autenticación fuerte a las aplicaciones de un administrador autorizado. Los sistemas de logs generarán las pruebas que garantizan el no repudio de la acción realizada por el administrador de LOGALTY.

6.6.2.10 Estado de la revocación

La aplicación del estado de la revocación dispone de un control de acceso basado en la autenticación con certificados o con doble factor de identificación para evitar el intento de modificación de la información del estado de la revocación.

6.6.2.11 Gestión del ciclo de vida del hardware criptográfico

LOGALTY se asegura que el hardware criptográfico usado para la firma de certificados no se manipula durante su transporte mediante la inspección del material entregado.

El hardware criptográfico se traslada sobre soportes preparados para evitar cualquier manipulación.

LOGALTY registra toda la información pertinente del dispositivo para añadir al catálogo de activos. El uso del hardware criptográfico de firma de certificados requiere el uso de al menos dos empleados de confianza.

LOGALTY realiza test de pruebas periódicas para asegurar el correcto funcionamiento del dispositivo.

El dispositivo hardware criptográfico solo es manipulado por personal confiable.

La clave privada de firma de LOGALTY almacenada en el hardware criptográfico se eliminará una vez se haya retirado el dispositivo.

La configuración del sistema de LOGALTY, así como sus modificaciones y actualizaciones son documentadas y controladas.

LOGALTY posee un contrato de mantenimiento del dispositivo. Los cambios o actualizaciones son autorizados por el responsable de seguridad y quedan reflejados en las actas de trabajo

correspondientes. Estas configuraciones se realizan al menos por dos personas confiables.

6.7 Controles de seguridad de red

LOGALTY protege el acceso físico a los dispositivos de gestión de red, y dispone de una arquitectura que ordena el tráfico generado basándose en sus características de seguridad, creando secciones de red claramente definidas. Esta división se realiza mediante el uso de cortafuegos.

La información confidencial que se transfiere por redes no seguras se realiza de forma cifrada mediante uso de protocolos SSL o del sistema VPN con autenticación por doble factor.

6.8 Fuentes de Tiempo

LOGALTY dispone de un Reloj Atómico de Rubidio con una precisión garantizada por el fabricante de un desfase inferior a 1 microsegundo al día. El reloj atómico se sincroniza por GPS, permitiendo un nivel de confianza de STRATUM 1. Se añade también una sincronización de tiempos con el ROA mediante el protocolo NTP a través de internet.

7 Perfiles de certificados, CRL y OCSP

7.1 Perfil de certificado

Todos los certificados cualificados emitidos bajo esta política cumplen el estándar X.509 versión 3, RFC 5280 y las siguientes normas:

- ETSI EN 319 422 para la definición de los perfiles de los sellos de tiempo.

7.1.1 Número de versión

LOGALTY emite certificados X.509 Versión 3

7.1.2 Extensiones del certificado

Las extensiones de los certificados se encuentran detalladas en los documentos de perfiles que son

accesibles desde la página web de LOGALTY https://www.logalty.com/certificateauthority/ De esta forma se permite mantener unas versiones más estables de la DPC desligándolas de los frecuentes ajustes en los perfiles.

7.1.3 Identificadores de objeto (OID) de los algoritmos

El identificador de objeto del algoritmo de firma es:

- 1.2.840.113549.1.1.11 sha256WithRSAEncryption
- 1.2.840.10045.3.1.7 prime256v1 (ANSI X9.62 named elliptic curve) para TimeStamping

El identificador de objeto del algoritmo de la clave pública es:

- 1.2.840.113549.1.1.1 rsaEncryption
- 1.2.840.10045.2.1 ecPublicKey (ANSI X9.62 public key type) para TimeStamping

7.1.4 Formato de Nombres

Los certificados deberán contener las informaciones que resulten necesarias para su uso, según determine la correspondiente política. La codificación de los certificados sigue las recomendaciones de la RFC 5280 de la forma que se describe en el punto 3.1.1 de este documento.

7.1.5 Restricción de los nombres

Los nombres contenidos en los certificados están restringidos a “Distinguished Names” X.500, que

son únicos y no ambiguos.

Adicionalmente se pueden establecer restricciones de nombres en relación con los certificados en la correspondiente política de autenticación, firma electrónica, cifrado o evidencia electrónica, siempre que las mismas resulten objetivas, proporcionadas, transparentes y no discriminatorias.

7.1.6 Identificador de objeto (OID) de los tipos de certificados

Todos los certificados incluyen un identificador de política de certificados bajo la que han sido emitidos, de acuerdo con la estructura indicada en el punto 1.2.1.

7.1.7 Uso de la extensión "Policy Constraints"

No se usa en los certificados raíz.

