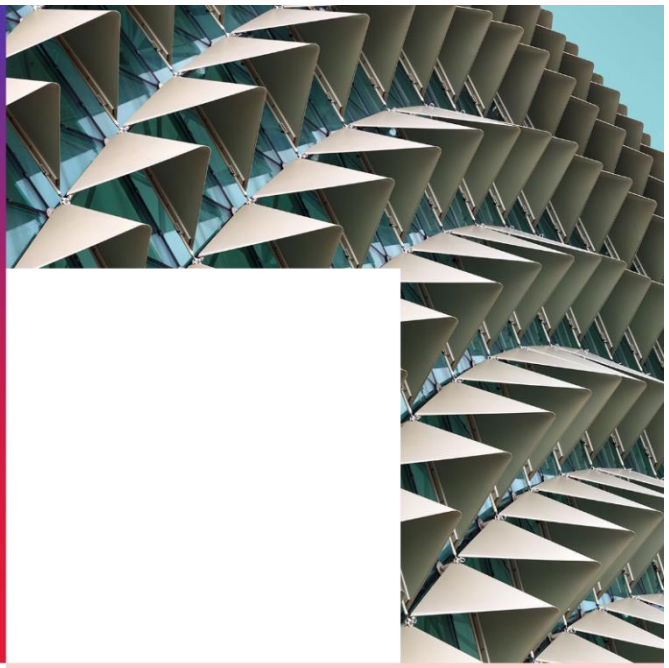

DECLARACIÓN DE PRÁCTICAS DEL SERVICIO ELECTRÓNICO DE CONFIANZA DE ENTREGA ELECTRÓNICA CERTIFICADA

Spain Delivery Center - CGI Information Systems and Management Consultants España S.A.

2024-10-10

Índice

HISTORIAL DE CAMBIOS				
VERSIÓN	DESCRIPCIÓN/HISTORIAL DE CAMBIOS	APROBADO POR	FECHA APROBACIÓN	OID
V. 1.0	Primera emisión	Alberto Anaya	16/06/2021	1.3.6.1.4.1.53726.01.1
V. 2.0	Cambio domicilio social Cambio de cargo del órgano que aprueba la DPC Cambio de correo electrónico de contacto	Alberto Anaya	10/02/2023	1.3.6.1.4.1.53726.01.2
V. 3.0	Adaptación de contenido por cambio de titularidad del Servicio de Entrega Electrónica Certificada.	Alberto Anaya	01/11/2023	1.3.6.1.4.1.53726.01.3
V.3.1	Revisión de mantenimiento anual del Servicio de Entrega Electrónica Certificada de acuerdo con la siguiente normativa: - Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) nº 910/2014. - Estándar ETSI EN 319401 V3.1.1. - Directiva (UE) 2022/2555 (Directiva NIS 2) y su Reglamento de Ejecución de 17 /10/2024. -	Alberto Anaya	10/10/2024	1.3.6.1.4.1.53726.01.3.1

Public

1 Introducción

CGI INFORMATION SYSTEMS AND MANAGEMENT CONSULTANTS ESPAÑA S.A. es una empresa dedicada a la consultoría de negocio, integración de sistemas, ofrecer servicios de TI, de aplicaciones o de infraestructuras o servicios de outsourcing disponiendo de la tecnología propia para procesar, gestionar y analizar todo tipo de datos. En adelante, se hará referencia a “CGI”.

En los servicios que presta CGI se encuentra el Servicio electrónico de Confianza de Entrega Electrónica Certificada o “Electronic Registered Delivery Service”, por sus siglas en inglés “ERDS”, bajo el nombre comercial “**CGI DigitalTrust360-ERDS**” (antes “O2Certify”) en el marco de la unidad “Spain Delivery Center” de CGI.

Este servicio 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. En adelante, se hará referencia al servicio como “**el Servicio**” o “**el Servicio de ERDS**” “**CGI DigitalTrust360-ERDS**”).

