DECLARACIÓN DE PRÁCTICAS DEL SERVICIO ELECTRÓNICO DE CONFIANZA DE ENTREGA ELECTRÓNICA CERTIFICADA

Documento	DPC- DECLARACION DE PRACTICAS DEL SERVICIO DE ENTREGA ELECTRÓNICA
Versión	1.0
Autor/es	
Aprobado por	Jaime Hortelano
Fecha de aprobación	21/01/2022
OID	1.3.6.1.4.1.53726.01.1

12362591E JAIME HORTELANO (R: B80440795)

Firmado digitalmente por 12362591E JAIME HORTELANO (R: B80440795)
Fecha: 2022.01.21 14:30:46 +01'00'

CMC

INDICE

HISTORIAL DE CAMBIOS		
Fecha	**Descripción**	**Versión**
16/06/2021	Primera Emisión	v.1.0

1. Introducción

Cognicase Managment Consulting S.L. (CMC en adelante) es una empresa dedicada a la consultoría de gestión, la tecnología y el outsourcing, que disponen de la tecnología propia para procesar, gestionar y analizar todo tipo de datos.

CMC presta los Servicios electrónicos de Confianza bajo la marca O2Certify, y bajo dicha marca se constituyó en Prestador de Servicios de Confianza conforme al Reglamento (UE) nº 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 y por el que se deroga la Directiva 1999/93/CE (en adelante Reglamento eIDAS).

Para realizar los servicios de confianza, CMC pone a disposición de sus clientes un conjunto de medios técnicos y organizativos que permiten a las partes intervinientes contar con la participación de un tercero proporciona la entrega segura y confiable de mensajes electrónicos entre las partes, produciendo evidencias electrónicas suficientes y jurídicamente eficaces mediante la aplicación de sellos de tiempo y firma electrónica que confirman su existencia y le dotan de integridad. Todas las evidencias se conservan durante el plazo legalmente establecido.

Para cada transacción gestionada, el servicio de entrega electrónica certificada de CMC genera un ACTA en formato electrónico (PDF) en el que recogen las evidencias electrónicas asociadas al proceso de entrega.

Por ello, este servicio proporcionado por CMC se puede definir, tal y como se recoge en el artículo 3 del Reglamento eIDAS como un servicio que permite transmitir datos entre partes terceras 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.

La presente Declaración de Prácticas del Servicio Electrónico de Confianza (en adelante DPC) recoge las normas y condiciones generales que presta CMC en relación con el Servicio de Entrega Electrónica Certificada.

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

El servicio ofrecido por CMC es el "modelo caja negra" que consiste en un sistema bajo responsabilidad de un único Proveedor de servicios de entrega electrónica certificada, y que no interopera ni se relaciona con otros proveedores de servicios de entrega electrónica.

El contenido de la presente Declaración de Prácticas de Certificación se realiza en cumplimiento con la legislación vigente y alineada con el Reglamento eIDAS. CMC 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.

2. Identificación

Los datos de identificación de CMC son:

- Razon Social: COGNICASE MANAGEMENT CONSULTING S.L.
- CIF: B80440795
- Domicilio Social: Avenida de San Luis, nº25, 28033 Madrid.
- Teléfono: 915 556 238
- Email: soporte@o2certify.com
- Nombre comercial: O2Certify
- Dominio: www.grupocmc.es/psc-3/

El presente documento y sus modificaciones serán publicadas en la página web del servicio: www.grupocmc.es/psc-3/

3. Comunidad de usuarios de los servicios de entrega electrónica certificada de CMC

3.1 Prestador del Servicio de Entrega Electrónica Certificada

El Prestador del Servicio de Confianza de Entrega Electrónica Certificada será COGNICASE MANAGMENT CONSULTING SL (en adelante CMC).

3.2 Operador de Verificación de Identidad

El Operador de Verificador de Identidad es aquella persona a la que CMC como Prestador de Servicio de Confianza encomienda la función de identificar fehacientemente y comprobar las circunstancias personales de los solicitantes del servicio (emisores), así como de la entrega de las claves de autenticación para poder acceder al mismo y realizar la emisión de sus comunicaciones.

La identificación y la entrega de claves de autenticación se realizarán en un entorno seguro y controlado.

3.3 Emisor

El emisor es la persona física o jurídica que emite la comunicación. El emisor será debidamente identificado por la plataforma del servicio de entrega electrónica certificada de CMC, de forma previa a la presentación en dicha plataforma de los datos de emisión. La identificación inicial del emisor, en caso del proceso de entrega electrónica, se realiza de forma presencial ante el Operador de Verificación de Identidad designado por CMC, y en ese acto se le entregan unas claves de autenticación para que el emisor pueda utilizar el servicio de entrega.

El emisor podrá también identificarse inicialmente mediante su certificado electrónico cualificado admitido en el servicio, y, una vez identificado, se le entregarán sus claves de autenticación para el acceso al mismo.

3.4 Destinatario

El destinatario es la persona física o jurídica a la que va dirigida la comunicación. El destinatario será contactado por CMC a través de un correo electrónico, donde se le comunica la puesta a disposición de una documentación o información por parte del emisor, al que puede acceder a través de la url de acceso que se comunica en el mismo correo. El destinatario deberá identificarse ante el servicio de entrega electrónica certificada de CMC de forma fehaciente con su certificado electrónico emitido por un Prestador de Servicios de Certificación Cualificado (cuya relación de Prestadores admitidos se publicará en la página web de CMC

www.grupocmc.com/psc) antes de que CMC ponga a su disposición la información emitida por el emisor.