7.1.8 Sintaxis y semántica de los calificadores de política

Se incluyen dos campos:

- CPS Pointer: la URL donde se encuentra el documento de prácticas de confianza.
- User notice: Texto para que el usuario pueda visualizar la información del certificado.

7.1.9 Tratamiento semántico para la extensión crítica "certificate policy"

Se identifica la política asociada al certificado por parte de la jerarquía de LOGALTY y los campos indicados en el apartado anterior.

7.2 Perfil de la lista de revocación de certificados

Las CRL emitidas por LOGALTY son de la versión 2.

7.3 Perfil de OCSP

Según el estándar IETF RFC 6960.

8 Auditoría de conformidad

Logalty realiza auditorías de conformidad para asegurar el cumplimiento y adecuación con las políticas, normativas, planes y procedimientos de seguridad del sistema de gestión de seguridad de la información. Dichas auditorías, su alcance y periodicidad, se describen en el correspondiente Plan de Auditoría de Logalty, que se actualiza de forma anual. Como resultado de estas se elaboran planes de acciones correctivas como respuesta a las no conformidades y desviaciones detectadas.

Logalty realiza auditorías de conformidad del Reglamento eIDAS por medio de evaluaciones de conformidad anuales sobre los siguientes servicios:

- Servicio de expedición de sellos electrónicos cualificados de tiempo

Los controles para la realización de las auditorías de cumplimiento se basan en las siguientes guías de referencia:

- ETSI EN 319 401 General Policy Requirements for Trust Service Providers
- ETSI EN 319 421 Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
- ETSI EN 319 422 Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles

Logalty realiza las pertinentes auditorías sobre protección de datos con periodicidad bianual.

8.1 Frecuencia de la auditoría de conformidad

LOGALTY realiza evaluaciones de conformidad eIDAS con carácter bienal, además de revisiones anuales.

LOGALTY realiza auditorías relativas a la protección de los datos personales bianuales, con revisiones anuales.

LOGALTY realiza análisis de vulnerabilidades cada 3 meses. LOGALTY realiza un análisis de intrusión cada 6 meses.

8.2 Identificación y cualificación del auditor

Las auditorías son realizadas por una firma de auditoría independiente externa que demuestra competencia técnica y experiencia en seguridad informática, en seguridad de sistemas de información y en auditorías de conformidad de servicios de certificación de clave pública, y los elementos relacionados.

El auditor responsable de la evaluación de conformidad eIDAS debe estar acreditado según ETSI EN 319 403.

8.3 Relación del auditor con la entidad auditada

Los auditores internos o externos responsables de ejecutar las auditorías son independientes funcionalmente del servicio de producción objeto de auditoría.

8.4 Listado de elementos objeto de auditoría

La auditoría verifica respecto a LOGALTY:

- Que la entidad tiene un sistema de gestión que garantiza la calidad del servicio prestado.
- Que la entidad cumple con los requerimientos de la DPC y otra documentación vinculada con la emisión de los distintos certificados digitales, bajo el marco del Reglamento (UE) 910/2014 del parlamento europeo y del consejo de 23 de julio de 2014.
- Que la DPC y demás documentación jurídica vinculada, se ajusta a lo acordado por LOGALTY y con lo establecido en la normativa vigente.
- Que la entidad gestione de forma adecuada sus sistemas de información.

En particular, los elementos objeto de auditoría serán los siguientes:

- Procesos de la AC, ARs y elementos relacionados.
- Sistemas de información.
- Protección del centro de proceso de datos.
- Documentación asociada.

8.5 Acciones que emprender como resultado de una falta de conformidad

Una vez recibido por la dirección el informe de la auditoría de cumplimiento realizada, se analizan, con la firma que ha ejecutado la auditoría, las deficiencias encontradas y desarrolla y ejecuta un plan correctivo que solvente dichas deficiencias.

Si la Entidad de Certificación de LOGALTY es incapaz de desarrollar y/o ejecutar dicho plan o si las deficiencias encontradas suponen una amenaza inmediata para la seguridad o integridad del sistema, deberá comunicarlo inmediatamente al Comité de Seguridad de la Información de LOGALTY que podrá ejecutar las siguientes acciones:

- Cesar las operaciones transitoriamente.
- Revocar la clave de la AC y regenerar la infraestructura.
- Terminar el servicio de la AC.
- Otras acciones complementarias que resulten necesarias.

8.6 Tratamiento de los informes de auditoría

Los informes de resultados de auditoría se entregan al Comité de Seguridad de la Información de LOGALTY en un plazo máximo de 15 días tras la ejecución de la auditoría, para su análisis y tratamiento.

Si a causa de la auditoría realizada fuera necesaria la revocación de certificados, este informe servirá como justificante de dicha revocación.

