WISE SECURITY
a vargroup company

# ERDS MEE

Declaración de Prácticas del Servicio de Entrega Electrónica Certificada

Clasificación: Uso Público

| CONTROL DE VERSIONES | | | |
|---|---|---|---|
| Versión | Fecha de emisión | Cambios/Observaciones | Aprobado por |
| 1.0 | 03/02/2021 | Revisión inicial | Óscar Flor Lozano |
| 1.1 | 16/01/2023 | Revisión periódica. Sin modificaciones | Óscar Flor Lozano |
| 1.2 | 22/01/2024 | Revisión periódica. Sin modificaciones | Óscar Flor Lozano |
| 1.3 | 19/03/2024 | Cambio de estilos VarGroup | Óscar Flor Lozano |
| 1.4 | 25/03/2024 | Añadido Camerfirma en punto 2.6 Prestadores de Servicios de Confianza Cualificados intervinientes. Eliminada la referencia al documento de “Términos y Condiciones” del punto 9 REFERENCIAS DE TIEMPO | Óscar Flor Lozano |
| 1.5 | 15/04/2024 | Actualización secciones 8.1, 10.5 y 18.1 | Óscar Flor Lozano |
| 1.6 | 13/01/2025 | Revisión periódica. Sin modificaciones | Óscar Flor Lozano |
| OID: 1.3.6.1.4.1.56976.1.1.1.1 | | | |

# 1 INTRODUCCIÓN

Wise Security Global (en adelante, "WSG") es una compañía experta en ciberseguridad, firma digital y certificación electrónica y que tiene por misión proteger la actividad de sus clientes mediante la generación de entornos electrónicos confiables y seguros que les permitan mantener y mejorar la confianza de sus partes interesadas.

WSG es un proveedor de Servicio de Confianza conforme al Reglamento eIDAS (UE) Nº 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014, relativo a 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/EC y la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

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

Este Servicio de Entrega Electrónica Certificada consiste en la generación de una prueba que acredita la remisión de un documento por parte de un emisor, su recepción o rechazo por parte del destinatario, así cormo del momento en que ambas se produjeron y, en su caso, del acceso/descarga de documentación adjunta con la finalidad principal de que pueda ser utilizada en contextos jurídicos.

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

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

Además, WSG 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”; , y se ha redactado conforme a la RFC 3647 “Certificate Policy and Certification Practices Framework” propuesto por Network Working Group para este tipo de documentos.

# 2 COMUNIDAD DE USUARIOS DEL SERVICIO

## 2.1 Prestador del servicio de confianza

El proveedor del servicio de confianza definido bajo esta Declaración de Prácticas es Wise Security Global:

Wise Security Global SL
B-95732087
Alameda Recalde 34
48009 Bilbao
Contacto: info@wsg127.com

## 2.2 Emisor

Será emisor toda persona física o jurídica que emite una comunicación y la pone a disposición de un destinatario, a través del servicio de entrega electrónica certificada de WSG. Este emisor deberá estar previamente identificado por WSG, de tal forma que WSG pueda confirmar con un alto nivel de confianza, que esta persona es quien dice ser.
En el caso del servicio de entrega electrónica certificada cualificada, el emisor se autenticará siempre mediante un certificado electrónico emitido por un Prestador de Servicios de Confianza Cualificado.

## 2.3 Destinatario

Se entiende por destinatario aquella persona física o jurídica a la cual va dirigida la comunicación enviada por el emisor, y que será entregada por el servicio de entrega electrónica certificada de WSG, previa su autenticación.
En el caso del servicio de entrega electrónica certificada cualificada, el destinatario de la comunicación se autenticará siempre mediante un certificado electrónico emitido por un Prestador de Servicios de Confianza Cualificado.

## 2.4 Oficial de verificación de identidad

El Oficial de Verificación de Identidad es aquella persona que por cuenta de WSG, se le encomienda la función de comprobación de la identidad inicial del emisor y/ del destinatario. En el caso del servicio cualificado, dado que la autenticación es siempre por certificado electrónico cualificado, no es necesaria la validación de las identidades físicamente.

## 2.5 Terceras partes confiables

Terceras partes confiables son aquellas partes que confían en los servicios prestados por WSG.

Estas terceras partes deberán tener en cuenta las limitaciones del servicio, así como conocer los términos y condiciones del mismo. En concreto, las terceras partes deberán comprobar la autenticidad e integridad del documento, verificando la validez de la firma incluida en el documento final, y que está certificado por WSG como Prestador del Servicio de Confianza, así como que el certificado digital utilizado para la firma era válido en el momento de la firma, y que el documento se mantiene íntegro y que no ha sido modificado. Para ello, puede servirse de programas como ADOBE, que valida el documento PDF o VALIDe, o cualquier otro que realice dicha verificación.

Igualmente, el documento incorpora dos sellos de tiempo, el primero certifica que el documento existe en el momento de la firma, y el segundo asegura que las evidencias de revocación incorporadas en la propia firma son perdurables en el tiempo, se genera con ello una firma en formato PAdES LTV, para que se pueda verificar su validez a largo plazo. En el supuesto de que el programa que verifique su validez informe de que hay un problema en la firma (porque el certificado ha caducado), se puede comprobar la validez del certificado en el momento de la firma puesto que la información de revocación se añadió en “Detalles del certificado”.

No obstante, WSG resolverá cualquier duda relacionada con el servicio electrónico de confianza y la validez del documento final. Para ello, cualquier parte interesada puede dirigir un escrito a info@wsg127.com, solicitando la verificación de la validez de dicho documento.

## 2.6 Prestadores de Servicios de Confianza Cualificados intervinientes

La relación de prestadores de Servicios de Confianza Cualificados que intervienen en el servicio de entrega electrónica certificada cualificada es la siguiente:

- CAMERFIRMA: emisor del certificado de sello de empresa, que se utiliza para firmar las evidencias del servicio de entrega electrónica certificada.

- IVNOSYS: custodio del certificado de sello de empresa anterior, este certificado esta alojado en un HSM.
  También es emisor de sellos de tiempo que se utilizan para consignar la fecha y hora de los eventos ocurridos en el servicio de entrega electrónica certificada.

