logalty

Declaración de Prácticas de Confianza

Servicio de Entrega Electrónica

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	08/05/2023
Descripción	Declaración de Prácticas de Confianza Servicio de entrega electrónica certificada
Aprobado	CRS
Estado	Iniciado Borrador en curso Borrador para comentarios Borrador final para aprobación Aprobado **Publicado** Retirado

CONTROL DE VERSIONES

VERSIÓN	PARTES CAMBIADAS	DESCRIPCIÓN CAMBIO	AUTOR	FECHA
1.0	Original	Creación del documento	NA, DG, CO	27/07/2018
1.1	Varias	Aclaraciones periodos de custodia Cambios NTP	NA	14/09/2018
1.2	Secciones 1.2, 4.2 y 8	Inclusión indicación OID eIDAS, periodo mínimo de custodia de la notificación y ampliación descripción controles jurídicos.	NA/DG	06/11/2018
1.3	Secciones 4 y 8	Ajuste de procedimiento de destinatario	NA/DG	20/12/2018
1.4	Sección 4.2.3	Puesta a disposición de la formalización de la Contratación Electrónica Certificada	DG	29/06/2020
	Sección 5.6	Inclusión de referencia a la certificación ISO 22301 de continuidad	CO	29/06/2020
	5.4.8	Modificación del texto sobre gestión de vulnerabilidades	CO	30/06/2020
1.5	1.4.3	Modificación proceso de revisión de esta DPC	CO	13/05/2022
1.6	Sección 4	Ampliación textos operativas del servicio envío y recepción	SM/JLH	08/05/2023
	Sección 4.2.3 Sección 4.2.4	Supresión de secciones que ya no aplican	JLH	08/05/2023
	Sección 5.2.1	Inclusión Rol	AC	08/05/2023

1 Introducción

1.1 Presentación

Este documento declara las prácticas de confianza en la prestación de los servicios de entrega electrónica certificada por parte de LOGALTY.

El servicio se presta en dos modalidades:

- Entrega electrónica certificada.
- Entrega electrónica certificada cualificada.

El servicio de entrega electrónica certificada es ofrecido como parte de los servicios de tercero de confianza comercializados por LOGALTY. En particular, el servicio de entrega electrónica certificada se encuentra integrado en los siguientes servicios:

- Servicio de contratación electrónica certificada.
- Servicio de notificación electrónica certificada.
- Servicio de comunicación electrónica.

1.2 Nombre del documento e identificación

Este documento es la "Declaración de Prácticas de Confianza del Servicio de Entrega Electrónica Certificada de LOGALTY".

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

OID	Política de servicio
1.3.6.1.4.1.30210.1.8.1	Entrega electrónica certificada
1.3.6.1.4.1.30210.1.8.2	Entrega electrónica certificada cualificada conforme al Reglamento (UE) N.º 910/2014, de 23 de julio.

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 entrega electrónica certificada

1.3.1 Prestadores de servicios de confianza participantes en el servicio de entrega electrónica certificada

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, y las normas técnicas del ETSI aplicables a los servicios de entrega electrónica certificada, principalmente ETSI EN 319 401 y ETSI EN 319 521, al objeto de facilitar el cumplimiento de los requisitos legales y el reconocimiento internacional de los servicios de entrega electrónica certificada que ofrece.

1.3.2 Entidades finales

Las entidades finales son las personas y organizaciones destinatarias de los servicios de entrega electrónica certificada.

Serán entidades finales de los servicios de entrega electrónica certificada de Logalty las siguientes:

- Remitentes de comunicaciones y documentos, que tienen la condición de suscriptores del servicio.
- Destinatarios de comunicaciones y documentos.

1.3.2.1 Suscriptores del servicio de certificación

Entendemos por emisor a toda entidad, que normalmente en el marco de su actividad profesional, pone a disposición de LOGALTY la documentación necesaria respecto a la cual LOGALTY prestará los servicios estipulados en el contrato del servicio en el que se integra la entrega electrónica certificada.

En los servicios de LOGALTY, el emisor es el suscriptor del servicio, accediendo a dicha condición mediante la firma del contrato o de una petición de servicio. El servicio tiene una duración determinada, en su caso renovable conforme estipula el instrumento jurídico correspondiente.

Mientras el contrato de servicio se encuentra vigente, el emisor puede iniciar las operaciones contratadas, que incorporan la correspondiente entrega electrónica certificada, en su caso cualificada.

1.3.2.2 Destinatario

Entendemos por destinatario aquella persona física, empresa o institución a la cual va dirigido, de parte del emisor, la entrega electrónica certificada integrada en los servicios ofrecidos por LOGALTY.

1.4 Administración de la Declaración de Prácticas de Confianza

1.4.1 Organización que administra el documento

Este documento es administrado por la Gerencia de PKI, Servicios de Confianza y eIDAS de **Logalty Servicios de Tercero de Confianza SL**, con los siguientes datos de identificación:

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

1.4.2 Datos de contacto de la organización

Logalty Prueba por Interposición SL
Calle Valportillo Primera, 22-24, Edificio Caoba
28108 Alcobendas, Madrid
España
Phone: +34 902 78 99 74

E-mail: logalty@logalty.com

1.4.3 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 relacionadas con el mismo.

1.4.3.1 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 los cambios en las prácticas de confianza del Servicio de Entrega Electrónica Certificada, 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.

1.4.3.2 Aprobación del documento

Las modificaciones futuras de esta Declaración de Prácticas de Confianza, de la Política de Seguridad y de los restantes documentos del servicio de confianza son aprobadas por el Comité de 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://logalty.com/certificateauthority/

2 Publicación de información

2.1 Publicación de información del prestador de servicios de certificación

LOGALTY publica las siguientes informaciones en su Depósito:

- La Declaración de Prácticas de Certificación.
- Los certificados que se pueden emplear para validar las evidencias producidas por LOGALTY.

2.2 Frecuencia de publicación

La información del prestador de servicios de certificación se publica en cuanto se encuentra disponible.

