DIGITELTS

by MADISON

rolidentid

Servicio Cualificado de Entrega Electrónica Certificada

Declaración de Prácticas y Políticas

Control documental

Líder	Área de servicios de confianza		
Tipo	Declaración de prácticas del servicio electrónico de confianza de entrega electrónica certificada de DIGITELTS		
Distribución	**Público**		
Fecha	2025		
Descripción	Declaración de prácticas del servicio de entrega electrónica certificada		
Aprobado	Comité de Riesgos y Seguridad DIGITEL TS	Fecha	24 junio 2025
Estado	Aprobado		

Control de Cambios

Versión	Fecha	Detalle
V1.0	10 abril 2024	Primera versión del documento
V1.1	27 mayo 2024	Corrección de erratas
V2.0	18 junio 2025	Revisión anual. Adaptación a la normativa siguiente: ▪ Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) nº 910/2014. ▪ Directiva (UE) 2022/2555 (Directiva NIS 2) y su Reglamento de Ejecución 2024/2690 de 17/10/2024. ▪ Estándar ETSI EN 319401 V3.1.1 (2024-06) ▪ Estándar ETSI EN 319 521 V1.1. (2019-02). ▪ Estándar ETSI EN 319 522-1 V1.2.1 (2024-01) ▪ Estándar ETSI EN 319 522-2 V1.2.1 (2024-01)

1 Introducción

Este documento declara las prácticas de confianza (en adelante DPC) en la prestación de los servicios de entrega electrónica certificada cualificada por parte de DIGITELTS.

En esta DPC se detallan las condiciones aplicables para la identificación y autenticación del emisor y receptor, las medidas de seguridad organizativas y técnicas, la integridad de las transacciones, la exactitud de la fecha y hora de envío y recepción de los datos y el almacenamiento y custodia de todas las evidencias generadas en proceso. Las evidencias quedan recogidas en un certificado de evidencias generado por DIGITELTS, que queda a disposición de las partes interesadas, conservándose por el tiempo legal y/o contractualmente establecido.

DIGITELTS ofrece el servicio en 'modelo caja negra' que consiste en un sistema bajo responsabilidad de un único Proveedor de servicios de entrega electrónica certificada, y que no interopera ni se relaciona con otros proveedores de servicios de entrega electrónica certificada.

2 Identificación

Nombre del documento	Servicio de Entrega Electrónica Certificada. Declaración de Prácticas y Políticas
Versión del documento	2.0
Estado del documento	Vigente
OID	No aplicable

Ubicación del documento	https://pki.digitelts.es

3 Participantes en el servicio de entrega electrónica certificada cualificada

3.1 DIGITELTS como Prestador de servicios de confianza cualificado

DIGITEL TS es un Prestador de Servicios de Confianza Cualificado (PCSC) conforme al Reglamento (UE) del Parlamento 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, modificado por el Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, en lo que respecta al establecimiento del marco europeo de identidad digital (en adelante, Reglamento eIDAS) . Para la prestación de sus servicios de confianza Digitel TS cumple también con lo establecido en la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

Para garantizar la ciberseguridad y la ciberresiliencia de los servicios amparados en esta DPC, DIGITELTS ha alineado sus operaciones a los requisitos de seguridad de redes y de la información establecidos en la Directiva (UE) 2555/2022 (Directiva NIS2) y su Reglamento de Ejecución (UE) 2024/2690; así como, a la normativa de desarrollo que se dicte incluida la normativa de transposición al ordenamiento jurídico español.

El contenido de esta DPC de DIGITELTS para el servicio cualificado de entrega electrónica certificada se realiza en cumplimiento con la legislación vigente y alineada con el Reglamento eIDAS y sigue las indicaciones de las normas técnicas del Instituto Europeo de Estándares de Telecomunicaciones (en adelante ETSI) aplicables a los servicios de entrega electrónica certificada, principalmente ETSI EN 319 401 y ETSI EN 319 521 y ETSI EN 319 522.

3.2 Emisor

El emisor es la persona física o jurídica que emite la comunicación. En los servicios prestados por DIGITELTS, es el subscriptor del servicio, acreditado mediante la firma de un contrato o una petición de servicio y tiene una duración determinada, renovable según las condiciones estipuladas en el mismo.

El emisor será debidamente identificado de forma fehaciente por la plataforma del servicio de entrega electrónica certificada de DIGITELTS mediante su certificado electrónico cualificado admitido en el servicio, que se incluirá en la plataforma utilizando la parte pública del certificado. Digitel TS admitirá la identificación del emisor mediante los certificados electrónicos cualificados de persona física expedidos por el Prestador de Servicios de Confianza FNMT-CERES (AC FNMT Usuarios) o los certificados cualificados personales de DIGITELTS.).

3.3 Destinatario

El destinatario es la persona física o jurídica a la que va dirigida la comunicación. El destinatario será contactado por DIGITELTS mediante un canal de comunicación seleccionado por el emisor (email, SMS o WhatsApp) en el que se le comunica la puesta a disposición de una documentación o información por parte del emisor, al que puede acceder a través de la url de acceso que se comunica en el mensaje.

El destinatario deberá identificarse en el servicio de entrega electrónica certificada de DIGITELTS de forma fehaciente utilizando un certificado electrónico cualificado emitido por un Prestador de Servicios de Certificación Cualificado y, además, que este admitido por el servicio de DIGITELTS.

Digitel TS admitirá la identificación del destinatario mediante los certificados electrónicos cualificados de persona física expedidos por el Prestador de Servicos de Confianza FNMT-CERES (AC FNMT Usuarios) o los certificados cualificados personales de DIGITELTS. (Una vez que se ha completado el proceso de identificación del destinatario en la plataforma y este ha

resultado satisfactorio, la solución informática pone a su disposición el contenido de la comunicación enviada por el emisor para su aceptación y descarga o rechazo, en su caso.

La duración de la puesta a disposición del documento es de 15 días. . Una vez finalizado el plazo, el acceso a la comunicación dejará de estar disponible para el destinatario.

3.4 Partes usuarias

Las partes usuarias son aquellas partes que confían en el servicio de entrega electrónica certificada prestado por DIGITELTS y en las evidencias generadas por el servicio. En consecuencia, deberán tener en cuenta, los términos y condiciones del servicio.