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

3.5 Terceras Partes

Las Terceras Partes son aquellas partes que confían en los servicios prestados por CMC y en las evidencias generadas como resultado de la ejecución de los servicios.

Las terceras partes deberán tener en cuenta los términos y condiciones del servicio así como las limitaciones establecidas para el mismo.

Las terceras partes podrán acceder a la información de los servicios, incluyendo las actas del servicio de entrega electrónica certificada que deseen comprobar, y podrán verificar la autenticidad de la misma, en caso de que se le haya entregado en papel, a través de la comprobación del código seguro de verificación que está incorporado al documento, cuyo acceso se encuentra en la página web de CMC, en el apartado: https://o2edelivery.grupocmc.es/o2notify/#/

En todo caso, si el acta se presenta en formato electrónico, las terceras partes deberán comprobar la validez de la firma, bien con herramientas facilitadas por aplicaciones como ADOBE o VALIDe u otras, o bien mediante el propio código seguro de verificación (CSV) incorporado al documento. Si el certificado electrónico con el que se firmó el acta hubiera caducado, es posible que la aplicación de validación emita un mensaje de error en la firma; en este caso, las terceras partes deberán comprobar que la propia firma tiene incorporada la información de consulta al servicio de revocación del certificado y que, en el día de la firma, el certificado electrónico estaba vigente. Esta información se obtiene en el apartado de "Detalles del certificado".

3.6 Otros Prestadores de Servicios Cualificados intervinientes

CMC utiliza, para la Prestación del Servicio de Entrega Electrónica Certificada, los servicios de certificación cualificados de otros prestadores de servicios de confianza. Dichos prestadores, en la fecha de publicación de esta DPC son los siguientes:

- UANATACA: Es el Prestador de Servicios de Certificación que emite el Sello Electrónico de Entidad a CMC de forma centralizada, para la realización del sello electrónico cualificado en remoto.

- UANATACA es también Prestador de Servicios de Sellado de Tiempo Cualificados, y como tal emite los sellos de tiempo que se incorporan a las evidencias recabadas por CMC en el servicio de entrega electrónica certificada.

4. 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 (Reglamento eIDAS)
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".

5. Definiciones y Acrónimos

5.1 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 CMC.
- 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 Ley de Firma Electrónica 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 intervienen en una operación y hacen uso de los servicios proporcionados por CMC, aceptando los términos y condiciones en la que se prestan.
- Validación: Procedimiento a través del cual se verifica la validez de la firma empleada.

5.2 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
- LOPDGDD: Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales,
- LSEC: Ley 6/2020, de 11 de noviembre, reguladora de determinados servicios electrónicos de confianza

- 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

6. Requerimientos de Conformidad

CMC declara que la presente DPC es aplicable al Servicio 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 (Reglamento eIDAS).

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

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

- su política de seguridad de la información, alineada con las normas jurídicas aplicable.
- la política de servicio entrega electrónica certificada definida en esta Declaración de Prácticas de Certificación.
- los requerimientos organizativos definidos en el apartado 12.1 de esta DPC.
- 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 apartados 12 y 15 de esta DPC, incluyendo los requisitos organizativos.
- 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.

7. Roles de Confianza

Los roles de confianza de CMC son aprobados por el Consejero Delegado de COGNICASE MANAGMENT CONSULTING S.L

Las funciones que deben cumplir los roles de confianza son las siguientes:

7.1 Administrador de Sistemas

Deberá implementar, configurar, monitorizar, documentar y asegurar el correcto funcionamiento del sistema informático.

Se encargará de la administración de la plataforma de CMC, así como de la configuración de accesos a la misma.

Cumplirá con lo establecido en las Políticas definidas bajo los Sistemas de Gestión implantados en Grupo CMC y colaborará en la consecución de los objetivos definidos.

7.2 Operador de sistemas

Realiza la puesta en marcha y el cierre del sistema informático y máquinas auxiliares.

Controla y registra los datos de utilización del sistema, introduce información en el sistema para su posterior análisis o procesamiento, realiza la conservación de datos mediante la impresión de documentos y copias de seguridad.

Cumplirá con lo establecido en las Políticas definidas bajo los Sistemas de Gestión implantados en Grupo CMC y colaborará en la consecución de los objetivos definidos.

7.3 Responsable de Seguridad

Colabora en la elaboración, comunicación y seguimiento de un plan de seguridad para la mejora continua.

Mantiene las políticas y estándares de seguridad de la organización

Documenta y gestiona toda la documentación asociada a la implantación y certificación del SGSI

Colabora en la identificación de objetivos de seguridad y métricas e indicadores asociados

Participa en la comunicación y sensibilización con los empleados en los aspectos básicos de seguridad y de las políticas de la compañía

Es el responsable de hacer cumplir las políticas y las normas de seguridad.

Colabora en la realización de auditorías periódicas

Se responsabiliza de establecer las fechas para la ejecución de análisis de vulnerabilidades, ensayos y pruebas de los planes de continuidad del servicio, así como las auditorias de los sistemas de información.

