DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DEL SERVICIO DE ENTREGA ELECTRÓNICA CERTIFICADA

Título: DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DEL SERVICIO DE ENTREGA ELECTRÓNICA CERTIFICADA	
Fecha: 31/01/2022	**Versión: 1.5**
Estado: En vigor	**Páginas: 31**
Clasificación: PÚBLICO	**Autor: CUSTOMER COMMUNICATIONS**
OID: 1.3.6.1.4.1.53247.01.00	

ÍNDICE

1. INTRODUCCIÓN

1.1. PRESENTACIÓN

Customer Communications Tecknalia, en adelante Ccomms, nace para aportar soluciones enfocadas a facilitar la generación y gestión de la comunicación hacia el cliente-consumidor de manera eficaz conjugando las referencias de los consumidores con los intereses de la Empresa que comunica.

Ccomms basa sus soluciones de comunicación en el empleo activo de las herramientas tecnológicas de última generación para garantizar los resultados en la comunicación individualizada al cliente final.

La presente Declaración de Prácticas de Certificación detalla las normas y condiciones generales que presta Ccomms en relación con el Servicio de Entrega Electrónica Certificada, las condiciones aplicables para la identificación y autenticación del emisor y receptor, las medidas de seguridad organizativas y técnicas, la integridad de las transacciones, la exactitud de la fecha y hora de envío y recepción de los datos y el almacenamiento y custodia de todas las evidencias generadas en proceso.

Este servicio de Entrega Electrónica Certificada proporciona seguridad y confianza a la entrega de mensajes de forma electrónica entre las partes, produciendo evidencia del proceso de entrega, consistente en una declaración por parte de Ccomms de que un evento específico relativo al proceso de entrega ha sucedido en un momento dado.

De acuerdo con lo anterior, el contenido de esta Declaración de Prácticas de Certificación se realiza en cumplimiento con la legislación vigente y alineados con el Reglamento (UE) N.º 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/C y la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza

Así pues, la presente Declaración de Prácticas de Certificación constituye el compendio general de normas aplicables a la actividad de Ccomms en su condición de Prestador de Servicios de Confianza Cualificado.

Además, Ccomms sigue las indicaciones de los estándares del Instituto Europeo de Estándares de Telecomunicaciones -ETSI- guiándose para ello por las especificaciones técnicas de las normas EN 319 401 (requerimientos generales para proveedores de servicios de confianza), ETSI EN 319 521 “Policy and security requirements for Electronic Registered Delivery Service Providers” y ETSI EN 319 522 “Electronic Registered Delivery Services”; Part 1, 2, 3 & 4, y se ha redactado conforme a la RFC 3647 “Certificate Policy and Certification Practices Framework” propuesto por Network Working Group para este tipo de documentos.

1.2 NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN

Nombre	Declaración de Prácticas de Certificación del servicio de Entrega Electrónica Certificada
Versión	1.5
Estado	En vigor
Referencia/OID	1.3.6.1.4.1.53247.01.00
Fecha de emisión	31/1/2022
Localización	https://comunicaciones-legales.customercomms.com/

1.3 COMUNIDAD DE USUARIOS DE LOS SERVICIOS DE CCOMMS

1.3.1 PRESTADOR DEL SERVICIO DE ENTREGA ELECTRÓNICA CERTIFICADA

Customer Communications Tecknalia, S.L. referido en la documentación como Ccomms, es el proveedor de confianza del servicio de entrega electrónica certificada.

Dirección Avda. La Recomba 12 - 14. Pol. Industrial La Laguna. 28914 Leganés – Madrid

Correo de contacto: info@customercomms.com

1.3.2 AUTORIDADES DE REGISTRO

Son aquellas personas físicas y jurídicas a las que Ccomms encomienda la función de identificación y comprobación de las circunstancias personales de los solicitantes del servicio.

1.3.3 EMISOR

El emisor es la persona física o jurídica que emite la comunicación.

Para transaccionar con Ccomms, es necesario para el emisor identificarse electrónicamente para el acceso al servicio de entrega electrónica certificada, con un certificado electrónico, dado que la comunicación se realiza utilizando Servicios Web conforme al protocolo REST. En el caso del servicio de entrega electrónica certificada cualificada será necesario el uso de un certificado cualificado de firma electrónica o de sello electrónico.

El emisor será debidamente identificado por la plataforma del servicio de entrega electrónica certificada de Grupo Ccomms, de forma previa a la presentación en dicha plataforma de los datos de emisión.

1.3.4 DESTINATARIO

El destinatario es la persona física o jurídica a la que va dirigida la comunicación.

En el caso de la entrega electrónica certificada en proceso cualificado, el destinatario recibe un email que contiene un vínculo al sistema de autenticación de Ccomms. Se realiza la identificación del destinatario utilizando un mecanismo de autenticación basado en su certificado de autenticación, de firma electrónica o de sello electrónico emitido por un Prestador de Servicios de Confianza Cualificado, y, si el resultado es satisfactorio, se procede a la puesta a disposición del documento.

El destinatario será debidamente identificado por la plataforma del servicio de entrega electrónica certificada previamente a poner a su disposición el contenido de usuario del emisor.

1.3.5 TERCERAS PARTES

Son Terceras Partes aquellas partes que confían en las certificaciones de emisión y recepción realizadas por CertySign, así como en el propio servicio.

Deberán tener en cuenta tanto los términos y condiciones del servicio como las limitaciones establecidas para dicho servicio.

Las Terceras Partes podrán solicitar a Ccomms, a través de la dirección de correo electrónico soporte@certy-sign.com, incluyendo la referencia de la certificación que quieren comprobar, para que les sea enviada dicha certificación por correo electrónico con el fin de comprobar su veracidad.

Las Terceras Partes que confían en la certificación de CertySign deberán verificar que la firma incluida en el documento es válida, afirmando con ello que está firmado por Ccomms como Proveedor de Servicio de Confianza, y que el documento es íntegro, es decir, que no ha sido modificado desde que se firmó. Esta comprobación puede hacerse a través de la propia aplicación que visualiza el documento pdf, por ejemplo, ADOBE, al abrir el documento, o a través de servicios como VALIDe, facilitado por el Gobierno de España, u otros que permitan la validación de firmas electrónicas.

Igualmente el documento incluye un Código Seguro de Verificación (CSV) que permite verificar la validez e integridad del documento a través de la siguiente URL:

https://verificar.mailcomms.io/es

En caso de que el certificado con el que se selló el documento haya caducado, es posible que la aplicación comunique que haya una firma que presenta errores (por haber caducado). En este caso, se podrá comprobar que el certificado era válido en el momento

de la firma puesto que la información de consulta al servicio de revocación se encuentra incorporado en detalles del certificado y se ha generado una firma en formato PAdES LTV.

En caso de que una parte confiante tenga dudas de que el certificado continúe siendo válido, a pesar de la información contenida en el mismo, podrá solicitar a Ccomms su verificación y conformidad con la firma del mismo, escribiendo a soporte@certy-sign.com incluyendo la referencia de la certificación que quieren comprobar.

El formato original de la certificación de Certysign se garantizará como legible por el servicio de entrega electrónica certificada, almacenando también el software para visualizarlo, antes de que se convierta en no disponible.

Cuando existe el riesgo de que un sistema específico de documento/sistema visor se vuelva obsoleto, todos los documentos afectados se copiarán de forma fiable manteniendo su semántica sin cambios en otro sistema de documento/visor adecuado mientras el más antiguo esté todavía disponible. Se incluirá una certificación de confianza atestiguando la correspondencia del nuevo contenido del documento con el anterior.

