DECLARACIÓN DE PRÁCTICAS DE SERVICIO DE FULL CERTIFICATE

DICIEMBRE 2021

V. 1. 0

7. GESTION Y FUNCIONAMIENTO DE ERDSP

8. HISTORICO DE CAMBIOS

1. INTRODUCCIÓN

El objetivo de este documento es especificar las reglas y normas generales aplicadas por FULL CERTIFICATE S.L. (FULL CERTIFICATE) para la prestación del Servicio Cualificado de Entrega Electrónica Certificada (QERDS).

Se enfatiza que este document no especifica:

- Cómo los requisitos identificados (incluidos los requisitos de información que se pondrán a disposición de los evaluadores) pueden ser evaluados por el auditor independiente
- Los requisitos que debe cumplir la misma parte evaluadora.

Es decir, este documento define los requisitos de aplicación general para las actividades de FULL CERTIFICATE en su papel de Prestador de Servicio Cualificado de Entrega Electrónica Certificada (QERDSP). Además, la política también regula las disposiciones relativas al personal de la empresa, así como el plan de terminación/ finalizazión de los servicios.

Asimismo, destacamos que los servicios de confianza pueden incluir, entre otros, la emisión de certificados públicos, la prestación de servicios de registro, servicios de sellado digital de timbrado, servicios de conservación a largo plazo, servicios de entrega electrónica y/o servicios de validación de firmas. Estos requisitos no implican ninguna restricción en la prestación de servicios de TSP.

FULL CERTIFICATE, como prestador de servicios de confianza, ofrece seguridad, confiabilidad y legalidad, en sus procesos, ofrece un servicio cualificado y de calidad en la conservación de certificados emitidos, firmas y sellos electrónicos; mediante el cual lleva a cabo la conservación de certificados, firmas y sellos electrónicos cualificados mediante el uso de procedimientos y tecnologías capaces de extender la fiabilidad de los datos de la firma electrónica cualificada, más allá del periodo de validez del certificado electrónico.

El presente documento ha sido elaborado por las autoridades adminitrativas y Legales de FULL CERTIFICATE y fue leído y aprobado por la Dirección General el 22 de Noviembre del 2021.

La presente declaración de practices de servicio será revisado de manera anual por las áreas correspondientes y se notificará la aplicación de algun ajuste o modificación a todo el equipo.

Cuando el TSP realice cambios en el presente documento que puedan afectar la aceptación del servicio por parte del suscriptor o tercero de confianza, será resposabildiad de las partes resposables y legales realizar la debida notificación y la publicando del documento modificado en la página web.

2. *TÉRMINOS Y ABREVIATURAS*

A los efectos del presente documento, se aplican los siguientes términos:

TERMINO	DEFINICIÓN
DPC	**Declaración de Prácticas de Certificación (DCP)** Declaración de FULL CERTIFICATE puesto a disposición del público de forma electrónica y gratuita realizada como Prestador de Servicios de Confianza en cumplimiento de lo dispuesto en la Ley
PROVEEDOR DE SERVICIOS DE CONFIANZA	Persona física o jurídica que presta uno o más servicios de confianza, de conformidad con lo establecido en eIDAS.
PROVEEDOR DE SERVICIOS DE CONFIANZA CUALIFICADO	Un proveedor de servicios de confianza que brinda uno o más servicios de confianza calificados y al cual el organismo de control ha otorgado calificación (conformidad).
AUTORIDAD DE SELLADO DE TIEMPO - TSA	Persona física o jurídica que, de acuerdo con la normativa sobre Sellado de Tiempo, emita sellos de tiempo electrónicos.
SELLO ELECTRÓNICO DE TIEMPO	Datos en formato electrónico que vinculan otros datos en formato electrónico con un momento concreto, aportando la pruebas de que estos últimos datos existían en ese momento.
SELLO DE TIEMPO ELECTRÓNICO CUALIFICADO	Sello de tiempo electrónico que cumple los requisitos establecidos en el artículo 42 del eIDAS.
USER	Persona física o jurídica que utiliza los servicios de custodia cualificada de firma o sellos electrónicos habilitados, previa aceptación de las condiciones asociadas al servicio y al DPC.

DOCUMENTACIÓN	Conjunto de evidencias digitales recibidas por FULL CERTIFICATE por parte del Usuario, que cumplen con los requisitos establecidos en este DPC.
CERTIFICACIÓN	Expediente firmado electrónicamente por un proveedor de servicios de certificación que vincula los datos de verificación de la firma aún asignatario y confirma su identidad e incorpora un sello / marca de tiempo (Timbrado).
CLAVE PÚBLICA	Valor matemático conocido públicamente y usado para la verificación de una firma digital o el cifrado de datos. También llamada datos de verificación de firma.
CLAVE PRIVADA	Valor matemático que sólo conoce el suscriptor y que se utiliza para la creación de una firma digital o el descifrado de datos. También se denominan datos de creación de la firma.
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.
HUELLA DIGITAL O HASH	Es un conjunto de datos asociados a un mensaje que permiten asegurar que el mensaje no fue modificado. Se obtiene aplicando una función, denominada hash, a ese mensaje, esto da como resultado un conjunto de datos singular de longitud fija.
TIEMPO UNIVERSAL COORDINDADO (UTC)	Escala de tiempo basada en el segundo, tal como se define en la Recomendación UIT-R TF.460-6 [i.8].
PERSONA DE CONFIANZA	Persona física o jurídica que confía en una identificación electrónica o en un servicio de confianza.

SERVICIOS DE CONFIANZA	Servicio electrónico para: 1. Creación, verificación y validación de firmas digitales y certificados relacionados 2. Creación, verificación y validación de sellos / marca de tiempo (Timbrado) y certificados relacionados 3. Entrega certificada y certificado relacionado 4. Creación, verificación y validación de certificados para la autenticación de sitios web 5.Retención de firmas digitales o certificados relacionados con dichos servicios. 6. Los identificados en la cláusula 4.4 de ETSI EN 319 411-1. 7. 7. Adicionalmente, ETSI TS 119 431-1 define los requisitos de un componente Server Signature Application Service (SSASC) que puede desplegarse como parte del servicio TSP.
COMPONENTES DE SERVICIO DE CONFIANZA	Una parte del servicio global de un TSP.

POLITICAS DE LOS SERVICIOS DE CONFIANZA	Conjunto de reglas que indican la aplicabilidad de un servicio de confianza a una determinada comunidad y/o clase de aplicación con requisitos de seguridad comunes. Una política de servicios de confianza describe lo que se ofrece y proporciona información sobre el nivel de servicio. Se define con independencia de los detalles concretos del entorno operativo específico de un TSP; una política de servicios de confianza puede aplicarse a una comunidad a la que pertenecen varios TSP que se rigen por el conjunto común de normas especificadas en dicha política. Puede ser definida, por ejemplo, por el TSP, por normas nacionales. (por ejemplo, gubernamental) o internacional, por parte de los clientes y/o usuarios del TSP y no forma parte necesariamente de la documentación del TSP.
DECLARACIÓN DE PRÁCTICAS DE LOS SERVICIOS DE CONFIANZA	Declaración de las prácticas que un TSP emplea para proporcionar un servicio de confianza.
TOKEN DE SERVICIO DE CONFIANZA	Objeto físico o binario (lógico) generado o emitido como resultado del uso de un servicio de confianza. Ejemplos de tokens de servicios de confianza son: certificados, CRLs, tokens de marca de tiempo, respuestas OCSP.
SERVICIO DE ENTREGA ELECTRÓNICA CERTIFICADA / ERDS	Un servicio que permite la transmisión de datos entre personas por medios electrónicos, proporciona pruebas relativas sobre el tratamiento de los datos transmitidos, incluidas las pruebas del envío y la recepción de los datos, y protege los datos transmitidos contra el riesgo de pérdida, robo, daño o modificación no autorizada.

SERVICIO CUALIFICADO DE ENTREGA ELECTRÓNICA CERTIFICADA /QERDS	Servicio de entrega electrónica registrado que cumple con los requisitos del artículo 44 del Reglamento (EU) nº 910/2014.
PROVEEDOR DE SERVICIOS DE ENTREGA ELECTRÓNICA CERTIFICADA/ERDSP	Proveedor de servicios de confianza cualificado que proporciona un servicio de entrega electrónica registrado.
PROVEEDOR DE SERVICIOS CUALIFICADO DE ENTREGA ELECTRÓNICA CERTIFICADA /QERDSP	Proveedor de servicios de confianza cualificado que presta un servicio de entrega electrónica registrado de conformidad con el Reglamento (EU) No. 910/2014.
EVIDENCIAS DE ERDS	Datos generados dentro de un servicio de entrega electrónica registrado que están destinados a demostrar que un evento en particular ha ocurrido en un momento dado.
DESTINATARIO	Persona física o jurídica a la que se dirige el contenido de un usuario.
REMITENTE	Persona física o jurídica que envía el contenido a un usuario.
TRANSFERENCIA	Por medio del contenido del Usuario, el límite de entrega electrónica registrada del usuario se ha cruzado con éxito, es decir, al agente del destinatario / la aplicación ERD del Usuario.

Las siglas utilizadas en este documento serán las siguientes:

ACRÓNIMO	DEFINICIÓN
LFE	Ley 59/2003, de 19 de diciembre, de firma electrónica
eIDAS	Reglamento 910/2014 de la Parlamento Europeo y del Consejo, de 23 de julio de 2014, sobre 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
RGPD	Reglamento 2016/679, 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
LSSI	Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico
CSP	Proveedores de servicios de certificación
TSA	Time Stamp Authority – Autoridad de Sellado de Tiempo
DPC	Centro de Procesamiento de Datos
NTP	Network Time Protocol – Protocolo de Internet para sincronizar los relojes de los sistemas informáticos
PKI	Public Key Infraestructure – Infraestructura de clave pública
WF	Work Flow – Flujos de trabajo para cada proceso
CRL	Lista de revocación de certificados
OID	Object Identifier - Valor, de carácter jerárquico y comprensivo de una secuencia de componentes variables, aunque siempre constituida por enteros no negativos separados por un punto, que pueden ser asignados a objetos registrados y que tienen la propiedad de ser únicos entre el resto del OID
CA	Autoridad de certificación
IP	Protocolo de Internet
IT	Tecnología de la información
SSASC	Componente de servicio de aplicación de firma de servidor
TSP	Proveedor de servicios de confianza

GMT	Hora del meridiano de Greenwich
UTC	Tiempo universal coordinado
QTSP	Proveedor de servicios cualificados de confianza
ERD	Entrega Electrónica Certificada
ERDS	Servicio de Entrega Electrónica Certificada
QERDS	Servicio Cualificado de Entrega Electrónica Certificada
ERDSP	Proveedor de Servicios de Entrega Electrónica Certificada
QERDSP	Proveedor de Servicios Cualificado de Entrega Electrónica Certificada
R-ERDS	Servicio de Entrega Electrónica Certificada por el Destinatario
S-ERDS	Servicio de Entrega Electrónica Certificada por el Destinatario por el Remitente
EU	UE abreviatura en ingles de "Unión Europea"

3. ***REFERENCIAS NORMATIVAS E INFORMATIVAS***

- Referencias Normativas:

[1] Regulación n.º 910/2014 del Parlamento Europeo y del Consejo, del 23 de julio de 2014, relativo a la identificación electrónica y a los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.

[2] Ley 59/2003, de 19 de diciembre, de firma electrónica.

[3] Orden del 21 de febrero de 2000 por la que se aprueba el Reglamento de acreditación de los prestadores de servicios de certificación y certificación de determinados productos por vía electrónica.

[4] Regulación 2016/679 del 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.

[5] Ley 34/2002, del 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

[6] Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

[7] ETSI TS 102 573 v2.1.1 / Requisitos de directiva para los proveedores de servicios de confianza que firman y/o almacenan objetos de datos

[8] ETSI EN 319 401 v2.1.1 / Requisitos generales de la política para los proveedores de servicios de confianza.

[9] ETSI TS 102 778 1-6 / Firmas Electrónicas e Infraestructuras (ESI); PDF Perfiles avanzados de firma electrónica.

[10] ETSI TS 101 533-1 / Seguridad de los Sistemas de Preservación de la Información; Parte 1: Requisitos para la implementación y gestión.

[11] ETSI EN 319 421 v1.0.0 / Firmas Electrónicas e Infraestructuras (ESI); Requisitos de política y seguridad para los proveedores de servicios de confianza que emiten sellos de tiempo

[12] ISO/IEC 14641-1 / Archivo electrónico

[13] ISO/IEC 27001:2014 / Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos

[14] ISO/IEC 27002:2013 / Tecnología de la información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información

[15] ETSI SR 019 510. / Firmas Electrónicas e Infraestructuras (ESI); Estudio de alcance y marco para la estandarización de los servicios de preservación de datos a largo plazo, incluida la preservación de / con firmas digitales.

Asimismo, destacamos que prestamos nuestros servicios de acuerdo con la legislación española vigente en la materia. En concreto, de acuerdo con la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, en los siguientes términos:

Requisito de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico	**Como lo lleva a cabo FULL CERTIFICATE:**
INSCRIPCIÓN EN EL REGISTRO MERCANTIL	FULL CERTIFICATE se encuentra inscrito en el Registro Mercantil de Madrid, en el tomo volumen 33,481, hoja 201, página M-602717.
DATOS DE IDENTIFICACIÓN	Los datos requeridos por las autoridades correspondientes se encuentran publican en: https://fullcertificate.com/legal-notice/
CONSERVACIÓN DE DATOS DE CONEXIÓN Y TRÁFICO	Los datos de conexión se utilizan de acuerdo con la Política de Privacidad: https://fullcertificate.com/privacy-policy-2/
RESPONSABILIDAD	FULL CERTIFICATE ha contratado un seguro de Responsabilidad Civil Profesional con un Límite de Indemnización de: 1.500.000 €.
SPAM - CORREO NO DESEADO	FULL CERTIFICATE envía comunicaciones comerciales a aquellos usuarios que han dado su consentimiento a tal efecto y/o a aquellas personas físicas y jurídicas con las que mantiene una relación contractual.
CONTRATOS ELECTRÓNICOS	FULL CERTIFICATE proporciona información clara y concisa sobre los siguientes términos: • La metodología, procedimientos y tramites que hay que seguir para la realización del contrato. • La manera en la que se debe realizar y guardar el documento electrónico que formaliza el contrato y su accesibilidad. • Los medios técnicos de que dispone para identificar y corregir los errores de introducción de datos • El idioma o idiomas en los que pueda celebrarse el contrato.
PROPIEDAD INTELECTUAL	Nos remitimos al Aviso Legal - Términos y Condiciones: https://fullcertificate.com/legal-notice/.

• Referencias Informativas:

[1] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales ya la libre circulación de estos datos.

[2] Regulación (EU) No. 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, sobre identificación electrónica y servicios de confianza para transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.

[3] ISO/IEC 27002:2013: "Tecnologías de la información - Técnicas de seguridad - Código de prácticas para la gestión de la seguridad de la información".

[4] CA/Browser Forum: " Requisitos básicos para la emisión y gestión de certificados de confianza pública".

[5] ISO/IEC 27005:2011: " Tecnología de la información - Técnicas de seguridad - Gestión de riesgos de seguridad de la información".

[6] ETSI EN 319 403: " Firmas e infraestructuras electrónicas (ESI); Evaluación de la conformidad del proveedor de servicios de confianza: requisitos para los organismos de evaluación de la conformidad que evalúan a los proveedores de servicios de confianza".

[7] CA/Browser Forum: "Requisitos de seguridad de la red y del sistema de certificados". Recomendación ITU-R TF.460-6 (2002): "Emisiones de frecuencias y señales horarias normalizadas".

[8] ETSI EN 319 411-1: "Firmas Electrónicas e Infraestructuras (ESI); Requisitos de Política y Seguridad para los Proveedores de Servicios de Confianza que emiten certificados; Parte 1: Requisitos generales".

[9] ETSI EN 301 549: "Requisitos de accesibilidad para los productos y servicios de TIC”

[10] ETSI EN 319 411-2: "Firmas Electrónicas e Infraestructuras (ESI); Requisitos de Política y Seguridad para los Proveedores de Servicios de Confianza que emiten certificados; Parte 2: Requisitos para los proveedores de servicios de confianza que emiten certificados calificados de la EU".