- IZENPE: emisor de los sellos de tiempo que se utilizan para consignar la fecha y hora de los eventos ocurridos en el servicio de entrega electrónica certificada

# 3 DEFINICIONES Y ACRÓNIMOS

## 3.1 Definiciones

- **Agente/aplicación de usuario de entrega electrónica certificada**: Sistema consistente en componentes de software y/o hardware mediante el cual los remitentes y los destinatarios participan en el intercambio de datos con los proveedores 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.
- **Certificado Cualificado**: Certificado expedido por un Prestador Cualificado de Servicios de Confianza y que cumple los requisitos establecidos en el Anexo I del Reglamento UE 910/2014 (eIDAS) y que cumple los requisitos establecidos en el artículo 7 de la Ley 6/2020 (LSEC) en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes, y a la fiabilidad y las garantías de los servicios de confianza que presten, de conformidad con el Título III de la mencionada Ley 6/2020 LSEC .
- **Cifrado**: Operación mediante la cual un mensaje en claro se transforma en un mensaje ilegible.
- **Contenido del usuario**: Datos originales producidos por el remitente que deben entregarse al destinatario.
- **Consignación**: acto de poner el contenido del usuario a disposición del destinatario, dentro de los límites del servicio de entrega electrónica certificada
- **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.
- **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.
- **Evento**: Paso relevante en un proceso de entrega electrónica que puede estar avalado por una evidencia del servicio de entrega electrónica certificada.
- **Evidencia**: Datos generados por el servicio de entrega electrónica certificada que tiene como objetivo probar que un determinado evento ha ocurrido en un momento determinado.
- **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.
- **Proveedor 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 confianza.
- **Proveedor de Servicio de Entrega Electrónica Certificada**: proveedor del servicio de confianza que presta el servicio de entrega electrónica certificada
- **Proveedor 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.
- **Traspaso**: acto de hacer que el contenido del usuario cruce con éxito el borde del servicio de entrega electrónica certificada hacia la Aplicación del destinatario.
- **Usuario**: personas físicas o jurídicas que utilizan los servicios de entrega electrónica certificada proporcionado por WSG

## 3.2 Acrónimos

- **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.
- **LSEC**: Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

- **ERD**: Un paso relevante en el proceso de entrega electrónica que puede estar atestiguado por una evidencia del servicio
- **ERDS**: Siglas en inglés de Electronic Registered Delivery Service, o Servicio de Entrega Electrónica Certificada. Es el servicio electrónico proporcionado el cual puede transmitir datos entre terceros por medios electrónicos proporcionando evidencias relacionadas con la gestión de los datos y que protege así mismo los datos transmitidos contra el riesgo de pérdida, robo, daño o cualquier alteración no autorizada.
- **ERDSP**: Proveedor de servicio de entrega electrónica certificada.
- **ERD-UA**: Agente/ aplicación de usuario de entrega electrónica certificada.
- **OTP**: One-Time Password
- **SGSI**: Sistema de Gestión de Seguridad de la Información.
- **TSP**: Trust Service Provider. Prestador de Servicios de Confianza.

# 4 REQUERIMIENTOS DE CONFORMIDAD

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

WSG garantiza, de acuerdo con los requisitos legales y normativos que:

- Cumple con su Política de Seguridad de la Información, que se encuentra vigente y alineada con la regulación jurídica de aplicación.
- Cumple con su política de Servicio Entrega Electrónica Certificada Cualificada definida en la presente Declaración de Prácticas.
- Cumple con los requerimientos organizativos que se definen en el punto 5 de la presente Declaración de Prácticas.
- La presente DPC es conforme a la norma el ETSI EN 319 521 “Policy and security requierements for Electronic Registered Delivery Service Providers, y se han implementado los controles que cumplen con los requerimientos especificados por dicha norma ETSI, así como la norma ETSI EN 319 401, como prestador de servicios electrónicos de confianza.

# 5 OBLIGACIONES DE LAS PARTES

## 5.1 Obligaciones del prestador del servicio

WSG, actuando como Proveedor del Servicio de Entrega Electrónica Certificada se compromete a:

- Respetar lo dispuesto en esta Declaración de Prácticas del Servicio Cualificado de Entrega Electrónica Certificada.
- Asegurar la protección de sus claves privadas de sus certificados de forma segura.
- Gestionar el Servicio de Entrega Electrónica Certificada según la información enviada por el cliente y libre de error en la entrega de datos.
- Utilizar los medios adecuados para la obtención de las evidencias resultantes del servicio.
- Custodiar las evidencias emitidas para los clientes que contraten el Servicio Cualificado de Entrega Electrónica Certificada.
- Informar al suscriptor del servicio de las características de la prestación del servicio, las obligaciones que asume y los límites de responsabilidad.
- Publicar esta Declaración de Practicas del Servicio Cualificado de Entrega Electrónica Certificada, y mantenerla actualizada.
- Utilizar tecnologías y equipos adecuados, así como contar con el personal capacitado para realizar sus funciones.
- En caso de no disponibilidad del servicio por mantenimiento, trabajos de mejora o modificación, comunicarlo a sus clientes con la suficiente antelación.
- En caso de incidencia en el servicio, comunicarlo inmediatamente a las partes implicadas que resulten o puedan resultar afectadas.
- Utilizar sellos de tiempo cualificados para garantizar que los eventos producidos en el servicio operan en sincronía con fuentes fiables de tiempo.
- Garantizar la integridad, confidencialidad y disponibilidad del contenido del usuario, dentro del servicio de entrega electrónica certificada de WSG.
- Establecer mecanismos de custodia de las evidencias producidas por el ERDS, quedando protegidas de cualquier manipulación no autorizada, falsificación, pérdida, o destrucción.
- Atender las solicitudes, consultas, quejas y reclamaciones de clientes y terceros en un plazo razonable. Las quejas y sugerencias entran por formulario en la página: https://erds-mee.com/quejas-y-sugerencias/
- Conservar la información relativa a los servicios prestados durante 15 años a contar desde la finalización del servicio prestado y, en todo caso, durante el periodo que establezca la legislación vigente.

- Notificar al Órgano Supervisor cualquier modificación sustancial que se produzca en la presente DPC. Si la modificación afecta a las partes interesadas, éstas serán igualmente informadas.
- Notificar al Órgano Supervisor, en un plazo de 24 horas, la violación de seguridad con impacto significativo en el servicio electrónico de confianza. Igualmente, si la violación afecta a datos personales, se comunicará a la Agencia Española de Protección de Datos en un plazo máximo de 72 horas desde que se tiene conocimiento del mismo.