2. NORMATIVA Y ESTÁNDARES APLICABLES

Las normas y estándares de aplicación descrito en esta Declaración de Prácticas de Certificación son las siguientes:

1. Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE
2. Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
3. Reglamento de Ejecución (UE) 2015/1502 de la Comisión, de 8 de septiembre de 2015 sobre la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica con arreglo a lo dispuesto en el artículo 8, apartado 3, del Reglamento (UE) no 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.
4. Reglamento (UE) 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
5. Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales.

6. Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico
7. ETSI EN 319 521 “Policy and security requirements for Electronic Registered Delivery Service Providers”
8. ETSI EN 319 522-1: "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 1: Framework and Architecture".
9. ETSI EN 319 522-2: "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 2: Semantic content".
10. ETSI EN 319 401: “Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers”.
11. ETSI EN 319 411 “Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates”
12. ETSI EN 319 102-1 “Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part1: Creation and Validation”
13. ETSI TS 119 461 “Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects”
14. ISO/IEC 29115: “Information Technology - Security techniques - Entity authentication assurance framework
15. ISO/IEC 27001:2014. Information technology. Security techniques. Information security management systems. Requirements
16. ISO/IEC 27002:2013. Information technology. Security techniques. Code of practice for information security controls
17. NIST SP 800-63B “Digital Identity Guidelines Authentication an Lifecycle Management”.

3. DEFINICIONES Y ACRÓNIMOS

3.1. DEFINICIONES

Para una mayor comprensión del contenido de la DPC se facilita, por orden alfabético, una breve definición de los siguientes términos:

- **Aplicación/agente de entrega electrónica certificada:** sistema consistente en un software y/o hardware por medio del cual emisores y destinatarios participan en el intercambio de datos con prestadores de servicios de entrega electrónica certificada.

- **Autenticación:** Es el proceso electrónico que posibilita la identificación de una persona física o jurídica, o del origen y la integridad de datos en formato electrónico.
- **Cambio sustancial en la DPC:** Por cambio sustancial en la DPC se hace referencia a cualquier modificación que afecte a los derechos y obligaciones del conjunto de intervinientes o a la naturaleza jurídica de los servicios a los que la DPC se refiere.
- **Cifrado:** Operación mediante la cual un mensaje en claro se transforma en un mensaje ilegible.
- **Contenido del usuario:** datos originales producido por el emisor que ha de ser puesto a disposición del destinatario
- **Criptografía:** Ciencia que estudia la alteración del texto original con el objetivo de que el significado del mensaje solo pueda ser comprendido por su destinatario.
- **Destinatario:** persona física o jurídica a quien va dirigida la comunicación.
- **Emisor:** persona física o jurídica que remite la comunicación
- **Entrega:** acto de cruzar con éxito la barrera del servicio de entrega electrónica certificada del destinatario a través de la aplicación/agente de entrega electrónica del destinatario.
- **Envío:** acto de hacer que el contenido del usuario esté disponible para el destinatario, dentro de los límites del servicio de entrega electrónica certificada.
- **Evidencias:** Hace referencia a todos los datos y elementos acreditativos generados durante el proceso de entrega electrónica, que permiten probar que un evento ha ocurrido en un momento determinado. Son archivados y custodiados por Ccomms.
- **Función hash (o función resumen):** Algoritmo que permite obtener un código alfanumérico único del documento sobre el que se aplica, no resultando posible obtener, del código alfanumérico único, el documento original por lo que se dice es irreversible. Generalmente se basan en protocolos internacionales. Aunque tiene diversas funcionalidades, se utiliza principalmente para cifrar contenido y para comprobar, por contraste, si un documento ha sufrido modificaciones ulteriores a su firma.
- **Huella digital:** La huella digital es el código alfanumérico obtenido tras haber aplicado la función hash a un documento. En ocasiones también se la denomina "resumen único" o "hash".
- **Identificación:** Proceso mediante el cual una persona acredita su identidad.
- **Integridad del contenido:** La integridad del contenido se refiere a todo documento o conjunto de datos que no han sido objeto de cambios o alteraciones con posterioridad a su firma.
- **Prestador de Servicios de Certificación (o PSC):** Según dispone la LFE es la "persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica".

- **Prestador de Servicios de Confianza:** una persona física o jurídica que presta uno o más servicios de confianza, bien como prestador cualificado o como prestador no cualificado de servicios de confianzas".
- **Prestador de Servicio de Entrega Electrónica Certificada:** proveedor del servicio de confianza que presta el servicio de entrega electrónica certificada
- **Prestador Cualificado del Servicio de Entrega Electrónica Certificada:** Proveedor del servicio que proporciona servicios cualificados de entrega electrónica certificada
- **Repudio:** Desde el punto de vista del emisor, el repudio del mensaje supone negar haberlo enviado. Desde el punto de vista del destinatario, negar haberlo recibido.
- **Sello de tiempo electrónico**: datos en formato electrónico que vinculan otros datos en formato electrónico con un instante concreto, aportando la prueba de que estos últimos datos existían en ese instante;
- **Servicio de entrega electrónica certificada**: un servicio que permite transmitir datos entre terceras partes por medios electrónicos y aporta pruebas relacionadas con la gestión de los datos transmitidos, incluida la prueba del envío y la recepción de los datos, y que protege los datos transmitidos frente a los riesgos de pérdida, robo, deterioro o alteración no autorizada;
- **Servicio cualificado de entrega electrónica certificada:** un servicio de entrega electrónica certificada que cumple los requisitos establecidos en el artículo 44 del Reglamento 910/2014 (eIDAS)
- **Usuarios:** Hace referencia a toda persona física o jurídica que hace uso de los servicios proporcionados por Ccomms.
- **Validación:** Procedimiento a través del cual la Autoridad de Certificación verifica la validez de la firma empleada.

3.2. ACRÓNIMOS

- **AEPD:** Agencia Española de Protección de Protección de Datos
- **CPD:** Centro de Proceso de Datos.
- **DPC:** Declaración de Prácticas de Certificación
- **eIDAS:** Reglamento 910/2014 del Parlamento y del Consejo, de 23 de julio de 2014, de identificación electrónica y servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/937CE
- **ERDS**: Servicio de Entrega Electrónica Certificada
- **ERDSQ:** Servicio Cualificado de Entrega Electrónica Certificada
- **LSEC:** Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- **LOPDGDD:** Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales,

- **LSSI:** Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico
- **PSC:** Prestador de Servicios de Confianza
- **OTP:** One Time Password
- **SGSI:** Sistema de Gestión de Seguridad de la Información.
- **TSP:** Trust Service Provider. Prestador de Servicios de Confianza

4. REQUERIMIENTOS DE CONFORMIDAD

Ccomms declara que la presente Declaración de Prácticas es aplicable al Servicio Cualificado de Entrega Electrónica Certificada cumpliendo los requisitos establecidos por el Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (eIDAS).

Ccomms considera que el objeto de este servicio de entrega electrónica certificada cualificada es la generación de una prueba documental que acredita el envío, la remisión por parte un remitente, la recepción y, en su caso, el acceso/descarga del contenido adjunto, por parte de uno o más destinatarios, de un determinado contenido del usuario, así como del momento en que se produjeron.