Participa en la evaluación periódica de vulnerabilidades en el control e investigación incidentes de seguridad, dejando siempre registro de las incidencias y de las acciones realizadas.

Cumple con lo establecido en las Políticas definidas bajo los Sistemas de Gestión implantados en Grupo CMC y colabora en la consecución de los objetivos definidos.

7.4 Auditor

Comprueba la existencia de toda la documentación requerida y enumerada.

Comprueba la coherencia de la documentación con los procedimientos, activos inventariados, etc.

Comprueba el seguimiento de incidencias y eventos

Comprueba la protección de los sistemas (explotación de vulnerabilidades, logs de acceso, usuarios, etc.).

Comprueba las alarmas y elementos de seguridad física

Comprueba la adecuación a la normativa aplicable

7.5 Oficial de Verificación de la Identidad

Es la persona encargada de la verificación inicial de la identidad del emisor y/o del destinatario, asegurándose de que se cumplen las condiciones requeridas para la identificación, así como los procesos establecidos. Igualmente es el encargado de recabar el consentimiento del usuario para el tratamiento de sus datos.

8. Integridad y confidencialidad del contenido del usuario

CMC garantiza la adecuada disponibilidad, integridad y confidencialidad del contenido del usuario cuando utiliza el servicio de Entrega Electrónica Certificada, firmando el contenido con un certificado cualificado de sello electrónico centralizado emitido por

un Prestador de Servicios de Confianza Cualificado e instalado en su HSM homologado como dispositivo seguro de creación de firma.

Además, CMC 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 algoritmos RSA.

CMC 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.

En ningún caso el contenido del usuario será modificado por el servicio de Entrega Electrónica Certificada, una vez incorporado al servicio.

9. Identificación y autenticación de los usuarios

9.1 Verificación de la identidad inicial del emisor

CMC verificará la identidad inicial del emisor por uno de los siguientes métodos:

1. Mediante un certificado cualificado de firma electrónica.

2. Mediante presencia física ante el Operador de Verificación de la Identidad de CMC, diferenciando:

    a. Si el suscriptor es una persona natural, deberá identificarse mediante su documento de identidad (DNI, NIE, pasaporte o cualquier otro documento admitido en derecho).

    b. Si el suscriptor es una persona jurídica, el solicitante será su representante legal o voluntario con poder bastante para representar a la persona jurídica, debiendo aportar en el momento de su identificación, el CIF de la entidad, el poder de representación en vigor y su documento de identidad.

3. Dicha verificación de la identidad permanecerá vigente con un período máximo de 5 años desde la identificación, o hasta que sea revocada.

4. Será necesario que, en el momento de la identificación, el usuario aporte una cuenta de correo electrónico propia y su número de móvil.

5. Una vez realizada la verificación inicial, el sistema O2Certify de CMC asocia un identificador único a cada suscriptor del servicio, para que se pueda autenticar ante el mismo.

6. Cada vez que el usuario quiera enviar una comunicación, será necesaria su autenticación mediante las claves que se le generaron, y la inclusión de un código de un solo uso (OTP) que recibirá a través de SMS y que tiene la condición de doble factor de autenticación. Una vez autenticado en el servicio, cada envío que quiera realizar el usuario generará un nuevo OTP que deberá ser incluido previamente a la realización del mismo.

9.2 Identificación del destinatario y entrega del contenido de usuario

CMC entregará el contenido del usuario al destinatario únicamente después de haberle identificado de forma exitosa.

La identificación del destinatario esta basada en el uso de un certificado cualificado. Dicho certificado deberá estar emitido por alguno de los Prestadores de Servicios de Certificación cualificado que la plataforma admita, y que se encuentran publicados en la página web del servicio. Igualmente, la relación de Prestadores de servicios de certificación admitidos serán comunicados al destinatario en el correo electrónico de puesta a disposición de la documentación.

El mensaje y la documentación adjunta estará disponible para la descarga por parte del destinatario, previa su identificación, por un plazo de 15 días.

Las pruebas de identificación del emisor y del destinatario serán conservadas y protegidas, según se expone en el punto 11 de esta DPC.

10. Referencias de tiempo

Las evidencias sucedidas en la utilización del servicio serán selladas mediante un sello electrónico de tiempo cualificado, emitido un Prestador de Servicios de Confianza cualificado en dicho servicio. Igualmente se sellará con un sello de tiempo cualificado el acta final, donde se recopilan todas las evidencias sucedidas en el servicio durante el envío y recepción.

CMC comprobará que el certificado de sello de tiempo utilizado se encuentra vigente, es decir, que no ha caducado ni ha sido revocado.

CMC comprobará, al menos una vez al año, que el Prestador de Servicios de Sello de tiempo continúa cualificado, realizando una interpretación de la TSL conforme con lo indicado por la Comisión Europea.

11. Eventos y evidencias

11.1 Registro de eventos

CMC registrará los eventos producidos en el servicio de entrega electrónica certificada. CMC conservará obligatoriamente los siguientes eventos:

- datos de identificación de emisor y destinatario; incluidos los eventos e información de verificación de la identidad.
- datos de autenticación de emisor y destinatario; incluidos los eventos e información de verificación de la autenticidad.
- 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. Ello se realiza mediante el sellado de la evidencia en el momento de la entrega del contenido por parte del emisor al servicio, mediante un sello de entidad e incorporando un sello de tiempo.
- una referencia o una recopilación completa del contenido del usuario presentado;
- tokens de sello de tiempo correspondientes a la fecha y hora de envío, consignación y entrega o rechazo en la entrega, según proceda.

