eGarante
testigo online

Declaración de Prácticas de Certificación

Versión: 1.0

Fecha: 21 de abril de 2016

Introducción

En la actualidad, el uso de Internet para el establecimiento de relaciones comerciales o regular otro tipo de relaciones entre las personas es muy habitual. En el aspecto de las comunicaciones públicas, los proveedores de servicios publican información y condiciones acerca de sus productos o servicios. En el ámbito de las comunicaciones privadas, el correo electrónico se utiliza de manera continua para negociar, acordar y notificar condiciones contractuales y decisiones como pedidos, cancelaciones, etc.

La naturaleza de la tecnología empleada en estas comunicaciones hace que la prueba de que las mismas se hayan producido y con qué contenido sea compleja.

Ámbito de comunicaciones públicas – contenidos web

Si nos centramos en el ámbito público, en muchas ocasiones se toman decisiones basadas en la información presentada por una persona (física o jurídica) en Internet. Por este medio, se producen violaciones de derechos como el derecho a la propiedad intelectual, el derecho al honor o a la seguridad. El problema surge de la existencia de una enorme facilidad de cambiar los contenidos de una página web sin que quede rastro fiable de la publicación anterior. Esto hace necesaria la existencia de un medio que permita probar que en un momento determinado existía un contenido determinado en una web.

Ámbito privado – correos electrónicos e intercambio de documentos

Si nos centramos en el ámbito privado, algo similar sucede con los correos electrónicos. En numerosas ocasiones las relaciones entre las personas se basan en ofertas y contraofertas realizadas mediante correo electrónico. Lamentablemente, los protocolos comúnmente utilizados no ofrecen garantías sólidas para poder usar los mismos en caso de disputa sin tener que pasar por un complejo, y en muchas ocasiones impredecible, proceso de peritaje de las comunicaciones. Por tanto, es también necesaria la existencia de un medio que permita obtener una prueba independiente de la realización de estas comunicaciones electrónicas privadas entre partes.

Solución de eGarante

eGarante, en el contexto de la Ley 59/2003 de Firma Electrónica, ha diseñado unos procesos que, haciendo uso de la firma electrónica y del sello de tiempo, permiten actuar como tercero independiente para certificar el acaecimiento de determinadas comunicaciones por medios electrónicos, tanto en el ámbito público (páginas web) como privado (correos electrónicos y entrega certificada de documentos).

eGarante desarrolla por tanto un conjunto de servicios enfocados a obtener evidencias digitales de estas comunicaciones haciendo uso de la firma electrónica y los sellos de tiempo. Para poder hacer esto, además de tener que ser un sistema fiable desde el punto de vista de certificación, nos hemos esforzado para cumplir con 3 características importantes:

1. Que sea sencillo y no altere el medio de trabajo habitual del usuario, es decir que no suponga cambios en el uso del correo electrónico.

2. Que permita certificar no solo los correos electrónicos enviados sino también los correos recibidos.
3. Que tenga un coste económico que permita ser utilizado de manera generalizada para todas las comunicaciones realizadas por un usuario.

Administración de las políticas

Entidad responsable

EGARANTE SL, con domicilio social en Madrid, Paseo de la Castellana 100, Esc. Dcha., 2ºB (28046), con N.I.F. nº B86669819 es la empresa responsable de la elaboración de este documento de Declaración de Prácticas de Certificación.

Datos de contacto

Organización	eGarante, S.L.
Persona de contacto	Director Técnico de eGarante
Correo electrónico	administracion@egarante.com
Teléfono	+34 910 052 653
Dirección	Paseo de la Castellana 100 Escalera Derecha 2ºB Madrid 28046

Procedimientos de aprobación y responsables de adecuación

Los Administradores de eGarante S.L. (en adelante, eGarante) son los responsables de la aprobación de la primera versión de este documento, así como de sus sucesivas versiones.

Definiciones

A los efectos de clarificar los términos y conceptos del presente Documento de Seguridad, se establecen las siguientes definiciones:

- **Accesos autorizados**: autorizaciones concedidas a un usuario para la utilización de los diversos recursos. En su caso, incluirán las autorizaciones o funciones que tenga atribuidas un usuario por delegación del responsable del fichero o tratamiento o del responsable de seguridad.
- **Afectado o interesado**: persona física titular de los datos que sean objeto del tratamiento.
- **Autenticación**: procedimiento de comprobación de la identidad de un usuario.
- **Bloqueo de datos**: la identificación y reserva de los datos de carácter personal con el fin de impedir su tratamiento.

- **Cancelación**: Procedimiento en virtud del cual el responsable cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, con el fin de impedir su tratamiento, excepto para su puesta a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y solo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos.
- **Cesión o comunicación de datos**: toda revelación de datos realizada a una persona distinta del titular. Toda obtención de datos resultante de la consulta de un Fichero, la publicación de los datos contenidos en el Fichero, su interconexión con otros Ficheros y la comunicación de datos realizada por una persona distinta de la afectada.
- **Cesionario**: toda persona o entidad, de titularidad pública o privada, receptora de los datos cedidos.
- **Consentimiento del interesado**: toda manifestación de voluntad mediante la que el interesado consienta el tratamiento de datos personales que le conciernen. Esta manifestación ha de ser libre, inequívoca, específica e informada.
- **Contraseña/llave de acceso**: información confidencial frecuentemente constituida por una cadena de caracteres, que puede ser usada para la autenticación de un usuario o en el acceso a un recurso. Para los ficheros en formato papel, al archivador que guarde el fichero se accederá mediante una llave o clave de acceso.
- **Control de acceso**: mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.
- **Copia de respaldo**: copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.
- **Dato de carácter personal**: cualquier información numérica, alfabética, gráfica, fotográfica, acústica, o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión, concerniente a una persona física identificada o identificable.
- **Datos accesibles al público**: son todos aquellos datos que pueden encontrarse a disposición del público en general. Su acceso y conocimiento no se encuentra limitado por norma legal alguna, y suelen estar recogidos en Diarios y Boletines Oficiales, medios de comunicación, censos, anuarios, bases de datos públicas, repertorios y anuarios legales y de jurisprudencia, archivos de prensa, repertorios telefónicos y análogos, así como los datos publicados referentes a grupos de personas en los que su agrupación lo es en función de categorías o actividades y grupos profesionales y que contengan

exclusivamente los nombres, títulos profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo.

- **Datos de carácter personal relacionados con la salud**: Las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética.
- **Dato disociado**: Aquél que no permite la identificación de un afectado o interesado.
- **Declarante**: Persona física que cumplimenta la solicitud de inscripción y actúa como mediador entre la Agencia y el titular/responsable del fichero. No debe necesariamente coincidir con el titular/responsable.
- **Derechos de acceso**: autorizaciones concedidas a un usuario para la utilización de los diversos recursos de un sistema, normalmente informático.
- **Destinatario o cesionario**: La persona física o jurídica, pública o privada u órgano administrativo, al que se revelen los datos. Podrán ser también destinatarios los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.
- **Documento**: todo escrito, gráfico, sonido, imagen o cualquier otra clase de información que puede ser tratada en un sistema de información como una unidad diferenciada.
- **Encargado del tratamiento**: La persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio. Podrán ser también encargados del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.
- **Exportador de datos personales**: la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice, conforme a lo dispuesto en el presente Reglamento, una transferencia de datos de carácter personal a un país tercero.
- **Fichero**: Todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.
- **Ficheros de titularidad privada**: los ficheros de los que sean responsables las personas, EGARANTE o entidades de derecho privado, con independencia de quien ostente la titularidad de su capital o de la procedencia de sus recursos económicos, así como los ficheros de los que sean responsables las corporaciones de derecho público, en cuanto

dichos ficheros no se encuentren estrictamente vinculados al ejercicio de potestades de derecho público que a las mismas atribuye su normativa específica.