1. Las partes podrán acceder a la información de los servicios, incluyendo las actas del servicio de entrega electrónica certificada que deseen comprobar, bien logándose en la plataforma, si estuviera autorizado, o bien enviando un correo a DIGITELTS, a comercial@digitelts.com, si no tuviera acceso.

3.5 Prestadores de Servicios Cualificados intervinientes

Para la prestación del servicio de entrega electrónica certificada amparado en esta DPC, DIGITELTS utiliza los servicios cualificados de otros prestadores cualificados de servicios de confianza, concretamente los siguientes:

2. El certificado cualificado de Sello electrónico de entidad jurídica que utiliza Digitel TS para sellar las evidencias de su servicio de entrega electrónica certificada es expedido por VINTEGRIS.

El certificado cualificado de sello de tiempo utilizado para sellar temporalmente las evidencias es emitido por la TSA de DIGITEL TS.

3.6 Otros prestadores de servicios

DIGITELTS utiliza en la prestación de su Servicios de Entrega Electrónica Certificada, los servicios de los proveedores siguientes:

- Infraestructura donde se aloja el servicio a través de AMAZON WEB SERVICES (AWS)

- El certificado de SSL utilizado por la plataforma es de la CA AWS

4 Administración de la política

4.1 Organización que administra el documento

Autoridad de Certificación de DIGITELTS.

DIGITEL ON TRUSTED SERVICES S.L.U

C/ Enrique Cubero, 9, 47014 Valladolid (España)

+34 91 015 05 10

pki@digitelts.es

4.2 Datos de contacto de la organización

- Razón Social: DIGITEL ON TRUSTED SERVICES S.L.U
- Denominación Comercial: Autoridad de Certificación de DIGITELTS TS
- CIF: B47447560
- Domicilio Social: C/ Enrique Cubero, 9, 47014 Valladolid (España).
- Servicio de Atención al Cliente (SAC): 91 015 05 10
- Correo electrónico: comercial@digitelts.com
- Web: https://pki.digitelts.es
- Identificación en el Registro Mercantil de Valladolid: Tomo 891, Folio 38, Hoja VA-11307

4.3 Responsables en el procedimiento de gestión del documento

El sistema documental y de organización de DIGITELTS 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.

El Comité de seguridad de la información ostenta la capacidad para proponer, revisar y aprobar este procedimiento de revisión.

4.4 Revisión del documento

DIGITELTS revisa este documento al menos una vez al año, o cuando se produzcan incidentes importantes o cambios significativos en las operaciones o en los riesgos. El responsable del servicio será el responsable del mantenimiento de este documento siguiendo las indicaciones de la Política de Seguridad de DIGITELTS.

El responsable de seguridad enviará al Comité de Seguridad cambios, sugerencias y propuestas de modificaciones de este documento para su aprobación.

El Comité de Seguridad trata si las modificaciones aprobadas necesitan ser notificadas ante el supervisor español. DIGITELTS informará al supervisor español los cambios en los servicios amparados en esta DPC con una antelación mínima de un mes antes de llevarlos a cabo, conforme estipula el artículo 24. 2 letra a) del Reglamento eIDAS.

Los cambios en esta Declaración de Prácticas que puedan afectar a la aceptación del servicio por los suscriptores o por las partes usuarias, serán informados con la publicación de este documento en la página web de DIGITEL TS: https://pki.digitelts.es

Fases del procedimiento de cambios:

1. Recogida de propuestas
2. Análisis y estudio de las propuestas.
3. Redacción de los borradores

4. Presentación en el Comité de Seguridad para comentarios y aprobación.
5. Redacción final
6. Publicación en la web para informar a suscriptores y partes interesadas
7. En caso de necesidad, notificación al supervisor español.

DIGITELTS realiza una nueva revisión de este documento ante la inclusión de cambios suficientemente relevantes para la gestión de los servicios cualificados de entrega electrónica certificada. La descripción de los cambios se incluirán en el apartado "control de versiones" de la sección "Información General" en el inicio de este documento.

4.5 Aprobación del documento

Las siguientes modificaciones de esta Declaración de Prácticas de Confianza y de la Política de Seguridad son aprobadas por el Comité de Seguridad de la Información, el cual de forma adicional se responsabilizará de su correcta implementación.

DIGITELTS comunica de forma permanente los cambios que se produzcan en sus obligaciones publicando nuevas versiones de su documentación jurídica en su web https://pki.digitelts.es

5 Definiciones y acrónimos

5.1 Definiciones

Concepto	Definición
Servicio de entrega electrónica certificada (ERDS)	Servicio electrónico que permite transmitir datos entre el remitente y los destinatarios por medios electrónicos y que proporciona pruebas relativas al tratamiento de los datos transmitidos incluida la prueba de envío y recepción de los datos, y que protege los datos transmitidos contra el riesgo de pérdida, robo, daños o cualquier alteración no autorizada
Servicio cualificado de entrega electrónica certificada (QERDS)	Un servicio de entrega electrónica certificada que cumple los requisitos establecidos en el artículo 44 del Reglamento (UE) nº 910/2014
Pruebas del servicio de entrega electrónica certificada (ERDS)	Datos generados en el marco del servicio de entrega electrónica certificada que tiene por objeto demostrar que un determinado hecho se ha producido en un determinado momento.
Autenticación	Es un proceso electrónico que de verificar la identidad de una persona física o jurídica.
Cifrado	Operación mediante la cual un mensaje en claro se transforma en un mensaje ilegible.

Envío	Acto de poner el contenido del usuario a disposición del destinatario, dentro de los límites del servicio de entrega electrónica certificada
Remitente	Persona física o jurídica que envía el contenido de la comunicación mediante el servicio de entrega electrónica certificada al destinatario.
Destinatario	Persona física o jurídica a quien va dirigida la comunicación.
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 titular 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.
DPC de entrega electrónica certificada	Conjunto de prácticas adoptadas por un proveedor de servicios de confianza de entrega electrónica certificada . El servicio puede proveerse de manera cualificada en el marco del Reglamento (UE) 910/2014 eIDAS y la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los

	servicios electrónicos de confianza y de sus disposiciones de desarrollo,
Proveedor de servicios de entrega electronica certificada	Proveedor de servicios de confianza que presta el servicio de entrega electrónica certificada
Proveedor cualificado de servicios de entrega electrónica certificada (QERDSP)	proveedor de servicios de confianza que presta servicios cualificados de entrega electrónica certificada
Firma electrónica	los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar
OID	Identificador numérico único registrado bajo la estandarización ISO y referido a un objeto o clase de objeto determinado.
FUNCIÓN HASH	Operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado.
HASH O HUELLA DIGITAL	Resultado de tamaño fijo que se obtiene tras aplicar una función hash a un mensaje y que cumple la propiedad de estar asociado unívocamente a los datos iniciales.