Ccomms garantiza, en línea con su declaración de aplicabilidad y con los requisitos legales que cumple con:

- su política de seguridad de la información, que está alineada con la regulación jurídica aplicable;
  la política de servicio entrega electrónica certificada cualificada definida en esta Declaración de Prácticas de Certificación;
- los requerimientos organizativos definidos en el punto 9.1;
- su obligación de facilitar la información requerida, cuando sea necesaria, a sus socios comerciales, auditores y autoridades reguladoras, tal y como se especifica en los puntos 9 y 13 del presente documento, incluyendo los requisitos organizativos;
- el presente documento es conforme a la norma del ETSI EN 319 521 “Policy and security requirements for Electronic Registered Delivery Service Providers”;
- ha implementado los controles que cumplen con los requerimientos especificados por la norma ETSI EN 319 521, garantizado por la implantación de un SGSI basado en la norma ISO/IEC 27001, como proveedor de servicios de confianza.

Los Prestadores de Servicios de Confianza Cualificados utilizados para la prestación del servicio de entrega electrónica certificada cualificada son los siguientes:

- Firmaprofesional: Prestador de Servicio Cualificado de Sellado de tiempo, emisor de los sellos de tiempo.

- Uanataca: Prestador de Servicio de Certificación Cualificado, emisor del certificado de sello cualificado de entidad, que utiliza el servicio para firmar las evidencias y Prestador de Servicio Cualificado de Sellado de tiempo, emisor de los sellos de tiempo.

5. INTEGRIDAD Y CONFIDENCIALIDAD DEL CONTENIDO DEL USUARIO

Ccomms garantiza la adecuada disponibilidad, integridad y confidencialidad del contenido del usuario cuando utiliza el servicio de Entrega Electrónica Certificada, firmando la transacción realizada con un certificado cualificado de sello electrónico emitido por un Prestador de Servicios de Certificación Cualificado, instalado en la plataforma. El sellado de tiempo se realiza por una Autoridad de Sellado de Tiempo cualificada.

Además, Ccomms protege la confidencialidad de la identidad del emisor y del destinatario, tanto durante el envío, como durante la custodia de las evidencias, cifrando las comunicaciones mediante protocolo TLS con algoritmos fuertes de cifrado.

Ccomms protege la integridad del contenido y sus metadatos asociados, tanto durante la transmisión del emisor al destinatario como entre los componentes del sistema distribuido del Servicio, así como durante el almacenamiento, debidamente conservado al menos hasta que prescriban las posibles acciones legales, mediante una firma digital soportada por un certificado cualificado generada por un Prestador de Servicios de Certificación Cualificado, e incorporando un sello de tiempo cualificado, de tal forma que se excluye la posibilidad de que los datos puedan cambiar de forma indetectable.

Ccomms establece unas condiciones sobre los ficheros a transmitir, que son las siguientes:

- Documentos admitidos: Documento PDF
- Tamaño máximo: 15 megabyte
- Número máximo de documentos por envío: 1

El servicio podrá rechazar el fichero en caso de ficheros corrompidos o no aceptados por no ser confiables (posibilidad de estar infectados, etc…).

Una vez admitido el fichero a transmitir, en ningún caso el contenido será modificado por el servicio de entrega electrónica certificada.

6. IDENTIFICACIÓN Y AUTENTICACIÓN DE LOS USUARIOS

6.1. VERIFICACIÓN DE LA IDENTIDAD INICIAL DE LOS USUARIOS

Ccomms verificará la identidad inicial del emisor. El emisor debe firmar electrónicamente cada petición con un certificado electrónico, dado que la comunicación se realiza utilizando Servicios Web conforme al protocolo REST. Para ello será necesario el uso,

por parte del emisor, de un certificado cualificado de firma electrónica o de sello electrónico emitido por algún Prestador de Servicios de Certificación cualificado y aceptado por la plataforma del servicio de entrega electrónica certificada. La relación de Prestadores de servicios de certificación aceptados se puede consultar en las condiciones generales de contratación del servicio de entrega electrónica certificada. En el caso de utilización de sello electrónico cualificado por parte del emisor, Ccomms realizará previamente, a través del Verificador de Identidad, la identificación fehaciente del representante legal de la entidad a cuyo nombre se emite el certificado de sello electrónico. Para ello, el representante legal suscriptor del certificado de sello de empresa deberá identificarse presencialmente y mediante su documento de identidad ante el Verificador de Identidad. La prueba de dicha identificación, así como el número de serie del certificado de sello electrónico que se va a utilizar para autenticarse en el servicio, se incorporará como anexo al contrato del servicio de entrega electrónica certificada, y será almacenado como prueba de verificación de la identidad durante el plazo legalmente establecido.

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

La llamada al API mediante certificado electrónico recepcionará los parámetros y recopilará los datos del certificado electrónico aportado. Si los parámetros recogidos en el certificado son correctos se generará el identificador único de la transacción si la llamada es correcta. En caso contrario, retornará un error.

6.2 IDENTIFICACIÓN DEL DESTINATARIO Y ENTREGA DEL CONTENIDO DE USUARIO

Ccomms entregará el contenido del usuario al destinatario únicamente después de haber identificado de forma exitosa al destinatario. Para ello será necesario el uso, por parte del emisor, de un certificado cualificado autenticación, de firma electrónica o de sello electrónico emitido por algún Prestador de Servicios de Certificación cualificado y aceptado por la plataforma del servicio de entrega electrónica certificada. La relación de Prestadores de servicios de certificación aceptados será puesta a disposición del destinatario en la propia plataforma, una vez ha accedido y antes de su autenticación. El plazo de tiempo en el que el mensaje estará disponible para el receptor será de 10 días.

La entrega del contenido al destinatario supone el acceso al contenido por parte del destinatario, una vez se haya identificado correctamente.

6.3. AUTENTICACIÓN

Para autenticar al destinatario se utiliza un mecanismo de autenticación basado en su certificado de firma electrónica o de sello electrónico y, si el resultado es satisfactorio, se procede a la puesta a disposición del documento.

7. REFERENCIAS DE TIEMPO

Las referencias de tiempo que se establecen en cada uno de los eventos del Servicio de Entrega Electrónica Certificada siguen la línea de lo establecido en el documento "Términos y Condiciones".

Se indicará la fecha y hora del acceso del emisor, del envío del contenido del usuario, de la recepción por parte del destinatario, así como de cualquier cambio que ocurra en el mismo, mediante un sello electrónico de tiempo cualificado, emitido por un Prestador de Servicios de Confianza que emite sellos de tiempo cualificados.

La prueba del envío y la prueba de la recepción están vinculadas al contenido del usuario y selladas mediante un sello de tiempo cualificado.

Ccomms comprueba la validez del certificado de sello de tiempo utilizado para sellar dichas evidencias.

Ccomms comprobará, al menos una vez al año, que el Prestador del Servicio de Sellado de Tiempo continúa siendo cualificado.

8. EVENTOS Y EVIDENCIAS

8.1 REGISTRO DE EVENTOS

Ccomms registrará los eventos producidos en el servicio, y almacenará al menos los siguientes:

- datos de identificación y autenticación de emisor y destinatario; incluidos los eventos e información de verificación de la identidad
- prueba de que la identidad del emisor ha sido verificada inicialmente;
- registros de operación, verificación de identidad del emisor y destinatario, y comunicación;
- prueba de la verificación de identidad del destinatario antes del envío/traspaso del contenido del usuario.
- demostrar que el contenido del usuario no se ha modificado durante la transmisión, mediante el sellado de la información con un sello de entidad y la inclusión de un sello de tiempo;
- una referencia o una recopilación completa del contenido del usuario presentado;
- tokens de sello de tiempo correspondientes a la fecha y hora de envío, consignación y entrega y modificación del contenido, según proceda.