- **Ficheros de titularidad pública**: los ficheros de los que sean responsables los órganos constitucionales o con relevancia constitucional del Estado o las instituciones autonómicas con funciones análogas a los mismos, las Administraciones públicas territoriales, así como las entidades u organismos vinculados o dependientes de las mismas y las Corporaciones de derecho público siempre que su finalidad sea el ejercicio de potestades de derecho público.
- **Fichero no automatizado**: todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica.
- **Ficheros temporales**: ficheros de trabajo creados por usuarios o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento.
- **Fuentes accesibles al público**: Aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público, los Diarios y Boletines oficiales y los medios de comunicación.
- **Identificación del afectado**: Cualquier elemento que permita determinar directa o indirectamente la identidad física, fisiológica, psíquica, económica, cultural o social de la persona afectada.
- **Identificación del usuario**: procedimiento de reconocimiento de la identidad de un usuario.
- **Importador de datos personales**: La persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargada del tratamiento o tercero.
- **Incidencia**: cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

- **Perfil de usuario**: accesos autorizados a un grupo de usuarios.
- **Persona identificable**: Toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados.
- **Procedimiento de disociación**: Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.
- **Recurso**: cualquier parte componente de un sistema de información.
- **Responsable del fichero o del tratamiento**: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que solo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente. Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.
- **Responsable de seguridad**: persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.
- **Sistema de información**: conjunto de ficheros, tratamientos, programas, soportes y en su caso, equipos empleados para el tratamiento de datos de carácter personal.
- **Sistema de tratamiento**: modo en que se organiza o utiliza un sistema de información. Atendiendo al sistema de tratamiento, los sistemas de información podrán ser automatizados, no automatizados o parcialmente automatizados.
- **Soporte**: objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos.
- **Tercero**: la persona física o jurídica, pública o privada u órgano administrativo distinta del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento. Podrán ser también terceros los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.
- **Transferencia de datos**: El transporte de los datos entre sistemas informáticos por cualquier medio de transmisión, así como el transporte de soportes de datos por correo o por cualquier otro medio convencional.
- **Transferencia internacional de datos**: Tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien

constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español.

- **Transmisión de documentos**: cualquier traslado, comunicación, envío, entrega o divulgación de la información contenida en el mismo.
- **Tratamiento de datos**: cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, modificación, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.
- **Usuario**: sujeto o proceso autorizado para acceder a datos o recursos. Tendrán la consideración de usuarios los procesos que permitan acceder a datos o recursos sin identificación de un usuario físico.

Repositorios y publicación de información

Repositorio

eGarante dispone de una sección en su web https://www.egarante.com con un repositorio de los documentos de información pública. Esta información está accesible 24 horas al día.

Publicación de información

eGarante pone a disposición en dicho repositorio las versiones corrientes de los siguientes documentos:

- Declaración de Políticas de Certificación
- Condiciones generales de uso de la web de eGarante
- Condiciones generales de contratación de los servicios de eGarante

Frecuencia de publicación

Las modificaciones realizadas a estos documentos supondrán la publicación inmediata de las nuevas versiones y el archivo de las anteriores, que dejarán de estar disponibles en la web y podrán ser solicitadas por clientes que hubiesen contratado cuando estaban vigentes.

Control de acceso al repositorio

Los repositorios disponibles en la web de eGarante están disponibles para acceso público.

Idioma y normativa

La presente Declaración de Prácticas de Certificación, así como los demás documentos oficiales y contractuales están redactados en español de España, idioma bajo el que deberán ser interpretados. La normativa aplicable a los mismos será, en todo caso, la española.

Descripción de los servicios

Como se ha informado en las secciones anteriores, los servicios prestados por eGarante no se centran en la emisión de Certificados de Firma ni en la validación de firmas sino en servicios relacionados con la Firma Electrónica ya que hacen uso de la Firma Electrónica y Sellado de Tiempo para actuar como testigo privado de las comunicaciones electrónicas.

Estos servicios estarían relacionados con la figura de Tercero de Confianza introducida por el artículo 25 de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE).

Los servicios prestados por eGarante no se enmarcan directamente en dicho artículo 25 de la LSSICE puesto que uno de los requisitos de dicho artículo es que las partes pacten previamente el archivo de sus declaraciones de voluntad, y en la mayoría de los servicios prestados por eGarante, la participación de eGarante es a petición unilateral de una de las partes.

Información común a los servicios

eGarante es una sociedad que presta servicios de comunicaciones electrónicas, en concreto de correo electrónico, que está inscrita en el registro de operadores de comunicaciones electrónicas bajo los servicios de Transmisión de Datos – Correo Electrónico.

Como consecuencia de ello, eGarante puede participar y participa como operador en el intercambio de información entre personas. En esta participación, y haciendo uso de la Firma Electrónica y Sellado de Tiempo recogidos en la legislación española, emite certificaciones sobre las actuaciones realizadas como operador que permiten generar evidencias sobre hechos acaecidos en los que la compañía ha intervenido.

Estas evidencias incluidas en soporte digital pueden ser posteriormente utilizadas como pruebas en documento privado para la resolución de disputas. No obstante, al ser emitidas por un operador registrado que es tercero ajeno a la controversia, deberían ser consideradas como dotadas de un valor adicional por su independencia por un lado y por su integridad derivada de la aplicación de robustos sistemas de sellado de tiempo y cifrado por otro.

En términos generales, en los servicios en los que participa eGarante, la compañía actúa de manera independiente, accediendo a la información y registrándola con sus propios sistemas en un entorno seguro que no es manipulable por el cliente de la compañía.

Para el caso de la certificación de páginas web, como se describe más adelante, accede a la url o URI identificada por el cliente con los propios sistemas de la compañía desde redes no manipulables por el cliente. En el caso de las comunicaciones entre direcciones de correo electrónico o de entrega de documentos certificada, la compañía certifica la información recibida del cliente así como las actuaciones llevadas a cabo para poner en conocimiento de otra parte, normalmente identificada mediante un correo electrónico, de la información previamente recibida.

Certificación de comunicaciones electrónicas entre direcciones de correo electrónico y a teléfonos móviles

Descripción general

Certificación de comunicaciones realizadas mediante correo electrónico actuando como testigo de dichas comunicaciones en dos modalidades.

Como testigo sin gestionar la totalidad de la comunicación en cuyo caso se podrá acreditar el envío, contenido, fecha y destinatarios de la comunicación, así como la entrega de un duplicado de la comunicación originariamente realizada a los destinatarios. Todo ello incluyendo un sello de tiempo que otorga a los datos una fecha de generación indubitada.