Los cambios en la Declaración de Prácticas de Certificación se rigen por lo establecido en la sección 1.4 de este documento.

2.3 Control de acceso

LOGALTY no limita el acceso de lectura a las informaciones establecidas en la sección 2.1, 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.
- 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 Identificación del remitente

Para transaccionar con Logalty, es necesario para el emisor firmar digitalmente cada petición con un certificado digital, dado que la comunicación se realiza utilizando Servicios Web conforme al protocolo SOAP. En el caso del servicio de entrega electrónica certificada cualificada será necesario el uso de un certificado de firma electrónica avanzada o de sello electrónico avanzado.

Una vez recibida la petición por parte de LOGALTY, la firma digital se comprueba con la clave pública del certificado almacenado en los sistemas y se le asigna un identificador único.

3.2 Identificación del destinatario

El destinatario recibe un email que contiene un vínculo al sistema de autenticación de LOGALTY o a uno propio del emisor. Una vez autenticado, se realiza la identificación del destinatario de distintas formas, dependiendo de si el proceso es cualificado o no.

- Si el proceso es cualificado, para autenticar al destinatario se utiliza un mecanismo de autenticación basado en su certificado de firma electrónica avanzada o de sello electrónico avanzado, y, si el resultado es satisfactorio, se procede a la puesta a disposición del documento.
- En relación con el proceso no cualificado, se utilizará un código OTP mediante SMS enviado al teléfono móvil del destinatario.

4 Operativa del servicio

El servicio de entrega electrónica certificada consiste en la puesta a disposición de medios electrónicos, informáticos y telemáticos para que el emisor pueda realizar las operativas descritas a continuación.

4.1 Notificaciones electrónicas certificadas

Este servicio permite enviar notificaciones de forma electrónica y certificada a terceros de su interés a través de LOGALTY, consignando además la fecha y la hora en que se produzca el envío, así como la fecha y hora en que se reciba por el destinatario, con integridad de contenido y custodia mínima determinada por el cliente en su petición de servicio.

Todas las comunicaciones entre el cliente y LOGALTY se realizan mediante transacciones telemáticas firmadas digitalmente y bajo un sistema seguro de comunicaciones. En el servicio cualificado, las transacciones se deberán realizar mediante un sistema de firma electrónica avanzada.

La Notificación Electrónica Certificada de LOGALTY incluye de manera estándar la copia certificada del documento, con mecanismos de control de la integridad del contenido, acuse de recibo del envío y realizándose depósito notarial de la función resumen del contenido de todos los documentos.

En caso de identificación del Receptor por el cliente, la autenticación del Usuario receptor que solicita el acceso al Portal web de LOGALTY se realizará por parte del cliente conforme a los protocolos, estándares y niveles de seguridad que el cliente considere oportunos.

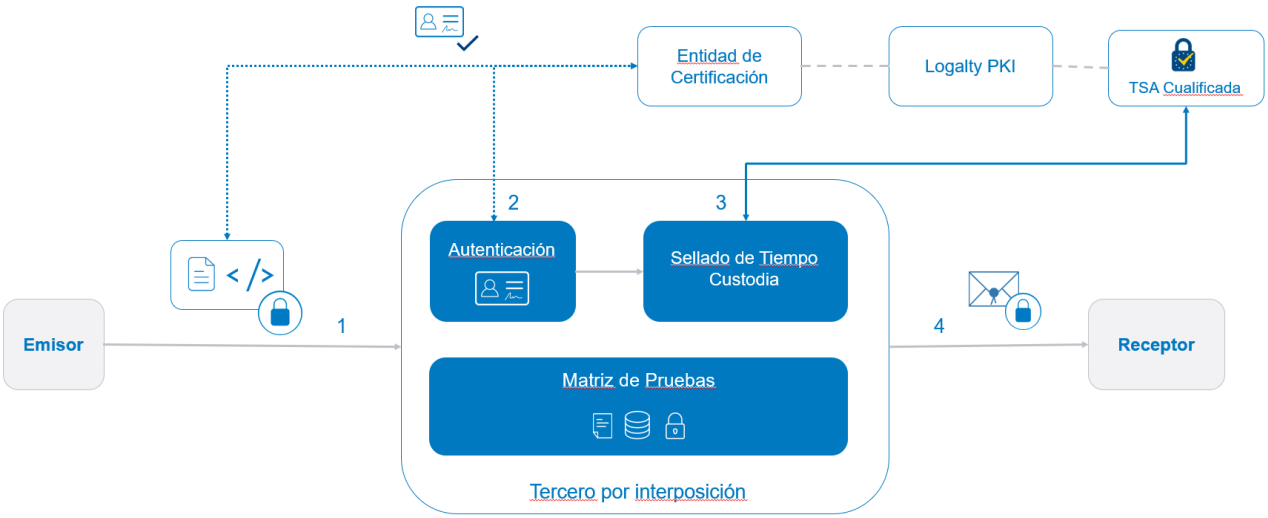
En caso de identificación por LOGALTY del Usuario receptor, LOGALTY aceptará como válida toda solicitud de acceso a su portal que cumpla con los requisitos establecidos para tal fin. Estos requisitos están basados en datos conocidos por el cliente y por el Receptor, que permiten acceder a las modificaciones realizadas por los sistemas del cliente.

Para la puesta del documento por parte del receptor, se podrá utilizar el sistema de PIN vía SMS a su móvil. En el caso del servicio cualificado, se procede a la identificación mediante certificado del receptor previa puesta a disposición del documento.

El sellado de tiempo se realizará con una autoridad de certificación cualificada.

En los siguientes epígrafes se muestran los pasos del proceso de notificación electrónica certificada.

4.1.1 Envío de Notificación Electrónica Certificada



1. Solicitud de envío de documentación.

   El cliente Emisor envía a Logalty, en formato PDF, la documentación que debe ser firmada por el receptor.

2. Logalty envía el hash de la petición

   Una vez Logalty ha recibido la documentación, genera un hash de la petición y lo envía a la Entidad de Certificación.