5.2 Acrónimos

Acrónimo	Definición
QERDS	Servicio Cualificado de Entrega Electrónica Certificada
AC (o también CA)	Certificate Authority Autoridad de Certificación
DPC (o también CPS)	Certification Practice Statement. Declaración de Prácticas de Certificación
ETSI EN	European Telecommunications Standards Institute – European Standard.
HSM	Hardware Security Module Módulo de seguridad en Hardware

LOPDGDD	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
NIF	Número de Identificación Fiscal
OCSP	On-line Certificate Status Protocol. Protocolo de acceso al estado de los certificados
OID	Object Identifier. Identificador de objeto
PKI	Public Key Infrastructure. Infraestructura de clave pública Conjunto de elementos hardware, software, recursos humanos, procedimientos, etc., que componen un sistema basado en la creación y gestión de certificados de clave pública
TSA	Time Stamping Authority Autoridad de Sellado de Tiempo Electrónico

6 Publicación de la información

6.1 Publicación de la información del prestador

DIGITELTS publica, en su depósito, la declaración de prácticas del servicio de entrega electrónica certificada y el historial de sus versiones; así como, los certificados que se emplean para validar las evidencias producidas por DIGITELTS en el marco de la prestación de este servicio de confianza.

Esta información puede encontrarse en la siguiente dirección: https://pki.digitelts.es/

6.2 Frecuencia de publicación

La información del prestador de servicios de entrega electrónica certificada se publica en cuanto se encuentra disponible.

Los cambios en la Declaración de Prácticas de Confianza se rigen por lo establecido en la sección 4 de este documento.

6.3 Control de acceso

DIGITELTS no limita el acceso de lectura a esta información, 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.

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

- Únicamente personas autorizadas puedan hacer anotaciones y modificaciones en los datos almacenados.
- Pueda comprobarse la autenticidad de la información.
- Los certificados sólo estén disponibles para consulta si la persona física o la persona jurídica ha prestado su consentimiento.
- Pueda detectarse cualquier cambio técnico que afecte a los requisitos de seguridad.

7 Identificación y autenticación de los usuarios

7.1 Verificación inicial de la identidad del emisor

El usuario que va a acceder a la plataforma de envío de notificaciones electrónicas certificadas deberá haberse dado de alta previamente en el sistema utilizando certificado electrónico cualificado expedido por un Prestador Cualificado de Servicios de Confianza, vigente y válido (no revocado). El certificado electrónico estará asociado a una a una persona física que habrá firmado el contrato o ficha de pedido con DIGITELTS.

DIGITELTS verificará la identidad del emisor mediante un certificado cualificado de firma electrónica Admitidos por la plataforma y que son los siguientes: certificados de ciudadano de FNMT (AC FNMT Usuarios) y certificados personales de DIGITEL TS.

Una vez se ha autenticado en el servicio, el emisor podrá realizar los envíos que correspondan asociándose el método de autenticación a estos envíos.

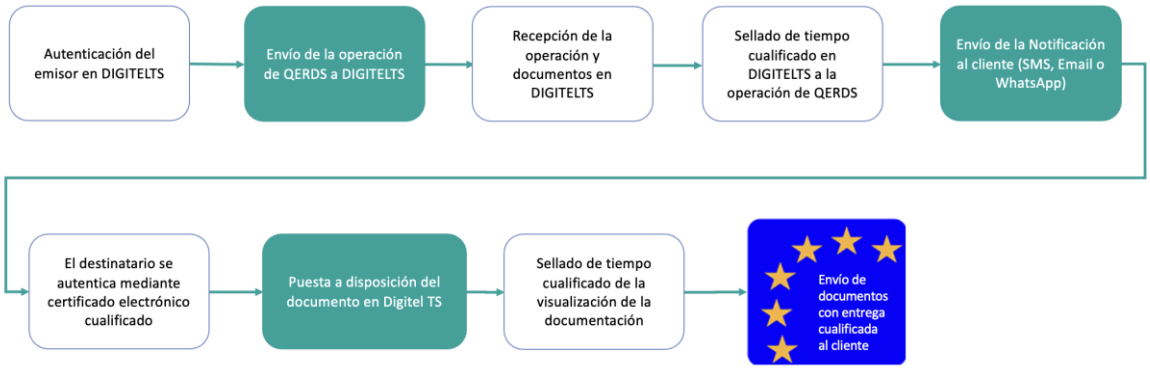
El tiempo de sesión máximo de inactividad está determinado a 10 minutos.

7.2 Identificación del destinatario y entrega del contenido

El destinatario del contenido puesto a disposición por parte del emisor únicamente se entregará una vez se haya identificado de forma correcta en la plataforma. Para ello deberá utilizar un certificado cualificado admitido por el servicio de QERDS de DIGITELTS que son los

siguientes: certificados de ciudadano de FNMT (AC FNMT Usuarios) y certificados personales de DIGITEL TS.

8 Operativa del servicio



El servicio de Entrega electrónica certificada cualificada consiste en el envío de comunicaciones o notificaciones electrónicas y de forma certificada por parte de subscriptores del servicio a terceros de su interés. Durante la prestación del servicio se generan las siguientes evidencias electrónicas:

- Fecha y hora de la generación del envío de la comunicación electrónica certificada e identificación del usuario que realiza el envío

3. certificado eDelivery.

- La recepción de la documentación a comunicar en la plataforma, enviada por el Emisor.
- El envío de la comunicación al Destinatario.
- Identificación del destinatario

4. El acceso o rechazo del Destinatario al servicio de entrega electrónica certificada.
5. El acceso del Destinatario, dentro del servicio a los documentos pendientes.

- En su caso, caducidad del envío por inacción del destinatario.
- En su caso descarga del documento. Certificado de evidencias que recopile todo lo sucedido durante el servicio cualificado de entrega electrónica certificada cualificada.

Al finalizar la operación se generará un documento de evidencias que recopilará todo lo sucedido durante el servicio cualificado de entrega electrónica certificada cualificada. Dicho documento de evidencias se enviará por correo electrónico

DIGITELTS custodia dichas evidencias durante 15 años, tal y como exige la Ley 6/2020, reguladora de determinados aspectos de los servicios electrónicos de confianza.