11.2 Eventos registrados por el Servicio de Entrega Electrónica Certificada

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

a. ACEPTACION DEL ENVIO DE LA NOTIFICACION POR PARTE DEL SERVICIO: el emisor, debidamente identificado, ha presentado el contenido del usuario ante la plataforma O2Certify de CMC como Prestador del Servicio de Entrega Electrónica, y éste lo ha aceptado para a su vez intentar hacer la entrega a su destinatario. Todo ello produce la evidencia de Aceptación del envió, que se produce en el momento indicado en dicha evidencia.
En el acta final del servicio esta evidencia se refleja como: ENVIO ACEPTADO

b. RECHAZO DEL ENVIO DE LA NOTIFICACION POR PARTE DEL SERVICIO: el emisor, debidamente identificado, ha presentado el contenido del usuario ante la plataforma O2Certify de CMC, y éste lo ha rechazado. Todo ello produce la evidencia de Aceptación del envío, que se produce en el momento indicado en dicha evidencia.

En el acta final del servicio esta evidencia se refleja como: ENVIO RECHAZADO

B. Eventos de la notificación del contenido al destinatario:

a. PUESTA A DISPOSICION DEL CONTENIDO AL DESTINATARIO: Se produce la evidencia que el Servicio de entrega electrónica certificada de CMC ((O2Certity) ha enviado una notificación al destinatario, en un momento dado, comunicando la puesta a su disposición de un mensaje, y solicitando su aceptación.

En el Acta final del servicio, el estado que alcanza este evento es: CORREO ENVIADO

b. FALLO EN LA NOTIFICACIÓN PARA LA ACEPTACIÓN: se produce la evidencia que el Servicio de entrega electrónica certificada de CMC 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, que queda establecido en 15 días.

En el Acta final del servicio, el estado que alcanza este evento es: CORREO FALLIDO

C. Eventos de aceptación/rechazo del envío por parte del destinatario

a. ACEPTACIÓN DEL ENVÍO POR EL DESTINATARIO: 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 el Acta final del servicio, el estado que alcanza este evento es: CONTENIDO ACEPTADO POR EL DESTINATARIO

b. RECHAZO DEL ENVÍO POR EL DESTINATARIO: 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 el Acta final del servicio, el estado que alcanza este evento es: CONTENIDO RECHAZADO POR EL DESTINATARIO

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, que se funcionalmente establece en 15 días.

En el Acta final del servicio, el estado que alcanza este evento es: ENVIO CADUCADO

D. Eventos del ERDS en destino

a. ENTREGA DEL CONTENIDO DEL USUARIO AL DESTINATARIO: se produce la evidencia de que el contenido del usuario ha cruzado con éxito la frontera del servicio de entrega electrónica certificada de CMC en un momento dado, hacia la aplicación del destinatario y fue entregada con éxito, previa autenticación del destinatario.

   En el Acta final del servicio, el estado que alcanza este evento es: CONTENIDO ENTREGADO

b. FALLO EN LA ENTREGA DEL CONTENIDO DEL USUARIO: El contenido del usuario no ha cruzado con éxito la frontera del servicio de entrega electrónica certificada de CMC, hacia la aplicación del destinatario, debido a errores técnicos o por caducidad del periodo de tiempo para acceder al contenido por parte del destinatario.

   En el Acta final del servicio, el estado que alcanza este evento es: ENTREGA FALLIDA

La plataforma O2Certify conserva todas estas evidencias, que serán incorporadas al Acta final emitida y sellada por CMC con un certificado de sello electrónico cualificado y un sello de tiempo igualmente cualificado. Este documento quedará a disposición de las partes y terceros interesados durante todo el plazo de conservación. Dicha Acta Final se enviará por correo electrónico al emisor y, en su caso, al destinatario, y quedará a disposición de los usuarios en el portal del servicio de entrega electrónica certificada de CMC durante un año. Las evidencias particulares de envío y recepción de la notificación siempre estarán a disposición del emisor mediante la solicitud al correo psc@grupocmc.es.

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

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

12. Obligaciones de las partes

12.1 Obligaciones de CMC como Prestador del Servicio

CMC, actuando como Prestador del Servicio de Confianza se obliga a:

- Prestar el servicio conforme a lo dispuesto en la presente Declaración de Prácticas de Certificación.
- Publicar toda la información relevante del servicio que deba ser conocida, como las características de la prestación del servicio, las obligaciones que asumen sus suscriptores y partes usuarias y los límites de responsabilidad.
- Utilizar la tecnología adecuada para proteger de manera fiable todos los datos de sus clientes, así como los registros de actividad y auditoria.
- Prestar el servicio de forma diligente, garantizando que el servicio está adecuado a su cualificación.
- Proporcionar el acceso ininterrumpido al servicio, y comunicar a sus usuarios con la suficiente antelación la no disponibilidad del sistema en caso de realizar procesos de modificación, mejora o mantenimiento que impliquen una paralización del mismo.
- Garantizar la integridad, confidencialidad y disponibilidad del contenido del usuario, dentro de la plataforma O2Certify.
- Conservar la información relativa al servicio de entrega electrónica certificada durante 15 años desde la finalización del servicio prestado.
- Notificar a las partes las incidencias en el servicio de O2Certify que puedan afectarles.
- Atender las solicitudes, consultas, quejas y reclamaciones de clientes y terceros en un plazo razonable.
- Notificar al Órgano Supervisor cualquier modificación sustancial producida en el servicio.