[11] Regulación (EU) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, sobre la protección de las personas físicas en relación con el tratamiento de datos personales y la libre circulación de dichos datos, y por la que se deroga la Directiva 95/46/CE.

[12] ETSI TS 119 431-1: "Firmas electrónicas e infraestructuras (ESI); Requisitos de política y seguridad para proveedores de servicios de confianza; Parte 1: Componentes de servicio TSP que operan un QSCD remoto / SCDev".

[13] ISO/IEC 27701:2019: "Técnicas de seguridad – Extensión a ISO/IEC 27001 e ISO/IEC 27002 para la gestión de la privacidad de la información - Requisitos y directrices".

4. ***POLÍTICAS DE SERVICIO***

FULL CERTIFICATE garantiza, de acuerdo con su declaración de aplicabilidad y requisitos legales, que:

a) Cumple con la creación y prestación del servicio de entrega certificada con las máximas garantías legales y probatorias de acuerdo con las disposiciones de la legislación y normativas vigentes en la materia a nivel nacional y europeo.

b) Presta servicios que se caracterizan por lo siguiente:

- Autenticación fiable (del remitente y del destinatario) según lo establecido por la normativa como pilar fundamental de los propios servicios

- Creación y puesta a disposición de todas las pruebas electrónicas que se produzcan dentro de los servicios prestados por FULL CERTIFICATE: por ejemplo, recordamos, de manera no limitativa, lo siguiente:
  - Evidencia Electrónica de presentación
  - Evidencia Electrónica de consignación
  - Evidencia Electrónica de entrega
- Creación de los Certificados correspondientes, de acuerdo con la normativa vigente en la materia, estando el contenido del mismo a disposición tanto del remitente como del destinatario y los certificados emitidos serán custodiados por un período mínimo de 15 (QUINCE) años.

Este capítulo debe considerarse como la política de seguridad de la información de FULL CERTIFICATE.

5. ***PRÁCTICA DE SERVICIO***

5.1 SERVICIO DE ENTREGA ELECTRÓNICA CERTIFICADA - ERDS

El Full Certificate le permite enviar mensajes y documentos/ archivos adjuntos (contenido del usuario) como envíos. La diferencia con el envío electrónico simple es que el remitente y el destinatario deben pasar primero por un proceso de identificación inicial antes de usar el sistema. En el proceso de servicio, el remitente de los documentos electrónicos se autentifica y solo entonces realiza el envío, y respectivamente el destinatario tiene acceso a su contenido después de haber sido autenticado también.

En el proceso de prestación del servicio de envío, el remitente del mensaje acredita su identidad a través de los siguientes niveles:

1. **Acreditación Básica:** El usuario acepta los términos y condiciones del servicio, confirma que sus datos son correctos mediante un código de un solo uso (OTP) a través de un correo electrónico que será a partir de ese momento su nombre de usuario en el sistema.
2. **Acreditación por documento:** El usuario carga al sistema una imagen de su documento de identidad donde se reflejen claramente sus datos de registro, los cuales son: Nombre, Apellido, Fecha de Nacimiento y Número de documento de identidad, los cuales deben coincidir con los datos previamente proporcionados en el registro básico de acreditación.

3. **Acreditación Cualificada:** Se solicita al usuario que presente un certificado electrónico acreditado emitido por una autoridad de certificación reconocida, el cual será validado y verificado con los datos proporcionados en la sección de Acreditación Básica.

La **identidad del destinatario** se acreditada por cualquiera de los siguientes procedimientos:

1. **Mediante autenticación de documentos.** Utilizando un código de uso único (OTP), para validar su registro en el nivel de confirmación del canal. El destinatario carga su documentación de identidad en el sistema y este procede a su revisión OCR con los datos proporcionados por el remitente.

2. **Autenticación cualificada.** El destinatario podrá presentar un certificado electrónico de identidad expedido por una autoridad certificadora válida cuyos datos contengan los indicados por el remitente

La identificación electrónica cumple los requisitos que refiere el artículo 8 del Reglamento (EU) No. 910/2014 en lo que respecta a los niveles de seguridad "significativos" o "elevados".

Una vez verificada la información proporcionada, se generarán datos sobre la identidad de los datos / registros que serán custodiados por FULL CERTIFICATE durante un período de 15 años, incluso después del cese de sus actividades. FULL CERTIFICATE cumple con los requisitos del art. 24 del Reglamento (EU) No. 910/2014, conservando toda la información pertinente para aportar pruebas en los procedimientos judiciales y garantizar la continuidad en la prestación del servicio, el período de 15 años se ha determinado de conformidad con el art. 21 (3) de la "*Ley de Servicios de Certificación Electrónica y de Documentos Electrónicos*".

Cuando no es posible la identificación remota, FULL CERTIFICATE no permite la acreditación presencial de ninguna de las partes.

5.1.1. IDENTIFICACIÓN Y CERTIFICACIÓN DE IDENTIDAD

El marco de interoperabilidad del Reglamento eIDAS especifica los datos de identificación que han de incluirse, tanto obligatorios como facultativos, en los mensajes que respondan a las solicitudes de autenticación. Estos datos deben derivarse del sistema de identificación empleado por el ciudadano para la autenticación.

A efectos de automatizar la verificación de la identidad de los colaboradores, existe una de las siguientes opciones:

- **Certificado electrónico de identidad.**
    - Expedido por una autoridad certificadora reconocida
    - Validez igual o superior a la fecha de envío.
    - No debe haber sido revocado
- **Validación por ID.**
    - Tener un documento de identidad válido
    - Tener un teléfono móvil para obtener la foto del documento de identidad para enviarlo a FULL CERTIFICATE.
    - FULL CERTIFICATE iniciará un proceso de verificación de la validez del documento de identidad a través de un sistema de reconocimiento (con la debida integración) o mediante el uso de un servicio de terceros.
    - Se pueden aplicar sistemas de reconocimiento facial a las fotos tomadas del documento de identidad para complementar la identificación con los siguientes parámetros: sexo, edad.
    - Si la verificación de identidad falla, se solicitará una nueva carga de una foto de un ID válido.

5.1.2. ESTACLECIMIENTO DE LA IDENTIDAD DE UNA PERSONA FÍSICA

En lo que respecta a las personas físicas, el marco de interoperabilidad contempla:

- Una serie de 4 datos obligatorios que deben facilitarse en todos los casos. Estos datos son:
    - Identificador de unicidad: Es un identificador vinculado de forma única a una persona específica, que permite asociar sucesivas autenticaciones con la misma persona. Cabe señalar que este identificador garantiza que no habrá dos personas con el mismo identificador, pero no que la misma persona siempre tenga el mismo identificador, ya que no es completamente persistente en todos los países (una persona puede tener diferentes identificadores a lo largo de su vida)
    - Nombre (generalmente uno o más nombres, según la costumbre de cada país)
    - Apellidos (generalmente uno o más apellidos, como es habitual en otros países europeos)
    - Fecha de nacimiento.
- Un conjunto de 5 datos opcionales que el país emisor de la autenticación puede decidir si proporciona o no, para facilitar la asociación de los datos de identificación ciudadana en autenticaciones sucesivas cuando el identificador de unicidad no es persistente. Estos datos opcionales son:
    - Nombre de nacimiento
    - Apellido de Nacimiento
    - Lugar de Nacimiento
    - Dirección Actual
    - Genero

5.1.3. ESTABLECIMIENTO DE LA IDENTIDAD DE UNA PERSONA JURÍDICA

Para las personas jurídicas, el régimen es similar al de las personas físicas, con un conjunto de datos obligatorio u optativo:

- El **conjunto de datos obligatorios** que se deben proporcionar en todos los casos consta de:
  - Identificador único (equivalente para las personas físicas, y puede no ser permanente)
  - Nombre legal (equivalente al nombre y apellido de la persona física)

El conjunto de datos facultativo, que el país emisor puede o no proporcionar en función de si la autenticación sucesiva es necesaria para obligar a la misma persona jurídica, consiste en:

- Dirección actual
- Número de identificación fiscal (VAT)
- Número de identificación (TAX)
- El identificador relacionado con el artículo 3(1) de la Directiva 2009/101/EC de la Unión Europea Parlamento y Consejo (registro de sociedades)
- El identificador de entidad jurídica (LEI)
- Número de registro e identificación de los operadores económicos (EORI)
- Número de impuestos especiales

En el caso de las personas jurídicas, es importante señalar que el marco de interoperabilidad exige que, al enviar datos de identificación de la persona jurídica, se envíen también los datos de la persona física que actúa en su nombre.

5.1.4 ESTABLECIMIENTO DE LA IDENTIDAD DE UNA PERSONA FISICA CON UN REPRESENTANTE AUTORIZADO

En FULL CERTIFICATE la validación de la identidad es proporcionada por el cliente al registrarse en nuestro portal de certificación. El Cliente y/o Usuario proporcionará los siguientes datos:

✓ Si es una persona física o autónoma:	✓ Si se trata de una entidad jurídica o asociaciones y colectivos:
• Nombre(s) • Apellidos, • País de residencia • Documento de identidad • Fecha de nacimiento, • Idioma • Genero • eMail, • Password / Clave • Número de teléfono móvil	• Nombre de la empresa • CIF • Datos del representante legal: - Nombre y Apellido (s) - País de Residencia - Documento de identidad - Fecha de nacimiento - Idioma - Genero - eMail - Password / Clave - Número de teléfono móvil

Una vez que el usuario y/o cliente se haya registrado, recibirá un correo electrónico de FULL CERTIFICATE para verificar su identidad. Después de eso, puede iniciar sesión y actualizar sus datos a través del control del panel.

Además de lo mencionado anteriormente, es importante mencionar que FULL CERTIFICATE tiene tres tipos diferentes de registro:

- **Registro Estándar**: El usuario ingresa sus datos como se indicó anteriormente. A continuación, se valida el correo electrónico y posteriormente se crea una firma holográfica por el usuario cuando este cumple, en primer lugar, con los términos y condiciones del servicio y, en segundo lugar, con el hecho de que ha proporcionado los datos correctos.

- **Registro Documental**: El usuario carga su documento de identidad al sistema. Posteriormente, un algoritmo, mediante lectura OCR, verifica que los datos proporcionados por el usuario coincidan con los datos contenidos en el documento de identidad.

- **Registro Cualificado**: El usuario realiza la carga del certificado electrónico. FULL CERTIFICATE lee el certificado para comprobar que los datos introducidos por el usuario coinciden con los del certificado.

Por lo tanto, FULL CERTIFICATE consigue la “autenticación eIDAS" a través del control de documentos. Con ello le permite al usuario acceder a servicios de certificación eIDAS, como, por ejemplo: el eMail Certificado Cualificado y SMS Certificado Cualificado (dentro de la categoría eIDAS). A continuación, se indican los niveles de registro que FULL CERTIFICATE permite:

1. Registro Estándar
2. Registro Documental
3. Registro Cualificado

Adicionalmente, resaltamos que en los servicios de comunicación y/o notificación:

- La identificación del remitente se valida según la normativa europea
- Carga de Documentos:
    - Si es una persona física (por ejemplo, pasaporte, identificación electrónica, identificación, etc.),
    - Si es Persona Jurídica u Organismo Público (por ej. NIF, Número de IVA, poder notarial, etc.…).
    - Si es necesario, la revisión manual será suficiente.
- Doble verificación de eMail y teléfono móvil por doble OTP.
- Registro mediante Certificado Cualificado de persona física o jurídica emitidos por un país de la Unión Europea.

Por otra parte, es importante recordar que antes de registrarse en nuestro portal, acepta de forma indiscutible los siguientes documentos: Aviso Legal, Política de Privacidad, Política de Cookies.

5.2 PROCESO DEL SERVICIO

5.2.1 REQUISITOS PARA EL SERVICIO DE ENTREGA CERTIFICADA ELECTRÓNICA CUALIFICADA

El servicio QERDS proporcionado por FULL CERTIFICATE cumple todos los requisitos de la norma ETSI EN 319 401, Apartado 6.1, así como los siguientes requisitos específicos:

- Las políticas y prácticas de ERDS son aprobadas por la dirección de ERDSP y comunicadas a las partes interesadas, poniéndolas a disposición en el sitio web de FULL CERTIFICATE
- El ERDSP cuenta con un procedimiento de revisión y actualización de las prácticas y un procedimiento de notificación de los cambios a las partes interesadas
- El servicio QERDS es prestado por "FULL CERTIFICATE SL" conjuntamente con los servicios de certificación electrónica y sellado de tiempo prestados por Camerfirma y Uanataca SA, respectivamente.
- De acuerdo con el punto mencionado anteriormente FULL CERTIFICATE conservará la responsabilidad general de la conformidad con los procedimientos prescritos en la seguridad de la información, incluso si la funcionalidad del TSP´s es realizada por contratistas externos. De todo esto es posible entender sus obligaciones.
- En relación con las obligaciones de apoyo a terceros, destacamos que:

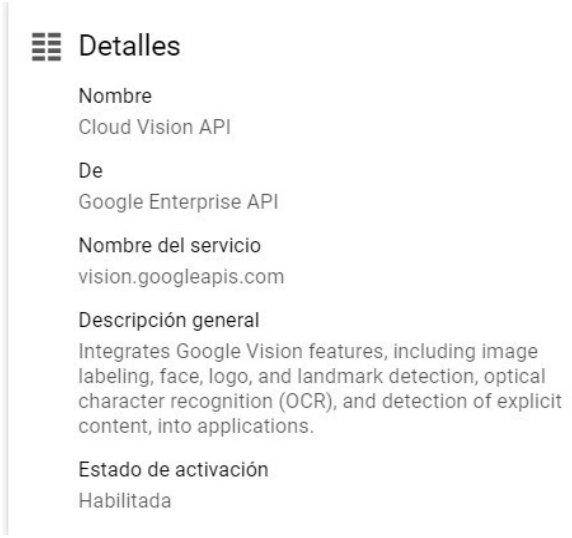
  1. Microsoft - Azure Compute Vision

  SLA definido en: https://azure.microsoft.com/es-es/support/legal/sla/cognitive-services/v1_1/

  Detalles del servicio para FullCertificate

2. Google Vision
Definición de SLA: https://cloud.google.com/vision/sla

Detalle del servicio:



3. Camerfirma
Servicios: Firma electrónica de servidor (eIDAS)
Nivel de Servicio SLA: https://www.camerfirma.com/ayuda/nivel-de-servicio-camerfirma/
Políticas de Servicio: https://www.camerfirma.com/practicas-de-certificacion-ac-camerfirma-cps-dpc/

4. Uanataca
Servicios: TSA Service
Políticas de Servicio: https://web.uanataca.com/en/policies-practices

5. NRS-GROUP
Servicios: SMS Gateway
Certificado ISO 27001: https://www.360nrs.com/iso27001/
Políticas de seguridad: https://www.nrs-group.com/politica-de-seguridad
Aviso Legal: https://www.nrs-group.com/aviso-legal
Políticas de privacidad: https://www.nrs-group.com/politica-de-privacidad

6. RedIRIS (www.rediris.es)
Servicios: NTP (Network Time Protocol)
Definición de servicios: https://www.rediris.es/servicios/conectividad/ntp/index.html.es

7. EU Trust Services
Servicios: Root Certificates for EU Qualified Autorities, Certificate Validations
Definición de servicios: https://esignature.ec.europa.eu/efda/swagger-ui.html#/api-browsercontroller
Referencias del servicio: https://esignature.ec.europa.eu/efda/tl-browser/#/screen/home