Además, DIGITELTS revisa los registros de auditoría periódicamente, verificando su normal actividad y que no han sido manipulados. Se utilizan controles de acceso físico y lógico para los ficheros de registro, quedando protegidos de accesos, modificaciones o eliminaciones no autorizadas. Estos registros de auditoria serán retenidos por un período mínimo de 2 años.

9 Integridad y confidencialidad del contenido del usuario

Digitel TS garantiza la adecuada disponibilidad, integridad y confidencialidad del contenido del usuario cuando utiliza el servicio de Entrega Electrónica Certificada, firmando las evidencias producidas durante el proceso de entrega con un certificado cualificado de sello electrónico emitido por un Prestador de Servicios de Confianza Cualificado.

Además, DIGITELTS protege la confidencialidad de la identidad del emisor y del destinatario, tanto durante el envío, como durante la custodia de las evidencias, cifrando las comunicaciones mediante certificados de autenticación web.

DIGITELTS protege la integridad del contenido y sus metadatos asociados, mediante una sello electrónico soportado por un certificado cualificado generado por un Prestador de Servicios de Certificación Cualificado, e incorporando un sello de tiempo cualificado, de tal forma que se excluye la posibilidad de que los datos puedan cambiar de forma indetectable.

El servicio de Entrega Electrónica certificada permite enviar ficheros en formato PDF con un máximo de 5 documentos.

El límite de tamaño por fichero es de 18Mb por documento.

6. Referencias de tiempo

Las evidencias sucedidas en la utilización del servicio serán selladas mediante un sello electrónico de tiempo cualificado, emitido por DIGITELTS en dicho servicio. Adicionalmente, se sellará el certificado de evidencias generado por la plataforma del servicio de entrega electrónica certificada, con un sello electrónico de entidad emitido por VINTEGRIS y un sello de tiempo cualificado.XXXXX.

DIGITELTS garantiza que el certificado electrónico de sello de entidad con el que sella las evidencias del servicio amparado en esta DPC se encuentra vigente y no ha sido revocado ni ha caducado.

10 Obligaciones de las partes

10.1 Obligaciones de Digitel TS

En el marco de la prestación del servicio de entrega electrónica certificada, DIGITELTS, se obliga a:

- Prestar el servicio conforme a lo dispuesto en esta DPC y en los términos y condiciones del servicio.
- Prestar el servicio de forma diligente, garantizando que el servicio está adecuado a su cualificación.
- Publicar toda la información relevante del servicio que deba ser conocida, como las características de la prestación del servicio, las obligaciones que asumen sus suscriptores y partes usuarias y los límites de responsabilidad.

7. Proporcionar el acceso ininterrumpido al servicio, y comunicar a sus usuarios con la suficiente antelación la no disponibilidad del sistema en caso de realizar procesos de modificación, mejora o mantenimiento que impliquen una paralización del mismo.
   - Garantizar la integridad, confidencialidad y disponibilidad del contenido del usuario, dentro de la plataforma de entrega electrónica certificada.

8. Establecer mecanismos de custodia y de transmisión segura de las evidencias producidas por el servicio de entrega electrónica certificada, quedando protegidas de cualquier manipulación no autorizada, falsificación, pérdida, o destrucción.
9. Garantizar que los eventos producidos por el sistema operen en sincronía con fuentes fiables de tiempo, utilizando para ello una Autoridad de Sellado de Tiempo cualificada.
    - Proteger las claves privadas de los certificados cualificados utilizados en el servicio de entrega electrónica certificada.
    - Proteger la confidencialidad de la información del usuario (emisor y destinatario) tanto durante el envío como durante la custodia de evidencia en el marco de las comunicaciones realizadas con el Servicio utilizando algoritmos de cifrado robustos.
    - Conservar la información relativa al servicio de entrega electrónica certificada durante 15 años desde la finalización del servicio prestado.
10. Notificar a las partes las incidencias en el servicio de entrega certificada que puedan afectarles.
11. Disponer de un canal de comunicación con clientes y terceros para solicitudes, consultas, quejas y reclamaciones y atender a las mismas en un plazo razonable.
    - Informar al Órgano Supervisor en materia de servicios de confianza, al menos un mes antes de cualquier auditoría prevista y permitir su participación en calidad de observador.
    12. Notificar al Órgano Supervisor en materia de servicios de confianza, cualquier modificación sustancial producida en el servicio, al menos un mes antes de llevar a cabo tal modificación o cambio, que afecte a su condición de Prestador de Servicio Electrónico de Confianza y con una antelación de al menos tres meses en caso de que tenga intención de cesar tales actividades.
13. Notificar al Órgano Supervisor en materia de servicios de confianza, al equipo de respuesta a incidentes de Seguridad (CSIRT) de referencia, o en su caso, al organismo competente en materia de ciberseguridad, en un plazo de 24 horas, la violación de seguridad con impacto significativo en el servicio electrónico de confianza.

14. Notificar a la Agencia Española de Protección de Datos las violaciones de seguridad que afecten a datos personales, en un plazo máximo de 72 horas desde que se tiene conocimiento del mismo.
15. Llevar a cabo las auditorias periódicas necesarias para asegurar la adecuación y cumplimiento de la normativa aplicable, tanto interna como externa.
16. Utilizar la tecnología adecuada para proteger de manera fiable todos los datos de sus clientes, así como los registros de actividad y auditoria.
17. Disponer de un seguro de responsabilidad civil para cubrir los riesgos derivados del servicio y que cubra, al menos, el valor mínimo exigido por la normativa vigente.
18. Seleccionar proveedores de servicios y de componentes de los servicios así como subcontratistas que ofrezcan garantías de ciberseguridad conformes a la legislación aplicable.
19. Exigir que los proveedores de servicios de TIC propaguen los requisitos de seguridad de Digitel TS a lo largo de su cadena de suministro, en caso de que subcontraten partes del servicio de TIC prestado a Digitel TS.
20. Aplicar prácticas estándar de ciberhigiene en la prestación de sus servicios que serán cumplidas por empleados, incluidos los órganos de dirección así como por los proveedores de servicios, los proveedores de componentes del servicio y otros subcontratistas.