8.2 EVENTOS REGISTRADOS POR EL ERDS

1. **Eventos del Servicio de Entrega Electrónica en origen:**

a. Certificado electrónico de emisor verificado: se produce la evidencia de que el emisor ha sido debidamente identificado para acceder al servicio y hacer uso del mismo para el envío de una comunicación a un destinatario.

   En la declaración final del servicio esta evidencia se refleja como "Certificado de emisor verificado".

b. Comunicación recibida: se produce la evidencia de que el emisor, debidamente identificado tal y como se puede probar con la información de los datos de identificación y verificación de la identidad del emisor, ha presentado el contenido del usuario, en el momento indicado en dicha evidencia, al Prestador del Servicio de Entrega Electrónica, y éste lo ha aceptado para a su vez intentar hacer la entrega a su destinatario.

   En la declaración final del servicio esta evidencia se refleja como "Transacción admitida".

c. Rechazo de comunicación recibida: se produce la evidencia de que el emisor, debidamente identificado tal y como se puede probar con la información de los datos de identificación y verificación de la identidad del emisor, ha presentado el contenido del usuario, en el momento indicado en dicha evidencia, al Prestador del Servicio de Entrega Electrónica, y éste ha rechazado intentar hacer la entrega al destinatario.

2. Eventos de la notificación del contenido al destinatario:

a. Publicado archivo a disposición del destinatario: Se evidencia que el ERDS ha enviado una notificación al destinatario, en un momento dado, comunicando la puesta a su disposición de un mensaje, y solicitando su aceptación.

   En la declaración final del servicio esta evidencia se refleja como "Publicado archivo a disposición del usuario".

b. Correo electrónico remitido: Se evidencia que el ERDS ha enviado un correo electrónico al destinatario informándole de la puesta a disposición del contenido y la URL de acceso.

   En la declaración final del servicio esta evidencia se refleja como "Correo electrónico remitido".

c. Notificación de modificación del contenido del usuario: Se evidencia que el ERDS ha enviado una notificación al destinatario, en un momento dado, comunicando la puesta a su disposición del mensaje con modificación del contenido, y solicitando su aceptación.

d. Fallo en la notificación para la aceptación: se evidencia que el ERDS no ha podido notificar al destinatario la puesta a disposición de un mensaje,

debido a un fallo técnico o de otro tipo, o que no se ha realizado la evidencia de notificación en un periodo de tiempo determinado, según las políticas aplicables (legales, contractuales o predefinidas en la plataforma). La plataforma dará un mensaje de caducidad en la entrega.

3. **Eventos de aceptación/rechazo del envío por parte del destinatario**

    a. Identificación del destinatario: se produce la evidencia de que el destinatario ha sido debidamente identificado tal y como se puede probar con la información de los datos de identificación y verificación de la identidad del destinatario.

    En la declaración final del servicio esta evidencia se refleja como "Identificación por certificado personal correcta".

    b. Notificación electrónica aceptada: se produce la evidencia de que el destinatario, debidamente identificado tal y como se puede probar con la información de los datos de identificación y verificación de la identidad del destinatario, ha aceptado recibir el contenido del usuario.

    En la declaración final del servicio esta evidencia se refleja como "Notificación electrónica aceptada".

    c. Notificación electrónica rechazada: : se produce la evidencia de que el destinatario, debidamente identificado tal y como se puede probar con la información de los datos de identificación y verificación de la identidad del destinatario, ha rechazado recibir el contenido del usuario.

    En la declaración final del servicio esta evidencia se refleja como "Notificación electrónica rechazada".

    d. Caducidad del envío: se produce la evidencia de que el destinatario no ha realizado ninguna acción para aceptar o rechazar el contenido del usuario, transcurrido un determinado periodo de tiempo según las políticas aplicables (legales, contractuales o predefinidas en la plataforma)

4. **Eventos del ERDS en destino**

    a. Entrega del contenido del usuario al destinatario: El contenido del usuario ha cruzado con éxito la frontera del ERDS en un momento dado, hacia la aplicación del destinatario y fue entregada con éxito, previa autenticación del destinatario. El evento indicará que la aplicación del destinatario recuperó el mensaje proactivamente a través de la solicitud de descarga por parte del destinatario.

    En la declaración final del servicio esta evidencia se refleja como "Documentación descargada".

    b. Fallo en la entrega del contenido del usuario: El contenido del usuario no ha cruzado con éxito la frontera del ERDS, hacia la aplicación del

destinatario, debido a errores técnicos o por caducidad del periodo de tiempo para acceder al contenido por parte del destinatario.

El registro de los eventos se realiza mediante logs de auditoría se almacenan en la plataforma de Ccomms. Las evidencias que se han producido por el servicio se incorporan a un PDF que será firmado con un sello electrónico cualificado de Ccomms y sellado con un sello de tiempo cualificado. Dicho PDF quedará a disposición de los usuarios y será enviado al emisor y al destinatario, de tal forma que queda garantizada la disponibilidad, confidencialidad e integridad de los registros. Estas evidencias se custodian en la plataforma durante mínimo 15 años.

Ccomms revisa los registros de auditoría de forma periódica, verificando su normal actividad y que no han sido manipulados. Se utilizan controles de acceso físico y lógico para los ficheros de registro, quedando protegidos de accesos, modificaciones o eliminaciones no autorizadas.

9. OBLIGACIONES Y RESPONSABILIDADES

9.1 OBLIGACIONES DE CCOMMS

Ccomms, como Prestador del Servicio de Confianza Cualificado se compromete a cumplir una serie de obligaciones detalladas en esta DPC, en el marco del eIDAS, sus disposiciones de desarrollo y otras legislaciones que sean de aplicación. En concreto, se obliga a:

- Respetar lo dispuesto en esta Declaración de Prácticas de Certificación.
- Prestar el servicio de entrega electrónica certificada de forma imparcial y objetiva.
- Garantizar la adecuación de sus procesos y servicios a los estándares a los que estos se adhieren.
- Informar al suscriptor del ERDS de las características de la prestación del servicio, las obligaciones que asume y los límites de responsabilidad.
- Proteger de manera fiable todos los datos de sus clientes, así como los registros de actividad y auditoria con los medios que para ello considere más adecuados y durante el periodo de tiempo contemplado según la naturaleza de los datos registrados.
- Procurar la prestación del ERDS de forma diligente e ininterrumpida
- Comunicar a sus clientes con la suficiente antelación la no disponibilidad del sistema en caso de realizar procesos de modificación, mejora o mantenimiento que impliquen una paralización del servicio.
- Notificar con la mayor prontitud a las partes implicadas siempre que se detecte incidencia alguna en el sistema con afectación para las mismas.