- La comunicación en la que fluyen los datos está protegida de forma fiable por un canal encriptado, lo que elimina el riesgo de cualquier cambio en el contenido del usuario antes de su envío/ transmisión. Las evidencias / pruebas relacionadas con el envío/transmisión de eventos de contenido de usuario se almacenan de forma confiable por pérdida y posterior robo en un entorno protegido bajo el control FULL CERTIFICATE durante 15 (quince) años.
- Este documento describe el proceso de identificación del remitente y el destinatario
- FULL CERTIFICATE garantiza la identificación/autenticación del remitente antes de enviar el contenido del usuario
- FULL CERTIFICATE garantiza la identificación/autenticación del destinatario antes de la entrega de los datos (envío/contenido del usuario)
- El envío y recepción de datos está protegido a través de una capa de conexión segura (SSL) de Full Certificado para excluir cualquier posibilidad de modificación involuntaria de los datos
- FULL CERTIFICATE especifica los tipos de eventos relacionados con el aprovisionamiento y proporciona pruebas de proceso
- Cualquier modificación de los datos necesarios para el envío o recepción de los mismos están claramente indicados para el remitente y el destinatario
- La fecha y hora de envío, recepción y modificación del contenido del usuario se indican mediante un sello / marca de tiempo (timbrado) electrónico cualificado
- El ERDSP deberá autenticar otros ERDSP antes de la emisión o entrega de contenido de usuario; en cualquier caso, enfatizamos que no tenemos interoperabilidad con ningún otro ERDS
- La ERDSP verificará que el servicio(s) con el que interopera es al menos un ERDS
- La disponibilidad, integridad y confidencialidad de los contenidos del usuario están garantizados desde el envío hasta la aceptación
- Se protege la integridad del contenido del usuario, especialmente cuando se intercambia entre remitente y destinatario o entre componentes del sistema de servicio distribuido
- Los resultados / datos relacionados con las actividades de entrega de contenidos de los usuarios están protegidas por un sello electrónico avanzado que excluye la posibilidad de modificar o alterar los datos
- El remitente especifica de antemano el período de tiempo en el que el sistema QERDS intenta entregar el contenido del usuario. Si el remitente no selecciona ninguna opción, este período será de 3 días por defecto
- En los casos en que el ERDS requiera modificaciones al contenido del usuario, estas modificaciones se indicarán claramente al remitente, el destinatario y a cualquier tercero
- La fecha y hora de envío, recepción y modificación del contenido del usuario se indican mediante un sello/marca (timbrado) de tiempo electrónica cualificado
- QERDS utiliza los servicios calificados de QCSP Camerfirma para la emisión y gestión de Certificados Cualificados (X.509) y Uanataca S.A. para sellos cualificados de Tiempo

- El ERDSP ha verificado que los servicios con los que interopera son al menos un ERDS
- Toda la información de entrega de QERDS se almacena durante un período de 15 años, de conformidad con la legislación europea
- Este documento describe los casos en los que la entrega en el R-ERDS no es posible. En estos casos, el sistema genera automáticamente las evidencias necesarias para este evento y se almacena por 15 años
- Este documento establece de forma clara e inequívoca que la política de ERDS está regulada por la (EU) No. 910/2014
- El TSP se someterá, una vez por trimestre, a un escaneo de vulnerabilidades en las direcciones IP públicas y privadas identificadas por el TSP y registrará evidencia de que cada escaneo de vulnerabilidad fue realizado por una persona o entidad con las habilidades, herramientas, competencia, código de ética e independencia necesarios para proporcionar un informe confiable
- FULL CERTIFICATE se someterá a una prueba de penetración en los sistemas del TSP, una vez al año. La prueba de penetración mencionada anteriormente será realizada por una persona o entidad con las habilidades, herramientas, competencia, código de ética e independencia necesarios para proporcionar un informe confiable
- FULL CERTIFICATE garantiza que se llevará a cabo un análisis de los requisitos de seguridad en la etapa de diseño y especificación de requisitos de cualquier proyecto de desarrollo de sistemas emprendido por el TSP o en nombre del TSP para garantizar que la seguridad esté incorporada en los sistemas de IT. FULL CERTIFICATE, también, declara que se aplicarán procedimientos de control de cambios para las versiones, modificaciones y correcciones de software de emergencia de cualquier software operativo y cambios en la configuración que aplique la política de seguridad de TSP
- Este documento incluye la lista completa de participantes de QTSP que proporcionan QERDS
- Este documento incluye todas las limitaciones para el uso de QERDRS: sin limitaciones excepto las indicadas en el SLA
- FULL CERTIFICATE resguarda de forma confiable los datos / evidencias contra perdidas y robos posteriores durante un periodo de 15 años
- La posibilidad de darse de baja del servicio está disponible las 24 horas del día. En todo caso, se conservará copia de los certificados emitidos hasta que finalice el período de custodia asignado.

5.2.2 DESCRIPCIÓN DE LA TECNOLOGÍA

QERDS utiliza una tecnología que, tras la identificación inicial del remitente y su autenticación, el contenido del usuario es aceptado por S-ERDS en un canal seguro protegido y encriptado de forma fiable. En este momento, el S-ERDS genera las evidencias necesarias, incluyendo datos veraces sobre el tipo de evento, entre ellos la fecha, hora y la suma de control/hash del contenido del usuario, firmada electrónicamente por la Camerfirma y sellada con tiempo calificado. estampilla. Si la aceptación por parte de S-ERDS no es posible, vuelva a generar automáticamente la prueba de rechazo necesaria.

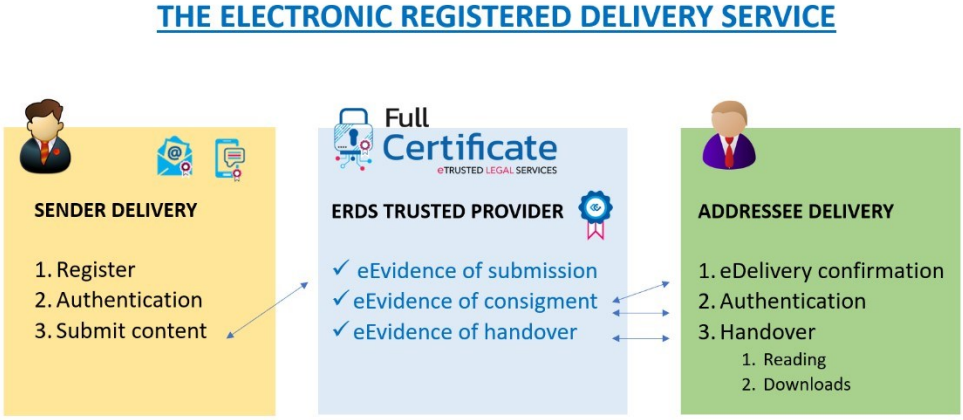
El S-ERDS transfiere de forma fiable el envío al R-ERDS. Nuevamente se generan automáticamente las pruebas necesarias, incluyendo datos precisos sobre el tipo de evento, entre ellos la fecha, la hora, la suma de control/hash del contenido del usuario, firmadas electrónicamente por la Autoridad de Certificación QERDS y selladas con un sello de tiempo calificado. Si la entrega a R-ERDS no es posible, el sistema generará automáticamente la evidencia necesaria de este evento.

En el momento en que el contenido del usuario llega al sistema del destinatario, es decir, ha sido entregado al destinatario, el R-ERDS genera la evidencia necesaria, incluidos datos precisos sobre el evento, incluida la fecha, la hora, la suma de control/hash del contenido del usuario. Además, al momento de la certificación se realizará la firma electrónica del QERDS y sellado de tiempo por parte de TSA Calificada, en este caso “Uanataca SA”. El servicio de firma que utilizan los QERDS se basa en un certificado emitido por la autoridad de certificación en este caso "CAMERFIRMA". Si la transferencia (entrega de la comunicación) no es posible, R-ERDS generará automáticamente la evidencia necesaria de este evento.

Al final destacamos que “Camerfirma” es responsable de la firma electrónica del FULL CERTIFICATE y se encarga de los procedimientos de custodia y almacenamiento de las firmas electrónicas emitidas, así como de la gestión de la clave privada de esta firma, todo ello esto de acuerdo con la normativa europea.

5.2.3 DIAGRAMA DEL PROCESO DE PRESTACIÓN DE UN SERVICIO CALIFICADO PARA ENTREGA ELECTRÓNICA Y CERTIFICADA - PROCESO DE PRESTACIÓN DEL SERVICIO

El siguiente gráfico detalla el proceso y sus participantes en el servicio ERDS.



5.2.4 AUTENTIFICACIÓN

Para recibir la autentificación como usuario de QERDS se requiere:

1. **Registro:** El usuario introduce los siguientes datos necesarios para la creación de una cuenta de usuario:
    - País de residencia
    - Número de identificación
    - Nombre
    - Apellido paterno
    - Apellido materno (opcional)
    - Fecha de da nacimiento
    - Idioma
    - Genero
    - Número de teléfono móvil
    - eMail (correo electrónico)
    - Password / Contraseña (mínimo 8 carácteres)

2. La edad mínima de inscripción es de 16 años.

3. **Confirmación OPTIN-2 del eMail** mediante el envío de un código de validación que debe introducirse en el registro para validar que efectivamente el sujeto tiene acceso a la dirección de correo electrónico indicada

4. Se solicita la **firma holográfica** para completar el registro.

5. **Acreditación de la identidad del usuario**. La identidad puede acreditarse de cualquiera de las siguientes maneras:

    a. **Documento de autentificación.** El destinatario confirma el canal de comunicación recibido confirmándolo explícitamente (escribiéndolo en un campo de texto). Entonces tendrá que confirmar con un código de uso único (OTP) y también proporcionar un documento de identidad que debe coincidir con los datos del destinatario proporcionados por el remitente.

    b. **Autenticación cualificada.** El destinatario puede presentar un certificado electrónico de identidad emitido por una autoridad de certificación válida en cuyos datos figuran los indicados por el remitente

5.2.5 IDENTIFICACIÓN DEL REMITENTE/RECEPTOR

REMITENTE / EMISOR

La identificación del remitente se realiza de la siguiente manera y siempre que hayan pasado el proceso de "Autenticación" de la sección anterior:

- **Canal API.**
    - Se proporciona un punto de acceso y un usuario + contraseña.
    - El canal de comunicación se realiza a un punto de conexión a través de SSL con las siguientes características (algoritmo de firma sha256RSA, clave pública RSA de 4096 Bits)
    - Si los datos de acceso son incorrectos, el sistema bloqueará nuevos intentos de acceso durante un período de 30 segundos.
    - Si los datos de acceso son correctos, el sistema devuelve un token de conexión para ese cliente con una validez de 24 horas, es responsabilidad del usuario del sistema la custodia y el uso de dicho token durante el período de validez.
    - Se establece el siguiente límite de solicitud (de cualquier tipo, inicio de sesión, consulta, ejecución):
        - Solicitudes por segundo: 100
        - Solicitudes por minuto: 1000
        - Solicitudes por hora: 5000
        - Solicitudes por día: 10000

    o En el caso de exceder cualquiera de los límites anteriores, el servicio denegará al usuario cualquier nueva solicitud hasta que transcurra el tiempo necesario para obtener un nuevo límite de tiempo.

- **Canal Web.**
    - Puede autenticarse mediante certificado electrónico emitido por una entidad certificadora válida.
    - Puede autenticarse a través de un punto de acceso y un usuario + contraseña.
    - El canal de comunicación se realiza a un punto de conexión a través de SSL con las siguientes características (algoritmo de firma sha256RSA, clave pública RSA de 4096 Bits)
    - Es necesario pasar la validación del sistema de Google® recaptcha®
    - Es posible habilitar la protección de un sistema de dos factores (2FA) opcionalmente, requiere un teléfono móvil e instalar una aplicación de

autenticación. En el caso de ser activado, después de ingresar las credenciales de inicio de sesión, siempre se solicitará el código de dos actores antes de permitir el acceso al Sistema.

RECEPTOR / DESTINATARIO

La identificación del receptor se realiza de cualquiera de las siguientes maneras:

1. **Acreditación cualificada.** Si el destinatario tiene un **certificado electrónico de identidad**, será válido siempre y cuando:
    a. El certificado es válido
    b. EL certificado no ha sido revocado
    c. Los datos del asunto coinciden con los datos introducidos por el remitente del mensaje
2. **Acreditación documentada.** El destinatario puede optar por esta acreditación, para lo cual se le pedirá que siga los siguientes pasos:
    a. Confirmar los datos relativos al medio por el cual ha recibido la notificación. Para el caso del correo electrónico, se le solicita que ingrese la dirección completa. En el caso de SMS, se solicita ingresar los últimos 4 dígitos del teléfono móvil.
    b. Se envía un código único (OTP) al mismo canal de notificación para confirmar el acceso.
    c. Si el destinatario introduce el código OTP correcto, se le pedirá que introduzca una foto de su ID, este debe contener el nombre y el apellido además del número de identidad especificado por el remitente.

5.2.6 GENERACIÓN DE EVIDENCIAS / REPORTES / INFORMES

QERDS proporciona prueba de envío y recepción de contenido de usuario.

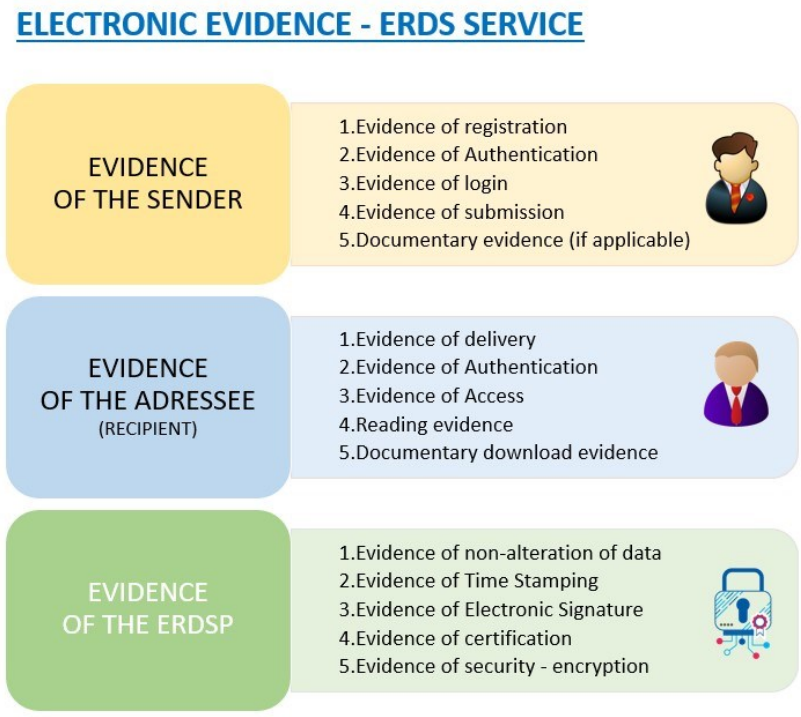
Los sistemas operativos involucrados en la generación de la evidencia electrónica mantienen sus registros de fecha/ hora actualizados con una frecuencia de 60 minutos y hasta un máximo de 72 horas contra el servicio NTP por RedIRIS https://www.rediris.es/servicios/conectividad/ntp/index.html.es

FULL CERTIFICATE recopila y almacena datos sobre:

- Todos los eventos relacionados con la verificación inicial de la identidad y la identificación del remitente
- Todos los eventos relacionados con la verificación inicial de la identidad y la identificación del destinatario

- En la verificación inicial de la identidad, se verifican los datos del documento de identidad de una persona física (por ejemplo, el DNI o pasaporte), los datos de identificación de una persona jurídica (por ejemplo, la verificación del registro, las facultades, etc.) y todos los demás datos necesarios para su correcta determinación
- Datos destinados a la identificación inicial del remitente/destinatario
- Nivel de autenticación remitente/destinatario
- Prueba de que el remitente ha sido debidamente autenticado antes de aceptar el envío
- Datos sobre el funcionamiento de los QERDS que confirman la autenticación del remitente y el destinatario, así como la comunicación entre ellos
- Prueba de que el contenido del usuario ha sido recibido por el destinatario
- Evidencia de que el contenido del usuario no ha sido modificado durante la transmisión
- La traza de actividad dentro del sistema de Full Certificate y, opcionalmente, la geolocalización de los usuarios.

Como resumen de la evidencia recopilada por FULL CERTIFICATE, se proporciona el siguiente diagrama.



5.2.6.1 EVIDENCIAS RELACIONADA CON EL REMITENTE (S-ERDS)

Después de la identificación inicial y autenticación del remitente y el uso de QERDS a través de S-ERDS, se genera una evidencia del envío, que también se puede proporcionar a un tercero. La evidencia muestra la fecha y hora exacta de envío del contenido del usuario por parte del remitente con una hora precisa fijada con respecto al GMT (Greenwich Time).