10.2 Obligaciones de los suscriptores del servicio

Tanto el emisor como el destinatario tendrán las obligaciones siguientes:

21. Deberán conocer lo dispuesto en la presente DPC, en particular las condiciones, responsabilidades y limitaciones del servicio y, en su caso, lo dispuesto en el contrato de prestación del servicio.
22. Deberán comunicar a DIGITELTS cualquier incidente de seguridad, fallo o situación anómala relativa al servicio de Entrega Electrónica Certificada, en el momento que lo identifique.
    - Deberán validar las firmas y sellos electrónicos que se han incorporado en la declaración de evidencias del Servicio.

23. El emisor deberá proporcionar a DIGITELTS información veraz, completa y exacta para la prestación del servicio de entrega electrónica certificada, incluidos los datos de los destinatarios sin errores y actualizados.
    - El emisor deberá comunicar sin demora cualquier modificación de las circunstancias que incidan en la prestación del servicio de Entrega Electrónica Certificada.

10.3 Obligaciones de las terceras parte usuarias

Las personas físicas o jurídicas que confíen en el servicio prestado en el servicio de entrega electrónica certificada deDIGITELTS deberán:

- Conocer las limitaciones de uso (si las hubiera) del servicio, según la presente DPC, así como los términos y condiciones del servicio.
- Cumplir con lo dispuesto en la normativa aplicable.
- Reportar tan pronto como sea posible, a DIGITELTS cualquier incidente relacionado con el servicio, que tenga conocimiento.
- Validar las firmas y sellos electrónicos que se han incorporado en las declaraciones de evidencias del servicio.

11 Controles de seguridad física, de gestión y de operaciones

11.1 Controles de seguridad física

Los edificios donde se encuentra ubicada la infraestructura del Prestador disponen de medidas de seguridad de control de acceso, de forma que solo se permite la entrada a los mismos a las personas debidamente autorizadas, los cuales cumplen los siguientes requisitos físicos.

En concreto, la política de seguridad física y ambiental aplicable a los dispositivos criptográficos 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.

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.

11.1.1 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.

11.1.2 Acceso físico

DIGITELTS 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 de los dispositivos criptográficos, debiendo accederse desde los niveles inferiores a los niveles superiores.

El acceso físico a las dependencias de DIGITELTS en el que se realizan los procesos operativos relacionados con el servicio de entrega electrónica certificada amparado en este documento, está limitado y protegido mediante una combinación de medidas físicas y procedimentales. De esta forma se siguen las siguientes indicaciones:

- 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 huella biométrica y es 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 DIGITELTS a los administradores del servicio de hospedaje que disponen de la llave para abrir la cabina.

En cuanto al acceso a las salas de acceso restringido en el CPD existe un listado con las personas autorizadas a pedir acceso a las personas que dependen directamente de ellos como empleado o como externos.

Para la intervención de un tercero en el CPD se requiere que los responsables de la gestión del CPD conozcan previamente el detalle de la intervención y se planifique en tiempo.

Para ello hay que abrir una solicitud de acceso donde indicar:

- 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.

11.1.3 Electricidad y aire acondicionado

Las instalaciones de DIGITELTS 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.

11.1.4 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.

11.1.5 Prevención y protección de incendios

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

11.1.6 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 fuerte fuera de las instalaciones de los Centros de Procesos de Datos.

11.1.7 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.

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

11.1.8 Copia de seguridad 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.

11.2 Controles de procedimientos

DIGITELTS 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 DIGITELTS ejecuta los procedimientos administrativos y de gestión de acuerdo con la política de seguridad.

11.2.1 Funciones fiables

- **Auditor Interno (*System Auditors*[1] en ETSI 310 401):** responsable del cumplimiento de los procedimientos operativos. Se trata de una persona externa al departamento de Sistemas de Información. Estas funciones estarán subordinadas a la jefatura de operaciones, reportando tanto a ésta como a la dirección técnica.
- **Administrador de Sistemas de certificación (*System administrator*[2] en ETSI 319 401):** responsable del funcionamiento correcto del hardware y software de soporte en la plataforma de entrega electrónica certificada

[1] REQ-7.2-15
[2] REQ-7.2-15

- **Operador del sistema (*System Operator*[3] en ETSI 319 401):** responsables de las operaciones diarias de los sistemas confiables del PSC para el servicio de entrega electrónica certificada. Autorizados a realizar copias de seguridad del sistema.

Responsable de Seguridad (*Security Officer*[4] en ETSI 319 401): encargado de coordinar, controlar y hacer cumplir las medidas de seguridad definidas por las políticas de seguridad de DIGITEL. Se encarga de los aspectos relacionados con la seguridad de la información: lógica, física, redes, organizativa, etc.

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

11.2.2 Número de personas por tarea

DIGITELTS garantiza al menos dos personas para realizar las tareas que se detallan en esta DPC.

11.2.3 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.

[3] REQ-7.2-15
[4] REQ-7.2-15

11.3 Controles de personal

11.3.1 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.

En general, DIGITELTS 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.

DIGITELTS no asignará a un rol de confianza 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.

11.3.2 Procedimientos de investigación de historial

DIGITELTS, 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.

DIGITELTS realiza dichas comprobaciones con observancia estricta del REGLAMENTO eIDAS, 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, advirtiéndose de que la negativa a someterse a la investigación implicará el rechazo de la solicitud.

11.3.3 Requisitos de formación

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

Existe un procedimiento de actualización de conocimientos del personal afectado ante cambios tecnológicos, introducción de nuevas herramientas o modificación de procedimientos operativos. También ante cambios organizativos y de documentación relevante se llevarán a cabo sesiones formativas y de sensibilización.

Asimismo, DIGITELTS garantiza que sus empleados, incluidos los miembros de los órganos de dirección; así como, los proveedores directos y los prestadores de servicios sean

conscientes de los riesgos, estén informados de la importancia de la ciberseguridad y apliquen prácticas de ciberhigiene conformes a las Políticas de DIGITELTS y la legislación aplicable.

11.3.4 Requisitos y frecuencia de actualización formativa

DIGITELTS 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 la prestación del servicio de QERDS, así como tras producirse incidentes significativos o cuando se produzcan cambios en las operaciones o en los riesgos .

11.3.5 Secuencia y frecuencia de rotación laboral

Sin estipulación.

11.3.6 Sanciones para acciones no autorizadas

Se consideran acciones no autorizadas las que contravengan la Declaración de Prácticas y Políticas pertinentes tanto de forma negligente como malintencionada.