- Garantizar que los eventos producidos por el sistema operen en sincronía con fuentes fiables de tiempo, utilizando para ello una Autoridad de Sellado de Tiempo cualificada.
- Garantizar la integridad, confidencialidad y disponibilidad del contenido del usuario, dentro del ERDS
- Establecer mecanismos de custodia de las evidencias producidas por el ERDS, quedando protegidas de cualquier manipulación no autorizada, falsificación, pérdida, o destrucción.
- La información relativa al servicio cualificado de entrega electrónica certificada será conservada durante 15 años desde la finalización del servicio prestado.
- Proteger las claves privadas de los certificados cualificados utilizados en el ERDS.
- Publicar las versiones más recientes de este documento y otras definiciones de prácticas de otros servicios de manera previa a la aplicación de las condiciones que en ellos se contemple.
- Disponer de un canal de comunicación con clientes y terceros para solicitudes, consultas, quejas y reclamaciones.
- Atender las solicitudes, consultas, quejas y reclamaciones de clientes y terceros en un plazo razonable
- Comunicar a la Autoridad Pública competente aquella información confidencial o que contenga datos de carácter personal cuando haya sido requerida por la misma y en los supuestos previstos legalmente. En concreto, Ccomms está obligada a revelar la identidad de los intervinientes en el servicio cuando lo soliciten los órganos judiciales en el ejercicio de las funciones que tengan atribuidas, y en el resto de los supuestos previstos en el RGPD.
- Notificar a la Autoridad de Supervisión y Control del Gobierno de España cualquier modificación en la presente Declaración de Prácticas Certificación.
- Notificar a la autoridad competente y a las partes implicadas el cambio en la infraestructura que pueda afectar a la prestación del servicio.
- Disponer de un seguro de responsabilidad civil para cubrir los riesgos derivados del servicio y que cubra, al menos, el valor mínimo exigido por la normativa vigente.
- Notificar a la Autoridad de Control y Supervisión competente en servicios electrónicos de confianza, y en su caso a la Agencia Española de Protección de Datos, cualquier violación de la seguridad o pérdida de la integridad que tenga un impacto significativo en el servicio de confianza prestado o en los datos personales correspondientes.

9.2. OBLIGACIONES DE LOS USUARIOS DEL SERVICIO

Tanto el emisor como el destinatario del contenido del usuario tendrán las obligaciones siguientes:

- Conocer y respetar lo dispuesto en la presente DPC.
- Conocer y respetar lo dispuesto en el contrato de prestación del servicio.
- Comunicar al Prestador del Servicio cualquier incidente de seguridad en el momento que sea identificado.
- El emisor deberá proporcionar a Ccomms los datos de los destinatarios sin errores y actualizados.
- Verificar y validar las firmas y sellos electrónicos que se han incorporado en los certificados de evidencias del ERDS.

9.3 OBLIGACIONES DE LOS PROVEEDORES DE CCOMMS

Los proveedores de servicios de valor añadido al ERDS, como los Prestadores de servicios de certificación que emitan los certificados electrónicos y los sellos de tiempo, deberán cumplir las siguientes obligaciones (si aplica):

- Proporcionar a Ccomms los certificados digitales necesarios para firmar o sellar electrónicamente las certificaciones de evidencias.
- Garantizar que los certificados emitidos a Ccomms en el ámbito de la prestación del ERDS son cualificados.
- Proporcionar a Ccomms los sellos de tiempo necesarios para sellar temporalmente los eventos y las certificaciones de evidencias.
- Comunicar a Ccomms cualquier cambio de condición en sus certificados vigentes.
- Garantizar que los sellos de tiempo emitidos en su caso son cualificados.

Ccomms se asegurará que lel proveedor del servicio de almacenamiento (Amazon WS) establezca las medidas necesarias para garantizar la integridad, confidencialidad y disponibilidad de la información.

9.4 RESPONSABILIDADES

Ccomms como Prestador de Servicios de Confianza se encuentra sujeto al régimen de responsabilidad recogido en el artículo 13 del eIDAS por lo que asumirá las responsabilidades por los perjuicios causados de forma deliberada o por negligencia a cualquier persona física o jurídica en los términos previstos en la legislación vigente.

A estos efectos, Ccomms ha suscrito un seguro de responsabilidad civil de 1.500.000 € (un millón y medio de euros) para afrontar el riesgo de la responsabilidad por los daños y perjuicios que pueda ocasionar con motivo del incumplimiento por su parte de las obligaciones que impone el Reglamento eIDAS.

Limitaciones de responsabilidad:

- Ccomms queda eximido de responsabilidad por los daños y perjuicios ocasionados en caso de fuerza mayor, caso fortuito o imprevisibles o que, siendo previsibles no se hayan podido evitar.

- Ccomms no será responsable de los actos u omisiones realizados por el Cliente, siendo éste quien asumirá todos los daños y perjuicios, directos e indirectos, que se pudieren ocasionar a cualquier persona, propiedad, empresa, servicio público o privado, concretamente por las pérdidas de beneficios, pérdida de información y datos, o los correspondientes daños, como consecuencia de los actos, omisiones o negligencias del Cliente así como de terceros a él ligados, por uso inadecuado, indebido o fraudulento, siendo de exclusivo riesgo del Cliente.

- Ccomms no será responsable por el contenido de los mensajes o de los documentos enviados.

- Ccomms no responde por la negligencia en la confidencialidad y conservación de los datos de acceso al servicio por parte de los usuarios del ERDS.

- Ccomms tampoco será responsable por los daños y perjuicios si el destinatario actúa de forma negligente. Entre otros supuestos, se entenderá que el destinatario actúa de forma negligente cuando no tenga en cuenta la suspensión o pérdida de vigencia del certificado electrónico, o cuando no verifique la firma o sello electrónicos.

10. TERMINACIÓN DEL SERVICIO

Ccomms cuenta con un Plan de Cese del Servicio Cualificado de Entrega Electrónica Certificada, reflejado en el documento "PE_SGSI 92-ERDS-PLAN DE CESE", y cuyos principales hitos son:

- Se informará, a través de una publicación en la página web del servicio, con una antelación mínima de 2 meses a los usuarios, clientes y aquellas personas físicas y jurídicas con las que Ccomms mantenga una relación. Entre ellas se encuentran los clientes, los proveedores de servicios de confianza, las autoridades de supervisión y control u otras autoridades relevantes. Adicionalmente también se informará y coordinará con los clientes que utilicen este servicio a través de los interlocutores que gestionan la relación.

- Se notificará al Organismo de Supervisión y Control del Gobierno de España tanto el cese de la actividad como todas las circunstancias relacionadas con el cese, entregando y registrando un escrito a través de la Sede Electrónica de dicho Organismo.

- Se transferirán las obligaciones a otro Prestador de Servicios de Confianza con el que se ha llegado a un acuerdo, para que mantenga y custodie toda la información necesaria sobre evidencias, logs y eventos de las operaciones por el plazo de tiempo que se haya comprometido. En caso de, que llegado el momento no sea posible realizar dicha transferencia ni acordar el traspaso con otro Prestador de Servicios de Confianza, esta información se remitirá al Ministerio competente en Servicios Electrónicos de Confianza.

- Se destruirán las claves privadas, incluyendo las copias de seguridad, según procedimiento de "CRIPTOGRAFÍA", de tal forma que no puedan ser recuperadas en ningún caso.

- Ccomms ha firmado un acuerdo de transferencia del servicio de confianza de ERDS con otro proveedor del servicio de ERDS, en caso de cese del mismo.

- En caso de quiebra o si por alguna otra razón Ccomms no fuera capaz de asumir los costes del servicio por sí mismo, transferirá toda la información necesaria al Proveedor del servicio con el que ha alcanzado el acuerdo para que continúe con el servicio, al menos para cumplir los requisitos mínimos y obligaciones por el período de tiempo necesario.

- Ccomms mantendrá disponible su clave pública a las partes de confianza durante un período de tiempo razonable, cumpliendo con sus obligaciones para que esto se cumpla.