- ✓ **Envío aceptado**

  El remitente entrega correctamente el contenido del usuario a S-ERDS. Se genera evidencia con fecha y hora preestablecida, indicando que el remitente inicialmente identificado y debidamente autenticado ha presentado un envío al sistema ERDS que ha sido aceptado por el proveedor que realizará todas las acciones necesarias para entregarlo a los respectivos destinatarios (s).

- ✓ **Envío rechazado**

  El contenido de usuario que ha sido enviado al S-ERDS por el remitente no ha sido aceptado por el S-ERDS. La evidencia generada muestra que el remitente que fue identificado inicialmente y debidamente autenticado ha transmitido el contenido del usuario a los usuarios en una fecha y hora determinadas, y que el sistema S-ERDS se ha negado a tomar las medidas necesarias.

5.2.6.2 EVIDENCIAS RELACIONADAS CON EL DESTINATARIO (R-ERDS)

Después de la identificación y autenticación iniciales exitosas del destinatario y el uso de QERDS a través de S-ERDS, se genera evidencia de recepción, que también puede proporcionarse a un tercero. La evidencia muestra la fecha y hora exacta de envío del contenido del usuario por el remitente con un tiempo precisa fijada con respecto al GMT (Greenwich Time).

- ✓ **Evidencias relacionadas con la entrega del contenido del mensaje**
  - o La notificación de mensaje disponible se ha entregado al destinatario.
  - o Las evidencias relacionadas muestran que el envío de la notificación de mensaje disponible se ha entregado al destinatario. También muestran si ha interactuado con el contenido del mensaje de notificación (descargar imágenes, hacer clic en enlaces) El contenido de la notificación se ha entregado al destinatario.
  - o Las pruebas relacionadas muestran que el contenido del mensaje se ha entregado al destinatario dentro del tiempo preestablecido después de que el destinatario se haya identificado inicialmente y se haya autenticado debidamente.

- ✓ **Error en la entrega del contenido del mensaje**

  La imposibilidad de entregar el contenido puede ser causada por diferentes eventos, tales como:

  - o El sistema ERDS no pudo enviar la notificación de mensaje disponible del remitente al destinatario. En tal caso, la evidencia es generada por R-ERDS.

- Si bien el mensaje figuraba en el sistema ERDS, no se han recibido pruebas de que la entrega haya tenido éxito en un período determinado. En tal caso, el ERDS genera las evidencias con el código apropiado del motivo de la falta de entrega.

5.2.6.3 EVIDENCIAS RELACIONADA CON LA ENTREGA DE CONTENIDOS POR EL USUARIO AL DESTINATARIO

Transferencia de contenidos

El contenido del usuario se ha trasladado correctamente de R-ERDS a la aplicación/agente de usuario (UA) del destinatario. Los eventos pueden ser: pull (es decir, el UA/ aplicación del destinatario recupera automáticamente el contenido del usuario del R-ERDS - en los destinatarios conectados a la API o a través de un portal) o push (el contenido del usuario se ha entregado correctamente al sistema del destinatario mediante la entrega directa del mensaje al sistema del destinatario - aplicación móvil, API o portal web).

La evidencia correspondiente muestra que el contenido del usuario ha sido entregado en una fecha y hora determinada por el R-ERDS a través del UA/app del destinatario y después de su correcta certificación.

Fallo en la transferencia de contenidos.

El contenido del usuario no puede ser transmitido por el R-ERDS al agente de usuario (UA)/a la aplicación del destinatario. En caso de extracción (es decir, la aplicación de UA/destinatario recupera automáticamente el mensaje del ERDS), el mensaje no se puede descargar dentro de un período determinado debido a errores técnicos y/u otras razones.

La evidencia relacionada muestra que el contenido no puede ser transmitido desde el R-ERDS a la solicitud del UA/receptor después de un cierto número de intentos o un plazo establecido. Estos parámetros son específicos y están configurados para el sistema específico.

5.2.6.4 CERTIFICACION DEL SERVICIO

Los sistemas operativos involucrados en la generación de evidencias electrónicas mantienen actualizados sus registros de fecha/ hora a con una frecuencia de 60 minutos y hasta un máximo de 72 horas contra el servicio NTP por RedIRIS (https://www.rediris.es/servicios/conectividad/ntp/index.html.es)

El sistema de generación de los certificados emitidos se basa en el siguiente procedimiento:

- Recopilación de las evidencias generadas hasta el momento de la certificación final
- Generación de un documento en formato PDF con las evidencias recabadas y el contenido de la notificación/mensaje transmitido
- Firma del documento por medio de una firma cualificada de servidor emitida por el tercero de confianza (CAMERFIRMA) utilizando el algoritmo de firma SHA256 RSA, clave pública RSA (2048 bits)

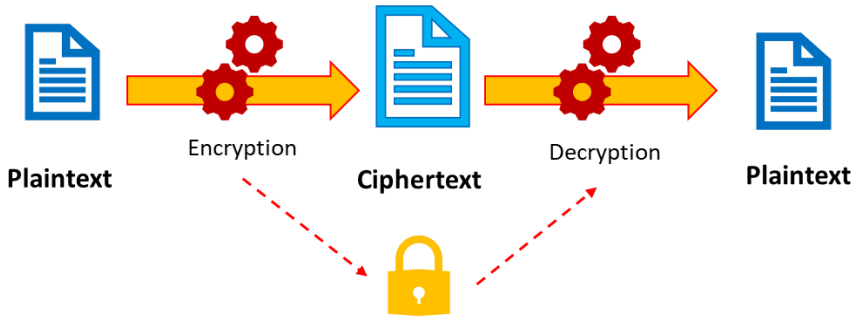
- Adicionalmente se añade el sello de tiempos emitido por Uanataca S.A. utilizando el algoritmo de firma SHA256 RSA, clave pública RSA (2048 bits)

Una vez generado se pone a disposición del remitente del mensaje (usuario del Sistema de FULL CERTIFICATE) y se almacena encriptado como se detalla en la siguiente sección.

5.2.6.5 LA ENCRIPTACIÓN Y CUSTODIA (RESGUARDO) DE LOS CERTIFICADOS

La encriptación de los documentos generados por el sistema se realiza mediante clave pública cifrada con RSA y clave simétrica, de la siguiente manera:

1. El archivo PDF está encriptado usando encriptación AES-256 bits, método hash SHA1. El resultado de la encriptación se guarda en formato Base64 dentro de un nuevo archivo con el mismo nombre que el original, pero cambiando la extensión por .txt y que contiene el resultado de la encriptación.
2. En el momento del cifrado se genera una clave de descifrado simétrica, que es cifrada por RSA con clave de longitud 4096 y luego guardada en formato Base64 en un nuevo archivo con el mismo nombre que el original, pero cambiando la extensión por .txt key.
3. Completados los pasos anteriores, el archivo original se elimina del sistema de inmediato, dejando solo sus pares encriptados.
4. A continuación, se indica el diagrama de proceso de Encriptación.



6. GESTIÓN DE RIESGOS

6.1 PROTECCIÓN DE LOS DATOS COMPARTIDOS CONTRA EL RIESGO DE PÉRDIDA, ROBO, DAÑO O MODIFICACIONES NO AUTORIZADAS

Todos los sistemas o plataformas que contienen software, repositorios de datos o información de auditoría se almacenan de forma segura en un centro de procesamiento de datos especial con control de acceso. FULL CERTIFICATE cuenta con un centro de datos que ofrece protección física y lógica de manera segura y confiable.

La confidencialidad y la integridad de los datos son importantes para el funcionamiento de FULL CERTIFICATE, por lo que se utilizan técnicas criptográficas de protección de datos en medios extraíbles. Para mitigar el riesgo de envejecimiento de los soportes, mientras se siguen necesitando los datos almacenados, se transfieren a nuevos soportes antes de que sean ilegibles. FULL CERTIFICATE almacena múltiples copias de datos valiosos en diferentes medios y sitios físicos para reducir aún más el riesgo de daños accidentales o pérdida de datos. La comunicación de datos está protegida de forma segura por un canal encriptado, eliminando así el riesgo de pérdida, robo, daño o modificación no autorizada de datos. Las pruebas se almacenan de forma fiable para evitar cualquier pérdida o robo posterior en un entorno protegido bajo el control de FULL CERTIFICATE durante un período de 15 años.

6.2 TEMINACIÓN / FINALIZACION DE LA SUSCRIPCIÓN DEL SERVICIO

El contrato para la prestación del servicio de entrega de documentos electrónicos cualificados se rescinde en una de las siguientes circunstancias:

a) Cancelación de la cuenta o cierre de un perfil desde la aplicación web de FULL CERTIFICATE con activación de la respectiva funcionalidad. Para ello, el usuario deberá confirmar la cancelación de la cuenta perdiendo el saldo disponible y el acceso a los certificados emitidos. Este certificado continuará en custodia por el tiempo legal requerido. La terminación es inmediata y el usuario ya no podrá acceder al sistema

b) Por uso indebido de la aplicación, siendo comunicado al usuario de la infracción cometida.

c) Después de 90 días con saldo negativo en la cuenta sin haber pagado los servicios de FULL CERTIFICATE.

La terminación del servicio está disponible las 24 horas del día, los 7 días de la semana. La hora en los sistemas asociada a la terminación de un contrato de servicio para la prestación del servicio de envío electrónico de registros se sincroniza con el GMT a través de NTP (Network Time Protocol) al menos cada 24 horas.

6.3 CONTROL DE SEGURIDAD FÍSICA Y ORGANIZACIONAL

6.3.1. CONTROLES DE SEGURIDAD FISICA

Las medidas relacionadas con la protección física de los datos de información, los sistemas tecnológicos, los locales y sus correspondientes sistemas de soporte tienen por objeto impedir:

- Acceso no autorizado, daño e interferencia con las condiciones de trabajo
- Pérdida, daño o compromiso de recursos
- Compromiso o robo de información o herramientas de procesamiento de información.

Las instalaciones de FULL CERTIFICARTE cuenta con medidas de control de acceso físico a los medios de procesamiento de datos que son los siguientes:

- Edificio en recinto privado, equipado con altas medidas de **seguridad**
- Vigilancia permanente perimetral en el edificio mediante guardias y cámaras de seguridad
- Control de acceso a las instalaciones 24x7x365;
- Control de acceso mediante tarjetas de proximidad con programación independiente
- Cámaras de seguridad IP de circuito cerrado, con grabación 24 horas, en CPD y puntos de acceso a las instalaciones
- Todos los accesos a las instalaciones son registrados para un mejor control;
- Guardaespaldas al personal externo para trabajos de mantenimiento

6.3.2 INDICACIONES DE USO / INSTALACIÓNES

FULL CERTIFICATE cuenta con instalaciones especialmente diseñadas y equipadas con el más alto nivel de control de acceso físico, que alberga todos los componentes principales de la infraestructura. Estos incluyen equipos de seguridad, refrigeración, redundancia eléctrica e infraestructuras de conectividad.

6.3.3 ACCESO FÍSICO

El acceso a los equipos (servidores, medios de almacenamiento de datos, etc.…) con el que cuenta FULL CERTIFICATE solo está habilitado para el equipo de TI responsable del mantenimiento y soporte de la infraestructura. Esto es a través de un control de acceso registrado en el centro de datos para el que es necesario presentar el documento de identidad válido.

6.3.4 CONTROL DE ACCESOS

Existen diferentes medios de acceso a los sistemas de FULL CERTIFICATE.

1. Acceso del usuario del sistema (remitente/destinatario)
   Acceso API. Tiene las siguientes medidas de seguridad:
   - Punto de acceso vía HTTPS (SSL)
   - Limitación de la tasa de solicitud (por segundo, minutos, horas y día) Evidencia de uso (solicitudes y respuestas).
   - Control de acceso inicial mediante usuario/contraseña
   - Control de consumo mediante tokens de portador. Los tokens de portador son el tipo predominante de token de acceso utilizado con OAuth 2.0. Un token al portador es una cadena opaca, que no pretende tener ningún significado para los clientes que lo utilizan. Los tokens emitidos son una cadena de caracteres alfanuméricos.

2. Acceso al portal web
   - El acceso al portal está controlado por usuario/contraseña
   - Capa de seguridad de accesos no deseados a través de Google recaptcha
   - Confirmación de acceso por 2FA (Doble factor de autenticación) la aplicación móvil Authenticator.

3. Acceso al sistema de control de acceso a los servicios críticos

El acceso a los sistemas de gestión de servicios (Sistemas Operativos, MTAs, SMS Carrirers, etc.) se realiza a través de accesos seguros VPN controlados por personal de TI responsable del mantenimiento y gestión de los servicios.

6.3.5 RESPONSABILIDAD DE PUBLICACIÓN Y ALMACENAMIENTO

El registro público está disponible en: https://www.fullcertificate.com

FULL CERTIFICATE publica en su sitio web notificaciones relacionadas con sus actividades y todos los documentos importantes de interés para los usuarios y partes de confianza.

Los clientes y las partes de confianza están informados sobre la política, la práctica y las condiciones generales de prestación del servicio de correo electrónico antes de firmar un contrato. La documentación, incluyendo Política y práctica, acuerdos, modelos, informes de auditoría, etc., se publica en el sitio web de FULL CERTIFICATE inmediatamente después de cada actualización. Los certificados de funcionamiento de la autoridad certificadora se publican inmediatamente después de cada emisión de nuevos certificados.

FULL CERTIFICATE ofrece servicios relacionados con el acceso a la información almacenada (el registro público) proporcionando acceso basado en HTTPS.

La información publicada en el almacenamiento de FULL CERTIFICATE es permanentemente accesible (24/7/365), excepto en caso de eventos fuera del control de FULL CERTIFICATE.

Finalmente le informamos:

- Todo cambio que tenga un impacto en el nivel de seguridad manifestado será aprobado por las autoridades de administración correspondientes
- Implementamos la opción de enviar un mensaje anónimo.

En relación al último párrafo se manifiesta que cualquier cambio deberá ser aprobado y validado por la Administración y Dirección general de FULL CERTIFICATE.

6.4 GESTION DE INCIDENCIAS

Los procedimientos a seguir en caso de incidencias son los siguientes:

1. IMPACTO Y CALIFICACIÓN DEL RIESGO

a) IMPACTO GRAVE. Este es un incidente que afecta completamente el servicio y el servicio no se puede proporcionar sin resolver el accidente.
b) IMPACTO MEDIO. Se trata de un incidente que afecta parcialmente al sistema y el servicio puede prestarse sin resolver el accidente.

c) BAJO IMPACTO. Se trata de un incidente que no afecta al servicio que puede prestarse sin resolver el accidente.

PROTOCOLO DE ACCIONES EN FUNCIÓN DE LA CALIFICACIÓN DEL IMPACTO

a) IMPACTO GRAVE: - HARDWARE

Fallo en el servidor

Todos los servidores son redundantes con un mínimo de 2 equipos similares o de características idénticas. Además, hay una sincronización de los archivos del sistema y la evidencia entre el servidor primario y secundario (independiente del sistema de copia de seguridad). En caso de un fallo en el hardware principal, el tráfico se enrutará al servidor secundario en el menor tiempo posible.

Una vez que se haya realizado el enrutamiento y los servicios estén nuevamente operativos, se realizará el análisis del problema en el servidor con la falla.

- En el caso de que la reparación sea factible y no comprometa la integridad del sistema en su conjunto, procederá a su reparación y se convertirá en un servidor secundario para reemplazar el principal en caso de fallo.

- En caso de que la reparación no sea factible, la información contenida en los medios de almacenamiento se destruirá y, tras su reciclado, en los puntos indicados por la autoridad competente.

- En caso de que la reparación no sea factible, la información contenida en los soportes de almacenamiento se destruirá y se reconsiderara de acuerdo a los puntos indicados por la autoridad competente.

Falla del firewall

Todos los servidores son redundantes con un mínimo de 2 equipos similares o de idénticas características. La configuración del sistema se respalda una vez al mes. En caso de falla en el servidor principal, el cableado físico del servidor se enrutará manualmente al nuevo servidor y se cargará la última copia de seguridad de la configuración del sistema en el menor tiempo posible.