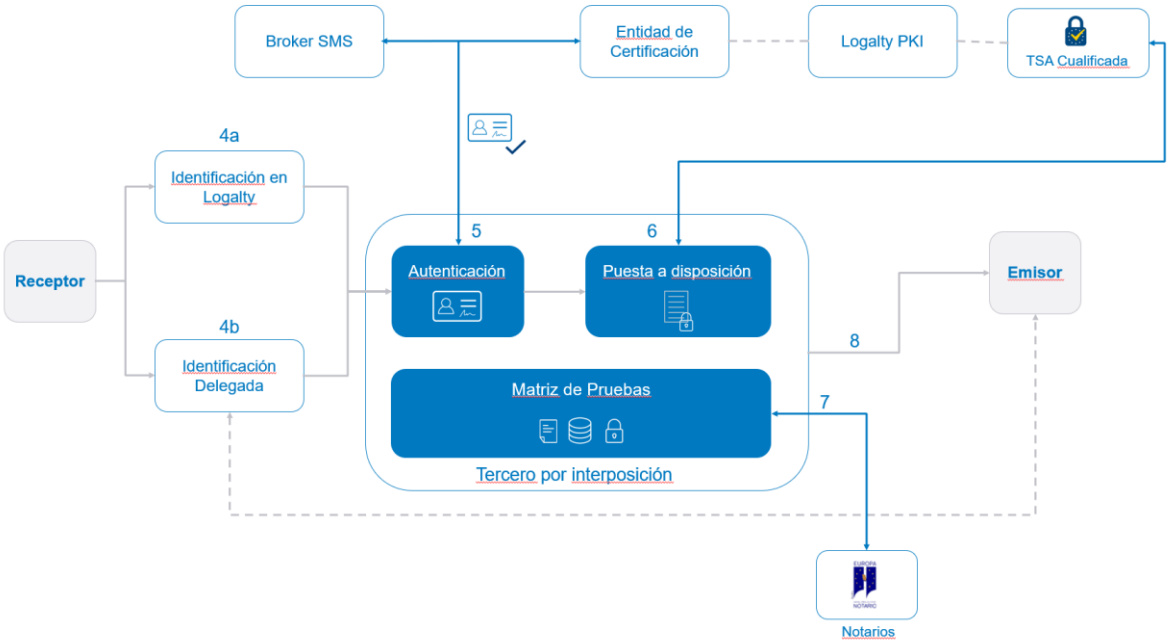
3. La Entidad de Certificación pone sellado de tiempo

   Tras haber recibido la petición, la Entidad de Certificación pone sellado de tiempo, guarda copia y devuelve a Logalty.

4. Logalty envía la documentación

   Genera un email que envía al Receptor con el enlace para acceder al documento.

4.1.2 Recepción de Notificación Electrónica Certificada



4. Autenticación

   Tras haber recibido el email de acceso, el receptor se identifica en la web de Logalty, introduciendo los datos solicitados por el Emisor:

   a. Identificación del receptor en Logalty. Si el proceso es asíncrono, el receptor, se debe identificar en Logalty previamente al acceso. Una vez identificado, accederá a la documentación desde la web de Logalty.

   b. Identificación delegada en el Receptor de Logalty. Si el proceso es síncrono, el receptor, ya identificado, accederá a la documentación desde la propia web del Emisor.

   El usuario se autentica mediante pin SMS enviado al móvil. En el caso de entrega electrónica certificada cualificada, se procederá a la identificación mediante certificado y autenticación mediante *clientauth*.

5. Puesta a disposición del documento

   Logalty registra la aceptación de la puesta a disposición, genera un hash de toda la historia del documento y se lo envía a la Entidad de Certificación para realizar el Sellado de Tiempo cualificado.

6. La Entidad de Certificación emite sellado de tiempo

   La Entidad de Certificación devuelve a Logalty el sellado de tiempo de toda la historia del documento.

7. Depósito notarial

   Logalty realiza un hash del contenido del documento y lo envía al Depósito Notarial.

8. Cierre de la transacción

   Para finalizar el proceso, Logalty cierra la transacción y emite certificado para entregar al emisor

4.2 Contrataciones electrónicas certificadas

Servicio consistente en la puesta a disposición de medios electrónicos, informáticos y telemáticos para que el cliente y sus terceros de interés (sus clientes, proveedores, empleados, etc.) contraten electrónicamente en LOGALTY, consignando la fecha y la hora del perfeccionamiento, así como la integridad de contenido y custodia mínima de cinco años o la que determine el cliente en su petición de servicio, siempre que sea superior.

Todas las comunicaciones entre el cliente y LOGALTY se realizan mediante transacciones telemáticas firmadas electrónicamente bajo un sistema seguro de comunicaciones. En el servicio cualificado, las transacciones se deberán firmar mediante un sistema de firma electrónica avanzada con certificado cualificado.

La Contratación Electrónica Certificada de LOGALTY incluye de manera estándar la copia certificada del documento perfeccionado por las partes, con mecanismos de control de la integridad del contenido y realizándose depósito notarial de la función resumen del contenido de todos los contratos.

La identificación del receptor se podrá realizar por parte de LOGALTY, que aceptará como válida toda solicitud de acceso a su portal que cumpla con los requisitos establecidos para tal fin. Estos requisitos están basados en datos conocidos por el Emisor y por el usuario receptor, que permiten acceder a las modificaciones realizadas por los sistemas del Emisor.