Si se produce alguna infracción, se suspenderá el acceso de las personas involucradas a todos los sistemas de información de DIGITEL TS de forma inmediata al conocimiento del hecho.

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.

11.3.7 Requisitos de contratación de profesionales

Los empleados contratados para realizar tareas confiables firman con anterioridad las cláusulas de confidencialidad y los requerimientos operacionales empleados para la prestación del servicio de QERDS de DIGITELTS. 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 parte de la operativa del servicio de entrega electrónica certificada amparado en esta DPC 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. Sin perjuicio de lo anterior, , DIGITELTS será responsable en todo caso de la efectiva ejecución del servicio y de su conformidad con la normativa aplicable. Estos aspectos quedan concretados en el instrumento jurídico utilizado para acordar la prestación de los servicios de entrega electrónica certificada por tercero distinto a DIGITELTS.

11.3.8 Suministro de documentación al personal

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

11.4 Procedimientos de auditoría de seguridad

La prestación de los servicios de confianza de DIGITELTS está sujeta a las validaciones cada dos años por medio de auditorías conforme a lo establecido en el Reglamento eIDAS y la Directiva NIS2, con mantenimiento anual.

DIGITELTS informará al organismo de supervisión en materia de servicios de confianza, al menos un mes antes de cualquier auditoría prevista y permitirán la participación del organismo de supervisión en calidad de observador conforme establece el artículo 20. 1 *bis* del Reglamento eIDAS.

Asimismo, DIGITELTS lleva a cabo auditorías sobre protección de datos

DIGITELTS es una empresa comprometida con la seguridad y la calidad de sus servicios mediante la obtención y mantenimiento de la certificación ISO/IEC 27001:2022 para las que realiza auditorias cada 3 años con revisiones anuales.

Por otro lado, DIGITELTS ha certificado en ENS (Media) los sistemas de información que dan soporte a los servicios electrónicos cualificados amparados en esta DPC con la categoría

media, conforme a las exigencias del Real Decreto 311/2022 de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

DIGITELTS realiza, también un análisis de riesgo anual. Además, dispone de una revisión interna mensual y auditoría externa anual de revisión de seguridad con el objetivo de identificar y analizar las vulnerabilidades potencialmente explotables.

11.4.1 Tipos de eventos registrados

El prestador de servicios de confianza de DIGITELTS produce y guarda registro, al menos, de los siguientes eventos relacionados con la seguridad de la entidad:

- Encendido y apagado del sistema.
- Caídas del sistema y fallos de hardware,
- 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.
- Actividad del firewall y routers
- Cambios en la configuración y mantenimiento del sistema.
  y enrutadores
- Acceso o cambios en archivos de configuración críticos y copias de seguridad.
- Tráfico de red saliente y entrante
- 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 a la prestación del servicio de QERDS.
- Registros de eventos y registros de herramientas de seguridad, como antivirus, sistemas de detección de intrusiones o cortafuegos.
- Uso de los recursos del sistema, así como su rendimiento.
- Acceso y uso de sus equipos y dispositivos de red.
- Activación, parada y pausa de los distintos registros.
- Acontecimientos medioambientales que impacten en los servicios
- Cambios en la Política de Seguridad.

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.

11.4.2 Frecuencia de tratamiento de registros de auditoría

El prestador de servicios de confianza cualificado de DIGITELTS 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.

El prestador de servicios de confianza cualificado de DIGITELTS 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.

11.4.3 Período de conservación de registros

DIGITELTS almacena la información de los logs al menos durante 2 años,.

Además, DIGITEL TS conserva las evidencias del servicio cualificado de entrega electrónica certificada durante 15 años.

11.4.4 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 solo 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

11.4.5 Procedimientos de copias de seguridad

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

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

11.4.6 Localización del sistema de acumulación de registros

La información de la auditoria de eventos es recogida automáticamente por el sistema operativo, las comunicaciones de red y por el software del servicio de QERDS, 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.

11.4.7 Notificación del evento de auditoría al causante del evento

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

11.4.8 Análisis de vulnerabilidades

Toda la infraestructura es objeto de una evaluación de vulnerabilidades mensualmente (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:

24. 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.

11.5 Archivos de informaciones

11.5.1 Tipos de registros archivados

DIGITELTS, garantiza que toda la información relativa a la prestación del servicio de entrega electrónica certificada se conserva durante un período de 15 años conforme establece la legislación aplicable. es responsable del correcto archivo de todo este material.

DIGITELTS archiva los siguientes documentos:

- Datos de identificación del emisor y el destinatario; incluidos los eventos e información de verificación de la identidad.

- Datos de autenticación del emisor y de los destinatarios; incluidos los eventos e información de verificación de la autenticidad
- .
- Evidencias para demostrar que el contenido del usuario no se ha modificado durante la transmisión. Ello se realiza mediante el sellado de la evidencia en el momento de la entrega del contenido por parte del emisor al servicio, mediante un sello de entidad e incorporando un sello de tiempo.
- una referencia o una recopilación completa del contenido del usuario presentado;
- Documentos originales enviados por el emisor.
- Documentos firmados en la recepción por parte de DIGITELTS.
- Logs de evidencia de accesos, recogidas, rechazos, atributos captados por pantalla, resultados de la transacción.
- Sellos de tiempo cualificados que sellan cada una de las evidencias.

11.5.2 Período de conservación de registros

Toda la información y documentación relativa a las notificaciones se conservará durante un mínimo de quince (15) años. tal y como exige la Ley 6/2020, reguladora de determinados aspectos de los servicios electrónicos de confianza.

Además, Digitel TS revisa los registros de auditoría periódicamente, verificando su normal actividad y que no han sido manipulados. Se utilizan controles de acceso físico y lógico para los ficheros de registro, quedando protegidos de accesos, modificaciones o eliminaciones no autorizadas. Estos registros de auditoria serán retenidos por un período mínimo de 2 años.

11.5.3 Protección del archivo

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

DIGITELTS 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.

11.5.4 Procedimientos de copia de seguridad

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

Además, DIGITELTS guarda copia de los documentos en papel en un lugar seguro diferente de las instalaciones de la propia Autoridad de certificación.

11.5.5 El sistema de archivo

El prestador de servicios de confianza cualificado DIGITELTS dispone de un sistema centralizado de recogida de información de la actividad de los equipos implicados en el servicio de QERDS.