Una vez realizado el cambio y los servicios nuevamente operativos, se realizará el análisis del problema en el servidor con la falla.

- En el caso de que la reparación sea factible y no comprometa la integridad del sistema en su conjunto, se procederá a su reparación y se convertirá en un servidor secundario con el fin de sustituir al principal en caso de fallo.
- En caso de que la reparación no sea factible, la información contenida en los soportes de almacenamiento se destruirá y se reconsiderara de acuerdo a los puntos indicados por la autoridad competente.

b) *SOFTWARE*

Falla del Sistema Operativo

- El servicio se enrutará al servidor secundario. Una vez que los servicios están disponibles de nuevo en el servidor secundario, se procederá al análisis de la incidencia que ha causado el fallo.
- En caso de que la reparación sea factible y no comprometa la integridad del sistema en su conjunto, se intentará restaurar el sistema utilizando la última copia de seguridad generada por el sistema operativo.
- En caso de que la restauración por copias de seguridad no sea posible, se procederá a su formateo y reinstalación del sistema operativo y se convertirá en un servidor secundario con el fin de reemplazar el principal en caso de fallo.
- En caso de que la reparación no sea factible, la información contenida en los soportes de almacenamiento se destruirá y se reconsiderara de acuerdo a los puntos indicados por la autoridad competente.

Falla en DBMS

Las bases de datos están bajo configuración "Reflex" en al menos 2 servidores (primario + secundario).

Si hay un fallo en el sistema principal, las conexiones al servidor secundario se enrutarán manualmente y en el menor tiempo posible. Esta redirección puede no ser automática en cualquier caso porque la sincronización en la reflexión es de una sola manera por lo que solo un servidor puede ser utilizado a la vez. Una vez que el enrutamiento se realiza y que los servicios están disponibles de nuevo, el impacto será revisado.

En caso de que la reparación sea factible y no comprometa la integridad del sistema en su conjunto, se intentará restaurar el sistema utilizando la última copia de seguridad generada por el sistema operativo.

- Si la restauración no es posible, se utilizará el kit de reparación de la instalación del DBMS
- Si lo anterior no resuelve el problema, el sistema operativo será formateado y reinstalado para la posterior instalación del DBMS, convirtiéndose ahora en un servidor secundario para reemplazar el servidor principal en caso de falla.
- En caso de que la reparación no sea factible, la información contenida en los soportes de almacenamiento se destruirá y se reconsiderara de acuerdo a los puntos indicados por la autoridad competente.

C) LA RED - NETWORK

Ataque DDoS

En caso de ataque de negación de servicio, se realizarán los siguientes pasos:

1. Primero hay que distinguir un ataque de una interrupción ordinaria.
2. Descartar las interrupciones más comunes:
    a. Verificación de la conectividad de salida
    b. Posibles problemas globales a través de "Internet Healht Reports" o "Internet Traffic Report"
    c. Verificar el acceso a la red externa
    d. Confirmar las respuestas del DNS.
3. Póngase en contacto con el equipo de asistencia del proveedor de conectividad en el centro de datos.
4. Aplicaciones jerarquizadas. Una vez confirmado el ataque, se jerarquizarán las aplicaciones. Esto implicará que se prioricen los servicios QERDS sobre el resto (por ejemplo, la información web).
5. Los usuarios asociados y los usuarios remotos son apoyados por la creación de una “whitelist (lista blanca)” antes de proceder al cierre de los puertos y rangos de IP.
6. Se definirá el ataque, determinando su naturaleza, catalogándolo de la siguiente manera:
    a. Volumétrico: ataques basados en la sobrecargar del ancho de banda que pueden ocurrir en las capas 3, 4, ¿o 7?
    b. Asimétrico: diseñado para solicitar límites de tiempo o cambios en el estado de la sesión
    c. Computacional: diseñado para atacar el CPU y memoria
    d. Por Vulnerabilidad: diseñado para atacar la vulnerabilidad en el software
7. Las opciones a reducir se evaluarán por dirección de origen. Si la lista de direcciones IP del agresor es pequeña, el firewall bloqueará todo. El bloqueo puede ser de las siguientes maneras:
    a. Geobloqueo: Es posible bloquear a los atacantes si todos están en la misma región geográfica o dentro de unas pocas regiones que utilizan rangos completos de IP.
    b. Spot blocking: Si el ataque proviene de una IP específica, esa dirección IP se bloqueará manteniendo una actividad de monitoreo de la misma.
8. Se reducirán los ataques contra aplicaciones específicas. Si se alcanza este paso, el ataque DDoS es lo suficientemente sofisticado como para que la mitigación por dirección de origen sea ineficaz. Se debe revisar si el ataque es contra el software de gestión de servicios (IIS, Apache, MTA...) y aplicar la solución dada por el proveedor.

9. Increase the security posture at the application level. If this step has been reached in an attack DDoS, has already been mitigated to the layer level 3 and 4, and mitigations have been evaluated for application-specific attacks, and problems continue to be experienced. This means that the attack is relatively sophisticated, and the ability to mitigate it will depend in part on the applications, the following should be taken into consideration:
10. Incrementar la postura de seguridad a nivel de aplicación. Si se ha alcanzado este paso en un ataque DDoS, ya se ha atenuado a los niveles de capa 3 y 4, y se ha evaluado la disminución para los ataques específicos de la aplicación, pero se siguen experimentando problemas. Esto significa que el ataque es relativamente sofisticado, y la capacidad de controlarlo dependerá en parte de las aplicaciones, para ello se debe tener en cuenta lo siguiente:
    a. Ataque asimétrico a aplicaciones: Es muy probable que se enfrente a uno de los ataques modernos más difíciles. Este tipo de ataque puede ser:
        i. Una ráfaga de GETs recursivos de la aplicación completa.
        ii. Una solicitud repetida de un objeto público de gran tamaño (como los certificados PDF).
        iii. Una petición repetida de una solicitud de base de datos.
    b. Los registros de la aplicación deben ser rastreados buscando signos de incrementos anormales en el tamaño y luego allí localizar el recurso atacado para poder implementar las medidas necesarias para minimizar o eliminar el problema.
11. Limitar los recursos. Si todos los pasos anteriores no consiguen detener el ataque DDoS, FULL CERTIFICATE se verá obligado a limitar simplemente los recursos para resistir al ataque. Esta técnica rechazará tanto el tráfico bueno como el malo, manteniendo de alguna manera la continuidad del servicio hasta encontrar la solución descrita en los pasos anteriores.
12. Gestionar las Relaciones Públicas. Los grupos de hackers actuales utilizan los medios de comunicación para llamar la atención sobre sus causas. Muchos hackers informan a los medios de comunicación cuando se produce un ataque y también pueden ponerse en contacto con la Empresa durante el ataque. Para ello FULL CERTIFICATE debe responder a los usuarios y medios de comunicación interesados en el problema de la siguiente manera:
    a. Para los usuarios del sistema. "Actualmente estamos experimentando algunas dificultades técnicas, pero somos optimistas de que nuestros clientes pronto podrán tener acceso a nuestros servicios en línea".
    b. Para la prensa. Debemos ser francos y admitir cuando ha sido atacado desde el exterior. Se debe asegurarse de que se están realizando las actividades y procesos necesarios para mitigar el problema.

    Para el personal interno, incluida cualquier persona con la que pueda ponerse en contacto la prensa. El comunicado interno indicara al personal que se dirijan todas las preguntas relacionadas con el evento al área de relaciones públicas, indicando el número de teléfono de contacto.

Caída de uno de los servidores de IDC

Los usuarios serán redirigidos lo más rápidamente posible a un nuevo servidor clon del antiguo. FULL CERTIFICATE funcionará según el SLA que es del 99,95%.

Servicios de IDC al proveedor:

Se solicitará la restitución del servicio de forma inmediata mediante correo electrónico y llamada con el área de soporte del proveedor de acuerdo con el SLA contratado.

Caída del certificado o sello de tiempo del proveedor:

Se solicitará la restitución del servicio de forma inmediata mediante correo electrónico y llamada con el área de soporte del proveedor de acuerdo con el SLA contratado.

b) IMPACTO MEDIO:

i. Se resolverá mediante el acceso inmediato a través de la revisión informática del incidente y los registros proporcionados. Habrá: 1) soporte de mesa electoral y en casos más graves 2) Asistencia telefónico a los usuarios por parte de FULL CERTIFICATE

ii. La asistencia al usuario se proporcionará a través de chats, conferencias telefónicas, tickets de asistencia, llamadas u otros canales de contacto.

Falla en MTA (Mail Transport Agent)

El servicio FULL CERTIFICATE dispone de 2 o más servidores de gestión MTA, el sistema detecta en tiempo real si deja de funcionar trasladándolo al estado de inactividad y generando alertas al equipo informático para que proceda a su sustitución lo antes posible.

En caso de fallo y recepción de alerta de caída de uno de los canales de salida, se comprobará el servidor.

- En el caso de que la caída se produzca por saturación de memoria o fallo puntual de algún proceso, bastará con reiniciar el sistema operativo.
- Si lo anterior no resuelve la incidencia, se formateará el sistema operativo y se reinstalará para la posterior instalación del MTA con las configuraciones necesarias. Una vez validado el funcionamiento se probará en un entorno de preproducción y si todo es correcto, volverá a formar parte del grupo principal de envío.
- En caso de que la reparación no sea factible, la información contenida en los soportes de almacenamiento deberá ser destruida y después reciclada en los puntos indicados por la autoridad competente.

c) BAJO IMPACTO:

i. Por ejemplo: el servicio ha tenido lugar, pero no ha sido certificado, la certificación se llevará a cabo con carácter de urgencia en las siguientes horas.

Actualizaciones del sistema

El Sistema debe ser reiniciado después de las actualizaciones del Sistema Operativo, esto resulta en un corte de servicio de aproximadamente 10 minutos. Se procurará que sean en momentos de poco uso de los servicios de FULL CERTIFICATE.

Atención oportuna de incidentes de usuarios.

Un sistema de tickets de soporte está disponible para los usuarios. Estos son atendidos por personal de FULL CERTIFICATE en un tiempo aproximado de 48-72 horas hábiles.

Fin de la validez del certificado SSL

La actualización de los certificados SSL se realizará a partir de 1 semana y hasta 1 día antes de su fecha de finalización de validez.

Sistema de copias de seguridad -Backup

En caso de que alguno de los elementos que reciben las copias de seguridad se quede sin espacio disponible en el disco, las copias más antiguas se extraerán a discos adicionales y luego se borrarán del Sistema Principal, liberando así espacio disponible en el disco para las nuevas copias.

Se planifica una revisión mensual del estado de las copias de seguridad y la realización de pruebas de restauración con respecto a la última copia disponible en entornos de prueba.

6.5 CONTROL DE PERSONAL - STAFF

FULL CERTIFICATE se asegura de que sus empleados lleven a cabo procedimientos administrativos y de gestión acordes con los procesos de seguridad de la información, garantizando así la fiabilidad y la seguridad de sus operaciones.

FULL CERTIFICATE contrata al personal y, en su caso, contrata a subcontratistas que cuentan con la experiencia, fiabilidad y cualificación necesarias y que han recibido formación en materia de seguridad y protección de datos personales.

FULL CERTIFICATE aplica las sanciones disciplinarias adecuadas a los empleados que infrinjan las políticas o el procedimiento de la empresa.

Las funciones y responsabilidades en materia de seguridad de la información están documentadas en las descripciones de los puestos de trabajo del personal.

Los gestores tienen la experiencia y los conocimientos necesarios en relación con el servicio QERDS, y están familiarizados con los procedimientos de seguridad y evaluación de riesgos suficientes para desempeñar sus funciones de gestión.

Todo el personal del proveedor no tiene ningún conflicto de intereses que pueda perjudicar la imparcialidad de la actividad de FULL CERTIFICATE.

El control organizacional implementado por FULL CERTIFICATE se describe en la sección "RECURSOS HUMANOS".

6.6 PROCEDIMIENTOS DE AUDITORIA

PERFIL DEL AUDITOR

El auditor externo o el equipo de auditores externos se seleccionará en el momento de planificar cada auditoría.

Cualquier empresa o persona contratada para realizar una auditoría de seguridad sobre FULL CERTIFICATE o cualquiera de sus servicios deberá cumplir con los siguientes requisitos:

- Formación y experiencia adecuadas y acreditadas en procesos de auditoría de seguridad y sistemas de información.
- Independencia a nivel organizativo de la autoridad de FULL CERTIFICATE, en el caso de las auditorías externas.

El auditor externo o el equipo de auditores externos tampoco debe tener ninguna relación, actual o prevista, financiera, legal o de cualquier otro tipo que pueda dar lugar a un conflicto de intereses con FULL CERTIFICATE. Para cumplir con la normativa vigente en materia de tratamiento de datos, y si el proceso de auditoría implica el acceso a datos personales, el auditor tendrá la consideración de Encargado del Tratamiento, en los términos de lo dispuesto en el artículo 28 del RGPD.

CRITERIOS DE AUDITORÍA

Sin perjuicio de ser ampliado por documentos de los servicios particulares ofrecidos por FULL CERTIFICATE, en este apartado se definirán todas las comprobaciones mínimas de la adecuación de los servicios ofrecidos. Los aspectos cubiertos por una auditoría incluirán, pero no se limitarán a:

- Política de seguridad
- Seguridad física de las instalaciones del servicio auditado.
- Seguridad lógica de los sistemas y servicios de FULL CERTIFICATE
- Evaluación tecnológica de los componentes del servicio
- Administración de los servicios, así como la seguridad en los mismos
- Este documento y las políticas de servicio vigentes
- Cumplimiento de los requisitos legales aplicables.

FRECUENCIA

Las auditorías de cumplimiento y conformidad se revisan al menos semestralmente, salvo que se produzcan cambios relevantes o esenciales en los sistemas y servicios de FULL CERTIFICATE, en cuyo caso se realizarán auditorías extraordinarias.

PLAN DE ACCIÓN

La identificación de deficiencias en la auditoría dará lugar, como medida inmediata, a la adopción de medidas correctoras. Las autoridades competentes en la materia definidas por la legislación vigente en colaboración con el auditor serán las encargadas de determinarlas.

COMUNICACIÓN DE RESULTADOS

El auditor externo o los auditores externos comunicarán los resultados de la auditoría a FULL CERTIFICATE, así como a los responsables de las distintas áreas en las que se detecten no conformidades, así como, en su caso, a la autoridad competente según determine la legislación vigente.

6.7 ARCHIVO

La información sobre acontecimientos importantes se archiva periódicamente en formato electrónico.

FULL CERTIFICATE archiva todos los datos y archivos relacionados con: la información de registro; la seguridad del sistema; todas las solicitudes presentadas por los clientes; toda la información de los clientes; todas las claves utilizadas por las Autoridades de Certificación y la Autoridad de Registro; y toda la correspondencia entre FULL CERTIFICATE y sus clientes. Se archivan todos los documentos y datos utilizados en el proceso de verificación de la identidad.

La información prevista en el artículo 24 (2) (h) del Reglamento (EU) No. 910/2014 (toda la información relevante en relación con los datos emitidos y recibidos por FULL CERTIFICATE, en particular a efectos de aportar pruebas en procedimientos judiciales y de asegurar la continuidad en la prestación del servicio) se almacena durante un período de 15 años, incluso después del cese de la actividad de FULL CERTIFICATE.

El almacenamiento de datos a largo plazo se realiza en un lugar seguro y protegido. Las condiciones específicas se ajustan a las normas, recomendaciones y reglamentos aplicables especificados en el ámbito de la seguridad de la información.

Los datos se recopilan de manera coherente con el tipo de documento.

El acceso a los datos almacenados a largo plazo sólo se permite a las personas autorizadas.

6.8 ALMACENAMIENTO DE SOPORTE DE DATOS

Se realizan copias de seguridad de los archivos que contienen los registros sujetos a resguardo, los cuales se almacenan en la nube.

La política actual de copias de seguridad para este entorno es:

- Servidores de aplicaciones: Completo semanalmente e incremental diario
- Servidor de bases de datos: Diario completo.
    - Archivo: Completo cada 8 semanas con incremento diario.