En el caso en que la identificación la realice el Emisor, se realizará conforme a los protocolos, estándares y niveles de seguridad que éste considere oportunos. LOGALTY aceptará como pertinente toda solicitud de acceso a su portal web que se le indique como autenticada por el Emisor y declinará todo tipo de responsabilidad asociada a la no autenticación o autenticación

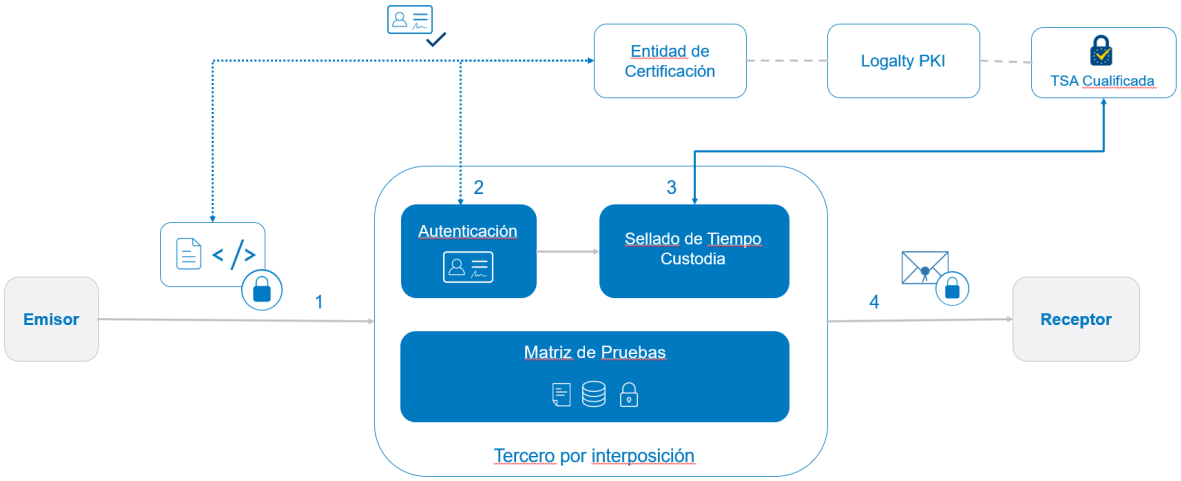
defectuosa del usuario receptor.

Para realizar la puesta a disposición de la documentación, se procede previamente a la identificación mediante certificado del destinatario. Tras esta identificación, éste tendrá acceso a los documentos.

El sellado de tiempo se realizará con una autoridad de certificación cualificada.

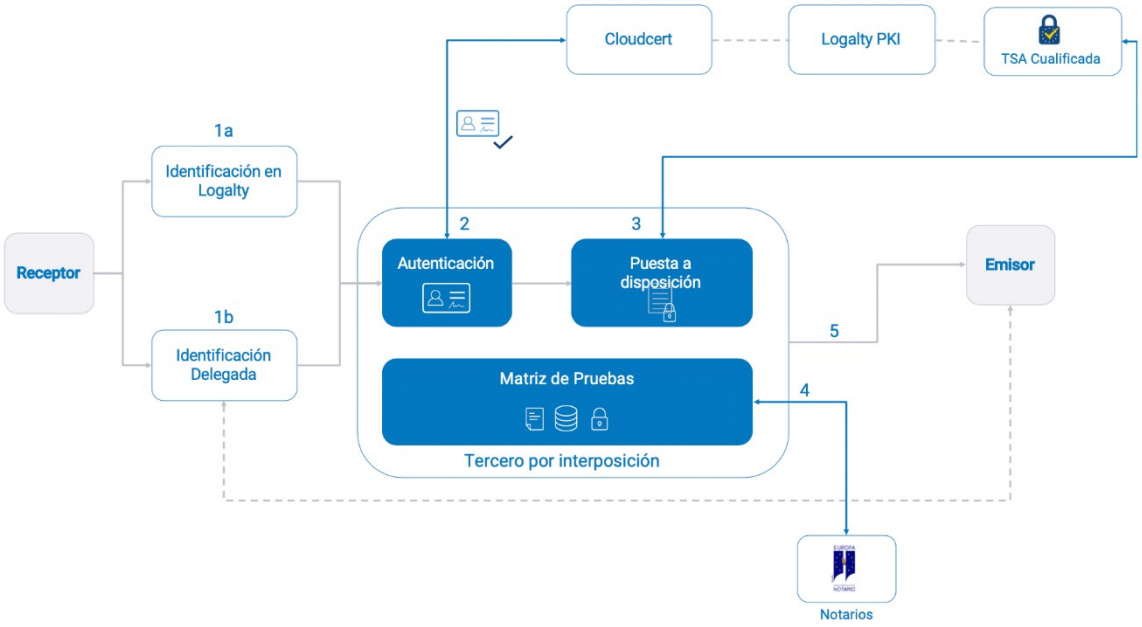
En los siguientes epígrafes se muestran los pasos del proceso de puesta a disposición de la contratación electrónica certificada.

4.2.1 Creación de Contratación Electrónica Certificada



1. Petición del cliente Emisor a Logalty de envío de documento en formato PDF
2. Logalty autentica al Emisor y envía el hash de la petición de envío a la Entidad de Certificación
3. La Entidad de Certificación pone sellado de tiempo, guarda copia y devuelve a Logalty el sellado de tiempo.
4. Logalty envía un email firmado al Receptor con el enlace para acceder al documento.

4.2.2 Puesta a disposición previa de la Contratación Electrónica Certificada



El usuario se identifica

a. Identificación del receptor en Logalty

b. Identificación delegada en el Receptor de Logalty

5. En el caso de entrega electrónica certificada cualificada se procederá a la identificación mediante certificado y autenticación mediante CLIENTAUTH SSL.

6. Se procede a la puesta a disposición del documento, Logalty registra la aceptación, genera un hash de toda la historia del documento y se lo envía a la Entidad de Certificación para realizar el Sellado de Tiempo cualificado.

7. La Entidad de Certificación devuelve a Logalty el sellado de tiempo de la historia del documento.

8. Logalty realiza un hash del contenido del documento y lo envía a Deposito Notarial.

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 del servicio de entrega electrónica certificada.

En concreto, la política de seguridad física y ambiental 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.
- Inundaciones.
- 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 las operaciones del servicio de entrega electrónica certificada 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

Logalty cuenta con dos disposiciones físicas para los sistemas redundados en una modalidad de activo-activo. 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 está ubicada en una zona de bajo riesgo de desastres y permite un rápido acceso.

La sala donde se realizan las operaciones 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 entrega electrónica certificada.