## 5.2 Obligaciones de los clientes/suscriptores de los servicios

Los clientes WSG, se comprometen a:

- Estar informados de lo dispuesto en la presente Declaración de Prácticas de Certificación.
- Utilizar los medios adecuados para la solicitud de los servicios.
- Limitar y adecuar el uso de las evidencias resultantes del servicio a lo permitido por esta DPC.
- Conocer y aceptar las condiciones y limitaciones de uso del servicio que se hayan establecido en esta DPC.
- Tener conocimiento de lo establecido en la presente DPC, aceptando y sujetándose a lo dispuesto en la misma y, en particular, a las responsabilidades aplicables en su aceptación y uso de los servicios que provee WSG, así como de las evidencias resultantes de los mismos.
- Notificar, sin dilación alguna, cualquier fallo, hecho o situación anómala relativa a los servicios que ofrece WSG sobre el presente servicio.

## 5.3 Obligaciones de las terceras partes

Las personas, sean físicas o jurídicas, que confíen en el servicio de entrega electrónica certificada prestado por WSG están obligados a:

- Conocer las limitaciones de uso (si las hubiera) del servicio, según la presente DPC y los términos y condiciones del servicio.
- Cumplir con lo dispuesto en la normativa aplicable.
- Reportar a WSG cualquier incidente relacionado con el servicio, tan pronto como sea tengan conocimiento de ello y sea posible.
- Verificar a validez de las firmas o sello electrónicos utilizados para firmar el documento certificado de evidencias.

## 5.4 Obligaciones de los proveedores de WSG

Los proveedores de WSG cuyos servicios tengan impacto en el servicio de entrega electrónica certificada prestado por WSG, tales como los proveedores de los certificados cualificados para la firma de evidencias y los proveedores del servicio de sellado de tiempo deberán:

- Garantizar que los certificados cualificados emitidos a nombre de WSG y los certificados que emiten los sellos de tiempo siguen siendo cualificados.
- Comunicar a WSG cualquier modificación de su condición de cualificados.

# 6 INTEGRIDAD Y CONFIDENCIALIDAD DEL CONTENIDO DEL USUARIO

WSG utiliza un certificado cualificado de Sello Electrónico emitido por Camerfirma que es Prestador de Servicios de Certificación Cualificado, que se encuentra instalado en la plataforma IvSign en el HSM de Ivnosys, el cual garantiza la adecuada disponibilidad, e integridad y confidencialidad del contenido del usuario cuando utiliza dicho servicio.

WSG garantiza la confidencialidad de la identidad del emisor y del destinatario, tanto durante el envío, como durante la custodia de las evidencias mediante el cifrado de las comunicaciones mediante algoritmos robustos (TLS con RSA y AES mínimo de 128 bits y modo CBC, SHA mínimo de 256 bits).

Se utiliza uno u otro algoritmo en función de las capacidades criptográficas del navegador del cliente conectado (se utilizará el algoritmo más fuerte dentro de las posibilidades del cliente), en todos los casos la versión del protocolo TLS es 1.3 y las claves asimétricas son de 2048 bits.

Este listado de algoritmos permitidos es configurable, permitiendo que el sistema sea más o menos restrictivo al respecto, no obstante, nunca se servirá bajo una algoritmia inferior a las listadas. El listado se va actualizando conforme a las directivas de seguridad vigentes.

El certificado que servirá el protocolo es un certificado cualificado de autenticación de sitio web solicitado por la sociedad Wise Security Global, y emitido por un Prestador de Servicios de Confianza Cualificado.

WSG garantiza 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 durante 15 años y 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.

El sistema nunca modificará el contenido del usuario, ni siquiera para cambios de formato, el contenido será íntegramente lo que el emisor haya creado.

En cada envío se podrán adjuntar hasta 3 ficheros únicamente en formato PDF, con un volumen máximo de 5MB cada uno de ellos.

# 7 IDENTIFICACIÓN Y AUTENTICACIÓN EN EL SERVICIO

## 7.1 Identificación inicial de las partes

La identidad tanto del emisor como del receptor se verifica a partir de su certificado electrónico válido, emitido por un Prestador incluido en la Lista de Prestadores de Servicios de Confianza del Ministerio competente en materia de servicios electrónicos de confianza.

Esta verificación se realiza cada vez que el usuario accede al servicio de ERDS MEE, de manera que se garantiza que la vigencia admitida para un mismo certificado no podrá superar en ningún caso un período máximo de 5 años desde la primera identificación, los tiempos de vigencia máximos establecidos por los diferentes PSCs en ningún caso se aproximan a 5 años, y en cada autenticación se verifica la caducidad del certificado, así como su estado de revocación.

## 7.2 Autenticación

Como método de autenticación en el servicio cualificado de entrega electrónica certificada, tanto del emisor como del destinatario, deben emplearse certificados de persona física o de representante legal de persona jurídica, emitidos por un Prestador de Servicios de Confianza Cualificado.

## 7.3 Identificación del destinatario y entrega del contenido de usuario

WSG entregará el contenido del usuario al destinatario, únicamente después de haber identificado de forma exitosa al destinatario. La identificación del destinatario esté basada en un certificado de persona física o de representante legal de persona jurídica, emitido por un Prestador de Servicios de Confianza Cualificado. La plataforma del servicio de entrega electrónica certificada de WSG realizará la previa verificación de su validez, antes de poner el contenido del usuario a disposición del destinatario.

# 8 EVENTOS Y EVIDENCIAS

## 8.1 Registro de eventos

WSG mantendrá un registro de los eventos del servicio, almacenando al menos los siguientes:

- Datos de identificación del emisor y del destinatario, incluyendo 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, si procede.
- 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.
- Prueba de que el contenido del usuario no se ha modificado durante la transmisión. Dicha prueba se realizará mediante la inclusión de un sello de entidad de WSG y el sellado 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, según proceda.

Las evidencias producidas por el servicio se pondrán a disposición de las partes en formato PDF. Estos ficheros estarán firmados electrónicamente en formato PAdES y dichas firmas estarán selladas por un sello de tiempo electrónico cualificado. Las firmas autocontendrán toda la información de comprobación de revocación de los certificados intervinientes en la firma, y tendrán un segundo sello de tiempo que lacre este contenido, todo ello siguiendo los requisitos definidos en la ETSI EN 319 142-1, de acuerdo con la decisión de la implementación (UE) 2015/1506 de la Comisión un 8 de septiembre de 2015, por la que se establecen especificaciones para formatos avanzados de firma electrónica y sellos electrónicos avanzados según el Reglamento eIDAS, generando firma en formato PAdES LTV.