Estas copias de seguridad se realizan en todos los componentes del servicio.

6.9 ELIMINACIÓN (DEPURACION)

Se han establecido procedimientos para la destrucción segura de los medios / dispositivos para minimizar el riesgo de filtración de información confidencial a personas no autorizadas.

Los procedimientos para la destrucción segura de los medios que contienen información confidencial son coherentes con la sensibilidad de dicha información.

Los medios / dispositivos que contienen información confidencial se almacenan de forma segura y se destruyen quemando, cotando o borrando los datos cuando son utilizados en otra aplicación. La destrucción de objetos sensibles se anota en un registro para mantener un historial de auditoría.

En el caso de los dispositivos dañados que contienen datos confidenciales, se evalúa el riesgo de si los objetos deben ser destruidos físicamente o enviados para su reparación.

Los soportes de papel que contengan información de seguridad significativa de FULL CERTIFICATE serán destruidos, después de la expiración del período de almacenamiento especificado en el reglamento, en dispositivos especiales de corte.

En algunos casos, la información de los soportes portátiles se destruye al borrar o formatear el dispositivo sin posibilidad de recuperación.

6.10 GESTION / MANEJO / ADMINISTRACIÓN DE ACTIVOS

FULL CERTIFICATE garantiza un nivel adecuado de protección de sus activos, incluidos los activos de información. El proveedor mantiene una lista de todos los activos de información y realiza una evaluación de riesgos.

FULL CERTIFICATE identifica los recursos correspondientes de acuerdo al periodo de vida útil de la información y los documenta según su nivel de importancia. El ciclo de vida de la información incluye la creación, el procesamiento, el almacenamiento, el intercambio/transmisión, la eliminación y la destrucción. La documentación se guarda en inventarios especiales. El control de activos es preciso, actualizado y consistente.

La información se clasifica en función de los requisitos normativos, su valor, criticidad y susceptibilidad a la divulgación o modificación no autorizada.

Los procedimientos de gestión de activos se han desarrollado de acuerdo con el esquema de clasificación de la información adoptado por FULL CERTIFICATE.

6.11 REGISTROS

- Eventos relacionados con la verificación inicial de la identidad del remitente y/o la autenticación adicional
- Eventos relacionados con la verificación inicial de la identidad del destinatario y/o la autenticación posterior
- Los registros contienen una descripción de los documentos presentados por la persona que desea ser identificada (por ejemplo, documento de identidad, poder notarial, etc.), así como datos relativos a los datos de identificación únicos, números o una combinación de los mismos o copias de solicitudes y documentos de identidad, incluyendo un contrato firmado, un acuerdo con la Política y la Práctica de FULL CERTIFICATE, y el suministro de datos personales.
- Eventos relacionados con el envío y la recepción de contenidos del usuario
- Eventos de seguridad, incluidos los cambios de política de seguridad, el arranque y apagado del sistema, fallas del sistema y del hardware como del firewall

- Los registros relacionados con el funcionamiento del servicio QERDS se archivan de forma confiable y confidencial de acuerdo con las prácticas comerciales de la empresa
- Se especifica la hora exacta de los eventos importantes de gestión de claves y la sincronización del reloj. La hora del sistema se sincroniza con GMT al menos una vez cada 24 horas
- Los eventos relacionados con las pruebas del servicio QERDS se registran de forma que no puedan borrarse o destruirse fácilmente
- Se registran los eventos que tienen un impacto significativo en la seguridad y confiabilidad del sistema tecnológico, el control del personal y de los clientes y el impacto en la seguridad de los QERDS proporcionados.
- Los documentos recogidos en relación con la prestación del servicio se facilitan como prueba, por ejemplo, a efectos de procedimientos judiciales.
- FULL CERTIFICATE garantiza la privacidad, la integridad y la disponibilidad de los registros de actividad registrados.
- La información logbook electrónico se genera automáticamente
- Los registros de los eventos realizados se guardan en archivos durante al menos 6 (seis) meses. Durante este periodo de tiempo están disponibles en línea o pueden ser consultados por un empleado autorizado de FULL CERTIFICATE. Después de este periodo, los registros se archivan para liberar espacio en el disco.
- Los registros archivados se conservan durante un periodo de 5 (cinco) años.
- Un archivo se firma con una firma electrónica avanzada y un sello de timbrado electrónico cualificado. La información de registro se controla periódicamente en soportes físicos almacenados en un servidor especial, localizado en un lugar con un alto nivel de protección física y control de acceso.

El ERDSP garantizará la confidencialidad, integridad y disponibilidad de los registros definidos en el presente documento.

FULL CERTIFICATE declaran que los registros relativos al funcionamiento de los servicios se pondrán a disposición en caso de que se requieran para aportar evidencias del correcto funcionamiento de los servicios a efectos de procedimientos judiciales.

6.12 CAMBIO DE CLAVES

FULL CERTIFICATE podrá cambiar de proveedor de firma electrónica cualificado en caso de:

- Expiración de la validez del certificado
- Cambios en los atributos de privacidad de las claves de seguridad y requisitos de nuevas combinaciones criptográficas y algoritmos aplicables
- En caso de sospecha de falta de compromiso
- Por cambio de proveedor de firma electrónica

FULL CERTIFICATE podrá cambiar de proveedor de Sellado de Tiempo (TSA) en el caso de:

- Expiración del contrato con el proveedor de servicios y no renovación del mismo.
- Cambios en los atributos de privacidad de las claves de seguridad y requisitos de nuevas combinaciones criptográficas y algoritmos aplicables
  En caso de sospecha de compromiso de los códigos de acceso al servicio.

6.13 COMPROMISOS Y SOLUCIONES EN CONTINGENCIAS

Los procedimientos seguidos por FULL CERTIFICATE para la intervención y reconstrucción en caso de contingencias se describen en el apartado "GESTIÓN DE INCIDENTES".

6.14 PLAN DE CONTINUIDAD DE LA ACTIVDIAD

La Continuidad de actividades es la capacidad táctica y estratégica que tiene FULL CERTIFICATE para planificar y responder a los incidentes e interrupciones de los servicios con el fin de continuar con las operaciones críticas dentro de un nivel de servicio aceptable y asumible por FULL CERTIFICATE.

FULL CERTIFICATE definirá y mantendrá un plan de continuidad que se utilizará en caso de contingencias.

FULL CERTIFICATE contempla que ante cualquier incidente / accidentes / desastres se tiene prioridad de salvaguardar y garantizar protección a su equipo. Dentro del presente documento no se contempla a detalle esta situación ya que sólo se está orientado desde el punto de vista tecnológico. No se considerará ninguna actividad hasta que se garantice la seguridad y el bienestar de las personas.

El personal que compone el equipo de recuperación estará familiarizado con las responsabilidades y el contenido de este documento.

En caso de situación de catástrofe, FULL CERTIFICATE se pondrá en contacto con el proveedor del suministro de material. Si no se puede asegurar el tiempo de reposición, puede ser necesaria la compra de material y su almacenamiento en un lugar alternativo a las instalaciones principales.

Una vez establecido el Procedimiento de Recuperación, su mantenimiento es obligatorio.

FULL CERTIFICATE ha previsto un plan financiero que le permite disponer de estabilidad financiera y recursos suficientes para responder a situaciones de contingencia.

En caso de contingencia, incluido el compromiso de una clave de firma privada o el compromiso de alguna otra credencial del PST, las operaciones se restablecerán en el plazo establecido en el plan de continuidad, habiendo abordado cualquier causa de la contingencia que pueda repetirse (por ejemplo, una vulnerabilidad de seguridad) con las medidas correctoras adecuadas.

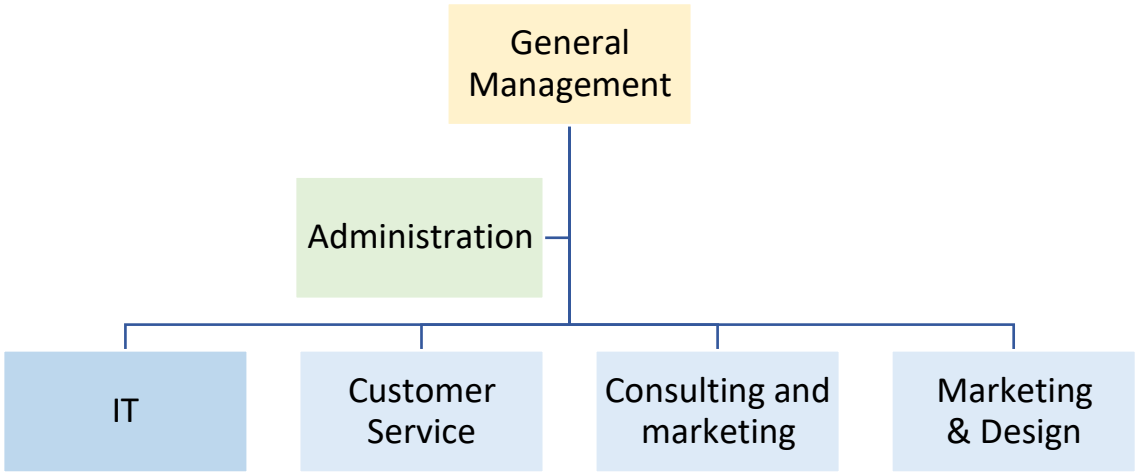
Relacionado con el último párrafo, subrayamos que en el caso de que el centro de datos falle por completo, FULL CERTIFICATE volverá a prestar sus servicios y restablecerá la situación inicial en un plazo de 2 - 4 semanas (en caso excepcional).

Otras situaciones de contingencia incluyen el fallo de componentes críticos del sistema TSP, incluyendo el hardware y el software. Ver documento relacionado.

7. GESTION Y FUNCIONAMIENTO DE ERDSP

7.1 ORGANIZACIÓN INTERNA

FULL CERTIFICATE tiene la siguiente organización estructural:



7.2 CONFIABILIDAD DE LA ORGANIZACIÓN

FULL CERTIFICATE se compromete a mantener una organización confiable.

A continuación, se detallan los requisitos organizativos de FULL CERTIFICATE:

- Proveer y gestionar la infraestructura de servicio asociadas a la firma digital
- Prestar el servicio de resguardo de certificados y firmas electrónicas y sellos electrónicos de forma imparcial y objetiva
- Garantizar la adecuación de sus procesos y servicios a las normas a las que se ciñen
- Informar al solicitante del servicio de las características de la prestación, las obligaciones asumidas y los límites de responsabilidad
- Proteger de forma confiable todos los datos de usuarios, así como los registros de actividad y auditoría con los medios que considere más adecuados y durante el periodo de tiempo contemplado según la naturaleza de los datos registrados.
- Garantizar la prestación del servicio de conservación de certificados y firmas electrónicas de forma diligente e ininterrumpida
- Comunicar a los usuarios con suficiente antelación la no disponibilidad del sistema en caso de realizar procesos de modificación, mejora o mantenimiento que impliquen una corte parcial del servicio.
- Notificar a las partes implicadas lo antes posible cuando se detecte alguna incidencia en el sistema con afectación para ellas
- Garantizar que los sistemas de firma digital funcionen en sincronía con fuentes de timbrado fiables, utilizando una Autoridad Europea de Certificación y Sellado de Tiempo Cualificada
- Disponer de un canal de comunicación con los usuarios y terceros para peticiones, consultas, quejas y reclamaciones.
- Responder a las peticiones, consultas, quejas y reclamaciones de los Usuarios y de terceros en un plazo razonable.

En particular:

- Los servicios de confianza FULL CERTIFICATE no son discriminatorios
  - FULL CERTIFICATE pone sus servicios a disposición de todos los solicitantes cuyas actividades entren en su ámbito de actuación y que se comprometan a cumplir con las obligaciones especificadas en sus condiciones
  - FULL CERTIFICATE mantendrá recursos financieros suficientes y/u obtendrá un seguro de responsabilidad civil adecuado, de acuerdo con la legislación aplicable, para cubrir las responsabilidades derivadas de sus operaciones y/o actividades.

En consecuencia, como se ha mencionado en los párrafos anteriores, en lo que respecta a la responsabilidad del TSP, se hace referencia al artículo 13 del Reglamento (EU) No 910/2014.

- FULL CERTIFICATE tendrá la estabilidad financiera y los recursos necesarios para operar de acuerdo con esta política
- El TSP dispondrá de políticas y procedimientos para la resolución de reclamaciones y disputas recibidas de clientes u otras partes usuarias sobre la prestación de servicios o cualquier otro asunto relacionado
- FULL CERTIFICATE tendrá un acuerdo documentado y una relación contractual cuando la prestación de servicios implique subcontratación, externalización u otros acuerdos con terceros.
- Cuando FULL CERTIFICATE recurra a otras partes, incluidos los proveedores de componentes de servicios de confianza, para proporcionar parte de su servicio a través de la subcontratación, la externalización u otros acuerdos con terceros, conservará la responsabilidad general del cumplimiento de los requisitos definidos en la política de servicios de confianza.
  - Cuando el FULL CERTIFICATE haga uso de un componente de servicio de confianza proporcionado por un tercero, se asegurará de que el uso de la interfaz del componente cumple los requisitos especificados por el proveedor del componente de servicio de confianza. Y, además, en estos casos, FULL CERTIFICATE se asegurará de que la seguridad y la funcionalidad requeridas por el componente de servicio de confianza cumplen los requisitos adecuados de la política y las prácticas aplicables.

7.3 DESIGNACIÓN DE FUNCIONES

FULL CERTIFICATE se compromete, en la medida de lo posible, a mantener separadas las funciones y áreas de responsabilidad en conflicto con el fin de reducir las oportunidades de modificación o uso indebido no autorizado o involuntario de los recursos de sus servicios.

7.4 RECURSOS HUMANOS

7.4.1 NORMAS COMUNES

FULL CERTIFICATE se asegurará de que los empleados y contratistas respalden la confiabilidad de sus operaciones.

En particular:

- FULL CERTIFICATE empleará personal y, en su caso, subcontratistas, que posean los conocimientos técnicos, la fiabilidad, la experiencia, la cualificación necesaria y que hayan recibido formación en estándares de seguridad y protección de datos personales, según corresponda a los servicios ofrecidos y a la función del puesto que ocupen
- El personal del TSP debe cumplir el requisito de "conocimientos especializados, experiencia y cualificación" mediante formación y credenciales formales, o experiencia real, o una combinación de ambas.

  • Todo lo mencionado en los dos puntos anteriores debe caracterizarse por actualizaciones periódicas cada 12 meses, en relación con las nuevas amenazas y las prácticas de seguridad vigentes.

  • Se aplicarán sanciones disciplinarias apropiadas al personal que infrinja las políticas o procedimientos de TSP.

  • Las funciones y responsabilidades en materia de seguridad, tal y como se especifica en la política de seguridad de la información del TSP, deberán estar documentadas en las descripciones de los puestos de trabajo o en documentos disponibles para todo el personal involucrado

  • Los roles de confianza, de los que depende la seguridad del funcionamiento del TSP, deben estar claramente identificados.

  • El personal de TSP (tanto temporal como permanente) tendrá definidas las descripciones de los puestos de trabajo desde el punto de vista de las actividades realizadas con la segregación de funciones y los privilegios mínimos, determinando la sensibilidad del puesto según las actividades y los niveles de acceso, la investigación de los antecedentes y la formación y concienciación de los empleados.

  • En su caso, las descripciones de los puestos de trabajo deberán diferenciar entre funciones generales y funciones específicas con respecto al TSP. Y, deben incluir los requisitos de competencias y experiencia.

  • El personal ejercerá procedimientos, procesos administrativos y de gestión que estén en línea con los procedimientos de gestión de la seguridad de la información de FULL CERTIFICATE.

  • Los Gerentes tienen experiencia o formación en relación con los servicios de confianza prestados, están familiarizados con los procedimientos de seguridad para el personal con responsabilidades, y tienen suficiente experiencia en seguridad de la información y evaluación de riesgos para desempeñar las funciones de administración

  • Todo el personal de FULL CERTIFICATE que desempeño funciones de confianza está libre de conflictos de intereses que puedan perjudicar la imparcialidad de las operaciones del TSP

  • Los roles de confianza incluirán puestos que impliquen las siguientes responsabilidades:

  • Responsables de seguridad: responsabilidad general de administrar de la aplicación de las prácticas de seguridad

  • Administradores del sistema: Autorizados a instalar, configurar y mantener los sistemas confiables del TSP para la administración de los servicios (incluyendo, el Sistema de Recuperación).