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 entrega electrónica certificada 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 de entrega electrónica certificada 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 esta es necesaria la apertura de una solicitud de acceso al CPD en el que

se debe detallar:

- Personal que accederá 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 a 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 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 aplicable, ya que las copias de respaldo de cada centro de proceso de datos se almacena en el otro centro de proceso de datos.

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 Operación del servicio e incompatibles con Sistemas. Estas funciones estarán subordinadas a la jefatura 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 del servicio.
- **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.
- **Responsable de verificación de identidad**: será responsable de verificar y asegurar que las actividades relativas a la verificación de la identidad del emisor del remitente y el receptor son acordes a los procedimientos definidos.

Estos roles son ocupados por personal que tiene el suficiente conocimiento experto, experiencia, cualificación y fiabilidad, además de haber recibido formación apropiada sobre seguridad, protección de datos personales, nuevas amenazas y prácticas de seguridad actuales. Esta formación se imparte al menos con periodicidad anual.

Dichos roles y sus responsabilidades son descritos en fichas, que son conocidas por todo el personal que participa en la prestación del servicio. Las funciones del personal asignado al servicio son asignadas bajos los principios de segregación de tareas y menor privilegio posible.

El personal con responsabilidades gerenciales y directivas asociados al servicio, tienen un conocimiento profundo del servicio, de los procedimientos de seguridad y de las obligaciones del personal.

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.

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

Los privilegios asignados a los diferentes roles, una vez asignados a un grupo no pueden compartirse con otro. Los grupos definidos en Logalty son:

- Desarrollo. Equipo encargado de realizar los evolutivos de las aplicaciones que componen el servicio.
- Integración. Realizan las integraciones de clientes emisores que han contratado los servicios de Logalty,
- Producción. Equipo que gestiona la infraestructura de producción y las posibles incidencias en ese nivel. Asegura la operativa de los servicios que componen el Core del producto.
- Operaciones. Grupo de personas que atiende y gestiona incidencias de nivel 2.

5.2.5 Marco normativo de aplicación al personal

Existe un marco de seguridad que es de obligado cumplimiento para todos los usuarios, tanto internos a la organización, como externos, que acceden a los sistemas de información de LOGALTY.

Como documento de mayor nivel estratégico, existe la Política de Seguridad de la Información, la cual se desarrolla de forma más específica en un cuerpo normativo que añade requisitos específicos por cada área. En concreto, existen las siguientes normativas:

- Gestión de los sistemas de información.
- Clasificación y tratamiento de la información
- Control de Acceso lógico
- Control de Acceso físico
- Desarrollo Seguro
- Uso del mail
- Uso de internet
- Trabajo fuera de las instalaciones de Trabajo

De forma adicional, existen planes que permiten organizar los procedimientos operativos alrededor de:

- Respuesta y Contención de Incidencias de seguridad de la información
- Recuperación de desastres.

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 validación de identidad es confiable y ha realizado un curso de preparación para la realización de las tareas propias de su rol.

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 a un sitio confiable o de gestión a una persona que no sea idónea para el puesto, especialmente por haber sido condenada por delito o falta que afecte su idoneidad 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.
- Morosidad.

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 obtiene el consentimiento inequívoco del afectado para dicha investigación previa, y procesa y protege todos sus datos personales de acuerdo con el Reglamento General de Protección de Datos y resto de normativa aplicable.

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 del servicio de entrega electrónica certificada, así como el entorno de usuario de la persona a formar.
- Tareas que debe realizar la persona.
- Políticas, normativas, planes 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.
- La importancia de los datos de carácter personal y la confidencialidad sobre los mismos.
- Nociones de desarrollo seguro.

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, y como mínimo con frecuencia anual.

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 diversos procesos de auditoría que pretenden aportar un nivel suficientemente profundo sobre las vulnerabilidades potencialmente explotables y la madurez de

sus controles de seguridad. Estas auditorías incluyen:

- Auditoría anual exhaustiva de revisión de seguridad.
- Revisiones trimestrales sobre existencia de vulnerabilidades.
- Test de intrusión a la infraestructura, tanto en modalidad externa como interna.
- Revisión periódica de los log y eventos registrados.

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 archivos.
- Acceso físico a los logs.
- Cambios en la configuración y mantenimiento del sistema.
- Las actividades de los cortafuegos y enrutadores.
- Registros de acceso físico.
- Cambios en el personal.
- Informes de compromisos y discrepancias.
- Informes completos de los intentos de intrusión física en las infraestructuras que dan soporte al servicio.
- Confidencialidad e integridad de los registros de la actividad.
- Tiempo preciso de los eventos registrados.

Con respecto al servicio de entrega electrónica certificada, se registran los siguientes logs:

- Log de resultado de los envíos de email.
- Log del visor de peticiones.
- Log de ciclo de vida de peticiones.
- Log del servicio de envíos de email.

- Log de envío de códigos de totp (sms, voz).
- Log de la cabina de cifrado de datos.
- Log de comunicaciones.
- Log del servicio de generación de portadas del operador postal.

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.

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 log
- Que los ficheros de log 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 log 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 archiva los registros especificados anteriormente en función del plazo de conservación de las operaciones sustentadas por el servicio de entrega electrónica certificada. De este modo, si una operación dura cinco años, transcurrido dicho plazo, se inicia el cómputo del periodo de conservación de los registros de auditoría.

El cliente puede ampliar el periodo de custodia de su operación (contratación, notificación, etc.), o reducirlo, siempre que se respete el mínimo legal, hasta la fecha de la solicitud, lo que modifica el inicio del cómputo de ese periodo de conservación.

El plazo de conservación de los registros será, al menos, de 2 años desde el transcurso del plazo anteriormente indicado, conforme al requerimiento REQ-ERDSP-7.10-02 de la norma EN 319 521.

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.

El acceso a los ficheros de log 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 log 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 Backus seguro de los logs de auditoría, realizando semanalmente una copia de todos los logs en un medio externo. Adicionalmente se mantiene copia en centro de custodia externo.

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 paras las categorizadas como críticas.