## 8.2 Frecuencia de control

Los registros de auditoría son examinados periódicamente en búsqueda de actividades sospechosas o maliciosas. Las acciones realizadas tras la auditoría deben estar perfectamente accesibles y documentadas. El procesamiento de los registros de auditoría consiste en una revisión de los registros que incluye la verificación de que

éstos no han sido manipulados, una breve inspección de todas las entradas de registro y una investigación más profunda de cualquier alerta o irregularidad.

## 8.3 Periodo de retención y validez

WSG, retendrá todos los registros durante un tiempo mínimo de 2 años según el requerimiento REQ-ERDSP-7.10-02 de la norma EN 319 521.

No obstante, las evidencias producidas por el servicio e incluidas en la Declaración final serán conservadas por WSG durante 15 años.

## 8.4 Eventos registrados por el servicio

### 8.4.1 Eventos del Servicio de Entrega Electrónica Certificada registrados en origen

- **A.1 SubmissionAcceptance**:
  Aceptación del envío: Se evidencia que el emisor, debidamente identificado, tal y como se puede probar con la información de los datos de identificación y verificación de la identidad del emisor, en un momento dado ha presentado con éxito el contenido de la notificación ante el servicio de entrega electrónica certificada de WSG, y WSG lo ha aceptado, para a su vez, intentar entregárselo al destinatario del mismo.
  A nivel funcional, esta evidencia se produce cuando, en el Portal del Emisor, el usuario emisor pulsa el botón Enviar en el formulario de alta de notificaciones.
  Estado alcanzado del acta: Enviada

### 8.4.2 Eventos de notificación del envío al destinatario

- **C.1 NotificationForAcceptance:**
  Notificación del envío al destinatario para su aceptación: Se produce la evidencia de que WSG envió una notificación al destinatario, en un momento determinado, comunicando la puesta a disposición de un mensaje enviado por el emisor y solicitando su aceptación.
  A nivel funcional, esta evidencia se produce acto seguido de A.1 SubmissionAcceptance, como parte del proceso que se desencadena en el envío.
  Estado alcanzado del acta: Enviada

- **C.2 NotificationForAcceptanceFailure:**
  Fallo en la notificación para la aceptación: Se produce la evidencia de que no se pudo notificar al destinatario la puesta a disposición del contenido de la notificación debido a errores técnicos. La evidencia relacionada atestigua que una notificación que solicita la aceptación de un mensaje no se pudo enviar al destinatario especificado.
  A nivel funcional, esta evidencia se produce cuando el servidor de correo configurado para la realización del envío de la notificación por Email devuelve una respuesta de que Email no se ha podido entregar a su destinatario, por ejemplo, porque la dirección de Email proporcionada por el emisor no existe.
  Estado alcanzado del acta: Envío fallido

### 8.4.3 Eventos de aceptación o rechazo del contenido de usuario por parte del destinatario

- **C.3 ConsignmentAcceptance:**
  Aceptación de la notificación: se evidencia que el destinatario, debidamente identificado, realizó una acción explícita indicando al ERDS que acepta recibir el contenido de la notificación enviada por el emisor.
  A nivel funcional, esta evidencia se produce cuando, el usuario pulsa el link que le llega en el correo electrónico de aviso de notificación, y este link le lleva a una ventana donde puede aceptar o rechazar, esta evidencia es la que se genera en el caso de que acepte.
  Estado alcanzado del acta: Puesta a disposición

- **C.4 ConsignmentRejection:**
  Rechazo de la notificación: se evidencia que el destinatario, debidamente identificado, realizó una acción explícita indicando al ERDS que rechaza recibir el contenido de la notificación enviada por el emisor
  A nivel funcional, esta evidencia se produce cuando, el usuario pulsa el link que le llega en el correo electrónico de aviso de notificación, y este link le lleva a una ventana donde puede aceptar o rechazar, esta evidencia es la que se genera en el caso de que rechace.
  Estado alcanzado del acta: Rechazada

- **C.5 AcceptanceRejectionExpiry:**
  Caducidad de la aceptación/rechazo: El servicio de entrega electrónica certificada de WSG envió una notificación al destinatario, pero éste no respondió a la notificación con una aceptación/ rechazo. Es decir, se evidencia 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.
A nivel funcional, esta evidencia se produce cuando, pasados 10 días desde la fecha de envío del correo electrónico al destinatario, no se ha producido aceptación o rechazo de la notificación.
Estado alcanzado del acta: Caducada

### 8.4.4 Eventos de entrega del contenido de usuario al destinatario

- **D.1 ContentConsignment:**
  Contenido de la notificación: se evidencia el propio contenido de la notificación, donde consta la fecha de puesta a disposición hacia el destinatario.
  Estado alcanzado del acta: Puesta a disposición

- **E.1 ContentHandover:**
  Entrega del contenido de usuario al destinatario: Se evidencia que el contenido de la notificación ha pasado con éxito la frontera del servicio de entrega electrónica certificada y se entrega con éxito al destinatario, previa su autenticación.
  El evento indicará un “PULL”, es decir, que el destinatario, proactivamente, solicita la descarga del contenido.
  A nivel funcional, esta evidencia se produce cuando, en el Portal del Receptor, el usuario destinatario pulsa el botón Detalle en el listado de sus notificaciones.
  Estado alcanzado del acta: Entregada

WSG conserva todas estas evidencias, y se incorporan al documento PDF emitido y sellado por WSG con un certificado de sello electrónico cualificado y un sello de tiempo. Este documento quedará a disposición de las partes y terceros interesados durante todo el plazo de conservación. Para obtener una copia electrónica del mismo, la parte interesada puede descargarlo en cualquier momento desde los portales de emisión y recepción de ERDS MEE.

# 9 REFERENCIAS DE TIEMPO

Las referencias de tiempo se establecen en cada uno de los eventos del Servicio de Entrega Electrónica Certificada, en concreto:

Se indicará la fecha y hora del envío del contenido del usuario por parte del emisor al servicio de entrega electrónica certificada de WSG y de la recepción por parte del destinatario, mediante un sello electrónico de tiempo cualificado, emitido por Ivnosys o por Izenpe; ambos son Prestadores de Servicio de Sellado de Tiempo Cualificados.