- Notificar al Órgano Supervisor, en un plazo de 24 horas, la violación de seguridad con impacto significativo en el servicio electrónico de confianza.

- Notificar a la Agencia Española de Protección de Datos las violaciones de seguridad que afecten a datos personales, en un plazo máximo de 72 horas desde que se tiene conocimiento del mismo.

- Llevar a cabo las auditorias periódicas necesarias para asegurar al adecuación y cumplimiento de la normativa aplicable, tanto interna como externa.

12.2 Obligaciones de los usuarios del servicio

Tanto el emisor como el destinatario tendrán las obligaciones siguientes:

- Deberán conocer y aceptar lo dispuesto en la presente DPC, las condiciones, responsabilidades y limitaciones del servicio y, en su caso, lo dispuesto en el contrato de prestación del servicio.

- Deberán comunicar a CMC cualquier incidente de seguridad, fallo o situación anómala relativa al servicio de O2Certify, en el momento que lo identifique.

- Deberán validar las firmas y sellos electrónicos que se han incorporado en las Actas de evidencias del servicio.

- El emisor deberá proporcionar a CMC información veraz, completa y exacta para la prestación del servicio de entrega electrónica certificada, incluidos los datos de los destinatarios sin errores y actualizados.

- El emisor deberá comunicar sin demora cualquier modificación de las circunstancias que incidan en la prestación del servicio de O2Certify.

12.3 Obligaciones de los proveedores

Los proveedores de servicios que puedan tener alguna actuación en el servicio de entrega electrónica certificada de CMC, como los Prestadores de servicios de certificación que emitan los certificados electrónicos y los sellos de tiempo, deberán cumplir las siguientes obligaciones:

- Proporcionar a CMC los certificados digitales necesarios para firmar o sellar electrónicamente las evidencias, garantizando que son cualificados.

- Custodiar de forma diligente los certificados cualificados que se alojen en las instalaciones del Prestador del Servicio de Confianza.

- Comunicar a CMC cualquier cambio de condición en sus certificados vigentes.

- Proporcionar a CMC los sellos de tiempo necesarios para sellar temporalmente los eventos y las actas finales, garantizando que el certificado que los emite es cualificado.

12.4 Obligaciones de Terceras Partes confiantes

Las personas físicas o jurídicas que confíen en el servicio prestado en O2Certify por CMC deberán:

- Conocer las limitaciones de uso (si las hubiera) del servicio, según la presente DPC, así como los términos y condiciones del servicio.

- Cumplir con lo dispuesto en la normativa aplicable.

- Reportar tan pronto como sea posible, a CMC cualquier incidente relacionado con el servicio, que tenga conocimiento.

- Validar las firmas y sellos electrónicos que se han incorporado en las Actas de evidencias del servicio.

12.5 Responsabilidades

CMC 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, CMC ha suscrito un seguro de responsabilidad civil de 1.500.000 € (un millón quinientos mil 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.

12.5.1 LIMITACIONES DE RESPONSABILIDAD

CMC, en el ámbito de la prestación del servicio de entrega electrónica certificada cualificada será responsable en caso de incumplimiento de las obligaciones contenidas en la presente DPC y en la legislación aplicable.

CMC no asumirá responsabilidad alguna respecto de:

- Los daños y perjuicios ocasionados en caso de fuerza mayor, caso fortuito o imprevisibles o que, siendo previsibles no se hayan podido evitar.

- Los actos u omisiones realizados por el Cliente sin respetar lo establecido en esta DPC o en la legislación aplicable siendo éste quien asumirá todos los daños y

perjuicios que se pudieran ocasionar. por uso inadecuado, indebido o fraudulento, siendo de exclusivo riesgo del Cliente.

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

- CMC no será responsable por los daños y perjuicios si el destinatario actúa de forma negligente. Proporcionar a CMC los sellos de tiempo necesarios para sellar temporalmente los eventos y las actas finales.

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

- No responderá por ataques externos causados a los algoritmos criptográficos, siempre que haya aplicado la diligencia debida según el estado de la técnica, y hubiere actuado conforme a lo dispuesto en la legislación aplicable y en la presente DPC.

13. Terminación del servicio

En el caso de que CMC cese en la prestación del servicio cualificado de entrega electrónica certificada, realizará las siguientes acciones para la ejecución de la terminación:

- Notificará a los usuarios, clientes y aquellas personas físicas y jurídicas con las que CMC mantenga una relación, con una antelación mínima de 2 meses, mediante correo electrónico que conste en su base de datos, y si no fuera posible, mediante publicación en su página web.

- Notificará al Organismo de Supervisión español, tanto el cese de la actividad como todas las circunstancias relacionadas con el cese, a través de un escrito presentado por Registro electrónico administrativo.