Como testigo gestionando la totalidad de la comunicación hasta el servidor de correo electrónico del destinatario en cuyo caso, además de los aspectos recogidos en el párrafo anterior se podrá acreditar la entrega al servidor del destinatario del correo electrónico enviado por el emisor. De manera similar al punto anterior, esta información quedará firmada con un sello de tiempo que otorga a los datos una fecha de generación indubitada.

Descripción detallada

eGarante es contratada por sus clientes para dejar constancia de una comunicación realizada entre el cliente y otro u otros destinatarios o de una comunicación recibida por un cliente de eGarante en una cuenta gestionada por eGarante y puesta a disposición del cliente.

En resumen, la certificación de envío de correo electrónico de eGarante tiene las siguientes características:

1. Certifica la existencia de un correo electrónico que puede haberse originado bien en una cuenta de correo del cliente gestionada por terceros o en la cuenta de correo que eGarante gestiona y pone a disposición del cliente. Como información adicional se recoge en la certificación todos los datos del correo, asunto, contenido, destinatarios, servidor desde el cual fue enviado y otra información recogida en las cabeceras del correo que puede someterse a análisis pericial.
2. Certifica, en caso de que conste en la segunda página de la certificación, la respuesta dada por los servidores de los destinatarios de los correos a la entrega de bien una copia del correo original en caso de que el origen sea una cuenta no gestionada por eGarante o bien de la entrega del correo original en caso de haber sido enviado por una cuenta gestionada por eGarante. Una respuesta con el código 250 significa que el servidor del destinatario ha recibido correctamente la copia del mensaje original y lo guarda para entregarlo al destinatario.
3. La certificación emitida por eGarante tiene una firma electrónica lo que convierte el documento en inalterable e incorpora un sello de tiempo emitido por otro Prestador de Servicios de Certificación, lo que le otorga una fecha indubitada al documento.
4. La validez de la firma puede comprobarse en la página web del gobierno de España siguiente: https://valide.redsara.es/valide/validarFirma/ejecutar.html
5. Con la certificación puede reconstruirse el contenido exacto del correo original siguiendo el procedimiento descrito en la página indicada en la misma certificación.

Información detallada del proceso seguido por eGarante para emitir la certificación

Para comprender bien la extensión de la certificación de eGarante hacemos una breve introducción de cómo funciona el servicio de correos electrónicos y posteriormente describimos cómo actúa eGarante y qué recoge exactamente su certificado.

Un correo electrónico desde que es enviado hasta que es recibido transcurre de manera esquemática por 5 lugares:

1. Programa de correo electrónico del emisor: aquí se redacta y mientras está en borrador no ha salido de ese dispositivo que está en manos del emisor.
2. Servidor de correo electrónico del emisor. Una vez se le da a enviar, el correo llega al servidor del dominio del emisor (dominio @dominiocliente.com que podría ser cualquier proveedor)
3. Internet. El servidor mira los destinatarios de los correos y busca en internet a qué servidor ha de hacer llegar los correos. En este paso comprueba que está el destinatario y además eGarante. Por un lado, manda el correo al servidor del destinatario y por otro a eGarante
4. Servidor de correo electrónico del destinatario. El servidor del dominio del destinatario, pongamos por ejemplo el de otra empresa, recibe un correo electrónico que va dirigido a persona x y lo guarda temporalmente en el buzón x@otraempresa.com esperando a que x se conecte y lo descargue
5. El programa de correo electrónico del destinatario (ya sea en PC o móvil) se conecta al servidor y le pregunta si hay nuevos mensajes. Si los hay, los descarga y le llega el mensaje al destinatario. Es similar a mirar el buzón de correos de casa o preguntar al portero si ha llegado algo.

eGarante actúa como testigo en dos escenarios distintos, si la cuenta de correo del cliente es gestionada por eGarante y si la cuenta de correo del cliente es Gestionada por un tercero. La diferencia fundamental es que en el caso de que la cuenta de correo del cliente en la que se origina la comunicación es gestionada por un tercero, la entrega del correo original al destinatario no la realiza eGarante. Por esta razón, eGarante, para asegurarse de que dicha entrega se realiza, envía una copia idéntica del correo original al destinatario.

En este proceso, eGarante tiene control para afirmar lo siguiente:

1. **Certifica la existencia de un correo electrónico con un contenido concreto.** Si el correo se ha originado en una cuenta no gestionada por eGarante, eGarante tiene conocimiento del mismo por estar en copia. Si ha sido originado en una cuenta gestionada por eGarante, tiene conocimiento del mismo por haberse originado en sus servidores. La información recogida permite conocer y regenerar el contenido íntegro del correo incluyendo texto, emisor, destinatarios y documentos adjuntos además de la información técnica de los servidores y horas que han participado en la comunicación hasta este punto.
2. En caso de ser gestor de la cuenta origen del correo, eGarante hace entrega directa del mismo al servidor/es del/de los destinatario/s. Si no gestiona la cuenta de origen, envía una copia idéntica del correo recibido junto con una certificación de haber recibido dicho correo a los destinatarios. Esto supone de manera efectiva una segunda comunicación idéntica que hace eGarante al destinatario. Tras esta

actuación, **certifica también que bien el mensaje original o bien una copia idéntica del mismo, ha sido entregada al servidor del destinatario según venga establecido en la segunda página de la certificación** (está puesto a su disposición).

3. Esta certificación la **incluye dentro de un archivo PDF firmado digitalmente** con una firma avanzada realizada con un sello de empresa emitido por un proveedor registrado en el Ministerio de Industria de servicios de certificación. Por tanto, es un documento INALTERABLE.
4. Además, **incluye una marca de tiempo, emitida por otro tercero que es Prestador de Servicios de Certificación, que fija la fecha de manera indubitada** a un momento específico incluyendo todo el contenido. Por tanto, la inalterabilidad se establece desde la fecha de su creación, que fue inmediatamente posterior al envío (plazo máximo de unos minutos) siendo dicha fecha fijada por otro tercero también registrado como prestador de servicios de certificación inscrito en el Ministerio de Industria de España.

Entrega certificada de documentos

Descripción general

Este servicio tiene como finalidad generar una evidencia de que un documento electrónico en formato pdf ha sido entregado a un destinatario identificado al menos mediante correo electrónico, pudiendo incluir otros medios de identificación adicionales como podría ser el número de teléfono o un sistema de firma electrónica como el DNI electrónico.

En dicha certificación se recogen los datos fundamentales del proceso de entrega incluyendo fecha de envío, documento entregado, fecha de entrega de la información al servidor del destinatario y, en caso de que se produzca, fecha y características de la respuesta ofrecida por el destinatario de la comunicación en los servidores controlados por la compañía, siendo dicha respuesta ligada al destinatario mediante la utilización de sistemas de validación como un código de validación específico para cada transacción.

Descripción detallada

El proceso de entrega y certificación llevado a cabo por eGarante se realiza siguiendo los pasos descritos a continuación:

1. El cliente inicia el proceso entregando a eGarante un documento en pdf así como la dirección de correo electrónico a la que desea que se efectúe la entrega del documento. Adicionalmente puede definir modelos de identificación adicional del destinatario como un teléfono móvil, un código de coordenadas previamente compartido con el destinatario u otros métodos reforzados de verificación de la identidad.
2. eGarante genera un código único de documento en base al contenido del mismo y el destinatario. Adicionalmente firma electrónicamente el documento que tiene que poner a disposición del destinatario poniendo en el campo visible de la firma dicho código y lo cifra con una contraseña para asegurar la privacidad de la información contenida en el documento. Este será el documento entregado al destinatario y objeto de la certificación.
3. eGarante crea un correo electrónico informando del proceso de entrega certificada y añade como adjunto a ese correo el pdf firmado y cifrado. Envía al destinatario dicho correo electrónico. En este correo se informa de que el emisor ha querido poner a disposición del destinatario de la información contenida en el pdf que está cifrada por razones de privacidad y que para acceder al contenido puede identificarse en la web de eGarante establecida al efecto.
4. Al entregar eGarante el correo al servidor de correo electrónico del destinatario, captura la respuesta emitida por el servidor de correo electrónico. Esta respuesta suele ser con el código 250 que significa que ha sido recibido correctamente y que se pone en cola para entregar al destinatario. También es posible que se informe de otras situaciones.
5. En el caso de que el destinatario accede a los servidores de eGarante para consultar la contraseña, eGarante refleja este acceso como confirmación de la entrega del documento al destinatario. El hecho de que solicite la contraseña es una prueba de

que ha recibido el correo y el documento. Adicionalmente para proporcionar la contraseña se requiere que nos facilite de nuevo el documento para comprobar su integridad. Como consecuencia de ello solo se facilita la contraseña si el archivo recibido está íntegro.

6. En el último paso, si el destinatario accede a la página de respuesta habilitada en los servidores de eGarante, se guarda la información de la respuesta facilitada por el destinatario. En este paso se identifica al destinatario mediante el correo electrónico (ya que el link de acceso lo tiene él) junto con al menos un pin y la ip de acceso. En el caso de que el cliente de eGarante hubiese definido algún sistema de identificación adicional como el teléfono, código de tarjeta de coordenadas o firma electrónica quedará identificado en la certificación emitida por eGarante.

En el momento de iniciar el proceso, el cliente de eGarante establecerá un plazo de tiempo máximo en el que podrá obtenerse la contraseña del documento, así como responder al mismo. En el caso de que haya transcurrido dicho plazo sin respuesta, se emitirá una certificación con la información de los primeros pasos considerándose que el destinatario ha rechazado recibir la comunicación.

Como resultado de todo el proceso, eGarante genera tres documentos firmados digitalmente con sello de tiempo que forman parte de la certificación.

1. Versión firmada digitalmente del documento pdf originariamente entregado por el cliente de eGarante. Este documento además de la firma incluirá un sello de tiempo del momento de su generación y estará cifrado. La contraseña será entregada al emisor tras el envío y al destinatario tras identificarse.
2. Certificación de haber entregado al servidor de correo electrónico del destinatario el correo que incluye la explicación del proceso, el pdf referenciado en el punto 1 y los links para obtener la contraseña y responder al documento. Este documento también estará firmado digitalmente con sello de tiempo.
3. Certificación resumen del proceso de entrega incluyendo la fecha de envío, referencia única del pdf, fecha de entrega de la contraseña (acuse de recibo) en caso de que se haya producido, fecha e información de respuesta del destinatario en caso de que exista y procedimientos de identificación del destinatario.

Certificación de contenidos web

Descripción general

Servicio por el que se acredita el contenido de una página web accesible al público en un momento determinado del tiempo desde un terminal independiente no controlable por el cliente, acreditándose el momento temporal mediante la incorporación de un sello de tiempo.

El servicio puede incluir también la certificación de páginas protegidas por usuario y contraseña mostrándose en tal caso la página en cuestión tal y cómo la vería la persona que dispone de dichas credenciales de acceso en el momento identificado en la firma de la certificación desde un terminal independiente no influido por otras características especiales.

El servicio puede involucrar también el seguimiento del contenido de una página web durante un período de tiempo mediante la realización de una serie de capturas en momentos aleatorios del tiempo generándose una certificación para cada una de dichas capturas así como una certificación resumen que indica todas las capturas realizadas aleatoriamente en dicho intervalo de tiempo.

Además del contenido visual de la página a la que accede eGarante, esta podrá incluir en la certificación información adicional obtenida durante la certificación.

Descripción detallada

eGarante es contratada por sus clientes para que acceda a una página web alojada en una dirección de internet definida disponible al público y/o al cliente de eGarante para que visualice el contenido y lo capture con la mayor fiabilidad posible teniendo en cuenta el funcionamiento de las páginas web modernas con contenido dinámico.

El proceso de verificación del contenido de la página consta de los siguientes pasos:

1. Un cliente registrado en eGarante envía la dirección de la página que desea certificar
2. eGarante, en un proceso mayoritariamente automatizado, recibe dicha página y en el plazo de unos escasos minutos pone en marcha el proceso de revisión y certificación incluyendo las siguientes actividades:
    a. Acceso automatizado a la dirección de internet "url" identificada por el usuario del servicio
    b. Captura del contenido de dicha página en un documento pdf teniendo en cuenta las siguientes particularidades:
        i. La página se carga con un sistema estándar de mercado, existiendo en algunas ocasiones pequeñas diferencias en cuanto al formato en el que se muestra la información
        ii. La captura que se realiza es de la primera carga sin haber posibilidad de acceder a partes de la página que requieren de una actuación del usuario como por ejemplo un desplegable o una pestaña que requiere de un clic para abrirse. Para casos en los que los clientes soliciten este tipo de actuación se realizará un proceso semiautomático en el que el acceso a la página y la funcionalidad se realizará por personal de eGarante de manera independiente al cliente
        iii. En caso de existencia de sonidos, no se capturan los mismos, y en caso de existencia de vídeos, se captura solo el fotograma que aparece por defecto
        iv. Salvo para el caso de acceso a una página protegida con usuario y contraseña en cuyo caso nos presentamos como el usuario en cuestión, el acceso a la página es anónimo
        v. La captura puede incluir información adicional sobre la página que no es visible en el navegador para poder entender mejor el origen y contenido de la misma.

c. El pdf es firmado electrónicamente con un certificado de sello de empresa facilitado por Firma Profesional, entidad Prestadora de Servicios de Certificación inscrita en el Ministerio de Industria

d. La firma del pdf lleva un sello de tiempo incrustado también facilitado por Firma Profesional, del cual se deduce de manera indubitada la fecha y hora en la que fue realizada la firma, que coincide temporalmente (con un espacio de muy pocos segundos) con el momento de captura del contenido de la página

3. eGarante envía al cliente la certificación firmada electrónicamente

El resultado de este proceso es una certificación expedida por eGarante que tiene unas importantes características probatorias sobre el contenido de la página web indicada:

1. Es una visualización realizada por un tercero independiente (contratado por el usuario) desde los ordenadores de eGarante sin posibilidad de manipulación por el usuario
2. La visualización se captura en un documento fácilmente visible, pdf que es un estándar, y es firmada con una firma avanzada con un sello de empresa emitido por una entidad Prestadora de Servicios de certificación. Dicha firma garantiza el origen de los datos y la integridad de los mismos, ya que el documento no puede ser modificado sin romper la firma
3. La firma lleva incrustada un Sello de tiempo de una entidad Prestadora de Servicios de Certificación inscrita en el Ministerio de Industria (Firmaprofesional s.l.) que fecha de manera indubitada el momento en el que se incluyó la firma en la certificación, por lo tanto, la visualización de la página no pudo hacerse después de ese momento
4. La validez de la firma del documento puede comprobarse con servicios de validación de firma como el presentado por el Gobierno de España en la página web https://valide.redsara.es

Para la certificación de páginas propias del cliente, se deberá usar el servicio de certificación en momentos aleatorios de tiempo para los cuales, previa petición por el cliente, se usarán también direcciones IP aleatorias para reforzar la validez de la prueba.