Para poder prestar el servicio de confianza, CGI 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 ERDS de CGI genera un ACTA en formato electrónico (PDF) en el que recogen las evidencias electrónicas asociadas al proceso de entrega, y queda a disposición de las partes interesadas, conservándose por el tiempo legal y/o contractualmente establecido.

De acuerdo con lo anterior, la presente Declaración de Prácticas del Servicio Electrónico de Confianza (en adelante “**DPC**”) recoge las normas y condiciones generales que presta CGI en relación con el Servicio de referencia.

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.

El Servicio ofrecido por CGI 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 DPC se realiza en cumplimiento con la legislación vigente y alineada con el Reglamento eIDAS. CGI sigue las indicaciones de los estándares del Instituto Europeo de Estándares de

Public

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 identificativos de CGI son:

Datos	Información
Razón Social	CGI INFORMATION SYSTEMS AND MANAGEMENT CONSULTANTS ESPAÑA S.A.
CIF	A81154197
Domicilio Social	Avenida de Manoteras, 10, Edificio C., 28050, Madrid.
Teléfono	91 304 80 94
Email	psc.ES@cgi.com
Nombre comercial	CGI DigitalTrust360-ERDS
Dominio	https://www.cgi.com/spain/es/solution/cgidigitaltrust360/psc
OID	1.2.6.1.4.1.53726.01.3.1

El presente documento y sus modificaciones serán publicadas en la página web del servicio: https://www.cgi.com/spain/es/solution/cgidigitaltrust360/psc

3 Comunidad de usuarios del servicio de entrega electrónica certificada de CGI

3.1 Prestador del Servicio de Entrega Electrónica Certificada

El Prestador del Servicio de Confianza de Entrega Electrónica Certificada será CGI INFORMATION SYSTEMS AND MANAGEMENT CONSULTANTS ESPAÑA S.A (CGI).

3.2 Operador de Verificación de Identidad

El Operador de Verificador de Identidad es aquella persona a la que CGI 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 CGI, 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 cualificada, se realiza de forma presencial ante el Operador de Verificación de Identidad designado por CGI, 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 CGI 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 CGI de forma fehaciente con su certificado electrónico emitido por un Prestador de Servicios de Certificación Cualificado (cuya relación de Prestadores y certificados admitidos se informará al emisor y destinatario en la aplicación de gestión antes de que CGI 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 CGI 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.

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

Public

CGI 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 CGI 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 CGI 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 Confianza son las siguientes:

- Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE modificado por el Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, en lo que respecta al establecimiento del marco europeo de identidad digital (Reglamento eIDAS).
- 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. (Reglamento General de Protección de Datos)
- 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
- ETSI EN 319 521 “Policy and security requirements for Electronic Registered Delivery Service Providers”
- ETSI EN 319 522-1: "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 1: Framework and Architecture".
- ETSI EN 319 522-2: "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 2: Semantic content".
- 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 permite la confirmación de la identificación electrónica de una persona física o jurídica, o la confirmación 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 CGI.
- **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):** es la “persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica”.

Public

- **Prestador de Servicios de Confianza**: es 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 modificado por el Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, en lo que respecta al establecimiento del marco europeo de identidad digital (Reglamento eIDAS).
- **Usuarios**: persona física o jurídica, o persona física que representa a otra persona física o a una persona jurídica, que intervienen en una operación y hacen uso de los servicios proporcionados por CGI, aceptando los términos y condiciones en la que se prestan.
- **Validación**: proceso consistente en verificar y confirmar que los datos en formato electrónico son válidos.

5.2 Acrónimos

- **AEPD**: Agencia Española de Protección de Protección de Datos
- **CPD**: Centro de Proceso de Datos.
- **DPC**: Declaración de Prácticas de Confianza
- **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 modificado por el Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, en lo que respecta al establecimiento del marco europeo de identidad digital.
- **ERDS**: Electronic Registered Delivery Service (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

CGI declara que la presente DPC es aplicable al Servicio de Entrega Electrónica Certificada cumpliendo los requisitos establecidos por el Reglamento eIDAS.