  • Operadores de sistemas: Responsables de operar los sistemas de confianza del TSP en el día a día. Autorizados a realizar copias de seguridad del sistema
- Auditores de sistemas: Autorizados a ver los archivos y registros de auditoría de los sistemas de confianza del TSP.

Hacemos referencia al documento Plan de Continuidad de Negocio en el que se describe el Puesto de Trabajo, las funciones y responsabilidades de Seguridad.

Asimismo, el manejo de la información que se genere de la gestión de riesgos se refleja en lo descrito en el BCP. La política de seguridad de la información es aprobada por el equipo directivo del TPS y se transmite a todos los empleados.

Además, FULL CERTIFICATE designará al responsable del Servicio de Atención al Cliente como funcionario de verificación de identidad. Dicho responsable se encargará de que los procesos realizados para verificar la identidad del remitente y del destinatario cumplan con el proceso de verificación de identidad inicial especificado.

POLÍTICA DE FORMACIÓN DEL PERSONAL:

Por otra parte, FULL CERTIFICATE en relación con la formación / capacitación de su personal indica que es responsable de la implantación, revisión anual y aplicación concreta de su política de seguridad y concienciación sobre amenazas.

La política de formación de FULL CERTIFICATE se caracteriza por lo siguiente:

- Todos los empleados reciben formación y conocen perfectamente las características de los servicios ofrecidos por FULL CERTIFICATE, sus normas de seguridad y las normas de protección de datos personales que se aplican, en cuanto han recibido formación en relación con ellos y tienen contacto práctico diario con los servicios
- Si hay actualizaciones en los servicios y/o en el desarrollo de nuevos productos etc….: todos los empleados se reúnen para darles información, explicaciones sobre el funcionamiento del nuevo producto y/o servicio
- Cada 12 meses los procedimientos se actualizarán y todos los empleados recibirán capacitación, por parte de la Dirección y el Departamento TI, sobre los riesgos electrónicos, las amenazas a la red y las prácticas de seguridad,
- Cada 24 meses, el responsable de FULL CERTIFICATE realizará un curso de capacitación, impartido por una empresa especializada en ofrecer este tipo de cursos, que tiene como objetivo la seguridad electrónica del mercado y de los servicios que ofrece FULL CERTIFICATE. Y la conclusión se transmitirá al equipo de servicio involucrado.

Descripciones de puestos de trabajo y sus funciones relacionadas:

Puesto de Trabajo	Profesión	Externo	Funciones
Dirección General	MBA & Ingeniero	No	Gestión estratégica, desarrollo de proyectos informáticos y de mercado
Gerente IT	Ingeniero de Sistemas	No	Gestión y desarrollo de aplicaciones, dimensionamiento de infraestructuras informáticas, seguridad informática, gestión de equipos de programación.
Dirección de Administración	MBA, Licenciatura en Administración de Empresas	No	Gestión de los recursos económicos, financieros y humanos y relación con las administraciones
Área legal	Abogado	Yes	Asesoramiento y apoyo a la formación jurídica especializada en nuevas tecnologías.

Customer Manager	Master, Administrador de Negocios	No	Gestión de clientes y proyectos. Revisión y control de los servicios a nivel de prueba de calidad de los servicios.
Servicios de atención al cliente	Licenciatura / Titulado	No	
Diseñadores gráficos de páginas web	Diseño gráfico/artes plásticas	No	Desarrollo de la imagen visual de la empresa y del sitio web. Realización de logotipos, folletos y piezas de comunicación.
Programadores .NET & C#	Ingeniero en Sistemas o similar	No	Desarrollo de aplicaciones y código fuente.
Programadores externos	Ingeniero en Sistemas o similar	Yes	Subcontratación para desarrollo de aplicaciones y código fuente adecuados.

7.5 GESTIÓN DE ACTIVOS

7.5.1 REQUISITOS GENERALES

FULL CERTIFICATE garantiza un nivel adecuado de protección de sus activos, incluidos los de información.

Además, FULL CERTIFICATE mantendrá un inventario de todos los activos de información y determinará una clasificación consistente con la evaluación de riesgos. Los activos de información y su inventario se describen en el documento Plan de Continuidad de Negocio de FULL CERTIFICATE. El TSP revisará la norma establecida semestralmente-

Los procedimientos de control de cambios se aplicarán a las versiones, modificaciones y correcciones de emergencia de cualquier software operativo y a los cambios de configuración que se apliquen. Y los procedimientos, si se llevan a cabo, incluirán la documentación de los cambios respectivamente.

7.5.2 GESTION DE MEDIOS

FULL CERTIFICATE, en caso de que sea necesario, se compromete a que todos los dispositivos (servidores) en donde se encuentre almacenen la información sean tratados de forma segura de acuerdo con los requisitos del sistema de clasificación de la información. Los controles de información que contengan datos sensibles se eliminarán de forma segura cuando ya no sean necesarios.

Además, los procedimientos de gestión de los dispositivos sirven para protegerlos contra la obsolescencia y el deterioro de los mismos, dentro del periodo de tiempo necesario para la conservación de los registros.

7.6 CONTROL DE ACCESO

El acceso al sistema FULL CERTIFICATE estará limitado a las personas autorizadas.

En particular:

- El TSP gestionará el acceso de los administradores de usuarios y de los auditores del sistema aplicando el principio de "privilegios mínimos" al configurar los privilegios de acceso.
- La administración de FULL CERTIFICATE prevé la gestión de las cuentas de usuarios, así como la modificación o la eliminación del acceso en determinados casos
- El acceso a la información y a las funciones del sistema de aplicación se restringirá de acuerdo con la política de control de acceso.
- El sistema de FULL CERTIFICATE proporcionará suficientes controles de seguridad informática para la separación de las funciones de confianza identificadas en sus prácticas, incluyendo, en este sentido, la separación de las funciones de administración y operación de la seguridad.
- El personal de FULL CERTIFICATE se identificará y autenticará antes de utilizar las aplicaciones críticas relacionadas con el servicio (por ejemplo, conservar los registros de eventos, etc.)
- Los datos confidenciales deberán estar protegidos para que no se divulguen a través de objetos de almacenamiento reutilizados (por ejemplo, archivos eliminados) o medios a los que puedan accesar usuarios no autorizados.

En virtud de lo anterior, se indica que el acceso del personal, tanto interno como externo, a los sistemas de información de FULL CERTIFICATE, así como a la información que procesan y almacenan, se regula en función de las necesidades informativas y operativas de cada usuario, concediendo el acceso exclusivamente a aquellas funciones e información que sean necesarias para el correcto desempeño de su actividad laboral, de acuerdo con su función y/o perfil operativo. Los responsables de los activos de información serán los responsables de definir los niveles de acceso a los recursos y de autorizar cualquier acceso extraordinario, todo ello de conformidad con las directrices de los propietarios de la información o, en su caso, de los propietarios del proceso o negocio.

Sin perjuicio de especificar mayor detalle en su aplicación, ni de la delegación formal de funciones, se entienden como propietarios del proceso o negocio los responsables en los siguientes cargos:

- Dirección General
- Gerente de IT
- Director de Administración

Todos los accesos que los usuarios realicen a los sistemas de información de FULL CERTIFICATE estarán asociados a un proceso de identificación, autenticación y autorización, estableciendo los controles adecuados para que dichos procesos se realicen de forma segura.

Para ello, se han diseñado e implantado mecanismos de registro, monitorización de acceso y uso de los sistemas, que permiten conocer la efectividad de las medidas instaladas y detectar posibles incidencias de seguridad.

7.7 CONTROLES CRIPTOGRÁFICOS

Para garantizar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información, FULL CERTIFICATE establecerá controles de seguridad adecuados para la gestión de cualquier clave criptográfica y de cualquier dispositivo criptográfico a lo largo de su operatividad.

Además, FULL CERTIFICATE garantiza que las claves de firma se mantendrán físicamente aisladas de las operaciones normales de forma que sólo el personal de confianza designado tenga acceso a las claves para su uso en la firma de contenidos y/o pruebas del usuario.

Adicionalmente FULL CERTIFICATE en relación con sus servicios prestados, declara que los mismos tienen con las siguientes características:

- La clave de firma privada del ERDS se mantiene y se utiliza dentro de un dispositivo criptográfico seguro y que la misma clave está protegida de forma que se garantice el mismo nivel de protección proporcionado por el dispositivo criptográfico seguro
- La clave privada de la firma del ERDS es respaldada, almacenada y recuperada únicamente por el personal que desempeña funciones de confianza y que utiliza al menos un doble control en un entorno físicamente seguro. El número de personal autorizado para realizar esta función se mantendrá al mínimo y será coherente con las prácticas del ERDS.
- La clave privada de la firma ERDS almacenada en el dispositivo criptográfico seguro ERDSP se destruirá cuando se retire el dispositivo.
- Las copias de la clave privada de la firma ERDS estarán sujetas al mismo o mayor nivel de controles de seguridad que las claves actualmente en uso.
- El dispositivo criptográfico seguro, que funciona correctamente, no se manipula durante el envío y el almacenamiento.

7.8 SEGURIDAD FÍSICA Y AMBIENTAL

FULL CERTIFICATE controla el acceso físico a los componentes de su sistema, cuya seguridad es esencial para la prestación de sus servicios de confianza y minimiza los riesgos relacionados con su seguridad física.

En particular:

- El acceso físico a los componentes del sistema del TSP, cuya seguridad es esencial para la prestación de sus servicios de confianza, estará limitado a las personas autorizadas
- Se aplicarán controles para evitar:
  - La pérdida, el daño o la puesta en peligro de los recursos y la interrupción de las actividades operativas.
  - La confidencialidad de la información y el correcto uso de las instalaciones de procesamiento de información.
- Los componentes/dispositivos (Servidores) que son críticos para el funcionamiento seguro del servicio de confianza estarán ubicados en un

perímetro de seguridad protegido con protección física contra la intrusión. Y habrá controles de acceso en todo el perímetro de seguridad y alarmas para detectar intrusiones.

En relación con lo anterior, destacamos que:

FULL CERTIFICATE garantiza el cumplimiento de la normativa aplicable y de las principales normas y buenas prácticas en materia de seguridad física, tal y como se describe en este apartado.

En las instalaciones de FULL CERTIFICATE se han establecido diferentes perímetros de seguridad con barreras de protección y controles de entrada adecuados a las actividades que se desarrollan en cada uno de ellos. Todo ello con el fin de reducir el riesgo de acceso no autorizado o de daños a los recursos informáticos.

FULL CERTIFICATE a ubicado sus sistemas de información en áreas de acceso restringido que han sido debidamente protegidos mediante mecanismos apropiados de control de acceso físico. Asimismo, estos sistemas han sido protegidos contra otro tipo de amenazas ambientales como incendios, inundaciones o cortes de energía.

Esta protección se extiende a aquellos sistemas cuya seguridad física se delega en un proveedor. Para ello, se han suscrito las cláusulas oportunas en los contratos y se establecen los mecanismos de seguimiento necesarios por parte de FULL CERTIFICATE. El tratamiento de la información fuera de los sistemas de FULL CERTIFICATE está debidamente autorizado, una vez garantizado el cumplimiento del nivel de confidencialidad y seguridad requerido.

FULL CERTIFICATE también ha implementado una política de gestión de activos basada en el control y la clasificación, el almacenamiento y los registros de entrada y salida. En el aspecto técnico, se adoptan procedimientos que garantizan la adecuada seguridad de la información contenida en ellos, así como que permiten la reutilización de los mismos sin presentar riesgos para la información.

Algunas de las medidas adoptadas por FULL CERTIFICATE son las siguientes:

- Autenticación y control de acceso. Control de acceso al edificio 7x24 por personal de seguridad privada
- Control de acceso a los centros de datos basado en la identificación biométrica por huella dactilar y autorización centralizada con registro de acceso, tanto de entrada como de salida.
    - Las condiciones de temperatura están garantizadas por equipos de refrigeración autónomos ubicados dentro del DataCenter que mantienen la temperatura del mismo dentro de los márgenes establecidos.
    - Circuito cerrado de televisión con grabación digital permanente y detección de actividad en las cámaras distribuidas por todo el edificio.
    - Fuente de alimentación redundante, que proporciona dos líneas de alimentación a los racks destinados a albergar los equipos.
    - El cableado utilizado en el DataCenter es de categoría 5e o 6,
    - Sistemas de alimentación ininterrumpida.
    - Detección de incendios, basada en detectores de humo y de aspiración
    - Climatización continua y adecuada de las zonas del CPD con redundancia n+1 en cada zona.
    - Detectores de humedad en las zonas del CPD y la sala eléctrica

- Tiene un acuerdo con un proveedor de servicios especializado para la custodia de soportes magnéticos, contando con una sala antisismos blindada.
- Acceso de personas externas (visitas) al CP
- Sensores para predecir la exposición de humedad
- Recuperación de información

7.9 SEGURIDAD DE LA OPERACIÓN

FULL CERTIFICATE utiliza sistemas y productos de confianza que están protegidos contra las modificaciones y que garantizan la seguridad técnica y la fiabilidad de los procesos que soportan.

En particular:

- Se llevará a cabo un análisis de los requisitos de seguridad en la fase de diseño y especificación de cualquier proyecto de desarrollo de sistemas realizado por el TSP o en su nombre, todo ello para garantizar la incorporación de la seguridad en los sistemas informáticos
- Los procedimientos de control de cambios se aplicarán a las versiones, modificaciones y correcciones de emergencia del software operativo y a los cambios de configuración que se apliquen a la política de seguridad del TSP
- Los procedimientos irán acompañados de la documentación de los cambios
- La integridad de los sistemas y de la información de FULL CERTIFICATE está protegida contra los virus y los programas informáticos.
- FULL CERTIFICATE ha establecido y aplica procedimientos para todas las funciones administrativas y de confianza que afectan a la prestación de servicios.
- FULL CERTIFICATE ha especificado y aplica procedimientos para garantizar que:

  a) Los parches de seguridad se aplican en un plazo razonable desde que están disponibles
  b) Los parches de seguridad no se aplican si introducen vulnerabilidades o inestabilidades adicionales que superan los beneficios de su aplicación
  c) Se documentan los motivos por los que no se aplican los parches de seguridad.

7.10 SEGURIADD EN LA RED

FULL CERTIFICATE ha implementado un método y/o realiza diversas actividades para proteger sus sistemas y su red de los ataques.

En particular:

- FULL CERTIFICATE ha segmentado sus sistemas en redes o zonas basándose en una evaluación de riesgos que tiene en cuenta la relación funcional, lógica y física (incluida la ubicación) entre los sistemas y servicios de confianza.
- TSP aplica los mismos controles de seguridad a todos los sistemas ubicados en la misma zona.
- FULL CERTIFICATE podrá restringir el acceso y las comunicaciones entre áreas a las necesarias para el funcionamiento de sus servicios.