11. CONTROLES DE SEGURIDAD

11.1. SEDE E INSTALACIONES Y MEDIDAS DE SEGURIDAD FÍSICAS Y AMBIENTALES

Ccomms tiene su sede principal en Avenida de la Recomba, 14, Parque Empresarial La Laguna - 28914 Leganés (Madrid). El recinto donde se ubica la sede cuenta con un perímetro cerrado de vigilancia que separa el patio exterior de la vía pública gracias a una verja de más de dos metros de altura. Asimismo, para acceder desde el patio exterior al propio edificio es preciso volver a identificarse. Dentro del edificio existen secciones en los que solo se permite el acceso a perfiles determinados.

En el lugar antes reseñado se ubica su Centro de Proceso de Datos (en lo sucesivo "CPD"). Este centro está dentro del alcance definido en la norma UNE-ISO/IEC 27001:2014 sobre "Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI)" que la compañía ha implantado y en la que está certificada con AENOR.

Con el objetivo de garantizar la seguridad y la continuidad de los servicios, Ccomms dispone de una infraestructura híbrida: en el CPD anteriormente mencionado, y en

Amazon AWS. Amazon AWS proporciona una arquitectura de red y un centro de datos diseñados para satisfacer los requisitos de seguridad de las organizaciones más exigentes (más información en https://aws.amazon.com/es/security/), con unos niveles de protección y solidez de la construcción adecuados y con vigilancia durante las 24 horas al día, los 7 días a la semana. Así mismo, esta configuración permite garantizar la continuidad de negocio, definiendo Alta Disponibilidad, despliegues Multi-AZ y planes de backup.

Por su parte, Ccomms ha aprobado el procedimiento de Seguridad Física y Ambiental donde se detallan las medidas físicas implantadas para evitar accesos físicos no autorizados a las instalaciones y proteger éstas, y por ende, la información en ellas gestionadas, de estas intromisiones y de los daños que pudieran ocasionar fenómenos ambientales como incendios, inundaciones o similares.

11.2 SEGURIDAD LÓGICA, CONTROLES DE ACCESO

De forma análoga a las medidas de seguridad físicas, los sistemas informáticos solo permiten que el usuario tenga acceso a aquella información que, según su perfil, resulte necesaria para el ejercicio de las funciones encomendadas.

La política, procedimiento y controles para el Control de Accesos están definidos en el Procedimiento aprobado por Ccomms, denominado “CONTROL DE ACCESOS”.

11.3 GESTIÓN DE SOPORTES Y DOCUMENTOS

La gestión de soportes informáticos se detalla en el procedimiento de Ccomms “Gestión de soportes en protección de datos”, donde se distingue, convenientemente, por los niveles de seguridad aplicables a cada fichero y según el dispositivo de almacenamiento sea fijo (por ej. los discos duros de los ordenadores de sobremesa) o móvil (CDs, USBs, PDAs…).

11.4 COPIAS DE RESPALDO Y PROCEDIMIENTO DE RECUPERACIÓN

Con una periodicidad de al menos una semana, el Responsable de Seguridad procede a realizar copias de respaldo que son almacenadas en un lugar seguro.

En caso de fallo del sistema con pérdida total o parcial de los datos de los ficheros el Procedimiento Recuperación de Datos implantado garantiza que partiendo de la última copia de respaldo y del registro de las operaciones realizadas desde el momento de la copia, se reconstruirán los datos de los ficheros al estado en que se encontraban en el momento del fallo.

11.5 MEDIDAS DE SEGURIDAD EN OPERACIONES Y COMUNICACIONES

Con el objetivo de garantizar el tratamiento adecuado de la documentación objeto de depósito y de la transmisión de datos a través de redes telemáticas, Ccomms cuenta con dos documentos de obligado cumplimiento para todo el personal en los que se detallan

las políticas, procedimientos y controles implementados y que son “SEGURIDAD DE LAS OPERACIONES” y “SEGURIDAD DE LAS COMUNICACIONES”.

11.6 ANÁLISIS DE VULNERABILIDADES Y AUDITORÍAS

En el documento “AUDITORÍAS INTERNAS se detalla la política, procedimiento y controles para la revisión y mejora continua del sistema mediante la realización de auditorías con una periodicidad, al menos, anual. El proceso terminará con la elaboración de un Informe de Auditoría en el que se recogen las acciones correctivas y/ o preventivas necesarias.

11.7 ESTRUCTURA ORGANIZATIVA DE CCOMMS

En el documento “ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN” se establece la estructura organizativa de Ccomms en la gestión de la Seguridad de la Información.

El organigrama con la estructura de personal de la compañía se encuentra publicado en la intranet corporativa y los roles con las responsabilidades de cada uno de los puestos se gestiona desde el Departamento de Recursos Humanos siguiendo el procedimiento y políticas detalladas en el documento: “SEGURIDAD LIGADA A LOS RRHH”.

11.8 ROLES DE CONFIANZA

Los roles de confianza son estatus referidos al grado de seguridad o la asignación de determinadas tareas por parte de alguien facultado y autorizado a ello de acuerdo con la ETSI EN 319 401 y la ETSI EN 319 521.

Los roles de confianza identificados para la gestión del servicio de entrega electrónica certificada son los siguientes:

- **Administrador de sistemas**: los Administradores de Sistemas son los encargados de configurar, instalar y mantener los sistemas confiables de Ccomms para la gestión de los servicios incluyendo la recuperación del sistema.

- **Operador del sistema**: son los responsables de operar los sistemas de CertySign de Ccomms de manera habitual. Dan soporte a los administradores de sistemas y a los operadores de identidad en aquellos aspectos que requieran.

- **Verificador de identidad**: es el encargado de garantizar que los procesos reales realizados para verificar la identidad del emisor y del destinatario sean conformes con el proceso de verificación de identidad inicial especificado.

- **Auditor interno**: está autorizado a visualizar archivos y registros de auditoría de los sistemas de confianza, así como, auditar los logs mismos. Se debe encargar de

comprobar el seguimiento de incidencias y eventos, la protección de los sistemas, así como comprobar alarmas y elementos de seguridad física.

- **Responsable de CertySign:** es el encargado de gestionar y mantener el servicio de confianza de entrega electrónica certificada. Se encarga de todos los aspectos relativos a la seguridad de CertySign. Asimismo, gestiona los incidentes de seguridad de forma conjunta con el responsable de seguridad de Ccomms.
- **Responsable de Seguridad**: Se encarga de la administración de la implementación de las prácticas de seguridad y de los procedimientos de seguridad, tanto de forma física como de forma lógica. Este debería encargarse de verificar que toda la documentación se halle accesible cuando sea requerida y se tenga correctamente enumerada, será, así mismo, el encargado de comprobar la coherencia de la documentación con los procedimientos, activos inventariados, etc.

11.9 REVISIONES DE SEGURIDAD

Ccomms se encarga periódicamente de la revisión de todos sus sistemas y aplicaciones implicadas en la gestión del servicio que tendrá una periodicidad anual y, en todo caso, cuando se produzca cualquier cambio relevante que afecte a los mismos.

Asimismo, la Política de Seguridad se revisará a intervalos planificados y como mínimo anualmente y, en todo caso si se producen cambios significativos en la organización con el objetivo de mantener la idoneidad, adecuación y eficacia de la misma.

12. PLAN DE CONTINGENCIA

Sin perjuicio de las medidas de seguridad aplicadas, la política, procedimiento y controles para la gestión de la Continuidad de Negocio están definidos en el procedimiento "CONTINUIDAD DE NEGOCIO" así como en una Instrucción Técnica.