CGI 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.

CGI 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 del Servicio de Confianza.
- los requerimientos organizativos definidos en 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 CGI, son aprobados por el Senior Vicepresidente de Consulting Services and Business Unit Leader de CGI.

7.1 Administrador de sistemas

Las funciones principales que realiza este rol son las siguientes:

- Deberá implementar, configurar, monitorizar, documentar y asegurar el correcto funcionamiento del sistema informático.
- Se encargará de la administración de la plataforma de CGI, 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 CGI y colaborará en la consecución de los objetivos definidos.

Public

7.2 Operador de sistemas

Las funciones principales que realiza este rol son las siguientes:

- 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 CGI y colaborará en la consecución de los objetivos definidos.

7.3 Responsable del Servicio Electrónico de Confianza

Las funciones principales que realiza este rol son las siguientes:

- Gestionar y mantener el servicio de entrega electrónica certificada.
- Mantener el proceso de mejora continua del sistema dedicado al servicio de entrega electrónica certificada.
- En relación con los procesos de gestión, debe planificar las auditorías internas relativas al servicio de entrega electrónica certificada.
- Gestionar los incidentes de seguridad de la información que afecten al servicio de entrega electrónica certificada de forma conjunta y colaborativa con el responsable de seguridad de CGI.
- Revisión anual de la declaración de prácticas de certificación y elevación a la dirección para su aprobación.
- Cumplir y hacer cumplir la declaración de prácticas de certificación y las políticas de seguridad de CGI.
- Se encarga de todos los aspectos relacionados con la seguridad de la plataforma y del servicio de confianza.
- Colabora con el responsable del SGSI o de Seguridad de CGI en las funciones que éste último tiene encomendadas en relación con la implantación, desarrollo y mantenimiento del miso en lo que respecta al servicio de entrega electrónica certificada.

7.4 Responsable de Seguridad de las redes y de los sistemas de información

Las funciones principales que realiza este rol son las siguientes:

- 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

Public

- 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 CGI y colabora en la consecución de los objetivos definidos.

7.5 Auditor

Las funciones principales que realiza este rol son las siguientes:

- Comprobar la existencia de toda documentación requerida y enumerada.
- Comprobar la coherencia de la documentación con los procedimientos, activos inventariados, etc.
- Comprobar el seguimiento de incidencias y eventos.
- Comprobar la protección de los sistemas (explotación de vulnerabilidades, logs de acceso, usuarios, etc.).
- Comprobar las alarmas y elementos de seguridad física.
- Comprobar la adecuación a la normativa aplicable.

7.6 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.

Public

8 Integridad y confidencialidad del contenido del usuario

CGI 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, CGI 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.

CGI 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

CGI 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 CGI, 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.

Public

5. Una vez realizada la verificación inicial, el sistema de entrega electrónica certificada de CGI 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

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

La identificación del destinatario está 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 informan en la aplicación de gestión del Servicio. Igualmente, la relación de Prestadores de servicios de certificación admitidos será comunicados al destinatario en el correo electrónico de puesta a disposición de la documentación. El certificado deberá ser válido y estar activo (no revocado y no caducado).

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 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.

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

CGI 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

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

Public

- 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:

1. **SubmissionAcceptance**: consiste en la aceptación del envío de la notificación por parte del Servicio: El emisor, debidamente identificado, ha presentado el contenido del usuario ante el sistema de CGI DigitalTrust360-ERDS 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: ENVÍO ACEPTADO

2. **SubmissionRejection**: consiste en el rechazo del envío de la notificación por parte del Servicio: El emisor, debidamente identificado, ha presentado el contenido del usuario ante el sistema de CGI DigitalTrust360-ERDS, y éste lo ha rechazado. Todo ello produce la evidencia de Rechazo del envío, que se produce en el momento indicado en dicha evidencia.