La Declaración de Prácticas de Certificación de Firma Profesional, el prestador de servicios de certificación del que hace uso eGarante, pueden ser consultadas a través de su sitio web: www.firmaprofesional.com

Controles de seguridad física, de procedimiento y de personal

Notas preliminares

El presente documento, de acuerdo con lo establecido en el apartado 1, del artículo 88, del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD),[1] es de obligado cumplimiento para todo el personal de ***EGARANTE, SL (EGARANTE, en adelante)*** *que tenga acceso a los datos de carácter personal y a los sistemas de información, referidos a los conjunto de datos definidos en este documento.*

eGarante mantiene este documento en todo momento actualizado y, de acuerdo con lo contemplado en el artículo 88.7 del Reglamento de la LOPD, será revisado cuando se produzcan cambios relevantes[2] en el sistema de información[3], en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los conjuntos de datos o tratamientos o, en su caso, como consecuencia de los controles periódicos realizados. De igual forma, se adecuará, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal. Todo ello de acuerdo, en general, con lo establecido en el Real Decreto 1720/2007, de 21 de diciembre, citado y, en particular, con lo especificado en los apartados 7 y 8 del artículo 88 de dicha norma.

Este documento es de aplicación tanto a los conjuntos de datos automatizados como a los mixtos, esto es, conjuntos de datos automatizados que tienen parte de su contenido no automatizado o, en otros términos, que se encuentran normalmente en soporte papel, para los que se deberán adoptar las medidas de seguridad contempladas en el mismo en la parte en que les sean aplicables. No obstante en todos los casos (automatizados y mixtos) las medidas de seguridad a establecer serán las necesarias para garantizar la seguridad de los datos de carácter personal y que eviten su alteración, pérdida, tratamiento o acceso no autorizado.

FECHA	VERSIÓN	AUDITORÍAS
3 de abril de 2013	1	Interna
30 de octubre de 2015	2	Auditoría bianual (realizada por Abanlex, S.L.)

[1] Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, publicado en el Boletín Oficial del Estado número 17, de 19 de enero de 2008; en adelante a este Real Decreto, por brevedad, se le denominará también como "el Reglamento" o el "Reglamento de la LOPD" o el "Real Decreto 1720/2007". El Título VIII de este Real Decreto gira bajo el epígrafe "De las medidas de seguridad en el tratamiento de datos de carácter personal" y es de especial aplicación a lo referido en este documento.

[2] Se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

[3] Por sistema de información se entiende (art. 5.2. m) del RD 1720/2007) el "conjunto de datos, tratamientos, programas, soportes y en su caso, equipos empleados para el tratamiento de datos de carácter personal"

Objeto de esta sección

La presente sección tendrá la consideración de parte fundamental del Documento de Seguridad interno de eGarante a los efectos de la obligación establecida en el artículo 9 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD) y en consonancia con los estándares establecidos en el Título VIII del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD. También responde a la Ley Orgánica 15/1999, de 13 de diciembre que resume y amplía la legislación ya existente sobre esta materia.

Ámbito de aplicación

Este documento ha sido elaborado bajo la responsabilidad de **EGARANTE**, con domicilio social en Madrid, Paseo de la Castellana 100, Esc. Dcha., 2ºB (28046), con N.I.F. nº B86669819, quien, como **Responsable del Conjunto de datos**, se compromete a implantar y actualizar esta Normativa de Seguridad de obligado cumplimiento para todo el personal con acceso a los datos protegidos o a los sistemas de información que permiten el acceso al mismo. Todas las personas que tengan acceso a los datos de los Conjuntos de datos, bien a través del sistema informático, o bien a través de cualquier otro medio de acceso al Conjunto de datos, y las que accedan a los Conjuntos de datos en su versión de soporte papel, se encuentran obligadas por la ley a conocer y cumplir lo establecido en este documento y sujetas a las consecuencias que se pudieran derivar en caso de incumplimiento.

Encargado del tratamiento

Cuando un tercero acceda a los datos de carácter personal referidos, a los soportes que los contengan o a los recursos del sistema de información que los traten para prestar un servicio a EGARANTE, y dicho acceso se realice en los locales de empresa, dicho tercero habrá suscrito un contrato con EGARANTE en cumplimiento de lo especificado en el artículo 12 de la LOPD y será considerado encargado del tratamiento, comprometiéndose su personal al cumplimiento de las medidas de seguridad previstas en este documento.

Si el servicio que se contrata fuera prestado por el encargado del tratamiento en sus propios locales y, consecuentemente, existe un traslado de los datos de carácter personal referidos, de los soportes que los contengan o de alguno de los recursos del sistema de información que los traten, fuera de los locales de la empresa, el encargado del tratamiento deberá elaborar un documento de seguridad que reúna todos los requisitos exigidos en el Título VIII, del Reglamento de la LOPD o, si ya hubiera elaborado su propio documento, deberá actualizarlo, identificando el conjunto de datos o tratamiento y al responsable del mismo (EGARANTE), e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento.

Cuando dicho acceso sea remoto habiéndose prohibido al encargado del tratamiento incorporar tales datos a sistemas o soportes distintos de los de la empresa, el personal del

encargado del tratamiento se comprometerá al cumplimiento de las medidas de seguridad previstas en este documento.

En todos los casos referidos, estas circunstancias se harán constar en un apartado interno del Documento de Seguridad de eGarante a disposición de la Agencia Española de Protección de Datos, indicando todas las cuestiones necesarias para una correcta información y documentación de la situación, bien sea referida al acceso a los datos por el encargado del tratamiento en los locales de EGARANTE, bien sea la prestación del servicio y consecuente traslado de los datos a los locales del Encargado del Tratamiento.

Recursos protegidos

La protección de datos frente a accesos no autorizados se deberá realizar mediante el control, a su vez, de todas las vías por las que se pueda tener acceso a dicha información.

Los centros de tratamiento y locales donde se encuentren ubicados los datos o se almacenen los soportes que los contengan, los datos referidos, así como los programas, soportes y equipos empleados para el almacenamiento y tratamiento de los datos de carácter personal.

En ningún caso saldrán los datos personales de los locales o del control de eGarante, salvo previa autorización expresa del responsable de privacidad de eGarante.

Funciones y obligaciones del personal

El personal afectado por esta normativa se clasifica en dos categorías:

- **Administradores del sistema**, encargados de mantener el entorno operativo de los Conjuntos de datos.
- **Usuarios del Conjunto de datos**, o personal que usualmente utiliza el sistema informático de acceso a los datos.

Los **administradores del sistema** se atienen, además, a aquellas normas, más extensas y estrictas aprobadas por cada departamento de eGarante, y que atañen, entre otras, al tratamiento de los respaldos de seguridad, normas para el alta de los usuarios y contraseñas, así como otras normas de obligado cumplimiento en la unidad administrativa a la que pertenecen los conjuntos de datos.

Normas y procedimientos de seguridad

1. Centros de tratamiento y locales

A) Concepto

Los locales donde se ubiquen los ordenadores y archivos que contienen los datos son objeto de protección y garantizan la disponibilidad y confidencialidad de los datos protegidos, especialmente cuando los datos estén ubicados en un servidor accedido a través de una red.

B) Medidas

Los locales cuentan con los medios necesarios de seguridad que evitan los riesgos que pudieran producirse como consecuencia de incidencias fortuitas o intencionadas que impidieran el acceso a los datos de las personas legitimadas para ello.

2. Puestos de trabajo

A) Concepto

Son todos aquellos dispositivos desde los cuales se puede acceder a los datos, como, por ejemplo, terminales u ordenadores personales. Se consideran también puestos de trabajo aquellos terminales del sistema donde, en algunos casos, también pueden aparecer datos protegidos.

B) Medidas

1. Cada puesto de trabajo está bajo la responsabilidad de una de las personas expresamente autorizadas, que garantizará que la información que muestra no podrá ser vista por personas no autorizadas.
2. Esto implica que tanto las pantallas como las impresoras u otro tipo de dispositivos conectados al puesto de trabajo están físicamente ubicados en lugares que garantizan esa confidencialidad. De igual manera, las fichas de clientes o contactos en soporte papel, están fuera del alcance y visión de personas no autorizadas.
3. Cuando el responsable de un puesto de trabajo lo abandone, ya sea temporalmente o al finalizar su turno de trabajo, deberá dejarlo en un estado que impida la visualización de los datos protegidos. Esto podrá realizarse a través de un protector de pantalla que impida la visualización de los datos protegidos o una suspensión del sistema. La reanudación del trabajo implicará la desactivación de la pantalla protectora o la suspensión del sistema con la introducción de la contraseña correspondiente.
4. En el caso de las impresoras, eGarante cuenta con un protocolo para asegurarse de que no queden documentos impresos en la bandeja de salida que contengan datos protegidos.
5. Queda expresamente prohibida la conexión a redes o sistemas exteriores que puedan ser considerados como no seguros, como las redes WiFi públicas y abiertas, de los puestos de trabajo desde los que se realiza el acceso al conjunto de datos. La revocación de esta prohibición será autorizada por el Responsable del Conjunto de datos, quedando constancia de esta modificación en el Libro de Incidencias.
6. Los puestos de trabajo desde los que se tiene acceso al Conjunto de datos tendrán una configuración fija en sus aplicaciones y sistema operativos que solo podrá ser cambiada bajo la autorización del Responsable del Conjunto de datos o por los administradores autorizados.

3. Entorno de Sistema Operativo y de Comunicaciones.

A) Introducción

Esta sección regula el uso y acceso de las partes del sistema operativo, herramientas o programas de utilidad, o el entorno de comunicaciones, de forma que se impida el acceso no autorizado a los datos del Conjunto de datos.

B) Medidas

1. Los sistemas operativos y de comunicaciones usados por eGarante tienen, al menos, un responsable autorizado.
2. En el caso más simple, como es que los datos estén ubicados en un ordenador personal y accedido mediante una aplicación local monopuesto, el administrador del sistema operativo podrá ser el mismo usuario que accede habitualmente al Conjunto de datos.
3. Ninguna herramienta o programa de utilidad que permita el acceso al Conjunto de datos deberá ser accesible a ningún usuario o administrador no autorizado.
4. En la norma anterior se incluye cualquier medio de acceso en bruto, es decir, no elaborado o editado, a los datos del Conjunto de datos, como las llamadas "*queries*", editores universales, analizadores de conjunto de datos, etc., que deberán estar bajo el control de los administradores autorizados.
5. El administrador deberá responsabilizarse de guardar en lugar protegido las copias de respaldo y seguridad del Conjunto de datos, de forma que ninguna persona no autorizada tenga acceso a las mismas.
6. Cuando la aplicación o sistema de acceso a los datos utilice ficheros temporales, ficheros de "*logging*", o cualquier otro medio en el que pudiesen ser grabadas copias de los datos protegidos, el administrador se asegurará de que esos datos no sean accesibles posteriormente por personal no autorizado.
7. Cuando el ordenador en el que están ubicados los datos está integrado en una red de comunicaciones de forma que desde otros ordenadores conectados a la misma sea posible el acceso al Conjunto de datos, el administrador responsable del sistema se asegurará de que este acceso no se permite a personas no autorizadas.

4. Sistema informático o aplicaciones de acceso al Conjunto de datos.

A) Concepto

Son todos aquellos sistemas informáticos, programas o aplicaciones con las que se puede acceder a los datos, y que son usualmente utilizados por los usuarios para acceder a ellos.

B) Medidas

1. Los sistemas informáticos usados por eGarante tienen su acceso restringido mediante un código de usuario y una contraseña.
2. Todos los usuarios autorizados para acceder tienen un código de usuario único y asociado a la contraseña correspondiente, que solo será conocida por el propio usuario.

3. Cuando la aplicación informática que permite el acceso a los datos no cuente con un control de acceso, deberá ser el sistema operativo, donde se ejecuta esa aplicación, el que impida el acceso no autorizado, mediante el control de los citados códigos de usuario y contraseñas.
4. En cualquier caso, se controlarán los intentos de acceso fraudulento a los datos, limitando el número máximo de intentos fallidos, y cuando sea técnicamente posible, guardando en un registro auxiliar la fecha, hora, código y claves erróneas que se han introducido, así como otros datos relevantes que ayuden a descubrir la autoría de esos intentos de acceso fraudulentos.

5. Salvaguarda y obtención de contraseñas y llaves personales.

A) Introducción

Las contraseñas personales y llaves de acceso constituyen uno de los componentes básicos de la seguridad de los datos, y deben, por tanto, estar especialmente protegidos. Como llaves de acceso al sistema, las contraseñas deberán ser estrictamente confidenciales y personales, y cualquier incidencia que comprometa su confidencialidad deberá ser inmediatamente comunicada al administrador y subsanada en el menor tiempo posible. Se procederá igualmente en caso de llaves físicas de acceso a los armarios que contengan el conjunto de datos.