El objetivo de ambos documentos es proteger los procesos críticos de negocio de los efectos derivados de fallos importantes o catastróficos de los sistemas de información, así como garantizar su oportuna reanudación. En ellos se detallan:

- Tipos de contingencias que pueden ocurrir y su nivel de gravedad.

- Medidas preventivas y reactivas.

- Procedimiento a seguir en la detección, tramitación, restauración y recuperación ante las posibles contingencias.

- Procedimiento de reevaluación tanto de las contingencias sufridas como del procedimiento seguido.

Aunque el sistema de creación de copias de seguridad independientes permite en la mayoría de supuestos la continuidad del servicio, no obstante, ante casos graves que pudieran afectar a la seguridad general del sistema, los servicios se suspenderán temporalmente, notificando a la mayor brevedad posible a los usuarios este extremo y, si fuera posible su estimación, la duración aproximada de la suspensión. Del mismo modo, se notificará a los usuarios su reanudación.

Ccomms ha establecido un Gabinete de Crisis cuyos integrantes son responsables de gestionar una situación de contingencia mayor estableciendo los mecanismos de recuperación y vuelta a la normalidad, así como la comunicación con las partes afectadas.

13. AUDITORÍAS DE CONFORMIDAD

13.1 FRECUENCIAS DE LAS AUDITORÍAS

Se realizará una auditoría al menos una vez al año, sobre Ccomms, para garantizar que su funcionamiento y operativa está adecuado con lo dispuesto en la presente DPC.

Se pueden llevar a cabo otras auditorías técnicas y de seguridad, según el procedimiento aprobado por Ccomms "AUDITORÍAS INTERNAS".

13.2 IDENTIFICACIÓN DEL AUDITOR

El auditor externo o equipo de auditores externos será seleccionado en el momento de la planificación de cada auditoría.

Cualquier empresa o persona contratada para realizar una auditoría de seguridad sobre Ccomms o alguno de sus servicios en concreto deberá cumplir con los siguientes requisitos:

- Adecuada y acreditada capacitación y experiencia en seguridad y procesos de auditoría de sistemas de información.

- Independencia a nivel organizativo de la autoridad de Ccomms.

El auditor externo o equipo de auditores externos además no deberán tener ninguna relación, actual o planificada, financiera, legal, o de cualquier otra clase que pueda derivar en un conflicto de intereses con Ccomms. Para poder cumplir con la normativa vigente en materia de protección de datos, y si el proceso de auditoría implicara el acceso a los datos de carácter personal, el auditor tendrá la consideración de Encargado de Tratamiento, en virtud de lo previsto en el artículo 28 del RGPD.

13.3 CRITERIOS DE AUDITORÍA

Sin perjuicio de verse ampliados por documentos de los servicios particulares ofrecidos por Ccomms, los aspectos cubiertos por una auditoria incluirán, al menos:

- Política de seguridad.
- Seguridad física de las instalaciones del servicio auditado.
- Seguridad lógica de los sistemas y servicios de Ccomms
- Evaluación tecnológica de los componentes del servicio.
- Administración de los servicios, así como seguridad en la misma.
- La presente DPC y políticas de servicios vigentes.
- Cumplimiento de las exigencias legales aplicables

13.4 PLAN DE ACCIÓN

La identificación de deficiencias en la auditoría dará lugar como medida inmediata a la adopción de medidas correctivas. Las autoridades competentes en la materia según lo definido por la legislación vigente en colaboración con el auditor será los responsables de la determinación de las mismas.

13.5 COMUNICACIONES DE RESULTADOS

El auditor externo o auditores externos comunicarán los resultados de la auditoría al Responsable de Seguridad de Ccomms y al Responsable de CertySign, así como a los responsables de las distintas áreas en las que se detecten no conformidades, y en su caso a la autoridad competente según lo determinado en la legislación vigente.

14. CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS PERSONALES

En general, existe el deber de confidencialidad respecto a la información que los empleados de Ccomms conozcan por razón de su puesto de trabajo. La información considerada como confidencial facilitada a Ccomms no será en ningún caso divulgada a terceros salvo que se encuentre amparada en los supuestos de requerimiento de colaboración con las instituciones competentes.

Se considera información del tipo “confidencial” toda la información de Ccomms que no se haya declarado expresamente como pública. En concreto, y sin perjuicio de que otro tipo de información pueda serlo también:

- Planes de continuidad de negocio y de emergencia.
- Información relativa a la operativa de operaciones y mantenimiento del servicio.
- Toda información relativa a las operaciones que lleve a cabo Ccomms.

- Toda información relativa a los parámetros de seguridad, control y procedimientos de auditoría.
- Toda la información de carácter personal proporcionada a Ccomms durante el proceso de registro de los suscriptores del servicio.
- La información de negocio suministrada por sus proveedores y otras personas con las que Ccomms tiene el deber de guardar secreto establecida legal o convencionalmente.
- Registros de transacciones, incluyendo los registros completos y los registros de auditoría de las transacciones.
- Y en general toda la información clasificada como "CONFIDENCIAL"

Se considera información pública, entre otros, los siguientes materiales:

- Declaración de Prácticas de Entrega Electrónica Certificada
- Condiciones Generales de Contratación
- Toda aquella información que sea considerada como "Pública"

14.1 PROTECCIÓN DE LA INFORMACIÓN PERSONAL

En cumplimiento de los requisitos establecidos en el Reglamento (UE) 2016/679 (en adelante, RGPD) y la Ley Orgánica 3/2018 de protección de datos personales y garantía en los derechos digitales (en adelante, LOPDGDD), Ccomms dispone de un Registro de Actividades de Tratamientos de datos de carácter personal en el que se encuentra el tratamiento necesario para la provisión y gestión del Servicio de Entrega Electrónica Certificada.

Con el objetivo de poder dar cumplimiento al servicio requerido por el usuario, Ccomms realiza un tratamiento de datos de carácter personal ajustado a las obligaciones recogidas en la normativa vigente de protección de datos de carácter personal y de acuerdo con su Política de Privacidad y Condiciones Generales de Contratación.

Asimismo, Ccomms está comprometido a prestar asistencia al Cliente en relación con el ejercicio de derechos, comunicación de una violación de datos, evaluación de impacto del tratamiento o realizar consultas previas a la Autoridad de Control.

Se informa al usuario de los siguientes aspectos relacionados con el tratamiento:

Los datos personales serán tratados por CUSTOMER COMMUNICATIONS TECKNALIA, S.L, con N.I.F. número B-86414000 y domicilio social sito en Leganés (28914 Madrid), Avda de la Recomba, núm. 12-14, inscrita en el Registro Mercantil de Madrid al Folio 92, Tomo 29.801, Hoja número M-536210, con la finalidad de poder prestar el servicio solicitado en los términos establecidos en la normativa vigente, en la

presente DPC y, en su caso, en las Condiciones Particulares alcanzadas entre los intervinientes y CUSTOMER COMMUNICATIONS TECKNALIA.

Fuera de los fines mencionados en el apartado anterior, no se llevará a cabo ningún otro tratamiento de datos, salvo que, previamente, se informe al usuario y se recabe su consentimiento o una norma permitiera el tratamiento previsto.

No obstante, lo anterior, y en previsión de lo dispuesto en el art. 21.2 de la Ley 34/2002 de Servicios de la Sociedad de la Información, cuando exista una relación contractual previa Ccomms podrá remitir al usuario comunicaciones comerciales por correo electrónico siempre que se refieran a productos o servicios similares a los que inicialmente fueron objeto de contratación. En cada una de las comunicaciones comerciales que así se realizaran se ofrecerá al destinatario la posibilidad de oponerse al tratamiento con este fin de un modo sencillo y gratuito.