- 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.

- CMC podrá firmar un acuerdo de transferencia del servicio de confianza de ERDS con otro proveedor del servicio de Entrega electrónica certificada, en caso de cese del mismo siguiendo las pautas descritas para la transferencia en el Plan de Cese del Servicio.

- El prestador del servicio de confianza con el que se llegue a un acuerdo deberá estar cualificado, y asumirá las obligaciones de mantenimiento y custodia de las actas del servicio, así como evidencias y eventos registrados, durante el plazo de tiempo que se hubiera. En caso de no llegar a un acuerdo con otro Prestador de Servicios de Confianza, esta información podrá ser mantenida por Grupo CMC

en caso de que la empresa continúe con el resto de actividades o se depositará ante notario y se informará a los interesados y al organismo supervisor, en todo caso, para que sirvan de prueba en los procedimientos legales y para garantizar la continuidad de servicio.

- CMC mantendrá disponible la clave pública de su certificado de sello electrónico cualificado a las partes de confianza, durante el plazo que sea necesario.

CMC cuenta con un Plan de Cese del Servicio de Entrega Electrónica Certificada, reflejado en el documento "Plan de Cese" de carácter interno.

14. Controles de seguridad

14.1 Sede e instalaciones y medidas de seguridad físicas y ambientales

CMC tiene sus oficinas en Avenida de San Luis, nº25, 28033 Madrid.

Se cuenta con un Centro de Procesos de Datos Principal del servicio que se encuentra ubicado en un país de la Unión Europea.

Además, se cuenta con un Centro de Procesos de Datos de Respaldo del servicio que se encuentra ubicado en un país de la Unión Europea.

El CPD Principal y el CPD de Respaldo del servicio cumplen con la normativa aplicable de protección de datos personales.

El CPD Principal y CPD de Respaldo del servicio se someten a auditorías de terceros independientes para probar la seguridad y privacidad de los datos, para lo cual cuenta con las siguientes certificaciones de calidad, técnicas y organizativas:

- ISO 27001
- SOC 2, SOC 3
- PCIDSS

El CPD Principal y CPD de Respaldo cuenta con un modelo de seguridad física por capas y cuenta con:

- Tarjetas electrónicas de acceso, alarma, barreras de acceso de vehículos, cercado perimetral, detector de metales, acceso mediante datos biométricos.
- El suelo cuenta con láser de haz de detección de intrusos.
- Monitoreo del interior y del exterior por cámaras de alta resolución que pueden detectar y rastrear los intrusos.
- Los registros de acceso, los registros de actividad y filmación de las cámaras están disponibles en caso de que ocurra un incidente.

- Se encuentran vigilados por guardias de seguridad de forma rutinaria con experiencia y formación adecuada.
- El acceso a la sala de proceso sólo es posible a través de un corredor de seguridad que implementa el control de acceso de múltiples factores mediante tarjetas de seguridad y datos biométricos. Sólo los empleados autorizados con roles específicos pueden entrar.
- Cuenta con sistemas de energía y aire acondicionado adecuados para garantizar un entorno operativo fiable.
- Dispone de medidas necesarias para minimizar los riesgos derivados de los daños por agua.
- Dispone de sistemas de detección automática de incendios.

CMC ha aprobado el procedimiento "SEGURIDAD FÍSICA Y DEL ENTORNO" 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.

14.2 Seguridad lógica, controles de acceso

Se han implantado procesos de gestión del control de acceso lógico. Cada perfil tiene asignado su acceso necesario para realizar sus funciones.

CMC ha elaborado un procedimiento interno donde se definen controles aplicados.

14.3 Clasificación de la información y gestión de activos documentos

CMC tiene un procedimiento denominado "CLASIFICACIÓN DE LA INFORMACIÓN Y GESTIÓN DE ACTIVOS", donde se detalla cómo está clasificada la información referente al servicio así como la gestión de activos dentro de la organización.

14.4 Copias de respaldo y procedimiento de recuperación

Se realizan copias de seguridad con una periodicidad diaria, y son almacenadas en un lugar seguro.

Existe un Procedimiento recuperación de datos implantado que garantiza que, en caso de fallo del sistema con pérdida total o parcial de los datos de los ficheros se pueden reconstruir los datos de los ficheros al estado en que se encontraban en el momento del fallo.

14.5 Medidas de seguridad en operaciones y comunicaciones

CMC tiene aprobada una Política de Seguridad, que debe conocer todo el personal y es de obligado cumplimiento, donde se establece el compromiso con la seguridad de la información, a través de reglas, y protocolos de actuación que velan por la misma.

Además, cuenta con un procedimiento de Seguridad en las comunicaciones en el que se detalla los controles implementados y se revisan de manera periódica cada 3 meses para detectar posibles vulnerabilidades.

14.6 Procedimientos de auditoría de seguridad

CMC se compromete a realizar, al menos, una auditoría interna anual en el servicio de entrega electrónica certificada.

CMC tiene un procedimiento donde se detallan los procesos y controles para la revisión y mejora continua de su plataforma O2Certify.

CMC realiza trimestralmente un análisis de vulnerabilidades de todos los sistemas de red del servicio de entrega electrónica certificada.

CMC realiza un test de penetración anual en el servicio de entrega electrónica certificada.