5.5 Archivos de informaciones

LOGALTY, garantiza que toda la información relativa al servicio de entrega electrónica certificada se conserva durante un período de tiempo apropiado, según lo establecido en la sección 5.5.2 de esta política.

5.5.1 Tipos de registros archivados

Los siguientes documentos implicados en el servicio son almacenados por LOGALTY:

- Petición del emisor firmada (PT_Request).
- Documentos originales enviados por el emisor.
- Documentos referenciados por Logalty.

- Referencia a los emails enviados a cada receptor/firmante (si ha sido necesario).
- Referencia a los sms enviados a cada receptor/firmante (si ha sido necesario).
- Diversos logs que evidencian: accesos, recogidas, rechazo, atributos captados por pantalla, resultado de la transacción.
- Sellos de tiempo para todo lo anterior.
- Fichero diario enviado para depósito notarial.
- Base de datos de firmas encriptadas.
- Políticas y Prácticas del servicio.

LOGALTY es responsable del correcto archivo de todo este material.

5.5.2 Período de conservación de registros

LOGALTY archiva los registros especificados anteriormente en función del plazo de conservación de las operaciones sustentadas por el servicio de entrega electrónica certificada. De este modo, si una operación dura **cinco años**, transcurrido dicho plazo, se inicia el cómputo del periodo de conservación de los registros con la información relativa al servicio de entrega electrónica.

El cliente puede ampliar el periodo de custodia de su operación (contratación, notificación, etc.), o reducirlo, siempre que se respete el mínimo legal, hasta la fecha de la solicitud, lo que modifica el inicio del cómputo de ese periodo de conservación.

El plazo de conservación de los registros será, al menos, de 2 años desde el transcurso del plazo anteriormente indicado, conforme al requerimiento REQ-ERDSP-7.10-02 de la norma EN 319 521.

5.5.3 Protección del archivo

LOGALTY protege el archivo de forma que sólo personas debidamente autorizadas puedan obtener acceso al mismo. Logalty emplea un producto que es un cifrador y firewall de datos. Permite proteger puntos de montaje (llamados Guardpoints) a partir de políticas de seguridad. Dichas políticas pueden ser muy granulares, pudiendo gestionar el acceso a los datos a una determinada serie de usuarios, procesos o incluso restringir el acceso en determinadas franjas horarias. El archivo está protegido contra visualización, modificación, borrado o cualquier otra manipulación mediante su almacenamiento en un sistema fiable.

Logalty entiende como tratamiento cualquier operación realizada con la información como son,

aunque no solo, su lectura, escritura, modificación, copia, transmisión, grabación o archivado mediante medios manuales o con aplicaciones informáticas. Dicho tratamiento está sujeto a medidas de trazabilidad las cuales permiten establecer, entendiendo como tal, la capacidad de conocer qué personas y cuando han accedido y tratado la información.

Logalty establece una segregación de funciones adecuada, que establece las medidas suficientes y necesarias para asegurar que los derechos de acceso (roles y perfiles) para cada usuario del servicio, se asignan de acuerdo con las necesidades funcionales de cada uno.

Se realizan revisiones periódicas sobre los permisos de acceso y los controles de acceso configurados en los sistemas involucrados en el servicio.

5.5.4 Procedimientos de copia de respaldo

LOGALTY dispone de un centro de almacenamiento externo para garantizar la disponibilidad de las copias del archivo de ficheros electrónicos. Los documentos físicos se encuentran almacenados en lugares seguros de acceso restringido sólo a personal autorizado.

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 ip virtual de Fujitsu (194.140.22.75) para acceder al servidor NTP stratum 1, que está situado en el propio Centro de Proceso de Datos.

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 entrega electrónica certificada.

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 Continuidad del Negocio y Recuperación de 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 a sí mismo 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 mínimo 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.

5.7 Terminación del servicio

En caso de terminación de la actividad, Logalty se regirá por lo dispuesto en la normativa vigente y contempla dos opciones:

1. El emisor puede solicitar la destrucción de los ficheros que LOGALTY tenga custodiados en la fecha de la efectiva terminación de los Servicios, emitiéndo en este caso por parte del Órgano de Administración de LOGALTY certificado acreditativo de que dicho borrado se ha realizado.

2. El emisor puede solicitar a LOGALTY que facilite la disposición de los ficheros custodiados a ASNEF (esto sólo es factible en el caso de las Entidades de Crédito al Consumo y sus Bancos matrices) o un tercero de confianza distinto de ASNEF; o que LOGALTY continúe con la custodia de los ficheros con su participación hasta la definitiva terminación y borrado de los mismos conforme a los criterios establecidos en los contratos firmados con los clientes, en ese caso estos contratos continuarán vigente, en lo referido a la custodia de los ficheros, conforme a las condiciones establecidas por las partes en el presente acuerdo.

En el primero de los supuestos del apartado anterior, el cliente emisor y LOGALTY acuerdan que el cliente emisor -una vez autorice la destrucción de los ficheros que correspondan, no podrá reclamar a LOGALTY indemnización alguna por la ruptura de la cadena de custodia de los mismos, si la destrucción se ha realizado en los plazos y condiciones establecidas entre las partes

En el segundo supuesto del apartado anterior, LOGALTY procederá a realizar una estimación de los costes de puesta a disposición de los ficheros custodiados al tercero indicado por el cliente emisor y previamente a la realización de dicho traslado de estos, se informará a éste de los costes estimados con el objeto de llegar a un acuerdo sobre el precio, forma de pago y condiciones de puesta a disposición para proceder posteriormente a su traslado.

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 entrega a los que sirven de soporte.

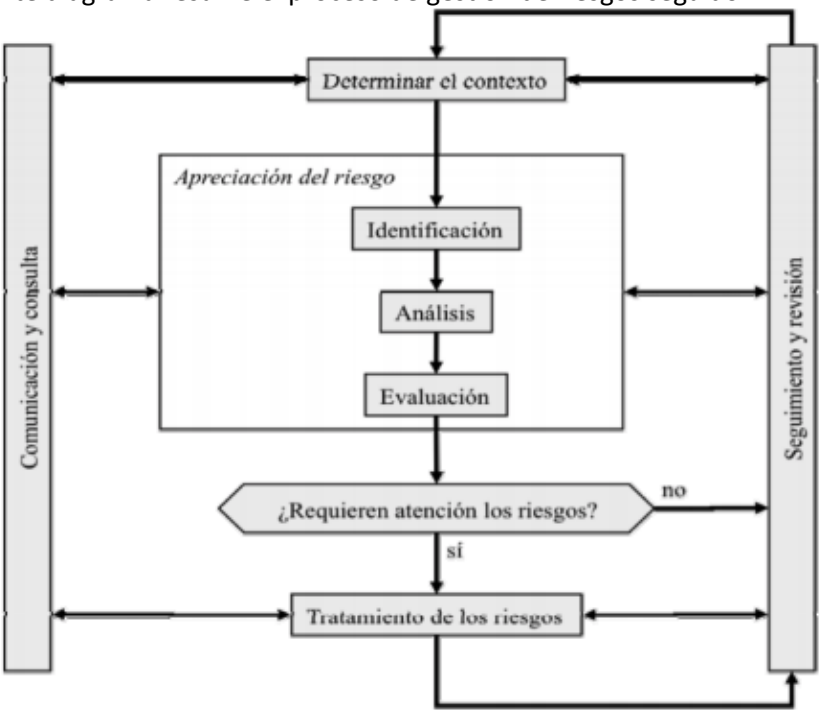
6.1 Análisis de riesgos

LOGALTY lleva a cabo un análisis de riesgos completo para el servicio de entrega electrónica certificada. Dicho análisis permite conocer el riesgo al que están sometidos los activos que soportan el servicio. Se incluyen activos técnicos, sistema de información, comunicaciones, ubicaciones, personal clave, y son los elementos que soportan el servicio.

Para ello se utiliza la herramienta PILAR que permite, de forma sistemática:

- Analizar el riesgo, en función de los activos existentes y lo que podría pasar
- Tratar los riesgos, que permite minimizar el riesgo, defendiendo para que no pase nada malo y al tiempo estando preparados para atajar las emergencias, sobrevivir a los incidentes y seguir operando en las mejores condiciones.

El siguiente diagrama resume el proceso de gestión de riesgos seguido:



Una vez calculado el riesgo residual, que es aquel que aún queda tras considerar loa controles existentes, se compara con el nivel de riesgo aceptable para Logalty. Si el riesgo estimado es mayor que el aceptable, se formula y ejecuta un Plan de Tratamiento del Riesgo.

6.2 Controles de seguridad de los sistemas informáticos

LOGALTY emplea sistemas fiables para ofrecer sus servicios de entrega electrónica certificada. 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 entrega electrónica certificada.

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 Backus y recuperación.
- Configuración de antivirus.
- Requerimientos de tráfico de red.

6.2.1 Requisitos técnicos específicos de seguridad informática

Los servidores de Logalty están plataformados de acuerdo con buenas prácticas reconocidas y sólo tienen activos los servicios necesarios.

El servidor de base de datos deberá instanciarse en un sistema distinto al de ejecución de la aplicación, habilitando únicamente la comunicación con el servidor donde se aloje la aplicación, no debiendo ser directamente accesible desde Internet

Cada servidor de LOGALTY incluye las siguientes funcionalidades:

- Imposición de separación de tareas para la gestión de privilegios.
- Identificación y autenticación de roles asociados a identidades.
- Auditoría de eventos relativos a la seguridad.
- Redes de gestión y de producción separadas.

- Zonas de red aisladas entre sí en función de los servicios que presten esos servidores (crypto, bbdd...)
- Uso de sistemas operativos con soporte para estar informados de bugs y vulnerabilidades.
- Necesidad de VPN para conectar a los servidores.
- Uso de doble barrera de seguridad: firewall compartido con el fabricante, por un lado, y firewall dedicado de Logalty a continuación.

6.2.2 Evaluación del nivel de seguridad informática

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

6.3 Controles técnicos del ciclo de vida

6.3.1 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.

6.3.2 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 por un grupo 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.

6.3.2.1 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.

Logalty dispone de una Normativa de Clasificación de la Información, que detalla los procedimientos de gestión de la información en función de su clasificación. Esta normativa establece pautas para su almacenamiento, tratamiento, transmisión y destrucción cuando proceda.

Los documentos están catalogados en tres niveles: PÚBLICA, INTERNA, CONFIDENCIAL, RESERVADA.

6.3.2.2 Operaciones de gestión

LOGALTY dispone de un Plan de Gestión de Incidencias, que se apoya en la implementación de un sistema de alertas y la generación de reportes periódicos.

Adicionalmente, Logalty tiene documentado todos los procesos de gestión que afectan a la operativa de los servicios de entrega electrónica certificada, como son: gestión de cambios, gestión de la capacidad, gestión de la configuración, gestión de vulnerabilidades y parches. Los tiempos de actuación no superan las 24 horas en casos de fallos de seguridad clasificados por el fabricante de carácter grave/alto.

Con respecto a la gestión de los cambios, el procedimiento incluye autorización, realización de pruebas, aprobaciones del usuario final y una separación adecuada de los entornos previos respecto del entorno de producción.

6.3.2.3 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.

(i) 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.

(ii) 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.

(iii) 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.

6.3.2.4 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:

- 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 una Normativa de Control de acceso que establece pautas para el acceso lógico.
- 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.

6.4 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.

Las comunicaciones con los CPD's son redundadas. La arquitectura de seguridad de Logalty cuenta con: Firewall, Sistemas de Detección y Prevención de Intrusos (IDS/IDPS), Zona Desmilitarizada (DMZ), Redes Privadas Virtuales (VPN) y Proxy.

6.5 Controles de ingeniería de módulos criptográficos

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

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

Todas las operaciones criptográficas de LOGALTY son realizadas empleando claves generadas y custodiadas de forma segura en módulos criptográficos con las certificaciones FIPS 140-2 level 3 y/o Common Criteria EAL 4+ (con el aumento ALC_FLR.1).