9 Requisitos comerciales y legales

9.1 Tarifas

9.1.1 Tarifa de emisión o renovación de certificados

LOGALTY puede establecer una tarifa por la emisión o por la renovación de los certificados, de la que, en su caso, se informará oportunamente a los suscriptores.

9.1.2 Tarifa de acceso a certificados

LOGALTY no ha establecido ninguna tarifa por el acceso a los certificados.

9.1.3 Tarifa de acceso a información de estado de certificado

LOGALTY no ha establecido ninguna tarifa por el acceso a la información de estado de certificados.

9.1.4 Tarifas de otros servicios

Sin estipulación.

9.1.5 Política de reintegro

Sin estipulación.

9.2 Responsabilidad financiera

LOGALTY dispone de recursos económicos suficientes para mantener sus operaciones y cumplir sus obligaciones, así como para afrontar el riesgo de la responsabilidad por daños y perjuicios, según lo establecido en la ETSI EN 319 401-1 7.12, en relación con la gestión de la finalización de los servicios y plan de cese.

9.2.1 Cobertura de seguro

LOGALTY dispone de una garantía de cobertura de su responsabilidad civil suficiente, mediante un seguro de responsabilidad civil profesional que cumple con lo indicado en el artículo 24.2.c) del Reglamento (UE) 910/2014, y con el artículo 9.3.b) de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, con un mínimo asegurado de 4.000.000 de euros.

9.2.2 Otros activos

Sin estipulación.

9.2.3 Cobertura de seguro para suscriptores y terceros que confían en certificados

LOGALTY dispone de una garantía de cobertura de su responsabilidad civil suficiente, mediante un seguro de responsabilidad civil profesional que cumple con lo indicado en el artículo 24.2.c) del Reglamento (UE) 910/2014, y con el artículo 9.3.b) de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, con un mínimo asegurado de 4.000.000 de euros.

9.3 Confidencialidad de la información

9.3.1 Informaciones confidenciales

Las siguientes informaciones son mantenidas confidencialmente por LOGALTY:

- Solicitudes de certificados, aprobadas o denegadas, así como toda otra información personal obtenida para la expedición y mantenimiento de certificados, excepto las informaciones indicadas en la sección siguiente.
- Claves privadas generadas y/o almacenadas por el prestador de servicios de certificación.
- Registros de transacciones, incluyendo los registros completos y los registros de auditoría de las transacciones.
- Registros de auditoría interna y externa, creados y/o mantenidos por la Entidad de Certificación y sus auditores.
- Planes de continuidad de negocio y de emergencia.
- Política y planes de seguridad.
- Documentación de operaciones y restantes planes de operación, como archivo, monitorización y otros análogos.

- Toda otra información identificada como “Confidencial”.

9.3.2 Informaciones no confidenciales

La siguiente información se considera no confidencial, cuando se haya consentido su publicación por el sujeto identificado:

- Los certificados emitidos o en trámite de emisión.
- La vinculación del suscriptor a un certificado emitido por la Entidad de Certificación.
- El nombre y los apellidos de la persona física identificada en el certificado, así como cualquiera otra circunstancia o dato personal del titular, en el supuesto de que sea significativa en función de la finalidad del certificado.
- La dirección de correo electrónico de la persona física identificada en el certificado, o la dirección de correo electrónico asignada por el suscriptor, en el supuesto de que sea significativa en función de la finalidad del certificado.
- Los usos y límites económicos reseñados en el certificado.
- El periodo de validez del certificado, así como la fecha de emisión del certificado y la fecha de caducidad.
- El número de serie del certificado.
- La información contenida en los depósitos de certificados.

Las siguientes informaciones serán públicas:

- Los diferentes estados o situaciones del certificado y la fecha del inicio de cada uno de ellos, en concreto: pendiente de generación y/o entrega, válido, revocado, suspendido o caducado y el motivo que provocó el cambio de estado.
- Las listas de revocación de certificados (LRCs), así como las restantes informaciones de estado de revocación.

9.3.3 Divulgación de información de revocación

Véase la sección anterior.

9.3.4 Divulgación legal de información

LOGALTY divulga la información confidencial únicamente en los casos legalmente previstos.

En concreto, los registros que avalan la fiabilidad de los datos contenidos en el certificado, así como los registros relacionados con la fiabilidad de los datos y los relacionados con la operativa, serán divulgados en caso de ser requerido para ofrecer evidencia de la certificación en un procedimiento judicial, incluso sin consentimiento del suscriptor del certificado.

La Entidad de Certificación indicará estas circunstancias en la política de privacidad prevista en la sección 9.4.

9.3.5 Divulgación de información por petición de su titular

LOGALTY incluye, en la política de privacidad prevista en la sección 9.4, prescripciones para permitir la divulgación de la información del suscriptor y, en su caso, de la persona física identificada en el certificado, directamente a los mismos o a terceros.

9.3.6 Otras circunstancias de divulgación de información

Sin estipulación.

9.4 Protección de la información personal

Para la prestación del servicio de confianza de expedición de sellos cualificados de tiempo electrónico, LOGALTY precisa recabar y almacenar ciertas informaciones que incluyen datos personales. Tales informaciones son recabadas en base a la relación corporativa directamente de los interesados, con cumplimiento estricto del Reglamento (UE) 910/2014, y la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza (LSEC). Asimismo, LOGALTY precisa recabar y almacenar datos personales para mantener la relación con clientes, así como la gestión comercial y de los servicios contratados en idénticas condiciones de cumplimiento normativo.

La base legal para el tratamiento de los datos personales es la ejecución del contrato de servicios de confianza (artículo 6.1.b) del RGPD). Específicamente, la base legal para el tratamiento de los datos mínimos que se deben contener dentro del certificado cualificado a expedir es el cumplimiento de una

obligación legal aplicable al responsable del tratamiento (artículo 6.1.c) del RGPD). Asimismo, la base legal para el mantenimiento de relaciones comerciales es el interés legítimo (artículo 6.1.f) del RGPD).

Los datos que se solicitan a los interesados son estrictamente los necesarios para la suscripción del contrato y la prestación del servicio de expedición del certificado. La no comunicación de los datos supone la imposibilidad de prestación del servicio, por exigencia legal.

Los datos personales proporcionados se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recaban y para determinar las posibles responsabilidades que se pudieran derivar de la finalidad, además de los períodos establecidos en la normativa de servicios de confianza, y aquellos que resulten del ejercicio de las correspondientes acciones de reclamación en la vía administrativa y judicial. Más en concreto, conforme al artículo 9.3.a) de la LSEC, los datos necesarios para la prestación del servicio de expedición del certificado se conservarán durante el plazo de quince años desde la expiración del certificado.

Con carácter general no se comunicarán los datos personales a terceros, salvo obligación legal, entre las que pudieran estar las comunicaciones a administraciones públicas, Jueces y Tribunales para la atención de las posibles responsabilidades nacidas del tratamiento de sus datos de carácter personal. En algunos casos, podría ser necesario comunicar la información proporcionada a terceras partes para poder prestar el servicio solicitado.

Cualquier persona tiene derecho a obtener confirmación sobre los tratamientos de sus datos que se llevan a cabo por Logalty. Puede ejercer sus derechos de acceso, rectificación, supresión y portabilidad de sus datos, de limitación y oposición a su tratamiento, así como a no ser objeto de decisiones basadas únicamente en el tratamiento automatizado de sus datos, cuando procedan, ante Logalty, Calle de Cantabria 2 (Ed. Amura) 28108 Alcobendas (Madrid), o en la dirección de correo electrónico dpo@logalty.com

Logalty no adopta decisiones automatizadas, ni siquiera la elaboración de perfiles.

Logalty no realiza transferencias de datos personales a terceros países.

9.5 Derechos de propiedad intelectual

9.5.1 Propiedad de los certificados e información de revocación

Únicamente LOGALTY goza de derechos de propiedad intelectual sobre los certificados que emita, sin perjuicio de los derechos de los suscriptores, poseedores de claves y terceros, a los que conceda licencia no exclusiva para reproducir y distribuir certificados, sin coste alguno, siempre y cuando la reproducción sea íntegra y no altere elemento alguno del certificado, y sea necesaria en relación con firmas digitales y/o sistemas de cifrado dentro del ámbito de uso del certificado, y de acuerdo con la documentación que los vincula.

Adicionalmente, los certificados emitidos por LOGALTY contienen un aviso legal relativo a la propiedad de estos.

Las mismas reglas resultan de aplicación al uso de la información de revocación de los certificados.

9.5.2 Propiedad de la Declaración de Prácticas de Confianza

Únicamente LOGALTY goza de derechos de propiedad intelectual sobre esta Declaración de Prácticas de Confianza.

9.5.3 Propiedad de la información relativa a nombres

El suscriptor y, en su caso, la persona física identificada en el certificado conserva la totalidad de derechos, de existir los mismos, sobre la marca, producto o nombre comercial contenido en el certificado.

El suscriptor es el propietario del nombre distinguido del certificado, formado por las informaciones especificadas en la sección 3.1 del presente documento.

9.5.4 Propiedad de claves

Los pares de claves son propiedad de los firmantes, las personas físicas que poseen de forma exclusiva las claves de firma digital.

Cuando una clave se encuentra fraccionada en partes, todas las partes de la clave son propiedad del propietario de la clave.

9.6 Obligaciones y responsabilidad civil

9.6.1 Obligaciones de la Entidad de Certificación de LOGALTY

LOGALTY garantiza, bajo su plena responsabilidad, que cumple con la totalidad de los requisitos establecidos en la DPC, siendo el único responsable del cumplimiento de los procedimientos descritos, incluso si una parte o la totalidad de las operaciones se subcontratan externamente.

LOGALTY presta los servicios de certificación conforme con esta Declaración de Prácticas de Confianza.

Con anterioridad de la emisión y entrega del certificado al suscriptor, LOGALTY informa al suscriptor de los términos y condiciones relativos al uso del certificado, de su precio y de sus limitaciones de uso, mediante un contrato de suscriptor.

Este requisito de información también se cumple mediante un documento PDS, también denominado texto de divulgación, que incorpora el contenido del anexo A de la norma técnica ETSI EN 319 411-1, documento que puede ser transmitido por medios electrónicos, empleando un medio de comunicación duradero en el tiempo, y en lenguaje comprensible.

LOGALTY comunica de forma permanente los cambios que se produzcan en sus obligaciones publicando nuevas versiones de su documentación jurídica en su web https://www.logalty.com/certificateauthority/, a suscriptores, poseedores de claves y terceros que confían en certificados mediante dicho PDS, en lenguaje escrito y comprensible, con los siguientes contenidos mínimos:

- Prescripciones para dar cumplimiento a lo establecido en las secciones 5.2 y 4.5.3.
- Indicación de la política aplicable.
- Manifestación de que la información contenida en el certificado es correcta, excepto notificación en contra por el suscriptor.
- Consentimiento para la publicación del certificado en el depósito y acceso por terceros al mismo.

- Consentimiento para el almacenamiento de la información empleada para el registro del suscriptor y para la cesión de dicha información a terceros, en caso de terminación de operaciones de la Entidad de Certificación sin revocación de certificados válidos.
- Límites de uso del certificado, incluyendo las establecidas en la sección 1.4.2
- Información sobre cómo validar un certificado, incluyendo el requisito de comprobar el estado del certificado, y las condiciones en las cuales se puede confiar razonablemente en el certificado, que resulta aplicable cuando el suscriptor actúa como tercero que confía en el certificado.
- Forma en que se garantiza la responsabilidad patrimonial de la Entidad de Certificación.
- Limitaciones de responsabilidad aplicables, incluyendo los usos por los cuales la Entidad de Certificación acepta o excluye su responsabilidad.
- Periodo de archivo de información de solicitud de certificados.
- Periodo de archivo de registros de auditoría.
- Procedimientos aplicables de resolución de disputas.
- Ley aplicable y jurisdicción competente.
- Si la Entidad de Certificación ha sido declarada conforme con la política de certificación y, en su caso, de acuerdo con qué sistema.

9.6.2 Garantías ofrecidas a suscriptores y terceros que confían en certificados

LOGALTY, en la documentación que la vincula con suscriptores y terceros que confían en certificados, establece y rechaza garantías, y limitaciones de responsabilidad aplicables.

LOGALTY, como mínimo, garantiza al suscriptor:

- Que no hay errores de hecho en las informaciones contenidas en los certificados, conocidos o realizados por la Entidad de Certificación.
- Que no hay errores de hecho en las informaciones contenidas en los certificados, debidos a

falta de la diligencia debida en la gestión de la solicitud de certificado o en la creación de este.

- Que los certificados cumplen con todos los requisitos materiales establecidos en la Declaración de Prácticas de Confianza.
- Que los servicios de revocación y el empleo del Depósito cumplen con todos los requisitos materiales establecidos en la Declaración de Prácticas de Confianza.

LOGALTY, como mínimo, garantizará al tercero que confía en el certificado:

- Que la información contenida o incorporada por referencia en el certificado es correcta, excepto cuando se indique lo contrario.
- En caso de certificados publicados en el Depósito, que el certificado ha sido emitido al suscriptor identificado en el mismo y que el certificado ha sido aceptado, de acuerdo con la sección 4
- Que en la aprobación de la solicitud de certificado y en la emisión del certificado se han cumplido todos los requisitos materiales establecidos en la Declaración de Prácticas de Confianza.
- La rapidez y seguridad en la prestación de los servicios, en especial de los servicios de revocación y Depósito.

Adicionalmente, LOGALTY garantiza al suscriptor y al tercero que confía en el certificado:

- Que el certificado contiene las informaciones que debe contener un certificado de acuerdo con la política NCP+
- La responsabilidad de la Entidad de Certificación, con los límites que se establezcan.

9.7 Exención de garantía

LOGALTY rechaza toda garantía que no sea legalmente exigible conforme las Leyes aplicables al servicio,

excepto las expresamente contempladas en la sección 9.6.2.

9.8 Limitaciones de responsabilidad

9.8.1 Responsabilidades de la Autoridad de Certificación

LOGALTY, en su actividad de prestación de servicios de certificación, responderá por el incumplimiento de lo establecido en la DPC, y allí donde sea aplicable, por lo que dispone Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza y el Reglamento (UE) 910/2014.

Sin perjuicio de lo anterior, LOGALTY no garantizará los algoritmos y estándares criptográficos utilizados ni responderá de los daños causados por ataques externos a los mismos, siempre que hubiere aplicado la diligencia debida según el estado de la técnica en cada momento, y hubiere actuado conforme a lo dispuesto en la presente DPC, en la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, y en el Reglamento (UE) 910/2014, donde sea aplicable.

LOGALTY será responsable del daño causado ante el Suscriptor o cualquier persona que de buena fe confíe en el certificado, siempre que exista dolo o culpa grave, respecto de:

- La exactitud de la información contenida en el certificado en la fecha de su emisión, siempre que ésta corresponda a información autenticada.
- La garantía de que la clave pública y privada funcionan conjunta y complementariamente.
- La correspondencia entre el certificado solicitado y el certificado entregado.
- Cualquier responsabilidad que se establezca por la legislación vigente aplicable.

En ningún caso será responsable de las acciones u omisiones de terceros distintos de LOGALTY o de los perjuicios de cualquier tipo que se pudieran irrogar a solicitantes, representantes, entidades representadas, usuarios o, en su caso, terceros involucrados cuando dichos perjuicios no se deban a errores imputables a LOGALTY en los referidos procedimientos de expedición y/o de gestión de los certificados.

En todo caso y con independencia de la naturaleza de la declaración de voluntad que se sustancie o la condición pública o privada de quien firma o confía en los certificados, así como de la cuantía de los perjuicios que se pudieran causar, la cantidad máxima por la que LOGATY responderá en el supuesto de actuación negligente en el cumplimiento de las obligaciones asumidas será de SEIS MIL EUROS (6.000€).

En el supuesto de liquidación de la compañía por cualquier motivo o de terminación de las actividades de emisión y gestión de los certificados de clave pública, LOGALTY se atendrá a la normativa de firma electrónica vigente en cada momento, informando en todo caso con suficiente antelación a los titulares de los certificados, así como a los usuarios de los servicios afectados y transferirá a otro Prestador de Servicios de Certificación que los asuma, con expreso consentimiento de sus titulares, aquellos certificados que sigan siendo válidos en la fecha efectiva de cese de actividad.

En el supuesto de que esta transferencia de los certificados no fuera posible por cualquier motivo, se procederá, previo aviso a los titulares de los certificados afectados, a la revocación de la validez de estos.

9.8.2 Responsabilidades de la Autoridad de Registro

La RA asumirá toda la responsabilidad en el procedimiento de identificación de los suscriptores, y en la verificación de la identidad. Deberá seguir lo estipulado en la presente DPC o según otro procedimiento aprobado por LOGALTY.

9.8.3 Responsabilidades del suscriptor

El suscriptor es responsable de cumplir con las obligaciones estipuladas en esta DPC, y en el contrato que le vincule.

9.8.4 Delimitación de responsabilidades

Hasta donde permita la Ley, LOGALTY no será responsable en ningún caso ante las siguientes circunstancias:

- Estado de Guerra, desastres naturales, funcionamiento defectuoso de los servicios eléctricos, las redes telemáticas y/o telefónicas o de los equipos informáticos utilizados por

el Suscriptor o por los Terceros, o cualquier otro caso de fuerza mayor.

- Por el uso indebido o fraudulento del directorio de certificados y CRL's (Lista de Certificados Revocados) emitidos por la Autoridad de Certificación.
- Por el uso indebido de la información contenida en el Certificado o en la CRL.
- Por el contenido de los mensajes o documentos firmados o encriptados mediante los certificados.
- En relación con las siguientes acciones u omisiones del Solicitante y Suscriptor:
    - Falta de veracidad de la información suministrada para emitir el certificado.
    - Retraso en la comunicación de las causas de suspensión o revocación del certificado.
- Ausencia de solicitud de suspensión o revocación del certificado cuando proceda.
    - Negligencia en la conservación de sus datos de creación de firma, en el aseguramiento de su confidencialidad y en la protección de todo acceso o revelación.
    - Uso del certificado fuera de su periodo de vigencia, o cuando LOGALTY o la RA le notifique la revocación o suspensión de este.
    - Extralimitación en el uso del certificado, según lo dispuesto en la normativa vigente y en la presente DPC, en particular, superar los límites que figuren en el certificado electrónico en cuanto a sus posibles usos y al importe individualizado de las transacciones que puedan realizarse con él o no utilizarlo conforme a las condiciones establecidas y comunicadas al firmante por LOGALTY.
- En relación con acciones u omisiones del tercero que confía en el certificado:
    - Falta de comprobación de las restricciones que figuren en el certificado electrónico o en la presente DPC en cuanto a sus posibles usos y al importe individualizado de las transacciones que puedan realizarse con él.
    - Falta de comprobación de la suspensión o pérdida de vigencia del certificado electrónico publicada en el servicio de consulta sobre la vigencia de los certificados o falta de verificación de la firma electrónica.

9.8.5 Cláusula de indemnidad de suscriptor

LOGALTY incluye en el contrato con el suscriptor, una cláusula por la cual el suscriptor se compromete a mantener indemne a la Entidad de Certificación de todo daño proveniente de cualquier acción u omisión que resulte en responsabilidad, daño o pérdida, gasto de cualquier tipo, incluyendo los judiciales y de representación letrada en que pueda incurrir, por la publicación y uso del certificado, cuando concurra alguna de las siguientes causas:

- Falsedad o manifestación errónea realizada por el usuario del certificado.
- Error del usuario del certificado al facilitar los datos de la solicitud, si en la acción u omisión ha mediado dolo o negligencia con respecto a la Entidad de Certificación o a cualquier persona que confía en el certificado.
- Negligencia en la protección de la clave privada, en el empleo de un sistema fiable o en el mantenimiento de las precauciones necesarias para evitar el compromiso, la pérdida, la divulgación, la modificación o el uso no autorizado de dicha clave.
- Empleo por el suscriptor de un nombre (incluyendo nombres comunes, dirección de correo electrónico y nombres de domino), u otras informaciones en el certificado, que infrinjan derechos de propiedad intelectual o industrial de terceros.

9.8.6 Cláusula de indemnidad de tercero que confía en el certificado

LOGALTY incluye en la PDS, una cláusula por la cual el tercero que confía en el certificado se compromete a mantener indemne a la Entidad de Certificación de todo daño proveniente de cualquier acción u omisión que resulte en responsabilidad, daño o pérdida, gasto de cualquier tipo, incluyendo los judiciales y de representación letrada en que pueda incurrir, por la publicación y uso del certificado, cuando concurra alguna de las siguientes causas:

- Incumplimiento de las obligaciones del tercero que confía en el certificado.
- Confianza temeraria en un certificado, a tenor de las circunstancias.
- Falta de comprobación del estado de un certificado, para determinar que no se encuentra

suspendido o revocado.

9.8.7 Caso fortuito y fuerza mayor

LOGALTY incluye en la PDS cláusulas que limitan su responsabilidad en caso fortuito y en caso de fuerza mayor.

9.9 Indemnizaciones

9.9.1 Alcance de la cobertura

LOGALTY dispone de un seguro que responde de las cantidades que LOGALTY resulte legalmente obligado a pagar, hasta el límite de cobertura contratado, como resultado de cualquier procedimiento judicial en el que pueda declararse su responsabilidad, derivada de cualquier acto negligente, error u incumplimiento no intencionado de la legislación vigente entre otros, en los términos expresamente pactados con la compañía aseguradora.

9.9.2 Limitaciones de pérdidas

LOGALTY limita su responsabilidad mediante la inclusión de los límites de uso del certificado con la extensión qcStatements en los perfiles de los certificados.

El suscriptor podrá, si lo desea, solicitar y en su caso contratar un límite superior al indicado, asumiendo los costes adicionales que en su caso se establezcan. Además, el suscriptor y terceras partes podrán acordar bilateralmente pactos o coberturas específicas para transacciones de valor superior, manteniéndose en este caso el límite de responsabilidad de la CA citado en los párrafos anteriores, según la política de certificación aplicable.

9.10 Período de validez

9.10.1 Plazo

La DPC, y las PDS entran en vigor en el momento de su publicación, salvo que las mismas indiquen otra

fecha.

9.10.2 Sustitución y derogación de la DPC

La presente DPC, y las PDS quedan derogadas en el momento que una nueva versión de los documentos sea publicada. La nueva versión sustituirá íntegramente el documento anterior.

9.10.3 Efectos de la finalización

Para los certificados vigentes emitidos bajo una DPC anterior, la nueva versión prevalecerá sobre la anterior en todo lo que no se oponga a ésta.

9.11 Notificaciones individuales y comunicaciones con los participantes

LOGALTY establece en el contrato con el suscriptor, los medios y plazos para las notificaciones. De modo general, se utilizará el sitio web de LOGALTY www.logalty.com para realizar cualquier tipo de notificación y comunicación general, así como el correo electrónico o postal para notificaciones y comunicaciones individualizadas.

En caso de problemas de seguridad o de pérdida de integridad que puedan afectar a una persona física o jurídica, LOGALTY le notificará dicha incidencia sin ningún retraso.

9.12 Enmiendas

9.12.1 Procedimiento para los cambios

9.12.1.1 Elementos que pueden cambiar sin necesidad de notificación

Los únicos cambios que pueden realizarse a esta política sin requerir de notificación son las correcciones tipográficas o de edición o los cambios en los detalles de contacto.

9.12.1.2 Cambios con notificación

Los elementos de esta DPC pueden ser cambiados unilateralmente por LOGALTY sin preaviso. Las modificaciones pueden traer causa justificativa en motivos legales, técnicos o comerciales.

Cuando corresponda, dichas modificaciones serán notificadas al Organismo de Supervisión correspondiente, y tras su aprobación definitiva, se publicará la nueva documentación con un periodo de entrada en vigor que posibilite la posible rescisión de los suscriptores que no acepten los cambios. El momento de entrada en vigor se anunciará suficientemente en el momento de publicación de los cambios.

9.12.1.3 Mecanismo de notificación

Todos los cambios propuestos que puedan afectar sustancialmente a los suscriptores, usuarios o terceros serán notificados inmediatamente a los interesados mediante la publicación en la Web de LOGALTY.

Las RA podrán ser notificadas directamente mediante correo electrónico o telefónicamente en función de la naturaleza de los cambios realizados.

9.12.2 Periodo y procedimiento de notificación

Las personas, instituciones o entidades afectadas pueden presentar sus comentarios a la organización de la administración de las políticas dentro de los 30 días siguientes a la notificación. Cualquier acción tomada como resultado de unos comentarios queda a la discreción de la organización responsable de la administración de las políticas.

9.12.3 Circunstancias en las que el OID debe ser cambiado

Se procederá al cambio de OID en aquellas circunstancias que se altere alguno de los procedimientos descritos en el presente documento, y que afecte directamente al modo operativo de alguna de las entidades participantes.

9.13 Reclamaciones y resolución de conflictos

LOGALTY establece, en el contrato de suscriptor, y en la PDS, los procedimientos de mediación y resolución de conflictos aplicables.

9.14 Normativa aplicable

LOGALTY establece, en el contrato de suscriptor y en la PDS, que la legislación aplicable a la prestación de los servicios, incluyendo la política y prácticas de certificación, es la Ley española. Específicamente son de aplicación, en lo que proceda, las siguientes normas:

- Reglamento (UE) 910/2014 del parlamento europeo y del consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Añadir que las prácticas de los servicios de confianza de LOGALTY siguen las directrices de los siguientes estándares:

- ETSI EN 319 401: General Policy Requirements for Trust Service Providers
- ETSI EN 319 421: Policy and Security Requirements for Trust Service Providers issuing TimeStamps
- ETSI EN 319 422: Time-stamping protocol and time-stamp token profiles.

9.15 Cumplimiento de la normativa aplicable

LOGALTY cumple el Reglamento (UE) 910/2014, Ley 6/2020, de 11 de noviembre, reguladora de

determinados aspectos de los servicios electrónicos de confianza, así como el resto de la normativa relacionada en el punto anterior.

LOGALTY establece, en el contrato de suscriptor y en la PDS, una cláusula de jurisdicción competente, indicando que la competencia judicial internacional corresponde a los jueces españoles. La competencia territorial y funcional se determinará en virtud de las reglas de derecho internacional privado y reglas de derecho procesal que resulten de aplicación.

9.16 Otras disposiciones

9.16.1 Cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación

LOGALTY establece, en el contrato de suscriptor, y en la PDS, cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación:

- En virtud de la cláusula de divisibilidad, la invalidez de una cláusula no afectará al resto del contrato.
- En virtud de la cláusula de supervivencia, ciertas reglas continuarán vigentes tras la finalización de la relación jurídica reguladora del servicio entre las partes. A este efecto, la Entidad de Certificación vela porque, al menos los requisitos contenidos en las secciones 12.1 (Obligaciones y responsabilidad), 8 (Auditoría de conformidad) y 8.9 (Confidencialidad), continúen vigentes tras la terminación del servicio y de las condiciones generales de emisión/uso.
- En virtud de la cláusula de acuerdo íntegro se entenderá que el documento jurídico regulador del servicio contiene la voluntad completa y todos los acuerdos entre las partes.
- En virtud de la cláusula de notificación se establecerá el procedimiento por el cual las partes se notifican hechos mutuamente.

9.17 Otras provisiones

Sin estipulación.