Al momento de recabar los datos de carácter personal se informará del carácter obligatorio o facultativo de las respuestas. Solo será obligatorio proporcionar aquellos datos que, conforme al principio de calidad, resulten adecuados, pertinentes y no excesivos con respecto a la finalidad determinada. Debido a ello, su negativa a suministrarlos imposibilita la prestación del servicio.

El usuario se compromete a que toda la información que facilite sea exacta y veraz. Asimismo, deberá informar inmediatamente de cualquier actualización que sobre la misma tuviera que realizarse o cualquier error o inexactitud que detectase.

Los datos de carácter personal no serán objeto de cesión a terceras personas sin el previo consentimiento del interesado.

Lo dispuesto en este apartado no afecta al acceso a los datos por cuenta de terceros el cual se realizará conforme a lo dispuesto en la normativa de protección de datos.

Por otro lado, los datos personales que facilite directamente el interesado o por terceros forman parte de un fichero responsabilidad de Customer Communications Tecknalia, S.L. con la finalidad de gestionar y mantener los contactos y relaciones que se produzcan como consecuencia de la relación que mantiene con Customer Communications Tecknalia, S.L. La base jurídica que legitima este tratamiento, será la necesidad de gestionar una relación contractual o similar. Se deberán utilizar únicamente para la finalidad a la que se destina y no se permite transmitirlos a terceros. El plazo de conservación de estos datos vendrá determinado por la relación que mantenida entre el interesado y Ccomms.

Se informa al usuario de que estos datos podrán ser comunicadas al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de

las funciones que tiene atribuidas o a instituciones autonómicas con funciones análogas al Defensor del Pueblo o Ministerio Fiscal.

Para más información respecto al tratamiento de datos que realiza Ccomms, o para ejercer sus derechos de Acceso, Rectificación, Cancelación/Supresión, Oposición, limitación o portabilidad, el interesado puede ponerse en contacto con Ccomms enviando un escrito a la siguiente dirección: Avda. La Recomba 12 - 14. Pol. Industrial La Laguna. 28914 Leganés - Madrid, o mediante un correo electrónico al Delegado de Protección de Datos de Ccomms (dpo@customercomms.com), acompañando los documentos exigidos por la normativa.

No obstante, si el interesado piensa que su derecho puede haber sido vulnerado, puede realizar una reclamación ante la Agencia Española de Protección de Datos.

Ccomms ha adoptado todas las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos objeto de tratamiento y evitar su pérdida, sustracción, modificación, alteración o acceso no autorizado.

Las medidas implantadas dependen de la naturaleza de los datos gestionados y del nivel de seguridad que, debido a este motivo, les resulte aplicable. El conjunto de medidas de seguridad implantado será consecuencia del estado actual de la tecnología y objeto de adaptación conforme ésta evolucione.

15. TERMINOS Y CONDICIONES

El servicio de entrega electrónica certificada de Ccomms proporciona seguridad y confianza a la entrega de mensajes de forma electrónica entre las partes, produciendo evidencia del proceso de entrega, consistente en una declaración por parte de Ccomms de que un evento específico relativo al proceso de entrega ha sucedido en un momento dado. Dicha declaración será enviada por correo electrónico a cada una de las partes y quedará almacenada en el sistema donde las partes interesadas podrán acceder a ella previa solicitud al email soporte@certy-sign.com.

El plazo para que el destinatario puede disponer del contenido del usuario es de 10 (díez) días. Pasado dicho plazo, el mensaje dejará de estar disponible para la recepción del destinatario.

Las partes que confían en este servicio de entrega electrónica certificada pueden obtener información del servicio enviando un correo a soporte@certy-sign.com.

La información contenida en la declaración de Ccomms estará disponible para las partes y terceros que confían durante 15 años.

Disponibilidad del servicio

El servicio de entrega electrónica certificada de Ccomms estará disponible ininterrumpidamente 24 horas los 7 días de la semana.

Ccomms firmará con sus clientes un Acuerdo de Nivel de Servicio (SLA), relativos a tiempo de atención, calidad y disponibilidad de los servicios.

En la prestación de los servicios descritos en esta DPC, Ccomms garantiza que no operará de modo que se produzca algún tipo de discriminación.

Condiciones de contratación

Las tarifas y condiciones económicas del servicio de Entrega Electrónica Certificada se establecen en oferta comercial específica en cada caso. Las condiciones generales de contratación se encuentran en el documento "Condiciones generales de contratación de Grupo MailComms" publicado en la web del servicio https://comunicaciones-legales.customercomms.com/.

No obstante, Ccomms puede establecer marcos contractuales con clientes puntuales que particularicen estas condiciones para el escenario de colaboración establecido entre ambas partes.

Reclamaciones y resolución de conflictos

Ccomms pone a disposición de los interesados un formulario web que permite interponer reclamaciones, quejas o sugerencias para aquellas partes interesadas que deseen hacer llegar su disconformidad o sugerencia con algún aspecto del servicio de entrega electrónica certificada prestado. El acceso a dicho formulario se encuentra en la web del servicio con acceso a través de la siguiente url: https://comunicaciones-legales.customercomms.com/es/email-sms-formulario.php

Ccomms responderá en un plazo máximo de 30 días a cualquier reclamación que haya planteado el usuario de los servicios.

En caso de reclamaciones judiciales, se procederá según lo dispuesto en el apartado 17 de esta DPC.

16. APROBACION Y REVISION DE LA DECLARACIÓN DE PRÁCTICAS

Corresponde al Comité de Seguridad de Ccomms la aprobación de la presente DPC. Los cambios menores que se produzcan en la presente DPC podrán ser aprobados por la Dirección, y se comunicarán al Comité de Seguridad en la convocatoria siguiente.

Ccomms ha establecido un equipo de gestión responsable de la implantación de las prácticas de seguridad y organizativas requeridas para garantizar la confidencialidad, integridad y todo lo establecido en esta DPC.

Modificación de la DPC

La presente DPC podrá ser modificada por causas legales, técnicas o comerciales.

Cuando la DPC sea modificada, deberá ser notificada al Organismo de Supervisión.

Igualmente, los cambios que se realicen que puedan afectar de forma sustancial a los suscriptores del servicio o a terceros se notificarán haciéndolo público en la web del servicio https://comunicaciones-legales.customercomms.com/.

Los únicos cambios que pueden realizarse en esta DPC y que no requieren notificación son correcciones de estilo o tipográficas, cambios de edición o cambios en los contactos.

17. LEGISLACION Y JURISDICCION APLICABLE

Las relaciones entre Ccomms y los usuarios del servicio de Entrega Electrónica Certificada se regirán por la normativa española.

Las partes, con expresa renuncia a cualquier fuero propio que pudiera corresponderles, se someten a la Jurisdicción y Competencia de los Juzgados y Tribunales de Madrid para cualquier cuestión relativa a la interpretación, cumplimiento o ejecución del contrato establecido entre las partes.

A continuación, se referencia la legislación directamente aplicable:

- Reglamento (UE) 910/2014, del Parlamento y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Reglamento de Ejecución (UE) 2015/1502 de la Comisión, de 8 de septiembre de 2015 sobre la fijación de especificaciones y procedimientos técnicos mínimos

para los niveles de seguridad de medios de identificación electrónica con arreglo a lo dispuesto en el artículo 8, apartado 3, del Reglamento (UE) no 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

- Reglamento (UE) 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

- Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales.

- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.