11.5.6 Procedimientos de obtención y verificación de información de archivo

Estos sistemas disponen de un alto nivel de integridad, confidencialidad y disponibilidad para evitar intentos de manipulación.

11.6 Continuidad de negocio y Recuperación de desastre

11.6.1 Procedimientos de gestión de incidencias y compromisos

DIGITELTS almacena copias de seguridad de la siguiente información, que se ponen a disposición en caso de compromiso o desastre: Datos de auditoría y registros de base de datos de todos los eventos .

11.6.2 Corrupción de recursos, aplicaciones o datos

Cuando ocurra 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.

11.6.3 Continuidad del negocio después de un desastre

DIGITELTS dispone de un Plan de Continuidad del negocio en el que se indican las actuaciones a realizar en casos de desastre. Se cuenta con un sistema de copia de seguridad que almacena de forma segura aquellos datos necesarios para reanudar las operaciones de los sistemas que dan soporte al servicio de QERDS de DIGITELTS. Se incluye también las oportunas referencias al centro de respaldo alternativo que garantice que toda la información esencial y las aplicaciones puedan recuperarse ante un desastre o fallo.

DIGITELTS prueba los medios alternativos mediante simulacros al menos una vez al año. De esta forma, se establecen procedimientos de entrenamiento, prueba y mantenimiento de este plan. Todo el personal, 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.

Las actividades indicadas en el plan de recuperación de desastres se diseñan acorde con los parámetros de continuidad (RTO y RPO) definidos para los servicios.

Para garantizar de forma proactiva la continuidad del servicio, se 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 Centros de proceso de datos se encuentran ubicados en un prestador 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).

De forma adicional, se 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 mecanismos de teletrabajo que permiten acceder a los sistemas productivos de forma remota.

11.7 Terminación del servicio

En caso de cese del servicio de entrega electrónica certificada, DIGITELTS 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, se ha desarrollado un plan de cese actualizado 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 del servicio amparado en esta DPC. Este plan cubre:

- Se provisionará la cantidad necesaria, mediante seguro de responsabilidad civil, para cubrir los costes a efectos de contingencia de cierre.

- Informará a todos Suscriptores y Terceros que confían del cese del servicio con una anticipación mínima de 2 meses.

- Revocará toda autorización a entidades subcontratadas para actuar en alguna operativa del servicio.

- Podrá transferir la gestión del servicio a otro prestador de servicios de confianza que lo asuma o, en caso contrario, extinguir su vigencia. DIGITELTS informará, cuando sea el caso, sobre las características del prestador al que se propone la transferencia de la gestión de del servicio de entrega electrónica certificada y recabará previamente el consentimiento de los suscriptores .

- En caso de que al cese de operaciones el servicio no se transfiera a otro prestador, DIGITELTSpondrá en deposito ante notario público toda la informacion relacionada con la prestación del servicio.

- Destruirá o deshabilitará para su uso las claves privadas de los certificados utilizados para sellar las evidencias del servicio de entrega electrónica certificada.

- Comunicará al Organismo de Supervisión nacional en materia de servicios de confianza, con una antelación mínima de 3 meses, el cese de su actividad y el destino del servicio y las evidencias generadas, especificando si se transfiere su gestión y a quién. De manera que eel Supervisor ste pueda verificar la correcta aplicación del plan de terminación de los servicios, incluyendo la forma en que se hace accesible la información, de conformidad con el artículo 24.2 letras a); h) e i) y el artículo 46 ter, apartado 4, letra i) del Reglamento (UE) eIDAS.

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

En caso de cese de los servicios, DIGITELTS sigue siendo responsable de mantener accesible durante el período de quince (15) años, toda la información pertinente referente a los datos expedidos y recibidos como parte de la prestación del servicio de QERDS, en particular al

objeto de que sirvan de prueba en los procedimientos legales y para garantizar la continuidad del servicio.

12 Controles de seguridad técnica

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

12.1 Controles de seguridad informática

12.1.1 Requisitos técnicos específicos de seguridad informática

DIGITELTS emplea sistemas fiables para ofrecer sus servicios de entrega electrónica certificada. Se han realizado controles y auditorias 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, DIGITELTS sigue el esquema de certificación sobre sistemas de gestión de la información ISO 27001. Asimismo, se ha certificado conforme al ENS en categoría Media .

Los equipos usados son inicialmente configurados con los perfiles de seguridad adecuados por parte del personal de sistemas de DIGITELTS, 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.

25. Plan de backup y recuperación.

- Configuración antivirus.
- Requerimientos de tráfico de red.

Cada servidor de DIGITELTS 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.
- Necesidad de VPN para conectarse a los servidores.

12.1.2 Evaluación del nivel de seguridad informática

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

12.2 Controles de seguridad del ciclo de vida

12.2.1 Controles de desarrollo de sistemas

Las aplicaciones son desarrolladas e implementadas por DIGITELTS 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.

12.2.2 Controles de gestión de seguridad

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

12.2.2.1 Clasificación y gestión de información y bienes

DIGITELTS 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 DIGITELTS detalla los procedimientos de gestión de la información donde se clasifica según su nivel de confidencialidad.

Los documentos están catalogados en cuatro niveles: Uso Público, Uso Interno, Confidencial y Secreto.

12.2.2.2 Operaciones de gestión

DIGITELTS dispone de un procedimiento de gestión y respuesta de incidencias, mediante la implementación de un sistema de alertas y la generación de reportes periódicos.

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

DIGITELTS 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.

12.2.2.3 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.

12.2.2.4 Planificación del sistema

El departamento de Sistemas de DIGITELTS 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.

12.2.2.5 Reportes de incidencias y respuesta

DIGITELTS 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.

12.2.2.6 Procedimientos operacionales y responsabilidades

DIGITELTS 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.

12.2.2.7 Gestión del sistema de acceso

DIGITELTS 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.
- DIGITELTS dispone de un procedimiento documentado de gestión de altas y bajas de usuarios y política de acceso detallado en su política de seguridad.
- DIGITELTS 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 DIGITELTS es responsable de sus actos mediante el compromiso de confidencialidad firmado con la empresa.
- El acceso se produce mediante VPN y certificado electrónico de autenticación en USB y PIN.

12.3 Controles de seguridad de red

DIGITELTS 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 de VPN con autenticación por doble factor.

Digitel TS supervisa las demandas de capacidad de los sistemas que soportan el servicio de entrega electronica certificada y garantiza que este dispone en todo momento de la potencia de procesamiento y almacenamiento adecuados.