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

WSG comprobará, al menos una vez al año, que los Prestadores del Servicio de Sello de tiempo utilizados continúan siendo cualificados, realizando una interpretación de la TSL conforme con lo indicado por la Comisión Europea.

# 10 SEGURIDAD FÍSICA, GESTIÓN Y OPERACIONES

## 10.1 Controles de seguridad física

WSG garantiza que cumple plenamente con la legislación aplicable en todos los aspectos de seguridad física descritos a lo largo de este documento y en sus procedimientos internos.

Para dar cumplimiento al servicio, se han establecido distintos centros donde se llevan a cabo las actividades críticas o sensibles, con barreras de seguridad y controles de entrada apropiados dotados de mecanismos de control de seguridad para reducir el riesgo de accesos no autorizados o de daños a recursos informáticos.

**Ubicación de las instalaciones**

Todas las instalaciones desde donde se ofrece el servicio disponen de medidas de seguridad de control de acceso de forma que el desarrollo de la actividad, así como, la prestación de los servicios, sean realizados con las suficientes garantías de confidencialidad y seguridad.

Con el objetivo de garantizar la seguridad y la continuidad de los servicios, WSG dispone de una infraestructura basada en proveedores de Cloud Pública que ofrecen un servicio de hosting. Se proporciona una arquitectura de red y un centro de datos diseñado para satisfacer los requisitos de seguridad más exigente , con unos niveles de protección y seguridad adecuados. El proveedor donde se alojan los servidores de producción que prestan el servicio poseen las certificaciones en seguridad más relevantes.

**Medidas de seguridad física**

A continuación, se citan, con carácter enunciativo, algunas medidas de seguridad en la prestación del servicio:

**Acceso físico**

- Los edificios tienen establecidas medidas físicas de control de accesos y seguridad perimetral compuesta por distintos anillos con los adecuados medios técnicos y humanos para garantizar la seguridad de las instalaciones.

  Además de la seguridad exterior perimetral, se dispone de diversos medios de control interior, salas e instalaciones protegidas mediante CCTV, detectores de intrusión, control de acceso, detectores de incendio, etc.

- Se dispone de un exhaustivo sistema de control físico de personas en el acceso al edificio.

- Todas las operaciones críticas se realizan en un entorno cerrado y controlado con medidas de seguridad adicionales.

**Electricidad y aire acondicionado**

- Las salas donde se ubican las máquinas de la infraestructura del servicio, disponen de suministro de electricidad, así como aire acondicionado, creando un entorno operativo fiable. Adicionalmente, el sistema está protegido contra caídas de tensión o cualquier anomalía ya que el sistema deviene redundado por doble acometida eléctrica.

- En el caso de AWS, ofrece sistemas de suministro eléctricos diseñados para que puedan duplicarse y mantenerse por completo sin que ello repercuta en las operaciones, 24 horas al día.

- Del mismo modo, se han instalado mecanismos de control de calor y humedad y sondas de líquidos para conseguir plena y correcta operatividad.

- Seguridad del cableado: el cableado se encuentra en un falso suelo o techo y dispone de los medios adecuados para su protección.

**Prevención y protección contra incendios**

- Las salas disponen de medios adecuados (equipos de detección y extinción de incendios) para protección del contenido sito en ellas.

**Almacenamiento de soportes y copias de seguridad/restauración**

- Las copias de seguridad se realizan también en entornos de los proveedores de hosting y se dispone de un registro de copias de seguridad para una eventual restauración de emergencia.
- Existen planes de contingencia del servicio que maneja WSG, todo encaminado a preservar la continuidad de negocio en caso de cualquier anomalía.

**Ubicación física del personal que presta el mantenimiento del servicio**

Todos los servicios de ERDS MEE se prestan 100% desde los entornos de los proveedores de hosting contratados a tal efecto, la ubicación física de dichos entornos, así como todas las medidas de seguridad descritas recaen en dichos proveedores.

El personal de WSG que realiza las labores de mantenimiento del servicio opera desde distintas oficinas físicas de WSG, las cuales tienen implementadas sus propias medidas de seguridad física.

WSG dispone de un procedimiento denominado "***ERDS_MEE_2.18._Seguridad_fisica_y_del_entorno***" donde se encuentran recogidas de forma detallada las medidas físicas que se han implantado tanto en WSG como en los proveedores que prestan servicios de hosting, de tal forma que se protejan las instalaciones, tanto de accesos no autorizados como de los daños que puedan ocasionar catástrofes naturales o fenómenos medioambientales.

## 10.2 Controles de seguridad lógica

Los empleados de WSG únicamente tendrán acceso a los sistemas de información del servicio de entrega electrónica certificada según su perfil y a aquella información que sea necesaria para el ejercicio de sus funciones.

Los datos concernientes a este apartado se consideran información confidencial y sólo se proporcionan a quien acredite necesidad de conocer, como en el caso de auditorías externas, internas o inspecciones por parte de las autoridades habilitadas.

WSG dispone de un procedimiento denominado "**ERDS_MEE_2.21._Control_de_acceso_logico**" donde se encuentra recogida de forma detallada la información referente a la seguridad lógica.

## 10.3 Evaluación de la seguridad informática

WSG evalúa de forma permanente su nivel de seguridad con el fin de identificar posibles debilidades y establecer las correspondientes acciones correctoras mediante la realización de auditorías internas y externas, así como la realización de controles periódicos de seguridad.

## 10.4 Controles de seguridad del ciclo de vida

WSG encarga periódicamente revisión de todos sus sistemas y aplicaciones implicadas en la gestión del servicio.

## 10.5 Controles de adquisición y desarrollo de sistemas

WSG se encarga de posicionar el nivel de seguridad exigible tanto en la adquisición como en la prueba y desarrollo de sistemas informáticos que puedan tener algún impacto en el servicio que realiza. Existe un procedimiento específico que lo regula.

La revisión de la configuración de los sistemas tiene una periodicidad mínima anual, ó cuando se produzca cualquier cambio relevante que afecte a la misma.