6.6 Fuentes de Tiempo

LOGALTY tiene un procedimiento de sincronización de tiempo coordinado con Fujitsu vía NTP.

Los servidores están conectados a una ip virtual de Fujitsu (193.148.29.99) que a su vez está conectado contra el servidor NTP de stratum 1 de RedIris (hora.rediris.es), que situado en la Universidad Autónoma de Madrid.

7 Auditoría de conformidad

7.1 Frecuencia de la auditoría de conformidad

LOGALTY lleva a cabo una auditoría de conformidad anualmente, además de las auditorías internas que realiza bajo su propio criterio o en cualquier momento, debido a una sospecha de incumplimiento de alguna medida de seguridad.

7.2 Identificación y calificación 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.

7.3 Relación del auditor con la entidad auditada

Las empresas de auditoría son de reconocido prestigio con departamentos especializados en la realización de auditorías informáticas, por lo que no existe ningún conflicto de intereses que pueda desvirtuar su actuación en relación con LOGALTY.

7.4 Listado de elementos objeto de auditoría

La auditoría verifica respecto a LOGALTY:

a) Que la entidad tiene un sistema de gestión que garantice la calidad del servicio prestado.

b) Que la entidad cumple con los requerimientos de la DPC y otra documentación vinculada con la emisión de los distintos certificados digitales.

c) Que la DPC y demás documentación jurídica vinculada, se ajusta a lo acordado por LOGALTY y con lo establecido en la normativa vigente.

d) Que la entidad gestiona de forma adecuada sus sistemas de información

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

a) Procesos de la AC, ARs y elementos relacionados.

b) Sistemas de información.

c) Protección del centro de proceso de datos.

d) Documentos.

7.5 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 gerencia responsable del servicio en 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.

7.6 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 30 días tras la ejecución de la auditoría.

8 Requisitos comerciales y legales

8.1 Tarifas

LOGALTY establece tarifas por la prestación del servicio, de las que, en su caso, se informa oportunamente a los clientes.

8.2 Capacidad 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 c), en relación con la gestión de la finalización de los servicios y plan de cese.

8.2.1 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 con un mínimo asegurado de 3.000.000 de euros.

8.2.2 Otros activos

Sin estipulación.

8.2.3 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, con un mínimo asegurado de 3.000.000 de euros.

8.3 Confidencialidad

8.3.1 Informaciones confidenciales

Las siguientes informaciones son mantenidas confidenciales por LOGALTY:

- Claves privadas generadas y/o almacenadas por el prestador de servicios de confianza.
- 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 LOGALTY 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”.

8.3.2 Informaciones no confidenciales

Sin estipulación.

8.3.3 Divulgación legal de información

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

8.3.4 Divulgación de información por petición de su titular

Sin estipulación.

8.3.5 Otras circunstancias de divulgación de información

Sin estipulación.

8.4 Protección de datos personales

Para la prestación del servicio, LOGALTY actúa como encargado del tratamiento, conforme a lo establecido en la normativa vigente y documenta sus obligaciones y controles en el contrato de servicio.

8.5 Derechos de propiedad intelectual

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

8.6 Obligaciones y responsabilidad civil

8.6.1 Obligaciones

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 entrega electrónica certificada conforme con esta Declaración de Prácticas de Certificación y los correspondientes contratos de servicio.

Con anterioridad a la prestación del servicio, LOGALTY informa al cliente de los términos y condiciones del servicio, de su precio y de sus limitaciones de uso. En el caso del Emisor, la información se contiene en el contrato de servicio que firman ambas partes, mientras que en el caso del Receptor, la información se contiene en las condiciones generales del servicio, que se ponen a su disposición mediante enlace en las comunicaciones que LOGALTY le dirige en el transcurso de la prestación del servicio contratado por el emisor.

Los servicios no requieren que LOGALTY acceda, en ningún momento, al contenido de los documentos que el Emisor pone a disposición del Receptor en su virtud. Sin perjuicio de lo anterior, LOGALTY procede a estampar su sello y un código identificativo a cada documento que entrega en el marco de sus procedimientos, no realizando modificación alguna del contenido.

Se entenderá que el Receptor ha accedido al contenido de usuario remitido por el Emisor cuando, una vez, identificado y autenticado, LOGALTY le permita visualizar o descargar el fichero correspondiente que ha puesto a su disposición.

Los clientes se obligan al uso correcto de los servicios, conforme a las instrucciones de LOGALTY. En el caso del Emisor, el mismo asume obligaciones de confidencialidad y protección de datos, en su condición de responsable del tratamiento. Los clientes serán responsables, conforme a la normativa legal vigente, del incumplimiento de sus obligaciones.

8.6.2 Limitación de uso y de responsabilidades

Los servicios de entrega electrónica certificada se encuentran limitados a su uso en los servicios de notificación y contratación ofrecidos por LOGALTY, en los que se integran, y para dichas finalidades. Cualquier otro uso se encuentra restringido y deberá ser previamente autorizado por LOGALTY.

Adicionalmente, LOGALTY se reserva el derecho a establecer limitaciones de responsabilidad en los contratos con los emisores, siempre que las mismas sean compatibles con lo establecido en el artículo 13 del Reglamento (UE) 910/2014, de 23 de julio.

8.6.3 Cláusulas de indemnidad

LOGALTY se reserva el derecho a establecer cláusulas de indemnidad en los contratos con los emisores, siempre que las mismas sean compatibles con lo establecido en el artículo 13 del Reglamento (UE) 910/2014, de 23 de julio.

8.6.4 Caso fortuito y fuerza mayor

Sin estipulación.

8.6.5 Ley aplicable

LOGALTY establece, en el contrato, que la ley aplicable a la prestación de los servicios es la Ley española.

8.6.6 Cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación

Sin estipulación.

8.6.7 Cláusula de jurisdicción competente

LOGALTY establece, en el contrato, 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.

8.6.8 Resolución de conflictos

LOGALTY puede establecer, en el contrato, los procedimientos de mediación y resolución de conflictos alternativos a los mecanismos judiciales legalmente aplicables.