B) Medidas

1. Solamente las personas autorizadas podrán tener acceso a los datos.
2. Cada usuario será responsable de la confidencialidad de su contraseña y la custodia de su llave. En caso de que la contraseña sea conocida fortuita o fraudulentamente por personas no autorizadas, deberá registrarlo como incidencia y proceder inmediatamente a su cambio. Igualmente se procederá al cambio en caso de extravío de la llave.
3. Las contraseñas y llaves se asignarán y se cambiarán mediante un mecanismo y periodicidad adecuado, aprobado por el responsable de privacidad de eGarante, bajo los siguientes mínimos:
   a. La asignación de contraseñas o llaves deberá ser realizada por el Responsable del Conjunto de datos y deberá ser completamente personal y confidencial.
   b. Si se precisa el cambio de contraseña por que ha sido olvidada, conocida fortuitamente por terceros, o cualquier otro motivo, se hará constar al Responsable del Conjunto de datos y este procederá a su cambio de la misma manera que procedió a su asignación, siempre guardando la mayor discreción posible. Igualmente se procederá en caso de pérdida de llave de acceso al armario donde se encuentren los conjuntos de datos en soporte papel.
   c. El Responsable del Conjunto de datos realizará un cambio de las contraseñas de todos los usuarios con una periodicidad de UN AÑO para aquellos sistemas que dependan únicamente del uso de contraseña y TRES AÑOS para los que además de la contraseña estén dotados de un segundo factor de verificación, como un certificado de usuario o OTP.
   d. Las contraseñas se almacenarán en un conjunto de datos aparte al que solo podrá tener acceso el Responsable del Conjunto de datos y que estará protegido por una contraseña confidencial que cambiará con una periodicidad de SEIS MESES.

El archivo donde se almacenen las contraseñas deberá estar protegido y bajo la responsabilidad del administrador del sistema

Gestión de incidencias

Se entiende por incidencia cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos; esto es, será una incidencia cualquier circunstancia que pueda darse y afecte a los datos de forma que constituya, o pueda constituir, un riesgo o inseguridad para la confidencialidad e integridad de los datos de carácter personal.

Por tanto, con el fin de garantizar la confidencialidad e integridad de la información contenida en el conjunto de datos, se establece un procedimiento de notificación y gestión de incidencias con vistas a prevenir el peligro que representen para la seguridad de la información y para poder tener conocimiento del lugar, fecha, hora y motivo por el que se ha producido la incidencia y el responsable o responsables de la misma.

Gestión de soportes y documentos

Soportes informáticos son aquellos medios de grabación y recuperación de datos que se utilizan para realizar copias o pasos intermedios en los procesos de aplicación que gestiona los datos. Soportes en papel son aquellos documentos que contienen datos personales y que son almacenados para cumplir la finalidad descrita en su creación.

Dado que la mayor parte de los soportes que hoy en día se utilizan son fácilmente transportables, reproducibles o copiables, es evidente la importancia que para la seguridad de los datos tiene el control de estos medios.

Entrada y salida de datos por red

La transmisión de datos por red, ya sea por medio de correo electrónico, mediante sistemas de transmisión de ficheros o mediante sistemas de transmisión, se está convirtiendo en uno de los medios más utilizados para el envío de datos, hasta el punto que está sustituyendo a los soportes físicos. Por ello merecen un tratamiento especial ya que, por sus características, pueden ser más vulnerables que los soportes físicos tradicionales.

Procedimientos de respaldo y recuperación

Introducción

La seguridad de los datos personales no solo supone la confidencialidad de los mismos sino que también conlleva la integridad y la disponibilidad de esos datos.

Para garantizar estos dos aspectos fundamentales de la seguridad es necesario que existan unos procesos de respaldo y recuperación que, en caso de fallo del sistema informático, permitan recuperar y en su caso reconstruir los datos.

Controles de seguridad técnica

Este apartado contempla los siguientes aspectos:

- Seguridad lógica de la infraestructura
- Seguridad criptográfica de la solución

Para implementar los mecanismos de seguridad asociados a la plataforma se siguieron múltiples metodologías de 'bastionado' (Hardening) como por ejemplo las relacionadas con el instituto SANS o CIS

Medidas adoptadas para la plataforma de servicio (servicios y servidores):

- Cortafuegos que gestiona las conexiones entrantes y salientes de la forma más restrictiva
- Acceso administrativo controlado mediante sistemas de clave pública / privada evitando, en la medida de lo posible, el uso de contraseñas
- Principio de 'Least privilege' a la hora de ejecutar servicios
- Reducción al mínimo de software en cada plataforma
- Virtualización de procesos y sistemas
- Auditorías periódicas y revisión de vulnerabilidades, haciendo hincapié en la metodología OWASP

A nivel criptográfico, se han seguido los criterios y estándares nacionales e internacionales vigentes y revisados cada año.

- Certificados RSA 2048
- Vigencia del certificado bi-anual
- Algoritmo de hash SHA

El producto de nuestras certificaciones es entregado en formato PDF, formato ampliamente utilizado en firma digital y pionero en el mercado.

Todos nuestros documentos PDF llevan incrustadas las CRLs asociadas a la CA que ha emitido el certificado que empleamos, de esa forma nuestros documentos cumplen con el estándar PAdES-LTV para que en un futuro las firmas se puedan revisar independientemente del tiempo transcurrido

Para realizar el proceso de firma digital se emplea un certificado digital expedido por un prestador de servicios de certificación acreditado por el Ministerio de Industria.

La clave privada de dicho certificado se encuentra alojada en un contenedor criptográfico que requiere PIN para poder realizar operaciones criptográficas de firmado digital.

Solo un reducido grupo de procesos tiene concedido acceso a dicho contenedor y el acceso se realiza bajo demanda por cada proceso de firma digital.

Controles periódicos de verificación del cumplimiento

La veracidad de los datos contenidos en este documento, así como el cumplimiento de las normas que contiene es periódicamente revisado y mantenido actualizado mediante auditorías internas y externas contratadas por eGarante.

Otros asuntos legales y de actividad

Obligaciones y garantías

1.1. Obligaciones de eGarante:

eGarante se compromete a prestar los servicios ofrecidos de conformidad con lo especificado en esta Declaración de Prácticas, en las Condiciones Generales de contratación de los Servicios de publicadas en su página web www.egarante.com y en las disposiciones legales que sean aplicables, garantizando que las evidencias emitidas no contienen datos erróneos.

Para ello, contará con personal cualificado, utilizará equipos y tecnología adecuados y llevará a cabo las revisiones y auditorías necesarias para asegurar la calidad de los servicios y el cumplimiento de la legislación.

1.2. Obligaciones de los Usuarios

Los Usuarios, por su parte, asumen las siguientes obligaciones:

- Cumplir las presentes condiciones y términos de uso y obrar conforme a la ley y la buena fe.
- Custodiar diligentemente el nombre de usuario y la contraseña para acceder al servicio y no ceder su uso ni permitir el acceso de terceros.
- Facilitar información actualizada, exacta y veraz cuando le sea solicitada por eGarante.
- Utilizar los recursos que eGarante ponga a su disposición exclusivamente a los efectos del desarrollo del servicio, absteniéndose de usos no permitidos, ilegales o que perjudiquen su normal funcionamiento.

Responsabilidades

Tanto eGarante como los Usuarios deberán responder de las obligaciones que les afectan

2.1. Delimitación de responsabilidades de eGarante:.

a) En cuanto al secreto de las comunicaciones: eGarante adoptará las medidas técnicas y organizativas necesarias, conforme a la legislación vigente, a fin de garantizar el secreto de las comunicaciones.

Quedará por tanto exonerada de toda responsabilidad que pueda derivarse del uso o publicación de contenido confidencial por parte del Cliente o de terceros y, en general, de cuantas acciones u omisiones que supongan un quebrantamiento del secreto de las comunicaciones electrónicas y que no le sean imputables, por haber adoptado las medidas pertinentes.

b) Sobre posibles daños: El acceso a la página web no implica la obligación por parte de eGarante, de controlar la ausencia de virus o cualquier otro elemento informático dañino. eGarante no se responsabiliza de los daños producidos en los elementos físicos y/o lógicos de los equipos informáticos del Cliente o de terceros, durante la prestación del servicio objeto del presente Contrato.

c) En cuanto al contenido de los documentos: eGarante no accede y, en consecuencia, no examina el contenido de los documentos que puedan ser remitidos o intercambiados en virtud de los servicios objeto del presente Contrato. En consecuencia, y de acuerdo con lo dispuesto en el artículo 16.1 de la LSSI, eGarante no será responsable de dichos contenidos en tanto en cuanto no tenga un conocimiento efectivo de los mismos según lo dispuesto en el citado artículo.

Por el mismo motivo, eGarante es ajeno a cualquier relación contractual que pueda establecerse mediante la utilización de sus servicios. No siendo responsable de sus deficiencias, resultados o consecuencias.

d) En cuanto a la identidad de los Usuarios: eGarante no se responsabiliza de verificar la identidad del USUARIO de los servicios. En consecuencia, no asume responsabilidad en el caso de que acceda al sistema un Receptor que no sea quien dice ser o de que acceda a un documento un Receptor que no fuera el destinatario del mismo.

e) En cuanto a la admisión y valoración como prueba del servicio prestado y la certificación emitida por eGarante: Su admisión a prueba y su valoración como tal, es una facultad de los órganos jurisdiccionales, arbitrales o administrativos, que, por tanto, no puede ser en ningún caso garantizada.

Indemnizaciones

eGarante dispone de un Seguro de Responsabilidad Civil que cubre los riesgos derivados de cualquier acto negligente, error u omisión, incluido el incumplimiento no intencionado de la normativa vigente.

Confidencialidad de la información y protección de datos personales

1. Información confidencial.

eGarante tiene establecida su política de tratamiento de la información, que deben suscribir todas las personas con las que tenga establecidas relaciones laborales o profesionales.

En particular tienen carácter confidencial, las operaciones que lleve a cabo la compañía, cualquier información sobre seguridad, control y auditoría, las claves privadas que utilicen directivos y empleados de la Sociedad y muy especialmente los datos de carácter personal de los Usuarios.

Será información pública la contenida en la presente Declaración de Prácticas, la publicada en la página web, la declarada como tal por eGarante y aquella cuya publicidad sea impuesta normativamente.

2. Protección de datos personales-

Confidencialidad y sujeción a la normativa vigente: Para la adecuada y completa prestación del servicio, puede ser necesario que eGarante acceda a datos de carácter personal titularidad del Usuario. En estos casos, de conformidad con el artículo 12 de la Ley Orgánica 15/1999, eGarante ostenta la condición de Encargado del Tratamiento y garantiza que dicho tratamiento de los datos personales se realizará bajo la más estricta confidencialidad y en pleno cumplimiento de las obligaciones y garantías que establece la LOPD y el Real Decreto 1720/2007 de 21 de Diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD o cualquier otra norma que la modifique o sustituya, tanto por su parte como por parte de todos sus empleados.

eGarante se compromete a implantar las medidas técnicas y organizativas que sean necesarias para garantizar la seguridad y confidencialidad de los datos de carácter personal y se evite su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana, del medio físico o natural.

Utilización de los datos personales y cesión a terceros: eGarante reconoce que los archivos son de titularidad exclusiva del Usuario y garantiza que los datos personales no se utilizarán ni serán cedidos a terceros con fines distintos a la prestación de los servicios, en las condiciones previstas en este documento y en las condiciones generales de los servicios publicadas en la página web de la Sociedad. No obstante, permitirá que algunos terceros, en calidad de Encargados del Tratamiento, accedan a los datos para posibilitar la prestación de dichos servicios.

En el caso de que eGarante destinare o cediese a terceros los datos personales con finalidades diferentes a las indicadas, sería considerado Responsable y debería responder de las infracciones en que hubiera incurrido.

Derechos del Usuario: El Usuario podrá ejercer sus derechos de acceso, rectificación, cancelación y oposición al tratamiento de sus datos de carácter personal, mediante el envío de un email a la dirección de correo electrónico privacidad@egarante.com, incluyendo copia de su DNI y concretando su solicitud.

Los datos personales una vez prestado el servicio: Una vez finalizada la prestación del servicio, eGarante se compromete a devolver los datos al Usuario o a destruirlos de forma certificada, a elección de este último. No obstante, podrá conservar tales datos personales, debidamente

bloqueados, durante el tiempo que pudiera ser necesario para atender responsabilidades nacidas de su tratamiento.

Período de validez de la presente declaración y modificaciones

1.- Periodo de validez:

La presente Declaración de Prácticas de Certificación entrará en vigor en el momento de su publicación y mantendrá su vigencia hasta su derogación expresa o hasta la publicación de una nueva versión que la sustituya.

2.- Modificaciones:

La Dirección de eGarante podrá acordar modificaciones en la Declaración, con base en requerimientos técnicos, comerciales o normativos, evaluando las implicaciones de todo tipo. Los cambios serán publicados en la página web de la sociedad y los que afecten de forma sustancial a los Usuarios, serán notificadas directamente a los interesados.

Tarifas

Las tarifas aplicables a los servicios de certificación, en las condiciones expuestas en la presente declaración, quedarán publicadas en la dirección: https://www.egarante.com

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.

Notificaciones

En general, las comunicaciones y notificaciones a los efectos de la presente Declaración serán efectuadas mediante su publicación en la página web de la Sociedad.
En cuanto a las notificaciones individuales, el sistema será el pactado con los Usuarios.

Normativa aplicable

La principal normativa española aplicable al contenido de la presente Declaración es la siguiente:

- La Ley 59/2003, de 19 de diciembre, sobre Firma Electrónica.
- La Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE).
- La Ley11/2.007, de 22 de Junio, sobre Acceso de los Ciudadanos a los Servicios Públicos
- La Ley Orgánica 15/1.999 de 13 de diciembre, sobre Protección de Datos de Carácter Personal y su Reglamento, aprobado por el Real Decreto 1720/2.007 de 21 de Diciembre.

Reclamaciones y resolución de conflicto

1.- Reclamaciones:

eGarante responderá en el plazo máximo de 15 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 electrónico contact@egarante.com

2.- Conflictos:

Para toda controversia que no pueda ser resuelta de forma amistosa, en relación con la prestación de los servicios eGarante, 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.

Otras estipulaciones

Los Usuarios de los servicios de eGarante a que se refiere la presente Declaración aceptan en su totalidad el contenido del documento.

La declaración de invalidez de alguna de sus apartados no afectará a la validez del resto.