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

B. Eventos de la notificación del contenido al destinatario:

Public

1. **NotificationForAcceptance:** consiste en el envío del mensaje al destinatario solicitando su aceptación. Se produce la evidencia que el Servicio de ERDS de CGI 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

2. **NotificationForAcceptanceFailure:** consiste en la existencia de un fallo en el envío de la notificación para la aceptación por el destinatario. Se produce la evidencia que el Servicio de entrega electrónica certificada de CGI 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

1. **ConsignmentAcceptance**: consiste en la aceptación por parte del destinatario del envío. 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

2. **ConsignmentRejection**: consiste en el rechazo por parte del destinatario del envío. 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

3. **AcceptanceRejectionExpiry.** consiste en la 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 de entrega del contenido del usuario al destinatario.

1. **ContentHandover**. Consiste en la entrega del contenido al destinatario con éxito. se produce la evidencia de que el contenido del usuario ha cruzado con éxito la frontera del servicio de entrega electrónica certificada de CGI 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

Public

2. **ContentHandoverFailure**: consiste en el fallo en la entrega del contenido al usuario. El contenido del usuario no ha cruzado con éxito la frontera del servicio de entrega electrónica certificada de CGI, 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.

CGI DigitalTrust360-ERDS conserva todas estas evidencias, que serán incorporadas al Acta final emitida y sellada por CGI 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 CGI 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.ES@cgi.com .

CGI 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, CGI 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 CGI como Prestador del Servicio

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

- Prestar el servicio conforme a lo dispuesto en la presente Declaración de Prácticas del Servicio de Confianza.

- 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.

Public

- Garantizar la integridad, confidencialidad y disponibilidad del contenido del usuario, dentro del sistema CGI DigitalTrust360-ERDS.

- 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 ERDS 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 al menos un mes antes de llevarla a cabo y, notificará con una antelación del al menos tres meses en caso de que se tenga la intención de cesar la actividad.

.

- 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 la adecuación y cumplimiento de la normativa aplicable, tanto interna como externa.

- Informará al organismo de supervisión al menos un mes antes de cualquier auditoría prevista y permitirán la participación del organismo de supervisión en calidad de observador.

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 los Términos y Condiciones del servicio.

- Deberán comunicar a CGI cualquier incidente de seguridad, fallo o situación anómala relativa al Servicio, 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 CGI información veraz, completa y exacta para la prestación del servicio de entrega electrónica certificada, incluidos los datos de los destinatarios sin errores y actualizados.

Public

El emisor deberá comunicar sin demora cualquier modificación de las circunstancias que incidan en la prestación del Servicio de ERDS.

12.3 Obligaciones de los proveedores

Los proveedores de servicios que puedan tener alguna actuación en el Servicio de ERDS de CGI, como los Prestadores de servicios de certificación que emitan los certificados electrónicos y los sellos de tiempo, deberán cumplir las siguientes obligaciones:

- Proporcionar a CGI 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 CGI cualquier cambio de condición en sus certificados vigentes.
- Proporcionar a CGI C 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 que confían en el servicio

Las personas físicas o jurídicas que confíen en el Servicio de ERDS prestado por CGI 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 CGI 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

CGI, como Prestador de Servicios de Confianza, se encuentra sujeto al régimen de responsabilidad recogido en el artículo 13 del Reglamento eIDAS por lo que asumirá las responsabilidades por los perjuicios causados de forma deliberada o por negligencia a cualquier persona física o jurídica dentro de los límites previstos en los Términos y Condicione del servicio.

Adicionalmente, CGI manifiesta que en cumplimiento de la normativa aplicable ha suscrito un seguro de responsabilidad civil suficiente para responder de las posibles reclamaciones de daños y perjuicios derivadas del incumplimiento de sus obligaciones contractuales y/o legales.

12.5.1 Limitaciones de responsabilidad

CGI, 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.

CGI 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.