14.7 Controles de personal

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: "PROCEDIMIENTO DE ROLES Y FUNCIONES".

CMC O2 se encuentra incluido dentro de CMC (Grupo CMC), siendo uno de sus servicios y cuenta con el siguiente esquema organizativo específico:

- Responsable del servicio: encargado de la modificación del presente documento, de la organización, supervisión y control y gestión del servicio, negociar las condiciones del servicio con el cliente y reportar con la periodicidad adecuada el funcionamiento del mismo tanto al cliente como a la dirección de CMC O2. Supervisar y garantizar la adecuación de los medios técnicos, organizativos y de personal del servicio. Procurar la adecuación del personal a las necesidades del servicio en cuanto a experiencia, conocimientos y requisitos de formación.

- Operadores de Sistemas: responsables de la gestión del día a día del sistema (Monitorización, backup, recovery,…)
- Técnicos de soporte: responsables de la gestión del día a día de las incidencias del servicio reportadas por los clientes.
- Auditor interno: encargado de realizar las auditorías internas del servicio.
- Responsable de Compliance, encargado de supervisar y actualizar el cumplimiento de normativas y regulaciones aplicables al servicio.

Existe procedimiento de actualización de conocimientos del personal afectado ante cambios tecnológicos, introducción de nuevas herramientas o modificación de procedimientos operativos. Ante cambios organizativos y de documentos relevantes se llevará a cabo sesiones formativas.

14.8 Plan de continuidad del servicio

Se dispone de un procedimiento de contingencia que define las acciones a realizar, recursos a utilizar y personal a emplear en el caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos y los servicios de certificación prestados por CMC.

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 "GESTION DE CONTINUIDAD"

El objetivo de esta Política es establecer las directrices de la estrategia de contingencia ante incidentes o desastres en los sistemas que soportan los procesos de negocio de CMC. Dicha política incluirá planes, procedimientos y medidas que permitan la continuidad o el restablecimiento de la operatividad de sistemas de TICs ante un incidente o desastre. La continuidad en sistemas incluye generalmente uno o más de los siguientes enfoques para restablecer servicios interrumpidos:

- Restableciendo las operaciones en una ubicación alternativa.
- Recuperar las operaciones utilizando sistemas alternativos.
- Ejecución de algunos o todos los procesos de negocio afectados utilizando medios manuales (sin sistemas de TICs). Esta opción sólo es aceptable para interrupciones muy cortas.
- Adopción de medidas de prevención de incidentes y desastres.

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.

14.9 Revisión periódica de la seguridad

CMC revisa periódicamente todos sus sistemas y aplicaciones implicados en la gestión del servicio con una periodicidad anual y, en todo caso, cuando se produzca cualquier cambio relevante que provoque un incidente de seguridad que afecte a los mismos.

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

15. Auditorías de conformidad

15.1 Identificación del auditor

Para la evaluación de la conformidad del servicio de entrega electrónica certificada es necesaria la selección de una empresa auditora homologada por ENAC para la realización de este tipo de auditorías, denominados CAB (Conformity Assestment Body).

CMC tiene que someterse a una auditoria bienal donde se evalúa de nuevo la conformidad con las normas relativas al servicio de confianza cualificado. Se someterá el año intermedio a una auditoria de vigilancia y seguimiento. El auditor externo será seleccionado en el momento de la planificación de cada auditoría.

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 CMC.

15.2 Plan de acciones correctivas

Cualquier deficiencia que se identifique en la auditoria provocará un plan de acción correctiva, que determinará su corrección.

15.3 Comunicaciones de resultados

Los resultados de la auditoria serán comunicados por el auditor al responsable del servicio O2Certify y a las áreas afectadas, y su caso a la autoridad competente según lo que determine la legislación vigente.

15.4 Frecuencias de las auditorías

Se realizará una auditoría anual, sobre el servicio de entrega electrónica certificada de CMC, 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 CMC "PROCEDIMIENTO DE AUDITORÍAS".

16. PROTECCION DE DATOS PERSONALES

En cumplimiento de los requisitos establecidos en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, "RGPD") y a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, "LOPDGDD") CMC está comprometido con la privacidad y la protección de datos de carácter personal, realizando el tratamiento de datos a los que tiene acceso respetando en todo caso las obligaciones recogidas en la normativa vigente.

El responsable de los datos personales suministrados es COGNICASE MANAGEMENT CONSULTING S.L. con CIF: B80440795 y domicilio social en la Avenida de San Luis, nº25, 28033 Madrid, 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, los términos y condiciones establecidos entre CMC y los intervinientes del servicio.

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. En caso de que el usuario no consienta el tratamiento de los datos obligatorios, 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 sin el previo consentimiento del interesado.

Se informa al usuario de que sus datos podrán ser comunicados 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.

También podrán ser comunicados a empresas del Grupo CMC así como a terceros en tanto en cuanto ésta resultare necesaria para el desarrollo, ejecución y control de los servicios contratados.

El interesado puede ejercer los derechos de acceso, rectificación, oposición, supresión, limitación al tratamiento y portabilidad de los datos de carácter personal, solicitándolo por correo electrónico en la dirección psc@grupocmc.es bajo el Asunto "Ejercicio de Derechos en el ámbito de protección de datos" y acompañando los documentos de identidad. El interesado puede reclamar ante la Agencia Española de Protección de Datos si cree que su derecho a la protección de datos personales puede haber sido vulnerado.