# 11 PRIVACIDAD Y PROTECCIÓN DE DATOS

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**") WSG se compromete a respetar la privacidad y protección de los datos de los interesados, de conformidad con la normativa anteriormente referenciada, con su Política de Privacidad y los Términos y Condiciones del servicio. En este sentido, WSG dispone de un Registro de Actividades de Tratamientos de datos de carácter personal en el que se encuentra el tratamiento necesario para la provisión y gestión del Servicio de Entrega Electrónica Certificada.

De acuerdo con lo anterior, se informa al usuario de los siguientes aspectos relacionados con el tratamiento de datos derivado de la prestación del Servicio de Entrega Electrónica Certificada:

WSG (WISE SECURITY GLOBAL, S.L.), con dirección postal Alameda Recalde 34, 48009 Bilbao (ESPAÑA) teléfono +34 910 700 549, tratará los datos con la finalidad de poder prestar el servicio solicitado en los términos establecidos en la normativa vigente, en la presente DPC y, en su caso, en los Términos y Condiciones alcanzados entre los intervinientes y WSG.

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

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

Por otro lado, cuando exista una relación contractual previa con WSG, esta última podrá remitir al usuario comunicaciones comerciales por correo electrónico siempre que se refieran a productos o servicios similares a los que inicialmente fueron objeto de contratación. En cada una de las comunicaciones comerciales que así se realizaran se ofrecerá al destinatario la posibilidad de oponerse al tratamiento con este fin de un modo sencillo y gratuito.

El usuario 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 a la dirección de correo electrónico

legal@wsg127.com como por correo postal, en la dirección arriba indicada, acompañándolo con el documento de identidad. No obstante, si el interesado piensa que su derecho puede haber sido vulnerado, puede realizar una reclamación ante la Agencia Española de Protección de Datos.

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

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

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

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

Por otro lado, los datos personales que facilite directamente el interesado o por terceros forman parte de un fichero responsabilidad de WSG. con la finalidad de gestionar y mantener los contactos y relaciones que se produzcan como consecuencia de la relación que mantiene con WSG. La base jurídica que legitima este tratamiento será la necesidad de gestionar una relación contractual o similar.

Se deberán utilizar únicamente para la finalidad a la que se destina y no se permite transmitirlos a terceros. El plazo de conservación de estos datos vendrá determinado por la relación que mantenida entre el interesado y WSG.

Los datos de carácter personal no serán objeto de cesión o comunicación a terceras personas sin el previo consentimiento del interesado, salvo aquellas cesiones que deban llevarse a cabo porque medie obligación legal, por ejemplo, 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.

WSG, en el marco de la prestación del servicio con el cliente, tratará los datos solo mediante instrucciones documentadas del cliente (quien intervendrá como Responsable del tratamiento), y adoptará en todo caso las medidas técnicas y organizativas adecuadas para que el tratamiento cumpla los requisitos legales, asegurando, concretamente, un nivel de seguridad adecuado al riesgo, la defensa de los derechos de los titulares de los datos, teniendo en cuenta las técnicas más avanzadas, los costes de aplicación y la naturaleza, el ámbito, el contexto y las finalidades del tratamiento, así como los riesgos, de probabilidad y gravedad variable, para los derechos y libertades de las personas físicas, incluyendo:

- La seudonimización y el cifrado de los datos personales.
- La capacidad de asegurar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y de los servicios de tratamiento.
- La capacidad de restablecer la disponibilidad y el acceso a los datos personales de forma oportuna en el caso de un incidente físico o técnico.
- Un proceso para probar, evaluar y valorar regularmente la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Para más información respecto al tratamiento de datos que realiza WSG, el interesado puede ponerse en contacto con WSG enviando un escrito a la siguiente dirección:

Alameda Recalde 34
48009 Bilbao
o mediante un correo electrónico al Delegado de Protección de Datos de WSG (dpo@wsg127.com), acompañando los documentos exigidos por la normativa.

Así mismo, el personal de WSG tiene deber de confidencialidad respecto de la información que maneje por razón de su puesto de trabajo. La información catalogada como “confidencial”, no será divulgada en ningún caso a terceros, salvo que se encuentre amparada en los supuestos de colaboración con autoridades e instituciones competentes.

Se considerará como información confidencial, toda aquella información que no se haya declarado como pública de forma expresa y de manera general:

- Planes de contingencia y continuidad de negocio.
- Información relativa a la operativa de operaciones y mantenimiento del servicio.

- Información relativa a parámetros de control. Seguridad y procedimientos de auditoría.
- Información de datos de carácter personal que haya sido proporcionada a WSG durante el proceso de registro de los suscriptores del servicio.
- Información relativa al negocio.
- Registros de transacciones, registros completos y registros de logs.
- En general todo aquello clasificado como “CONFIDENCIAL”.

Así mismo, se considerará como información pública:

- El presente documento de Declaración de Prácticas de Certificación del Servicio de Entrega Electrónica Certificada.
- Los Términos y Condiciones del Servicio.
- La Política de privacidad de WSG.
- Toda aquella información que se haya catalogado como “PÚBLICA”.

# 12 ROLES DE CONFIANZA

Los roles de confianza son estatus referidos al grado de seguridad o la asignación de determinadas tareas por parte de alguien facultado y autorizado a ello.

Estos roles incluyen:

- **Administrador de sistemas**: Los Administradores de Sistemas están autorizados a configurar, instalar y mantener los sistemas confiables de WSG para la gestión de los servicios incluyendo la recuperación del sistema.
- **Operador del sistema**: Son los responsables de operar los sistemas de WSG de manera habitual. Sus funciones versan sobre operación en general y backup.
- **Auditor interno**: Estará autorizado a visionar archivos, así como, auditar los logs de los sistemas confiables de WSG. Este se debe encargar de comprobar el seguimiento de incidencias y eventos, la protección de los sistemas, así como comprobar alarmas y elementos de seguridad física.
- **Responsable de seguridad**: Se encargará de la administración de la implementación de las prácticas de seguridad y de los procedimientos de seguridad, tanto de forma física como de forma lógica. Este debería encargarse de verificar que toda la documentación se halle accesible cuando sea requerida y se tenga correctamente enumerada, será, así mismo, el encargado de comprobar la coherencia de la documentación con los procedimientos, activos inventariados, etc.
- **Responsable del servicio:** se encargará del mantenimiento y gestión del servicio de entrega electrónica certificada de WSG, de tal forma que se implanten todos aquellos requerimientos técnicos y operativos que se vayan incorporando en las normas aplicables. Igualmente, se encarga de todos los aspectos de seguridad relacionados con el servicio, y los gestionará de forma conjunta con el Responsable de Seguridad.

# 13 AUDITORÍAS DE CUMPLIMIENTO

Todas las herramientas, informes o registros, ficheros y fuentes relacionadas con la elaboración o registro de una auditoría son consideradas información confidencial y sensible y como tal, son tratadas en todos sus aspectos, estando su acceso restringido a personas autorizadas.

## 13.1 Frecuencia de las auditorías

Periódicamente, se elaborarán los correspondientes planes de auditorías que contemplan como mínimo la revisión de:

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

El servicio cualificado de entrega electrónica certificada incluido en la presente DCP está sometido a auditorías periódicas, según dicta el esquema de certificación correspondiente, relacionadas con el estándar europeo ETSI EN 319 401 “General Policy Requirements for Trust Service Providers”.

Dicha auditoría será realizada anualmente por una empresa externa que se encuentre debidamente acreditada.

Cada uno de los Servicios cualificados de Confianza que presta WSG será auditado conforme al esquema correspondiente, y así queda manifestado en la correspondiente declaración de Prácticas Particulares de dicho servicio.

## 13.2 Cualificación del auditor

El auditor que verifique y compruebe la correcta operativa de WSG, deberá ser una persona con suficiente titulación oficial, así como deberá contar con la adecuada y demostrable experiencia sobre la materia a auditar, conforme a la legislación que se encuentre en cada momento en vigor.

Siempre y junto con el informe obtenido durante la auditoría, figurará el nombre e identificación de los auditores, estando este informe firmado por ellos y por el responsable de la entidad auditada.

## 13.3 Relación del auditor con la empresa auditada

La realización de las auditorías podrá ser encargada bien a Empresas Auditoras Externas o bien a personal interno cualificado para ello, según la legislación vigente al respecto, o bien a ambas cosas. En el caso del personal interno y, del mismo modo, dependiendo del nivel de criticidad del área o sistema a auditar, el grado de independencia del dicho personal, así como, su nivel de experiencia será objeto de concreción caso por caso, atendiendo a parámetros de independencia funcional.

En los casos en los que las auditorías sean realizadas por personal externo a WSG, se establecerán medidas y controles adicionales para garantizar que los requisitos de la auditoría son cumplidos con total rigurosidad. Adicionalmente, se firmarán acuerdos de acceso a información sensible y demás acuerdos de Confidencialidad y responsabilidad.

En las auditorías externas, el auditor, así como, la empresa auditora no tendrá nunca ningún tipo de relación laboral, comercial o de otra índole con WSG, ni con la parte que solicite la auditoría siendo siempre un profesional totalmente independiente quien realiza la auditoría solicitada.

En el caso de la auditoria del servicio de entrega electrónica certificada para ser considerado un servicio cualificado conforme a eIDAS, dicha auditoria será realizada obligatoriamente por una empresa externa que esté debidamente homologada para la realización de la misma.

## 13.4 Comunicación de los resultados de la auditoría

Las autoridades administrativas o judiciales independientes pueden solicitar los informes de auditorías para verificar el buen funcionamiento de la plataforma.

El resultado de la auditoria de la evaluación de la conformidad con eIDAS para que el servicio de entrega electrónica certificada de WSG sea considerado un servicio cualificado, será entregado al órgano de supervisión en España, para que éste le conceda o, en su caso, le mantenga dicha cualificación.

# 14 CONDICIONES Y GARANTÍAS DE USO

El servicio de entrega electrónica certificada se realizará siempre conforme a la función y finalidad que viene establecida en la Presente Declaración de Prácticas del Servicio de Entrega Electrónica Certificada, a los Términos y Condiciones del Servicio y con arreglo a la normativa vigente.

El Servicio Cualificado de Entrega Electrónica Certificada proporciona la entrega segura y confiable de mensajes electrónicos entre las partes implicadas produciendo una evidencia en el proceso de entrega lo que permite una certificación del hecho a nivel legal. De este modo, la evidencia puede verse como una declaración de una parte confiable de que un evento específico relacionado con el proceso de entrega ocurrió en un momento determinado.

**Disponibilidad del servicio**

El servicio Cualificado de Entrega Electrónica Certificada de WSG estará disponible 24 horas al día, durante 7 días de la semana. La disponibilidad es la capacidad de acceso al servicio por parte de quien lo demanda, con independencia de su rapidez. La disponibilidad a la que WSG se compromete quedará reflejada en un Acuerdo de Nivel de Servicio firmado con cada uno de sus clientes.

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

Las partes que confían en este servicio de entrega electrónica certificada pueden obtener información del servicio enviando un correo a info@wsg127.com. En la prestación de los servicios descritos en esta DPC, WSG garantiza que no operará de modo que se produzca algún tipo de práctica discriminatoria.

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 WSG.

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 “**ERDS_MEE_2.16.Gestion del plan de continuidad del servicio**”.

El objetivo de este procedimiento es establecer las directrices de la estrategia de contingencia ante incidentes o desastres en los sistemas que soportan los procesos de negocio de WSG. Dicha procedimiento incluye planes, instrucciones y medidas que

permitan la continuidad o el restablecimiento de la operatividad de sistemas de información 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.

## 14.1 Condiciones económicas

Las tarifas aplicables a los servicios de entrega electrónica certificada, en las condiciones expuestas en la presente DPC, serán facilitadas a los clientes o potenciales clientes por el Departamento Comercial de WSG. El precio por la prestación del servicio en condiciones especiales será el pactado en cada caso con el cliente y constará en el correspondiente contrato.

Serán aplicables únicamente al emisor de la comunicación, siendo éste un servicio gratuito para los destinatarios.

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

# 15 RESPONSABILIDADES

WSG como Prestador de Servicios de Confianza se encuentra sujeto al régimen de responsabilidad recogido en el artículo 13 del Reglamento eIDAS y 10 de la Ley 6/2020, reguladora de determinados aspectos de los servicios electrónicos de confianza (LSEC) 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, y cumpliendo con la obligación del artículo 9.3.b) de la LSEC, WSG ha suscrito un seguro de responsabilidad civil de Dos (2) millones de euros para afrontar el riesgo de la responsabilidad civil por los daños y perjuicios que pueda ocasionar con motivo del incumplimiento por su parte de las obligaciones que impone el Reglamento eIDAS.

## 15.1 Limitaciones de responsabilidad

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

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

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

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

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

# 16 CESE DEL SERVICIO

En caso de cese del Servicio Cualificado de Entrega Electrónica Certificada, deberán tenerse en cuenta los siguientes aspectos, WSG dispone de un Plan de Cese, donde se tiene en cuenta los siguientes aspectos

## 16.1 Acciones previas al cese de actividad

En el supuesto de que WSG cese como Prestador de Servicios de Confianza, notificará, con una antelación mínima de dos meses, o en un periodo de tiempo lo más corto posible, a usuarios, y personas interesadas, mediante una publicación en la página web del servicio.

## 16.2 Comunicación a interesados y terceras partes

WSG informará del cese del servicio a todos los clientes, así como entidades con las que existan acuerdos, contratos u otras formas de relación establecidas entre las que se incluyen las prácticas de confianza, por medio de un servicio que acredite la entrega y recepción efectiva de la comunicación, siempre que sea factible

## 16.3 Notificación al organismo de supervisión

WSG se compromete a comunicar al Ministerio y autoridades competentes en materia de Servicios Electrónicos de Confianza, en un plazo máximo de 3 meses, el cese de actividad como Prestador de Servicios de Confianza, así como de cualquiera otra circunstancia relevante con el cese de actividad.

## 16.4 Transferencia de obligaciones

WSG, se compromete a transferir sus obligaciones a un prestador de servicios de confianza para mantener y no comprometer, en ningún momento, toda la información necesaria sobre evidencias, logs y eventos de las operaciones durante el periodo de tiempo que se haya comprometido, a menos que se pueda demostrar que WSG no disponga de tal información.

WSG se compromete a recopilar toda la información y transferirla a un prestador de servicios de confianza con la que se disponga de un acuerdo de ejecución del Plan de Cese en caso quiebra.

En caso de, que llegado el momento no sea posible realizar dicha transferencia ni acordar el traspaso con otro Prestador de Servicios de Confianza, esta información se remitirá al Ministerio competente en Servicios Electrónicos de Confianza.

Cuando se produzca un cese de actividad sin que implique una situación de quiebra, la información será convenientemente almacenada.

## 16.5 Gestión de las claves del servicio

WSG se compromete a destruir tanto las claves privadas, como las copias de seguridad, de modo que éstas no puedan ser recuperadas de modo alguno. En el caso de que las claves privadas fueran gestionadas por un Prestador de Servicios de Confianza Cualificado, ordenará a éste la revocación del certificado y la destrucción de la clave privada.

## 16.6 Obligaciones por Wise Security Global, tras el cese de su actividad

WSG, dispone de un acuerdo suscrito, con el fin de cubrir los costes de operación para cumplir con unos requisitos de operabilidad mínima en caso de quiebra o por las razones en el caso de que no pudiera cubrir con los costes por sí misma, siempre atendiendo a la legislación aplicable en materia de quiebra.

WSG, se obliga a mantener sus obligaciones para dejar disponible su clave pública a las partes de confianza durante el periodo de tiempo legalmente establecido, cumpliendo con sus obligaciones para que esto se cumpla

# 17 LEGISLACION APLICABLE

WSG se someterá, en caso de controversia a los Tribunales de España para su resolución, sin perjuicio del derecho de que dispone WSG de iniciar un proceso judicial ante los tribunales de justicia del cliente.

Las normas de aplicación serán las siguientes:

- Reglamento (UE) Nº 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 (eIDAS)
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza (LSEC).
- 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 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos o RGPD).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).
- Ley 34/2002 de servicios de la sociedad de información y comercio electrónico.

Adicionalmente, podrán ser de aplicación los siguientes estándares:

- 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”.

- ETSI EN 319 102-1 “Electronic Signatures and Infrastructures (ESI). Procedures for Creation and Validation of AdES Digital Signatures. Part1: Creation and Validation”
- ISO/IEC 29115: “Information Technology - Security techniques - Entity authentication assurance framework
- ISO/IEC 27001:2014. Information technology. Security techniques. Information security management systems. Requirements
- ISO/IEC 27002:2013. Information technology. Security techniques. Code of practice for information security controls.
- NIST SP 800-63B “Digital Identity Guidelines Authentication an Lifecycle Management”.

# 18 APROBACION Y REVISIÓN DE LA PRESENTE DPC

## 18.1 Aprobación de la DPC

La aprobación de la presente Declaración de Prácticas de Certificación corresponde al Responsable del Servicio.

WSG ha creado un Comité de Ciberseguridad responsable de la implantación de las políticas y procedimientos organizativos y de seguridad necesarios para garantizar el cumplimiento de los requisitos establecidos en la presente Declaración de Prácticas de Certificación.

Una vez aprobada, la DPC se hará pública mediante su publicación en la página web de WSG.

## 18.2 Modificación de la DPC

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

Cuando la DPC sea modificada, deberá ser notificada al Organismo competente en materia de Servicios Electrónicos de Confianza.

La última versión aprobada de la DPC deberá publicarse en la página web de WSG.

Los cambios que se realicen que puedan afectar de forma sustancial a los suscriptores del servicio o a terceros se notificarán haciéndolo público en la web de WSG.

Los 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.

# 19 RECLAMACIONES Y RESOLUCIÓN DE CONFLICTOS

WSG responderá en el plazo máximo de 30 días a cualquier reclamación que puedan plantear los usuarios de los servicios. Dichas reclamaciones deberán ser remitidas por escrito a la siguiente dirección de correo info@wsg127.com

Para toda controversia que no pueda ser resuelta de forma amistosa, en relación con la prestación de los servicios WSG, los usuarios personas jurídicas aceptan la jurisdicción y competencia de los Juzgados y Tribunales de la Ciudad de Madrid, con expresa renuncia a cualquier otro fuero que pudiera corresponderles. En cuanto a las reclamaciones planteadas por personas físicas, la jurisdicción competente será aquella a la que en cada momento remita la legislación procesal española.

# 20 OTRAS ESTIPULACIONES

Los Usuarios de los servicios de WSG a los que se refiere la presente Declaración de Practicas, aceptan en su totalidad el contenido del documento. La declaración de invalidez de alguno de sus apartados no afectará a la validez del resto.