Public

- Los actos u omisiones realizados por el Cliente sin respetar lo establecido en la presente 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.
- El contenido de los mensajes o de los documentos enviados.
- Los daños y perjuicios si el destinatario actúa de forma negligente. Proporcionar a CGI los sellos de tiempo necesarios para sellar temporalmente los eventos y las actas finales.
- La negligencia en la confidencialidad y conservación de los datos de acceso al Servicio por parte de los usuarios del mismo.
- 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 CGI cese en la prestación del servicio de entrega electrónica certificada, realizará las siguientes acciones para la ejecución de la terminación:

- Notificará del cese del servicio a los clientes a los que preste los servicios con una antelación mínima de 2 meses, mediante correo electrónico que conste en su base de datos. Asimismo, CGI informará del cese a terceras partes con las que haya firmado un contrato referente a este servicio (proveedores, subcontratistas, otros).

- Notificará, con una antelación previa de 3 meses, 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 revocará el certificado que sella las evidencias del servicio de confianza cualificado, según el procedimiento de Criptografía, de tal forma que no puedan ser recuperadas en ningún caso.

- CGI podrá firmar un acuerdo de transferencia del servicio de confianza con otro proveedor del Servicio de Entrega electrónica certificada, en caso de cese del mismo.

- 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 el caso de no llegar a un acuerdo con algún Prestador de Servicios de Confianza, la información referente al servicio de entrega electrónica certificada podrá ser conservada por CGI en el caso de que la empresa continúe con el resto de actividades o se depositará ante un 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 del servicio.

- CGI mantendrá disponible la clave pública de su certificado de sello electrónico cualificado, durante el plazo que sea necesario.

CGI cuenta con un Plan de Cese del Servicio de Entrega Electrónica Certificada, reflejado en el documento “Plan de Cese” de carácter interno.

Public

14 Controles de seguridad

Sin perjuicio de las políticas y procedimientos de seguridad existentes en CGI, los siguientes controles de seguridad se aplican específicamente para el Servicio de Confianza de Entrega Electrónica Certificada.

14.1 Seguridad física y medioambiental

CGI tiene sus oficinas en Avenida Manoteras, nº 10, 28050 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/IEC: 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.

Se cuenta con un procedimiento de “SEGURIDAD FÍSICA Y DEL ENTORNO” en el marco del Servicio de confianza 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.

Public

Los servicios críticos (electricidad, redes, calefacción, ventilación y aire acondicionado, extinción de incendios, etc. se prestan de forma redundante, y todos los equipos críticos se mantienen mediante contratos con proveedores. Los activos se eliminan de forma segura cuando ya no se necesitan.

14.2 Seguridad lógica, controles de acceso

CGI ha definido políticas y normas relativas al acceso a la información, las redes y los servicios. El control de acceso a los sistemas y a la información se basa en los principios de “necesidad de conocer” y “mínimo privilegio”. El acceso y los permisos de los miembros y subcontratistas se basan en funciones. Se actualizan a medida que cambian las funciones del puesto y se eliminan cuando los miembros abandonan la empresa o cuando finaliza el contrato con un proveedor.

Se han implantado procesos de gestión del control de acceso lógico. Cada perfil tiene asignado su acceso necesario para realizar sus funciones en el marco del Servicio Electrónico de Confianza.

Se ha elaborado un procedimiento interno donde se definen los controles aplicados para el acceso a los sistemas del servicio de confianza.

14.3 Clasificación de la información y gestión de activos documentos

CGI tiene un procedimiento específico destinado al Servicio de ERDS denominado “CLASIFICACIÓN DE LA INFORMACIÓN Y GESTIÓN DE ACTIVOS” en el marco del servicio electrónico de confianza, donde se detalla cómo está clasificada la información referente al servicio, así como la gestión de activos dentro de la organización.

CGI clasifica la información en cuatro niveles:

- Pública o “Public”: esta información no es sensible ni requiere una protección especial. No hay ningún efecto adverso o consecuencia negativa para CGI si se divulga información pública.

- Interna o “Internal”: la información interna que se divulgue sin autorización podría tener un efecto adverso limitado en las operaciones de CGI, activos organizacionales o en los individuos tales como:

    - Desacreditación de la reputación de CGI.
    - Causar perjuicios a socios, clientes, vendedores o socios comerciales.

- Confidencial o “Confidential”: la información interna que se divulgue sin autorización podría tener un serio efecto adverso en las operaciones de activos organizacionales o en los individuos tales como:

    - Reducir la ventaja competitiva de CGI
    - Reducir el potencial de generación de ingresos de CGI.
    - Viola la intimidad y los derechos de las personas.

- Altamente confidencial o “Highly confidential”: la información interna que se divulgue sin autorización podría tener severos o catastróficos efectos adversos, activos organizacionales o en los individuos tales como:

    - Comprometer la reputación y credibilidad empresarial de CGI.

Public

- Causar pérdidas financieras importantes, graves problemas de responsabilidad o sanciones importantes.

En el marco del Servicio de ERDS la información se clasifica de la siguiente manera:

➔ **INFOMACION CONFIDENCIAL:**

- Toda información relativa a los parámetros de seguridad, control y procedimientos de auditoría.
- Toda la información de carácter personal proporcionada a CGI durante el proceso de registro de los suscriptores del servicio.
- La información de negocio suministrada por sus proveedores y otras personas con las que CGI 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.
- Las claves de firma.
- INTERNA: Políticas y normas internas de ERDS.
- Procedimientos Generales/Específicos de ERDS.
- Guías de trabajo/Instrucciones Técnicas del Servicio.
- Metodología de trabajo

➔ **INFORMACION PUBLICA: Se considera información pública, entre otros:**

- La Declaración de Prácticas del Servicio de Confianza de Entrega Electrónica Certificada.
- Los Términos y condiciones del servicio.
- Política de Privacidad del Servicio de ERDS.
- Política de cookies del Servicio.
- Toda aquella información que sea considerada como “Pública”.

En relación con la gestión de activos, CGI mantiene un inventario de los activos implicados en el Servicio de confianza y ofrece orientación sobre el tratamiento de la información en todo su ciclo de vida (almacenamiento, transmisión, impresión, destrucción, etc) en función de su clasificación.

La propiedad de los activos también se asigna y gestiona adecuadamente a lo largo de su ciclo de vida.

El uso aceptable de los activos informáticos y de la información se comunica a través de la Política de Seguridad la Política de uso aceptable de CGI.

14.4 Copias de respaldo y procedimiento de recuperación

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

Existe un Procedimiento de back 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

CGI en el marco de la seguridad de las operaciones, cuenta con medidas que garantizan la protección frente al malware, la gestión de cambios en los sistemas o la gestión de la capacidad y lleva a cabo medidas que garantizan la integridad del software y de la información tratada, como puede serla realización de copias de seguridad o el registro y supervisión de los logs.

Los sistemas de CGI se mantienen actualizados con la actualización de parches en función de las vulnerabilidades detectadas. Se realizan análisis de vulnerabilidades periódicos en los sistemas.

Los grupos de servicios de información, usuarios y sistemas de información están segregados en redes para preservar la confidencialidad, integridad y autenticidad de la información.

14.6 Procedimientos de auditoría de seguridad

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

CGI cuenta con un procedimiento donde se detallan los procesos y controles para la revisión y mejora continua del sistema CGI DigitalTrust360-ERDS.

Como se ha indicado, CGI realiza trimestralmente un análisis de vulnerabilidades de todos los sistemas de red del Servicio de ERDS así como un test de penetración anual en el marco de dicho Servicio.

14.7 Controles de personal

El organigrama con la estructura de personal de la compañía se encuentra publicado en la intranet corporativa de CGI y los roles con las responsabilidades de cada uno de los puestos se gestiona desde el Departamento de Recursos Humanos de CGI siguiendo los procedimientos y políticas elaboradas por la entidad relativas a la seguridad en los recursos humanos y la definición de roles y responsabilidades en materia de seguridad y en el marco de los servicios electrónicos de confianza. En concreto, los roles de confianza que contempla el servicio de ERDS son los descritos en el apartado 7 de la presente DPC.:

CGI cuenta con una organización de seguridad global que es dirigida por un CSO (Chief Security Officer) que informa directamente a la alta dirección ejecutiva a nivel global. Cada Unidad Estratégica de Negocio (SBU) cuenta con un equipo que lidera la seguridad y garantiza su mantenimiento en CGI.

El Servicio de Entrega Electrónica Certificada o el sistema “CGI DigitalTrust360-ERDS” se encuentra incluido dentro de la Unidad de CGI España denominada “Spain Delivery Center” y conforma uno de los servicios que presta dicha Unidad. El Servicio de ERDS cuenta con el siguiente esquema organizativo específico:

- Responsable del servicio: es 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 CGI. Supervisa y garantiza la adecuación de los medios técnicos, organizativos y de personal del servicio. Asimismo, procura la adecuación del personal a las necesidades del servicio en cuanto a experiencia, conocimientos y requisitos de formación.
- Operadores de Sistemas: son responsables de la gestión del día a día del sistema (Monitorización, backup, recovery, etc)

Public

- Técnicos de soporte: responsables de la gestión del día a día de las incidencias del Servicio reportadas por los clientes.
- Auditor interno: es el encargado de realizar las auditorías internas del Servicio.
- Responsable de Compliance: es el encargado de supervisar y actualizar el cumplimiento de normativas y regulaciones aplicables al servicio.
- Responsable de Seguridad de la Red y de la Información: es el encargado de supervisar y controlar la seguridad de las redes y de la información del servicio.

14.8 Plan de continuidad del servicio

En CGI se mantienen planes de continuidad del negocio para asegurar la restauración adecuada de los servicios internos y externos. El mantenimiento de los principios de seguridad se mantiene a lo largo de la vida de un desastre para garantizar que no se vuelva a producir. Los planes de continuidad se prueban regularmente por el equipo o equipos de gestión de crisis.

CGI dispone de procedimientos e instrucciones técnicas para la gestión de la continuidad del Servicio de ERDS 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 confianza prestados por CGI.

Sin perjuicio de las medidas de seguridad concretas aplicadas, los controles para la gestión de la Continuidad de Negocio en el marco del Servicio están definidos en el procedimiento “GESTION DE CONTINUIDAD” así como la planificación de los escenarios de contingencia y la evaluación de impacto en el negocio.

El objetivo de este documento es establecer las directrices de la estrategia de contingencia ante incidentes o desastres en los sistemas que soportan los procesos de negocio de CGI. 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

CGI 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.

Public

Asimismo, revisará la Política de Seguridad y el inventario de los activos 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 los mismos.

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).

CGI tiene que someterse a una auditoria bienal donde se evalúa de nuevo la conformidad con las normas relativas al servicio de confianza. 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 CGI.

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 de ERDS 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 CGI, 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 los procedimientos aprobados por CGI.

16 Protección 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”) CGI 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 CGI INFORMATION SYSTEMS AND MANAGEMENT CONSULTANTS ESPAÑA S.A. con CIF: A81154197 y domicilio social en Avenida de Manoteras Nº 10, Edificio C, 28050 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 CGI 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 CGI 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 privacy@cgi.com bajo el Asunto “Ejercicio de Derechos en el ámbito de protección de datos” y acompañando los documentos de identidad en caso de ser necesario. 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.

CGI 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.

CGI, 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, CGI 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.

Public

17 Deber de confidencialidad

Los empleados de CGI se comprometen a guardar el deber de confidencialidad respecto de la información que conozcan por razón de su puesto de trabajo.

En este sentido, dicha información no deberá ser en ningún caso divulgada a terceros salvo que apliquen excepciones en los supuestos de requerimiento o colaboración con las instituciones u órganos competentes.

Se tendrá en cuenta la clasificación de la información definida en CGI en cuanto a su mantenimiento, acceso, almacenamiento o transmisión.

CGI se compromete a garantizar la confidencialidad de los datos aportados por sus Clientes o Usuarios implementando las medidas técnicas y organizativas necesarias para minimizar los riesgos de pérdida de datos personales y/o información confidencial tal y como se indica en la Política de protección de datos.

El acceso a los datos del Usuario está restringido a aquellas personas autorizadas para su utilización aplicando la debida diligencia para evitar cualquier pérdida, alteración o uso indebido de los mismos.

Por su parte, el Cliente se obliga a mantener estricta confidencialidad sobre todos aquellos datos, documentación y demás información que hayan sido suministrados por CGI en o para la ejecución del Contrato o que por su propia naturaleza deba ser tratada como tal. Asimismo, se compromete a no comunicar esta información a ninguna otra persona o entidad, no pudiendo reproducirla, utilizarla, venderla, licenciarla, exponerla, publicarla o revelarla de cualquier forma sin autorización expresa de CGI. Las obligaciones de confidencialidad tendrán una duración indefinida, manteniéndose en vigor con posterioridad a la finalización por cualquier otra causa, de la relación entre el Cliente y CGI. Los proveedores y terceros deben firmar acuerdos de confidencialidad, someterse a evaluaciones de riesgos y comprometerse a respetar los elementos de seguridad incluidos en los contratos.

18 Términos y condiciones del servicio

Como se definió en la introducción de la presente DPC, para realizar el servicio de entrega electrónica certificada, CGI 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 del Servicio CGIDigitalTrust 360, donde CGI 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 CGI, así como con sello de tiempo.

El Acta queda en la plataforma del Servicio/CGI DigitalTrust360-ERDS y las partes interesadas podrán acceder a ella con un plazo de un (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.ES@cgi.com

La información será conservada por CGI, 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 https://www.cgi.com/spain/es/solution/cgidigitaltrust360/psc disponibles permanentemente.

CGI 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.

Public

18.1 Disponibilidad del servicio

CGI se compromete a prestar el servicio de entrega electrónica cualificada de conformidad a los SLA acordados con sus clientes.

A tal efecto, CGI firmará con sus clientes un Acuerdo de Nivel de Servicio (Service Level Agreement), relativo al tiempo de atención, calidad y disponibilidad del servicio ofrecido.

En la prestación de los servicios descritos en esta DPC, CGI 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 CGI, podrá hacerlo a través de la cuenta de correo electrónico psc.ES@cgi.com o bien, a través del mismo correo desde el apartado de “Buzón de Quejas y Sugerencias” del portal web de CGI siguiente : https://www.cgi.com/spain/es/solution/cgidigitaltrust360/psc

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

En caso de reclamaciones judiciales, se procederá según lo dispuesto en el apartado siguiente de la presente DPC.

20 Jurisdicción aplicable

Las relaciones entre CGI 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 creación de la presente DPC, así como cualquier modificación sustancial sobre la misma, será aprobada por el Senior Vicepresidente de Consulting Services and Business Unit Leader de CGI.

Public

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 o en la Política de Seguridad de CGI que afecte al Servicio, deberá ser notificada al Órgano de Supervisión competente.

Igualmente, cualquier cambio sustancial tanto en la Política de Seguridad de CGI como en la presente DPC que pueda afectar a los suscriptores del servicio o terceras partes confinantes, se comunicarán a través del sitio web de CGI, en concreto: https://www.cgi.com/spain/es/solution/cgidigitaltrust360/psc

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.

02876505X ALBERTO ANAYA (R: A81154197)
Digitally signed by 02876505X ALBERTO ANAYA (R: A81154197)
Date: 2025.01.22 12:44:39 +01'00'