CMC conservará durante, al menos, 15 años, conforme establece la normativa de servicios electrónicos de confianza, o un tiempo superior si así lo exigiera normativa sectorial aplicable.

CMC, como Responsable del tratamiento, ha adoptado todas las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos objeto de tratamiento, dependiendo de la naturaleza de los datos gestionados y el nivel de seguridad que resulte necesario aplicar.

En la prestación del servicio de entrega electrónica certificada, y respecto de los datos transmitidos por cuenta del emisor al destinatario, CMC actúa como Encargado del tratamiento, y por ello tomará todas las medidas organizativas y técnicas necesarias para garantizar el nivel de seguridad adecuado, pudiendo incluir entre otras, las siguientes medidas:

- La capacidad de asegurar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y de los servicios de tratamiento.
- La seudonimización y el cifrado de los datos personales.
- La posibilidad y capacidad para restablecer el servicio, la disponibilidad y el acceso a los datos personales de forma oportuna en el caso de cualquier incidente que se produzca.
- La posibilidad de realizar pruebas y evaluar de forma periódica la eficacia de las medidas tomadas para garantizar la seguridad en el tratamiento de los datos personales.

17. CLASIFICACION DE LA INFORMACION

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

- Toda información relativa a los parámetros de seguridad, control y procedimientos de auditoría.

- Toda la información de carácter personal proporcionada a CMC durante el proceso de registro de los suscriptores del servicio.

- La información de negocio suministrada por sus proveedores y otras personas con las que CMC tiene el deber de guardar secreto establecida legal o convencionalmente.

- Planes de continuidad de negocio.

- Información relativa a la operativa de operaciones y mantenimiento del servicio.

- Registros de transacciones.

- Y en general toda la información clasificada como "CONFIDENCIAL".

INFORMACION PUBLICA: Se considera información pública, entre otros:

- La Declaración de Prácticas de Entrega Electrónica Certificada.

- Los Términos y condiciones del servicio.

- Política de Privacidad de CMC.

- Política de cookies.

- Toda aquella información que sea considerada como "Pública".

18. Términos y condiciones del servicio

Como se definió en la introducción de la presente DPC, para realizar el servicio de entrega electrónica certificada, CMC pone a disposición de sus clientes un conjunto de medios técnicos y organizativos que permiten a las partes intervinientes contar con la participación de un tercero proporciona la entrega segura y confiable de mensajes electrónicos entre las partes, produciendo evidencias electrónicas suficientes y jurídicamente eficaces mediante la aplicación de sellos de tiempo y firma electrónica que confirman su existencia y le dotan de integridad.

El resultado final es la generación de un Acta de O2Certify, donde CMC certifica las evidencias producidas durante el proceso de entrega electrónica, que han sido selladas electrónicamente, dotándolas de integridad, e incluyendo un sello de tiempo certificando la fecha y hora de su producción. Dicho Acta se encuentra igualmente sellada con un sello de CMC, así como con sello de tiempo.

El Acta queda en la plataforma de O2Certify y las partes interesadas podrán acceder a ella con un plazo de 1 año desde la generación de la misma.

Las partes interesadas podrán solicitar el Acta generada del servicio (que incluye todos los eventos producidos durante el servicio) en cualquier momento, con posterioridad a la finalización del servicio, enviando un correo electrónico a: psc@grupocmc.es

La información será conservada por CMC, como prestador de servicios de confianza, durante 15 años.

Los términos y condiciones del servicio de Entrega Electrónica Certificada se encuentran publicadas en la web www.grupocmc.es/psc-3/ y disponibles permanentemente.

CMC puede establecer acuerdos y contratos con sus clientes, que generen condiciones particulares entre las partes, siempre que no afecte a los términos y condiciones establecidos en la presente DPC.

Disponibilidad del servicio

El servicio O2Certify de entrega electrónica certificada de CMC estará disponible ininterrumpidamente 24 horas los 7 días de la semana.

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

19. Quejas y reclamaciones

Cualquier parte interesada en realizar una sugerencia, queja o reclamación referente al servicio de entrega electrónica certificada de CMC, podrá hacerlo a través de la cuenta de correo electrónico psc@grupocmc.com.

En todo caso, CMC dispone de un plazo máximo de 30 días para atender la queja o reclamación formulada.

20. Jurisdicción aplicable

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

Las partes contratantes 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, con renuncia expresa a cualquier fuero propio que pudiera corresponderles

21. Aprobación y revisión de la DPC

La presente DPC, así como cualquier modificación sustancial sobre la misma, será aprobada por el Consejero Delegado de CMC.

La presente DPC será revisada anualmente, y podrá ser modificada en cualquier momento por publicación, modificación o derogación de normativa aplicable, por causas legales que le afecten así como causas técnicas o comerciales.

Cuando se produzca una modificación de la DPC, deberá ser notificada al Órgano de Supervisión competente.

Cualquier cambio sustancial que pueda afectar a los suscriptores del servicio o terceras partes confiantes, se comunicarán a través de la web www.grupocmc.es/psc-3/

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.

22. Legislación aplicable

La normativa directamente aplicable a este servicio es la siguiente:

- 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.