- El TSP prohibirá o inhabilitará las conexiones y servicios contestados.
- FULL CERTIFICATE revisará periódicamente el conjunto de normas establecidas.
- El TSP mantendrá todos los sistemas, que son críticos para las operaciones del TSP, en una o más zonas seguras.
- FULL CERTIFICATE separa la red dedicada a la administración de los sistemas informáticos de la red operativa del TSP.
- FULL CERTIFICATE utilizará los sistemas para la administración de la aplicación de la política de seguridad única y exclusivamente para sus fines.
- El TSP separa los sistemas de producción para los servicios del TSP de los sistemas utilizados en el desarrollo y las pruebas (por ejemplo, los sistemas de desarrollo, prueba y ensayo).
    - FULL CERTIFICATE establecerá la comunicación entre diferentes sistemas de confianza únicamente a través de canales de confianza que estén aislados por separación lógica, criptográfica o física de otros canales de comunicación y que proporcionen una identificación garantizada de sus puntos finales y la protección de los datos del canal contra su modificación o divulgación.
- Si se requiere un alto nivel de disponibilidad de acceso externo al servicio de confianza, la conexión de red externa es redundante para garantizar la disponibilidad de los servicios en caso de un único fallo.
- FULL CERTIFICATE se compromete a someterse o a realizar un escaneo de vulnerabilidad periódico en las direcciones IP públicas y privadas identificadas por el TSP y a registrar evidencia de que cada escaneo de vulnerabilidad fue realizado por una persona o entidad con las habilidades, las herramientas, la competencia, el código de ética y la independencia necesarios para proporcionar un informe confiable.
- El escaneo de la vulnerabilidad indicado en el punto anterior debe realizarse una vez por trimestre.
- El TSP se someterá a una prueba de implementación en sus sistemas en el momento de la puesta en servicio y después de las actualizaciones y/o modificaciones de la(s) aplicación(es) que el TSP determine como significativas
- La prueba de implementación mencionada en el punto anterior deberá realizarse al menos una vez al año
- FULL CERTIFICATE dejará constancia de que cada prueba de implementación ha sido realizada por una persona o entidad con los conocimientos, con las herramientas, la competencia, el código ético y la independencia necesarios para proporcionar un informe confiable
- Los controles (p ej. firewalls) protegerán los dominios de la red interna del TSP contra el acceso no autorizado, incluido el acceso de suscriptores y terceros
- Los Firewalls están configurados para impedir todo acceso que no sea necesario para el funcionamiento de los servicios de FULL CERTIFICATE
- Opcionalmente se pueden activar los servicios de ciberseguridad Anti-DDos by Azure – Microsoft.

En continuidad a los puntos antes mencionados, FULL CERTIFICATE declara, en relación a sus servicios de confianza, lo siguientes:

- Que monitoreara su capacidad de acuerdo a demanda
- Asegurarse de que tendrá una potencia de procesamiento y almacenamientoa adecuada en lo que respecta a los requisitos de capacidad a futuro
- Uso de protocolos y algoritmos de última generación para la encriptación de los niveles de traslado.
- Que utiliza certificados de autenticación de sitios web para la seguridad del traslado de los datos que sales fuera de las redes internas.

FULL CERTIFICATE emplea medidas de seguridad lógicas comunes a todos los sistemas. Los sistemas específicos utilizados para la prestación del servicio han sido respaldados por un segundo nivel de seguridad.

Formalmente, se han establecido responsabilidades y procedimientos documentados para asegurar la correcta configuración, administración, operación y monitoreo de los sistemas de información y comunicaciones de FULL CERTIFICATE.

Se ha establecido y definido un procedimiento de gestión de incidentes a fin de minimizar el impacto causado por incidentes de seguridad o fallos en el funcionamiento de los sistemas, lo que permite una rápida reacción ante los posibles incidentes producidos, así como el establecimiento de medidas correctoras que eviten su repetición.

También se ha establecido una adecuada segmentación de funciones en la asignación de responsabilidades con el objetivo de prevenir un uso inadecuado de los sistemas de información, en los casos en los que dicha segmentación no es factible, otros mecanismos de control adecuados que permitan su seguimiento y control.

Se han establecido procedimientos y controles para prevenir adecuadamente la introducción de software malicioso, garantizando la integridad del software y de la información de FULL CERTIFICATE.

De la misma manera se han adaptado medidas de salvaguarda, incluyendo las copias de seguridad necesarias, comprobando periódicamente su validez mediante su restauración, junto con la monitorización permanente de los sistemas, lo que permite garantizar la continuidad de los sistemas, información y los servicios prestados por FULL CERTIFICATE

La información transmitida por las redes de comunicaciones, públicas o privadas, está adecuadamente protegida mediante los mecanismos apropiados que garantizan su confidencialidad e integridad. Se han establecido los controles necesarios para evitar la suplantación del emisor, la modificación o la pérdida de la información proporcionada, tanto en las comunicaciones con sistemas ubicados en redes internas, como con otros sistemas externos, como aquellas entidades con las que FULL CERTIFICATE tiene presencia de sus servicios como parte interviniente en los mismos.

Se han establecido procedimientos que regulan la estrategia de encriptación de la información de FULL CERTIFICATE, describiendo las medidas organizativas y técnicas que garantizan la confidencialidad e integridad de la información.

También se establecen procedimientos que regulan detalladamente el almacenamiento, manipulación, transporte y destrucción de la información sensible tanto en soportes informáticos (cintas, discos, ordenadores portátiles, dispositivos móviles como agendas y teléfonos electrónicos, dispositivos extraíbles, etc.), como de forma residual, en soporte papel, todo ello con el fin de mitigar el riesgo de acceso no autorizado, pérdida o robo.

7.11 GESTIÓN DE INCIENCIAS

FULL CERTIFICATE monitorea todas las actividades del sistema relacionadas con el acceso a los sistemas informáticos, el uso de los propios sistemas y la solicitud de servicio.

En particular:

- Las actividades de monitoreo deben tener en cuenta la sensibilidad de cualquier información recopilada o analizada.
- Las actividades inapropiadas del sistema que indican una posible violación de la seguridad, incluida la intrusión en la red del TSP, se detectan y se notifican como alarmas.
- FULL CERTIFICATE monitoriza los siguientes eventos:

a) Puesta en marcha y cierre de las funciones de inicio de sesión

b) Disponibilidad y uso de los servicios necesarios en la red TSP.

- FULL CERTIFICATE actuará de manera oportuna y coordinada para responder rápidamente a los incidentes en la medida de limitar el impacto de posibles infracciones de seguridad.
- El TSP designará personal de confianza para dar seguimiento a las alertas de eventos de seguridad potencialmente críticos y se asegura de que los incidentes se reporten de acuerdo con los procedimientos prescritos por FULL CERTIFICATE
- El TSP establecerá procedimientos para notificar a las partes interesadas, de conformidad con la normativa reguladora aplicable, cualquier infracción de la seguridad que tenga un impacto significativo en el servicio de confianza prestado y en los datos personales, dentro de las 24 horas siguientes a la identificación de la infracción.
- Cuando la infracción de la seguridad o la pérdida de la integridad puedan afectar negativamente a una persona física o jurídica a la que se haya prestado el servicio de confianza, FULL CERTIFICATE notificará a la persona mencionada la violación de la seguridad o la pérdida de la integridad, sin demora.
- Los sistemas de FULL CERTIFICATE deben monitorearse, incluida la supervisión periódica de los registros de auditoría para identificar indicios de actividad maliciosa, aplicar mecanismos automáticos para procesar los registros de auditoría y alertar al personal sobre posibles eventos críticos de seguridad.
- FULL CERTIFICATE notifica cualquier vulnerabilidad crítica que no haya sido notificada previamente, dentro de las 48 horas de su descubrimiento.
- Para cualquier vulnerabilidad, en función del impacto potencial, el TSP podrá:
  a) Crear y aplicar un plan para mitigar la vulnerabilidad
  b) Documentar la base de datos para la determinación del TSP de que la vulnerabilidad no requiere corrección.
- Los procedimientos de notificación y respuesta a incidentes se llevarán a cabo en la medida en que se reduzcan al mínimo los daños resultantes de incidentes de seguridad y mal funcionamiento.
- Finalmente, FULL CERTIFICATE establece que los registros relacionados con los servicios se conservarán durante un período de tiempo (15 años) según corresponda para proporcionar la evidencia legal necesaria.

7.12 RECOLECCIÓN DE EVIDENCIAS INTERNAS DEL SISTEMA ERDSP

El TSP registrará y mantendrá accesible durante un período de tiempo adecuado, incluso después de que toda la información relativa a los datos emitidos y recibidos por el TSP haya cesado sus actividades, todo ello, con el fin de aportar pruebas en los procedimientos judiciales y garantizar la continuidad del servicio.

En particular:

- Se mantendrá la confidencialidad e integridad de los registros actuales y archivados relacionados con la operación de los servicios.
- Los registros relativos a la operación de los servicios serán archivados de forma completa y confidencialidad, de acuerdo con las buenas prácticas de FULL CERTIFICATE
- Los registros relacionados con el funcionamiento de los servicios se pondrán a disposición, si así se requiere, para proporcionar pruebas del correcto funcionamiento de los servicios en relación con cualquier procedimiento judicial.
- Se registrará la hora exacta de eventos significativos relacionados con el entorno TSP, la gestión de clave(s) y la sincronización de reloj.
- El tiempo utilizado para registrar los eventos, como se requiere en el registro de auditoría, se sincronizará con el UTC al menos una vez al día.
- Los registros relacionados con los servicios se mantendrán durante un período adecuado para proporcionar las pruebas legales necesarias y según lo notificado en los términos y condiciones del TSP.
- Los eventos se registrarán de una manera que no pueda ser fácilmente borrados o destruidos y dentro del período de tiempo necesario para su conservación.
- Se registran los eventos relacionados con la presentación, envío y entrega de contenido de usuario.
- Se registran todos los eventos de seguridad, incluidos los cambios relacionados con las políticas de seguridad, inicio y apagado del sistema, los bloqueos del sistema y fallos de hardware, actividades de firewall y enrutador e intentos de acceso al sistema PKI.
- El período de retención para los registros especificados en esta cláusula se definirá de conformidad con la legislación aplicable; este período de retención nunca será inferior a dos años.

De hecho, los registros mencionados anteriormente, incluidas las evidencias de entrega, se almacenarán y conservarán como documentos de prueba electrónicos durante un período mínimo de 15 años. Es decir, tendrán un apoyo mínimo de 15 años.

La integridad y disponibilidad de los registros de auditoría se mantendrá en todo momento, manteniendo la sincronización de las fuentes de tiempo con todos los sistemas que generan dichos registros, centralizando, siempre que sea tecnológicamente posible, el control y seguimiento de los registros a través de alguna herramienta de gestión.

Los registros de auditoría generados por los sistemas que tratan información confidencial deben ser almacenados de acuerdo con la ley, para el resto de los sistemas este tiempo se regulará por los procedimientos correspondientes.

Los sistemas de información tendrán capacidad suficiente para que el almacenamiento de los registros de auditoría no degrade el nivel de servicio.

Cualquier cambio que sea estrictamente necesario realizar en relación con la generación de registros de auditoría debe ser debidamente autorizado por el responsable de seguridad.

La supresión de los registros debe realizarse mediante mecanismos que no degraden la confidencialidad de los mismos. Y reiteramos que el acceso a los sistemas de archivo y custodia de la documentación de FULL CERTIFICATE está restringido exclusivamente al personal autorizado. Por lo tanto, un sistema de control de acceso, identificación y autenticación se ha configurado de tal manera que está protegido contra el acceso, modificación, eliminación u otras manipulaciones no autoriza.

Los sistemas, soportes y medios que contienen la documentación e información susceptible de archivo y custodia, así como las aplicaciones necesarias para procesar los datos custodiados se mantienen y se puede acceder al mismo durante el período de tiempo establecido en este documento.

7.13 GESTIÓN DE LA CONTINUIDAD DE LAS OPERACIONES

FULL CERTIFICATE definirá y mantendrá un plan de continuidad que se utilizará en caso de alguna contingencia.

En caso de contingencia, incluyendo el compromiso de una clave de firma privada o el compromiso de alguna otra credencial de TSP, las operaciones se restablecerán dentro del plazo establecido en el plan de continuidad, después de haber abordado cualquier causa de la contingencia que pueda repetirse (p. ej., una vulnerabilidad de seguridad) con las medidas correctivas apropiadas.

Otras situaciones de contingencia incluyen la falla de componentes críticos del sistema TSP, incluyendo el hardware y el software.

FULL CERTIFICATE declara que:

- Los sistemas de datos necesarios para reanudar las operaciones se respaldarán y almacenarán en ubicaciones seguras y adecuadas para permitir que el ERDSP regrese a las operaciones de manera oportuna en caso de incidentes o desastres
- Proporcionar copias de seguridad periódicas de la información y el software
- Proporciona instalaciones de recuperación adecuadas para garantizar que toda la información y el software esenciales se pueden recuperar después de una contingencia o fallo de los medios
- Los mecanismos de recuperación se verifican regularmente para garantizar que cumplen los requisitos de los planes de continuidad de la actividad.
  • El plan de continuidad de la operación contemplara el compromiso, la pérdida o la sospecha de compromiso de una clave privada de ERDSP como una contingencia y se deben implementar procesos planificados.
- Después de una contingencia FULL CERTIFICATE deberá poner en práctica adaptar medidas adecuadas para evitar nuevas incidencias.

7.14 ACUERDOS DE TERMINACIÓN DE SISTEMA ERDSP & ERDS

Las posibles interrupciones para los usuarios y/o clientes o terceros como consecuencia del cese de los servicios del TSP se minimizarán y, además, se mantendrá la información necesaria para verificar la corrección de los servicios de confianza.

Y en el caso de que FULL CERTIFICATE determine la terminación de sus actividades y/o servicios, se aplicarán las siguientes acciones:

- Aportará los fondos necesarios (entre 20.000 y 40.000 € como reserva para desastres y seguro de responsabilidad civil con una póliza de cobertura de hasta 1.500.000 €) para continuar la finalización de las actividades de revocación
- Informará de la terminación a todos los Sujetos/Firmantes, Partes Usuarios, Autoridades Administrativas Competentes, es decir, a todas las partes con las que tenga acuerdos u otras relaciones (incluidos los órganos de control), con una antelación mínima de tres meses. Y, publicará en su sitio web o en cualquier otro medio accesible a los usuarios, la información relevante sobre el cese de sus operaciones
- Los USUARIOS dispondrán de un plazo adicional de tres meses para descargar, si así lo desean, la información correspondiente a los servicios utilizados
- Revocará cualquier autorización a entidades subcontratadas para actuar en nombre de FULL CERTIFICATE en el procedimiento de emisión de certificados
- También enviará un recordatorio a todas las partes con respecto a la finalización de sus actividades un mes antes de la fecha de cierre de la actividad
- Las claves privadas serán destruidas o deshabilitadas para su uso
- FULL CERTIFICATE mantendrá los certificados activos en un lugar seguro (p. ej., caja de seguridad o disco duro) hasta la expiración de todos los certificados emitidos. Para ponerlas a disposición de las autoridades judiciales competentes, en caso de solicitud a tal efecto
- FULL CERTIFICATE antes de terminar sus servicios, transferirá las obligaciones a una parte confiable para mantener toda la información necesaria para proporcionar evidencias del funcionamiento del TSP durante un período razonable
- Si es posible y si se verifican las condiciones para proceder al respecto, antes de que el TSP termine sus servicios, el TSP debe tomar medidas para transferir la prestación de servicios fiduciarios para sus clientes existentes a otro TSP.

7.15 PRIVACIDAD DE LOS DATOS PERSONALES

- Consulte el documento de Políticas de privacidad.

7.16 AVISO LEGAL Y TÉRMINOS Y CONDICIONES PARA EL USO DE LOS SERVICIOS

- Consulte el documento Aviso Legal & Términos y Condiciones del servicio.

7.17 POLÍTICA DE COOKIES

- Consulte la Política de cookies del documento.

7.18 CUMPLIMIENTO DE LA NORMATIVA

FULL CERTIFICATE garantiza operar de manera legal y confiable.

En particular:

- FULL CERTIFICATE se compromete a proporcionar pruebas y/o evidencias de cómo cumple con los requisitos legales aplicables, en caso de ser necesario
- Los servicios de confianza prestados y los productos y/o servicios utilizados por el usuario final en la prestación del presente servicio, son accesibles para personas con discapacidad, salvo algunas excepciones
- FULL CERTIFICATE tendrá en cuenta las normas aplicables en materia de accesibilidad, como la ETSI EN 301 549
- Se tomarán las medidas técnicas y organizativas adecuadas contra el procesamiento no autorizado o ilegal de datos personales y contra la pérdida, destrucción accidental o daño de los datos personales.

Finalmente, se garantiza que FULL CERTIFICATE actuará de conformidad con la normativa y con la legislación vigente, Estatal y europea, en materia de Protección de Datos.

8. HISTORICO DE CAMBIOS

Versión	Fecha del último envío	Modificaciones
v.1.0	30/11/2021	Creación de Documento