13 Auditoría de conformidad

DIGITELTS 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 DIGITEL*, 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.

DIGITELTS realiza auditorías de conformidad del Reglamento eIDAS por medio de evaluaciones de conformidad anuales sobre el servicio cualificado de entrega electrónica certificada.

DIGITELTS realiza las pertinentes auditorías sobre protección de datos con periodicidad bienal.

13.1 Frecuencia de la auditoría de conformidad

Se realizan evaluaciones de conformidad eIDAS con carácter bienal, además de revisiones anuales.

Se realizan auditorías relativas a la protección de los datos personales bianuales.

Se realizan auditorías de ISO 27001 cada 3 años con seguimiento anual.

Se realizan análisis internas de vulnerabilidades cada mes, y externa cada año.

Se realiza un análisis de intrusión cada año.

13.2 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 prestación de servicios de confianza cualificados.

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

13.3 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.

13.4 Listado de elementos objeto de auditoría

La auditoría verifica:

- Que la entidad tiene un sistema de gestión que garantiza la calidad del servicio prestado.

26. Que la entidad cumple con los requerimientos de la DPC y otra documentación vinculada con la prestación de servicios de confianza cualificados, bajo el marco del Reglamento

(UE) 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014, modificado por el Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, en lo que respecta al establecimiento del marco europeo de identidad digital, asi como los requisitos de ciberseguridad de redes y de la informacion definidos en la Directiva NIS2, su Reglamento de Ejecución (UE) 2024/2690 y su normativa de desarrollo

- Los controles están en consonancia con los requisitos establecidos en la norma técnica ETSI EN 319 521. Además, también son aplicables los controles de las normas actualmente en vigor ETSI EN 319 401 y recomendaciones de las normas ISO/IEC 27002:2013 e ISO/IEC 27005, tal y como se referencia en las normas ETSI anteriormente citadas.
- Que la entidad gestiona de forma adecuada sus sistemas de información

13.5 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 el prestador de servicios de confianza cualificado DIGITELTS 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 DIGITEL que podrá ejecutar las siguientes acciones:

- Cesar las operaciones transitoriamente.
- Otras acciones complementarias que resulten necesarias.

13.6 Tratamiento de los informes de auditoría

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

14 Requisitos comerciales y legales

14.1 Tarifas

DIGITELTS establece tarifas por la prestación del servicio de QERDS y se informa oportunamente a los clientes.

14.2 Responsabilidad financiera

DIGITELTS 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 normativa de aplicación, en relación con la gestión de la finalización de los servicios y plan de cese.

14.2.1 Cobertura de seguro

DIGITELTS 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 3.000.000 de euros.

14.2.2 Otros activos

Sin estipulación.

14.3 Confidencialidad de la información

14.3.1 Informaciones confidenciales

Las siguientes informaciones son mantenidas confidenciales:

27. Claves privadas generadas y/o almacenadas por el prestador de servicios de de entrega electrónica certificada

- Registros de transacciones, incluyendo los registros completos y los registros de auditoría de las transacciones.

28. Registros de auditoría interna y externa, creados y/o mantenidos por DIGITELTS respecto al servicio de entrega electrónica certificada 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”.

14.3.2 Informaciones no confidenciales

Sin estipulación.

14.3.3 Divulgación legal de información

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

14.3.4 Divulgación de información por petición de su titular

Sin estipulación.

14.3.5 Otras circunstancias de divulgación de información

Sin estipulación.

14.4 Protección de la información personal

Para la prestación del servicio, DIGITELTS actúa como responsable del tratamiento respecto de los datos de emisor y destinatario, y como encargado del tratamiento respecto de los datos transmitidos por el emisor, conforme a lo establecido en la normativa vigente y documenta sus obligaciones y controles en el contrato de servicio.

14.5 Derechos de propiedad intelectual

14.5.1 Propiedad de la Declaración de Prácticas de Confianza

DIGITELTS goza de derechos de propiedad intelectual sobre esta Declaración de Prácticas de Confianza.

14.6 Obligaciones y responsabilidad civil

14.6.1 Obligaciones de DIGITELTS

DIGITELTS 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.

DIGITELTS presta el servicio cualificado de entrega electrónica certificada conforme a esta Declaración de Prácticas de Confianza.

DIGITELTS comunica de forma permanente los cambios que se produzcan en sus obligaciones publicando nuevas versiones de su documentación jurídica en su web https://pki.digitelts.es

14.7 Limitaciones de responsabilidad

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

DIGITELTS 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.

14.7.1 Cláusula de indemnidad

DIGITELTS 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.

14.7.2 Caso fortuito y fuerza mayor

DIGITELTS incluye en la DPC cláusulas que limitan su responsabilidad en caso fortuito y en caso de fuerza mayor.

14.8 Indemnizaciones

14.8.1 Alcance de la cobertura

DIGITELTS dispone de un seguro que responde de las cantidades que le 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 actonegligente, error u incumplimiento no intencionado de la legislación vigente entre otros, en los términos expresamente pactados con la compañía aseguradora.

14.9 Reclamaciones y resolución de conflictos

Para la resolución de cualquier conflicto que pudiera surgir en relación con este documento o el instrumento jurídico vinculante, las partes, con renuncia a cualquier otro fuero que pudiera corresponderles, se someten a los Tribunales de Justicia de Valladolid.

15 Normativa aplicable

La legislación aplicable al servicio de entrega electrónica certificada de DIGITELTS se relaciona a continuación:

29. 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,

modificado mediante Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo de 11 de abril de 2024. En lo que respecta al establecimiento del marco europeo de identidad digital.

30. Direectiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.o 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva NIS2)
31. Reglamento de Ejecución de la Directiva (UE) NIS2, de 17 de octubre de 2024, por el que se establecen los requisitos técnicos y metodológicos de las medidas de gestión de riesgos en materia de ciberseguridad y se especifican con mayor detalle los casos en que un incidente se considera significativo en relación con los proveedores de servicios de confianza y otros sujetos obligados.
32. Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza
33. 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).
34. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Además, el servicio de entrega electrónica certificada de DIGITELTS está alineado con las siguientes normas técnicas:

35. ETSI EN 319 401: General Policy Requirements for Trust Service Providers
36. ETSI EN 319 521: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers

37. ETSI EN 319 522-1: Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 1: Framework and Architecture.
38. ETSI TS 119 461 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects