Declaración de Prácticas De Certificación

Índice

Paperless S.A
Av. Andrés Bello 2687- Piso 25,
Las Condes, Santiago
56-2-5589 5400

Paperless S.A
Av. Andrés Bello 2687- Piso 25,
Las Condes, Santiago
56-2-5589 5400

Paperless S.A
Av. Andrés Bello 2687- Piso 25,
Las Condes, Santiago
56-2-5589 5400

1 Introducción

Paperless S.A tiene como objetivo la implementación de los Servicios de Seguridad Administrados para la Infraestructura de Llave Pública (PKI), a partir de una revisión metodológica acorde a las mejores prácticas internacionales en materia de Seguridad de la Información y la aplicación de las leyes y normativas existentes en Chile. Para ofrecer este servicio Paperless S.A se convierte en un Prestador de Servicios de Certificación (PSC).

¿Qué es un Prestador de Servicios de Certificación?

Es una persona física, institución pública o privada que presta servicios relacionados con Firmas Electrónicas y expide certificados, actuando como tercera parte de confianza entre las personas u organizaciones que intercambian mensajes utilizando firma electrónica.

Paperless S.A, en su deseo de promover la transparencia y calidad de los certificados que emite, ha adoptado criterios internacionalmente reconocidos en la definición, estructura y presentación de estas prácticas de certificación.

1.1 Sobre las Prácticas de Certificación

En este documento se presentan la Declaración de Prácticas de Certificación de Paperless S.A (DPC). Estas son una descripción detallada de las normas o prácticas que Paperless S.A declara convenir en la prestación de sus servicios de certificación, cuando emite y gestiona certificados digitales en su rol de PSC; además se incluyen las normas a seguir por la Entidad de Registro (RA) y los Agentes de Certificación acreditadas por Paperless S.A.
Al emitir un certificado digital, una PSC establece cierto nivel de seguridad a todos los agentes que depositarán su confianza en la validez de dicho certificado, como instrumento que da garantías sobre la identidad del titular del mismo. En ese sentido, establece que se han tomado las medidas y procedimientos adecuados para constituir la correspondencia entre dicho certificado y una cierta entidad en particular (individuo, servidor, etc.).

Un mecanismo para evaluar la calidad y grado de confianza que se puede depositar en un certificado digital, es a través de la revisión de las prácticas usadas por la PSC para emitir dicho certificado, es decir, las Prácticas de Certificación.

Esta Declaración de Prácticas de Certificación, en conjunto con la Política de Certificados, son los únicos instrumentos que establecen las reglas aplicables para la solicitud, validación, aceptación, entrega, emisión, y revocación de los certificados, así como las restricciones y aplicaciones en las cuales se deben utilizar dichos certificados.

Es una explicación detallada de las prácticas que Paperless S.A emplea para emitir y gestionar certificados, y que implementa y soporta los requerimientos de las Políticas de Certificados.

Tales prácticas son las que se prosigue en detallar, y están disponibles en el sitio Web de Paperless S.A (http://www.pkichile.cl) para conocimiento público.

Paperless S.A
Av. Andrés Bello 2687- Piso 25,
Las Condes, Santiago
56-2-5589 5400

1.2 Alcance

Describir la Declaración de Prácticas de Certificación, dentro de la Infraestructura de Llaves Públicas (PKI) de Paperless S.A.

El PSC Paperless S.A se establece para desarrollar y crear una Infraestructura de Llave Pública (PKI) a nivel nacional para el desarrollo del comercio electrónico; podrá certificar:

- Las claves públicas de personas físicas.
- Las claves públicas de las Entidades Intermedias.

En esta Declaración de Prácticas de Certificación se podrá encontrar las reglas y procedimientos que dan cumplimiento a:

- Ley N°19.799, Abril del 2002. Sobre documentos electrónicos, firma electrónica y los servicios de certificación de dicha firma. Ministerio de Economía.

- DS N°181, Julio del 2002. Reglamento Ley 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma, Ministerio de Economía.

- Ley N°20.217, Noviembre del 2007. Modifica el código de procedimiento civil y la ley N°19.799 sobre documentos electrónicos, firma electrónica y los servicios de certificación de dicha firma, Ministerio de Economía.

- Guía de Evaluación Procedimiento de Acreditación de Prestadores de Servicios de Certificación, Septiembre del 2002, Ministerio de Economía.

- Actualización Guía de Evaluación Procedimiento de Acreditación de Prestadores de Servicios de Certificación, Febrero 2013, Ministerio de Economía Fomento y Turismo.

- Guía inspección anual, Agosto del 2005. Guía para inspección anual de Prestadores de Servicios de Certificación, Ministerio de Economía.

- Actualización Guía Inspección anual, febrero del 2013. Guía para Inspección Anual de prestadores de servicios de certificación, Ministerio de Economía Fomento y Turismo.

- Resolución exenta N° 9 del 15 de Febrero del 2001 emitida por el Servicio de Impuestos Internos.

- Resolución exenta N° 280 del 11 de Febrero del 2013 emitida por el Ministerio de Economía, Fomento y Turismo.

- Resolución exenta N° 172 del 30 de Enero del 2013 emitida por el Ministerio de Economía, Fomento y Turismo.

Estos procedimientos se aplican a la Autoridad Certificadora, Autoridad de Registro, PSC, Solicitantes y Titulares, para la emisión de Certificados por parte de Paperless S.A, de acuerdo con cada tipo de certificado y las limitaciones de uso establecidas para cada caso.

Paperless S.A
Av. Andrés Bello 2687- Piso 25,
Las Condes, Santiago
56-2-5589 5400

1.3 Referencias

Prácticas de Certificación:

- ETSI TS 102 042: "Policy requirements for certification authorities issuing public key certificates".
- RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, Marzo 1999.

Seguridad:

- ISO/IEC 17799:2000 Information Technology – Code of Practice for Information Security Management (2000).
- ISO/IEC 15408: Common Criteria for Information Technology Security Evaluation, Version 2.1 (2000).
- FIPS PUB 140-1: Security Requirements for Cryptographic Modules (Mayo 2001).

Estructura de Certificados:

- IS0/IEC 9594-8:2001 "Information Technology – Open Systems Interconnection - The Directory attribute certificate framework".
- ITU-T Rec. X.690 (1997) / ISO/IEC 8825-1:1998. ASN.1 Basic Encoding Rules.

Repositorio de Información:

- [RFC 2559] Boeyen, S. et al., "Internet X.509 Public Key Infrastructure. Operational Protocols LDAPv2", April 1999.

1.4 Definiciones

- Certificado: Todo Mensaje de Datos u otro registro que confirme el vínculo entre un Firmante y los datos de creación de Firma Electrónica.
- Datos de Creación de Firma Electrónica: Son los datos únicos, como códigos o claves criptográficas privadas, que el Firmante genera de manera secreta y utiliza para crear su Firma Electrónica, a fin de lograr el vínculo entre dicha Firma Electrónica y el Firmante.
- Destinatario: La persona designada por el Emisor para recibir el Mensaje de Datos, pero que no esté actuando a título de Intermediario con respecto a dicho Mensaje.
- Emisor: Toda persona que, al tenor del Mensaje de Datos, haya actuado a nombre propio o en cuyo nombre se haya enviado o generado ese mensaje antes de ser archivado, si éste es el caso, pero que no haya actuado a título de Intermediario.
- Firma Electrónica: Los datos en forma electrónica consignados en un Mensaje de Datos, adjuntados o lógicamente asociados al mismo por cualquier tecnología, que son utilizados para identificar al Firmante en relación con el Mensaje de Datos e indicar que el Firmante aprueba la información contenida en el Mensaje de Datos, y que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio.
- Firma Electrónica Avanzada: Aquella Firma Electrónica que cumpla con los requisitos contemplados en las secciones de la Ley N°19.799. En aquellas disposiciones que se refieran a Firma Digital, se considerará a ésta como una especie de la Firma Electrónica.

Paperless S.A
Av. Andrés Bello 2687- Piso 25,
Las Condes, Santiago
56-2-5589 5400

- Firma Electrónica Tributaria: Aquella forma que cumpla con los requisitos contemplados en la resolución exenta N° 9 del 15 de febrero del 2001 emitida por el Servicio de Impuestos Internos.
- Firmante: La persona que posee los datos de la creación de la firma y que actúa en nombre propio o de la persona a la que representa.
- Intermediario: En relación con un determinado Mensaje de Datos, se entenderá toda persona que, actuando por cuenta de otra, envíe, reciba o archive dicho Mensaje o preste algún otro servicio con respecto a él.
- Mensaje de Datos: La información generada, enviada, recibida o archivada por medios electrónicos, ópticos o cualquier otra tecnología.
- Parte que Confía: La persona que, siendo o no el Destinatario, actúa sobre la base de un Certificado o de una Firma Electrónica.
- Prestador de Servicios de Certificación: La persona o institución que preste servicios relacionados con Firmas Electrónicas y que expide los Certificados, en su caso.
- Sistema de Información: Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma Mensajes de Datos.
- Solicitante: Se entenderá a la persona que tramita la Solicitud de Certificado.
- Titular: Se entenderá a la persona a cuyo favor fue expedido el Certificado.
- Certificador: A la institución o persona física que verifica la identidad de los Solicitantes.
- Autoridad Certificadora: A la institución que presta servicios de certificación mediante la expedición de Certificados Digitales.
- Autoridad de Registro: A la institución autorizada para llevar el registro electrónico de los Certificados Digitales expedidos por la Autoridad Certificadora.

1.5 Comunidad y Aplicabilidad

1.5.1 Comunidad de usuarios

Paperless S.A emite Certificados Digitales basados en la estándar ITU-T Recommendation X.509. Todos los certificados emitidos por Paperless S.A son emitidos a personas físicas y representantes legales de organizaciones públicas o privadas. En cada caso, asegura la identidad del suscriptor, requiriendo su presencia física ante una Autoridad de Registro.

1.5.2 Aplicabilidad de los certificados

Los Certificados emitidos por la Autoridad Certificadora Paperless S.A, no han sido diseñados, orientados ni se autoriza su utilización o reventa para controlar equipos en situaciones peligrosas o para su empleo en aplicaciones que requieran la ausencia total de fallas, tal como la operación de instalaciones nucleares, sistemas de navegación o comunicación de aeronaves, sistemas de control de tráfico aéreo o sistemas de control de armamento, en donde una falla puede derivar en muerte, lesiones a personas o daños serios al medio ambiente, siendo esta enumeración meramente ejemplificativa y no limitativa de supuestos de improcedencia de uso.

Los certificados de Paperless S.A podrán ser aplicados para soportar las siguientes necesidades de seguridad:

- Autentificación: Proporciona suficientes garantías respecto a la identidad del Titular del certificado, al requerirse su presencia física ante una Autoridad de Registro, junto con los documentos establecidos en el Formato de Solicitud del Certificado, que acreditan su identidad y/o personalidad.

Paperless S.A
Av. Andrés Bello 2687- Piso 25,
Las Condes, Santiago
56-2-5589 5400

- Integridad: Los mensajes firmados con los certificados de Paperless S.A, permiten validar que el contenido de un mensaje de datos no ha sido alterado en el tiempo transcurrido entre su envió y su recepción efectiva.
- No repudiación: Las firmas digitales producidas con los certificados de Paperless S.A, ofrecen los medios de respaldo frente a que una persona deniegue de la autoría y contenido de un mensaje de datos en particular, sí la persona ha firmado digitalmente dicho mensaje.
- Privacidad: los certificados de Paperless S.A, permiten cifrar mensajes de forma que al ser transmitidos o almacenados, solo sean observados por el Titular de los Datos de Creación de Firma Electrónica.

1.5.3 Tipos y usos de los certificados

Paperless S.A emite varios tipos de certificados de firma electrónica, de acuerdo a la naturaleza del solicitante y el uso o ámbito de aplicación del certificado. Cada tipo de certificado tiene un uso definido. Los suscriptores o solicitantes deben elegir el tipo de certificado que se adecue a sus necesidades. Los certificados de Firma Electrónica Avanzada se denominan también certificados Clase 3, y cumplen todos los requisitos de seguridad definidos en el capítulo 3 de estas DPC, relativo a la identificación del titular. Además Paperless S.A emite certificados de Firma Electrónica Tributaria que cumplen los mismos criterios de seguridad para los anteriormente mencionados.

Los certificados electrónicos de Firma Electrónica definidos por Paperless S.A son:

- Certificado de Firma Electrónica Avanzada (Clase 3).
- Certificado de Firma Electrónica Tributaria.

Paperless S.A emite certificados para firma electrónica conforme a la presente práctica.

1.5.4 Contenido de los Certificados

La estructura de datos del Certificado emitido por Paperless S.A es compatible con el estándar ISO/IEC 9594-8 y su contenido cumple con el Reglamento de la Ley N°19.799. Además de cumplir con la resolución exenta N°9 del 15 de febrero del 2001 del SII.

Los certificados emitidos por Paperless S.A contendrán

- RUT
- Correo electrónico
- Nombre Completo
- Tipo de certificado
- Datos de la acreditación de Paperless S.A

Adicionalmente los certificados de Firma Electrónica Tributaria contendrán en el campo “CERTIFICATE POLICIES” la glosa “Certificado para uso Tributario”.

Paperless S.A
Av. Andrés Bello 2687- Piso 25,
Las Condes, Santiago
56-2-5589 5400

1.6 Detalle de los contactos

1.6.1 Direcciones de Contactos

Paperless S.A tiene sus oficinas en Av. Andrés Bello 2687- Piso 25, Las Condes, Santiago

1.6.2 Contacto

Equipo PKI Paperless S.A, correo electrónico comunicaciones@pkichile.cl

Paperless S.A
Av. Andrés Bello 2687- Piso 25,
Las Condes, Santiago
56-2-5589 5400

2 Requerimientos Generales

2.1 Obligaciones

2.1.1 Obligaciones de la CA Raíz

Un certificado raíz es aquel que se utiliza para firmar los certificados de las entidades certificadoras subordinadas a dicha raíz. Estableciéndose de esa manera, una clara cadena de jerarquía de confianza. Paperless S.A es una entidad raíz y una entidad intermedia, por lo que ha emitido un certificado raíz para sí misma.

En el caso que otras entidades de certificación se subordinen a la jerarquía de certificación de Paperless S.A, ésta firmará los certificados raíz de dichas entidades subordinadas.

2.1.2 Obligaciones de la CA

Paperless S.A cumple con las siguientes obligaciones legales y de servicio para prestar un servicio de certificación electrónica. Cuenta con la infraestructura necesaria para prestar el servicio de certificación, así como los controles de seguridad física, de procedimiento y personales también necesarios para realizar esta actividad. Las obligaciones de Paperless S.A incluyen la emisión de certificados a quienes los soliciten, administrar el sistema de llaves (PKI) de modo de hacer operable la certificación y firmas electrónicas, y publicar y mantener listas de los certificados emitidos y revocados.

Asimismo, da cumplimiento a todas las obligaciones legales y reglamentarias relativas al ejercicio de esta actividad.

- **Emisión de Certificados**

  Paperless S.A emitirá los certificados que se le soliciten, una vez que se hayan aprobado dichas solicitudes mediante la comprobación del cumplimiento de los requisitos y antecedentes comerciales y legales necesarios.

- **Administración de Llaves**

  Paperless S.A provee a los titulares de certificados las llaves privada y pública necesarias para el buen funcionamiento del sistema (PKI). Estas llaves son generadas automáticamente por el sistema, garantizándose de esta manera su total confidencialidad.

- **Directorios de Certificados y Listas de Revocación**

  Paperless S.A cuenta con repositorios de datos en los que son almacenados por una parte los certificados emitidos y por otra los certificados revocados.

  El Directorio de Certificados es el listado de certificados emitidos, de los que queda constancia en www.pkichile.cl .

  La Lista de Revocación se encuentra en https://www.pkichile.cl/SolicitaCRL?type=FEA para los certificados de Firma Electrónica Avanzada y en https://www.pkichile.cl/SolicitaCRL?type=FES para los certificados de Firma Electrónica Tributaria

Paperless S.A
Av. Andrés Bello 2687- Piso 25,
Las Condes, Santiago
56-2-5589 5400

- **General**

La ley Chilena establece obligaciones comunes a la prestación de servicios de certificación, con las que deben cumplir tanto los prestadores no acreditados como los acreditados. En consecuencia, Paperless S.A declara cumplir las siguientes obligaciones:

a) Paperless S.A cuenta con Prácticas de Certificación Electrónica Avanzada, las que son objetivas y no discriminatorias, y se encuentran publicadas en castellano en http://www.pkichile.cl así como a disposición del público que así lo solicite.
b) Paperless S.A mantiene su registro de acceso público de certificados, en el que se dejará constancia de los emitidos y dejados sin efecto. Al registro podrá accederse electrónicamente. Paperless S.A está autorizado por la Ley N° 19.799 para hacer tratamiento de datos conforme los términos de la ley N° 19.628, con los datos personales entregados por los solicitantes de certificados.
c) Paperless S.A deberá comunicar el término de sus funciones a los titulares de firmas electrónicas certificadas por ellos, y transferir los datos a otro prestador. Los titulares pueden oponerse a la transferencia, en cuyo caso se dejarán sin efecto los certificados emitidos.
d) Paperless S.A dará cumplimiento a las demás obligaciones legales, especialmente las contempladas en las leyes N° 19.496 sobre Protección al Consumidor y N° 19.628, sobre Protección a la Vida Privada.
e) Paperless S.A da cumplimiento a lo expuesto en el punto 6° de la resolución exenta N°9 del 15 de febrero del 2001 del SII.

Además, de las anteriores, Paperless S.A da cumplimiento a las siguientes obligaciones:

a) Publica en su sitio de dominio electrónico http://www.pkichile.cl las resoluciones de la entidad acreditadora que le afecten;
b) En el otorgamiento de certificados de Firma Electrónica Avanzada, comprueba la identidad del solicitante. Para ello, el Paperless S.A requiere la comparecencia personal y directa del solicitante o del representante legal si es persona jurídica, ante sí o notario u oficial del registro civil, conforme se define en los requisitos de otorgamiento de los certificados de Firma Electrónica Avanzada que emite Paperless S.A;
c) Paperless S.A pagará anualmente el arancel de supervisión de la Entidad Acreditadora;
d) En caso de cesar actividades, Paperless S.A debe solicitar la cancelación de su inscripción en el registro de prestadores acreditados con un mes de anticipación a dicha cesación, y comunicar el destino de los certificados (transferencia o cancelación);
e) Paperless S.A deberá comunicar inmediatamente a cada uno de sus titulares la cancelación de la inscripción en el registro de prestadores acreditados, y traspasar los datos a otro prestador, en los mismos términos del cese voluntario de actividades.
f) Paperless S.A deberá comunicar a la entidad acreditadora cualquier hecho relevante que le afecte, especialmente la iniciación de un proceso de quiebra o de cesación de pagos.

En el cumplimiento de las obligaciones antes detalladas, Paperless S.A declara que se encuentra en condiciones de prestar el servicio de certificación para firma electrónica avanzada por cuanto:

a) Su servicio es fiable.
b) Garantiza la existencia de un servicio seguro de consulta del registro de certificados emitidos.

Paperless S.A
Av. Andrés Bello 2687- Piso 25,
Las Condes, Santiago
56-2-5589 5400

c) Emplea personal calificado para la prestación de los servicios ofrecidos, en el ámbito de la firma electrónica y los procedimientos de seguridad y de gestión adecuado.
d) Utiliza sistemas y productos confiables que garantizan la seguridad de sus procesos de certificación.
e) Cuenta con un seguro apropiado.
f) Cuenta con la capacidad tecnológica necesaria para el desarrollo de la ley.

En resumen, las obligaciones de Paperless S.A en cuanto a Autoridad Certificadora son:

- Ofrecer y mantener la infraestructura necesaria para la prestación de servicios de certificación electrónica, así como los controles de seguridad física, de procedimiento y personales necesarios para la práctica de la actividad de certificación.
- Aprobar o denegar las solicitudes de certificados.
- Poner copias de sus propios certificados y de cualquier información de revocación a disposición de quien desee verificar una firma digital con referencia a dichos certificados, para lo cual publicará en http://www.pkichile.cl toda la información necesaria.
- Publicar los certificados emitidos.
- Cumplir las demás obligaciones legales, reglamentarias y las de estas DPC.

2.1.3 Obligaciones de la Autoridad Registradora RA

Paperless S.A, en cuanto RA, asume las siguientes obligaciones de las cuales será responsable. Estas obligaciones son:

- Identificar y autenticar correctamente al solicitante y/o suscriptor y a la organización que represente, conforme los procedimientos que se establecen en estas DPC.
- Paperless S.A realizará por sí la verificación de identidades de los solicitantes de certificados digitales, en todos aquellos casos en que el solicitante pueda concurrir personalmente a las oficinas de Paperless S.A o los representantes de la empresa visiten al titular en el lugar que este último solicite.
- Formalizar los contratos de expedición de certificados con el solicitante/suscriptor en los términos y condiciones que establezca la CA.
- Almacenar en forma segura y por el período que exige la ley la documentación aportada en el proceso de emisión de un certificado y en el proceso de revocación del mismo.
- Llevar a cabo cualesquiera otras funciones que le correspondan, a través del personal que sea necesario para cada caso, conforme lo establecen la DPC.

En todo caso, las funciones antes descritas podrán ser realizadas directamente por la CA, en cualquier momento, es decir, Paperless S.A en el ejercicio de la actividad de certificación digital puede realizar las funciones descritas para una RA. En este caso, toda referencia hecha a los servicios de una RA se entenderá hecha a la CA. Tratándose de certificados para Firma Electrónica Avanzada, Clase 3, las actividades de RA debe realizarlas Paperless S.A directamente, a menos que la verificación de la identidad del solicitante se realice ante notario u oficial de registro civil, en cuyo caso el resto de las obligaciones de la RA las realizará igualmente Paperless S.A.

Paperless S.A se reserva la facultad de designar una o más Autoridades de Registro que validarán los antecedentes relativos a la identificación de los solicitantes que contraten los servicios de certificación digital, o para realizar otras determinadas funciones que Paperless S.A determine, de acuerdo con lo señalado anteriormente.

Paperless S.A
Av. Andrés Bello 2687- Piso 25,
Las Condes, Santiago
56-2-5589 5400

En todo caso, la RA permitirá a la CA el acceso a los archivos y a los procedimientos asumidos por la RA y le dará derecho a investigar cualquier sospecha de infracción de la CPS y/o de las Prácticas de Certificación Avanzada por parte de la RA o cualquier poseedor de un certificado. La RA y los poseedores de cualquier certificado deberán informar a la CA inmediatamente cualquier sospecha de infracción.

2.1.4 Obligaciones del Suscriptor

Corresponde al suscriptor la suscripción del contrato de prestación de servicios de certificación digital, sea para sí, o sus representados. En este rol, le corresponde verificar que la información proporcionada por los solicitantes sea efectiva. Asimismo, debe velar por el correcto uso y resguardo de los certificados utilizados por sus representados. Deberá notificar a la CA de cualquier cambio en la relación laboral que mantiene con sus representados de manera de actualizar la información, y solicitar la revocación de los certificados cuando dicha relación cambien o termine.

2.1.5 Obligaciones del Solicitante

El solicitante de un certificado deberá abonar la tarifa o precio establecido para el servicio solicitado. Asimismo, deberá proveer toda la información de identificación personal y de su empresa, dependiendo del tipo de certificado que se solicite. La solicitud de servicio deberá realizarse conforme estas DPC y las instrucciones pertinentes.

2.1.6 Obligaciones del Titular de la Llave

Corresponde al titular de los certificados de Firma Electrónica Avanzada y de la llave:

- Conservar y utilizar correctamente el certificado de Firma Electrónica Avanzada que se le entrega.
- Custodiar el certificado de forma diligente, tomando las precauciones razonables para evitar su pérdida, revelación, modificación o uso no autorizado;
- Solicitar la revocación del certificado cuando se cumpla alguno de los supuestos previstos en el capítulo “Revocación de Certificados” de estas DPC.
- No revelar la clave privada ni el código de activación del certificado.
- Asegurarse de que toda la información contenida en el certificado es cierta y notificar inmediatamente a la CA en caso de que se haya incluido cualquier información incorrecta o inexacta o en caso de que, en forma sobreviviente, la información del certificado ya no sea correcta. Por ello, deberá comunicar en forma inmediata los cambios en los datos aportados para adquirir y emitir el certificado, aunque no sea parte integrante de éstos (domicilio, teléfono, etc.).
- Informar inmediatamente a la CA de cualquier situación que pueda afectar la validez de los certificados.
- Destruir el certificado cuando lo exija la CA en virtud del derecho de propiedad que en todo caso ésta conserva sobre el certificado, cuando el certificado caduque o sea revocado.
- Realizar un uso debido y correcto del certificado, según se desprende de estas DPC. El uso indebido o fraudulento del certificado es responsabilidad del titular y suscriptor.
- Cualquiera otra obligación que derive de la Ley, el Reglamento, estas DPC o la naturaleza del certificado digital.

2.1.7 Obligaciones los Usuarios

Los terceros o usuarios que pretendan confiar en los certificados emitidos por Paperless S.A deberán verificar la validez de las firmas emitidas por los titulares. Si los usuarios no verificaren las firmas mediante los listados correspondientes, la CA no será responsable del uso y confianza que los usuarios otorguen a esos certificados.

Paperless S.A
Av. Andrés Bello 2687- Piso 25,
Las Condes, Santiago
56-2-5589 5400

Los usuarios del servicio de certificación de Paperless S.A se obligan a conocer y aceptar los términos y condiciones y límites de uso contenidos en estas Políticas y las correspondientes Prácticas de Certificación de Firma Electrónica Avanzada.

2.1.8 Confianza en las Firmas

Toda persona tendrá derecho a confiar en una firma electrónica emitida mediante un certificado de Paperless S.A en la medida que sea razonable hacerlo. Para determinar si es razonable confiar, deberá tenerse en cuenta para cada caso lo siguiente:

- La naturaleza de la operación correspondiente que la firma pretende avalar.
- Si la parte que confía ha adoptado medidas adecuadas para determinar la fiabilidad de la firma, y en particular si ha verificado que el certificado no esté caducado o revocado. La caducidad consta en el mismo certificado. La revocación debe ser consultada en el listado correspondiente.
- Si la parte que confía sabía o debía saber que la firma estaba revocada o en entredicho.
- Las normas legales, reglamentarias de estas DPC y las condiciones de cada tipo de certificado.

2.1.9 Confianza en los Certificados

Toda persona tendrá derecho a confiar en un certificado de Paperless S.A en la medida que sea razonable hacerlo.
Para determinar si es razonable confiar, deberá tenerse en cuenta para cada caso lo siguiente:

- Toda restricción a que esté sujeto el certificado.
- Si el usuario ha adoptado las medidas adecuadas para determinar la fiabilidad del certificado.
- Las políticas y procedimientos que rigen la actividad de Paperless S.A.

2.1.10 Obligaciones de los Repositorios

Paperless S.A llevará un registro actualizado de los certificados vigentes y revocados en un repositorio para tales efectos, y que se encuentra en https://www.pkichile.cl/vigencia.jsp

2.2 Responsabilidades Legales

2.2.1 Responsabilidades Generales

Paperless S.A será responsable de los daños y perjuicios que con ocasión del ejercicio de su actividad cause por la certificación y homologación de certificados de firma electrónica. En ningún caso Paperless S.A será responsable de los daños que tengan origen en el uso indebido o fraudulento de un certificado de firma electrónica avanzada.

Un certificado de Firma Electrónica Avanzada provisto por Paperless S.A podrá establecer límites en cuanto a los posibles usos del certificado, en cuyo caso, Paperless S.A queda eximido de cualquier responsabilidad por el uso que se dé a dichos certificados y que excedan tales límites. Paperless S.A será responsable del cumplimiento de sus obligaciones como CA y RA en los casos que le corresponda, y en virtud del cumplimiento de tales obligaciones ha tomado un seguro por responsabilidad civil por el monto exigido en la ley en una compañía de seguros del mercado, el que podrá hacerse efectivo una vez concluida la prueba de la

Paperless S.A
Av. Andrés Bello 2687- Piso 25,
Las Condes, Santiago
56-2-5589 5400

responsabilidad de Paperless S.A. Se presume que Paperless S.A ha actuado con la debida diligencia, por cuanto cumple con lo dispuesto en los artículos 12 y 13 de la Ley N° 19.799.

2.2.2 Fuerza Mayor

Paperless S.A quedará exenta de toda responsabilidad y liberada del cumplimiento de sus obligaciones cuando, por razones de caso fortuito o fuerza mayor tales como sismos, inundaciones, sobre voltajes, cortes del suministro eléctrico y/o telefónico y/o de líneas de transmisión de datos, actos terroristas, huelgas u otros imposibles de prever, no pueda emitir o revocar certificados o no permita consultar la lista de certificados revocados.

2.2.3 Responsabilidad de la CA y RA

Paperless S.A no será responsable de los daños derivados o relacionados con la no ejecución o ejecución defectuosa de las obligaciones que corresponden al Solicitante, Suscriptor y/o Usuario. Paperless S.A no será responsable de la incorrecta utilización de los certificados y las claves, ni de cualquier daño indirecto que pueda resultar de la utilización del certificado o de la información suministrada por la CA. En particular el lucro cesante, la pérdida de ingresos o pedidos o pérdida de datos tendrán la consideración de daños indirectos y los mismos no darán lugar a indemnización alguna.

Paperless S.A no será responsable de las eventuales inexactitudes en el certificado que resulten de la información proporcionada por el suscriptor. Paperless S.A no será responsable de los daños que se deriven de aquellas operaciones en que se hayan superado las limitaciones de uso que se señalan en estas políticas y las correspondientes prácticas de certificación correspondientes a cada tipo de certificado.

2.3 Interpretación y Resguardos Legales

Paperless S.A se rige por la legislación Chilena y se encuentra sometida a la jurisdicción de los tribunales de justicia de la República de Chile.

2.4 Publicación y Repositorios

Toda la información relevante para la comunidad de usuarios de certificados digitales se encuentra publicada en http://www.pkichile.cl. Esta información es permanentemente actualizada y no tiene controles de acceso.

Los repositorios se rigen por las mismas normas anteriores, sin perjuicio que por obligación legal el Listado de Certificados Revocados se actualiza con una frecuencia de 24 hrs.

2.5 Privacidad y Protección de los Datos

2.5.1 Tipos de Información a Proteger

Paperless S.A considera confidencial y para su uso exclusivo la información personal de los suscriptores, solicitantes y titulares de certificados. Paperless S.A no utilizará esta información personal para otros fines que los relacionados con sus actividades de certificación, ni comparte esta información con terceros salvo lo señalado en los números siguientes.

Paperless S.A
Av. Andrés Bello 2687- Piso 25,
Las Condes, Santiago
56-2-5589 5400

2.5.2 Tipos de Información que Puede ser Entregada

Concordante con lo anterior, Paperless S.A, como política general, no entrega información personal de sus clientes.

Sin perjuicio de lo anterior, los certificados emitidos por Paperless S.A contienen información de identificación del titular, y el contenido del certificado está definido en la Ley Nº 19.799.

2.5.3 Información del Certificado

El certificado de firma electrónica avanzado contiene los siguientes campos obligatorios de información de los titulares:

- RUT
- Correo electrónico
- Nombre
- Tipo de certificado
- Datos de la acreditación de Paperless S.A

2.5.4 Entrega de Información sobre la Revocación del Certificado

La información sobre el estado de vigencia o revocación de un certificado emitido por Paperless S.A se encuentra publicada en https://www.pkichile.cl/vigencia.jsp

2.5.5 Entrega de Información en virtud de un Procedimiento Judicial

Paperless S.A sólo entregará la información requerida en virtud de un procedimiento judicial.

2.5.6 Entrega de Información a Petición del Titular

Paperless S.A administra información proporcionada por el propio solicitante y/o titular.

2.6 Derechos de Propiedad Intelectual

Paperless S.A se reserva la propiedad intelectual, moral y patrimonial del presente documento de Prácticas de Certificación Electrónica Avanzada y de sus documentos relacionados o afines, tales como formularios de solicitud de certificados, contratos, anexos técnicos, etc. Por ende queda prohibida toda reproducción, comunicación, distribución, archivo o transmisión de cualquier tipo y por cualquier medio, mecánico, electrónico, fotográfico o magnético, total o parcial de las mismas sin previa y expresa autorización escrita de Paperless S.A.

Paperless S.A
Av. Andrés Bello 2687- Piso 25,
Las Condes, Santiago
56-2-5589 5400

3 Identificación y Autenticación

3.1 Registro Inicial

3.1.1 Registro de Nombres

Paperless S.A registrará los nombres completos, es decir nombres y apellidos paterno y materno conforme a la usanza Chilena, de las personas naturales, y la razón social de las personas jurídicas, en los campos correspondientes del formulario de inscripción. Adicionalmente, se registran los RUT – identificador único- de todas las personas naturales y jurídicas.

3.1.2 Verificación General

Además de los requisitos de nombres antes indicado, se solicita a los suscriptores copia de su Cédula de Identidad por ambos lados, título profesional si es del caso, y tratándose de personas jurídicas, todos los antecedentes legales correspondientes.

Estos antecedentes deben presentarse personalmente en Paperless S.A, a fin de verificar fehacientemente la identidad de los solicitantes. Paperless S.A publica en http://www.pkichile.cl los requisitos de identificación necesarios para cada tipo de certificado.

3.2 Reemisión de la Llave

Por razones de seguridad para garantizar la característica de no-repudio, Paperless S.A no reemite llaves una vez generado un certificado de Firma Electrónica Avanzada.

3.3 Reemisión de la Llave luego de una Revocación

Por razones de seguridad para garantizar la característica de no-repudio, Paperless S.A no reemite llaves una vez revocado un certificado de Firma Electrónica Avanzada.

3.4 Requerimiento de Revocación

Tratándose de personas naturales, la revocación de los certificados digitales emitidos por Paperless S.A debe ser solicitada por el titular, por vía electrónica a comunicaciones@pkichile.cl o a través de la página Web http://www.pkichile.cl.

Paperless S.A
Av. Andrés Bello 2687- Piso 25,
Las Condes, Santiago
56-2-5589 5400

4 Requisitos Operacionales

4.1 Manuales Operacionales

Paperless S.A cuenta con Manuales de Operación detallados que se encuentran a disposición de los interesados en sus oficinas. En ellos se describe el proceso de solicitud, instalación, verificación y respaldo de los certificados emitidos por Paperless S.A. A continuación se hace una descripción del proceso señalado.

4.2 Solicitud de Certificado

4.2.1 Verificación General

El registro de los solicitantes de certificados se realiza conforme las disposiciones de la Ley Nº 19.799, y las normas que se señalan a continuación.

4.2.2 Labores de CA y RA

Paperless S.A podrá realizar labores de registro de solicitantes de certificados a través de entidades con las cuales suscriba convenios para estos efectos. No obstante lo anterior, para el registro y revisión de antecedentes de solicitantes de certificados de firma avanzada, Paperless S.A realizará todas las actividades correspondientes a las autoridades de registro.

Para efectos del registro de solicitantes de certificados de firma electrónica avanzada, Paperless S.A realizará una comprobación fehaciente de la identidad del solicitante y cada uno de los futuros titulares de certificados. Dicha información será guardada y custodiada en las oficinas de Paperless S.A y sólo se utilizará para los propósitos de la emisión de los certificados y registro de clientes.

4.3 Emisión de Certificados

Paperless S.A sólo emitirá los certificados solicitados una vez cumplidos los requisitos de solicitud y comprobados los antecedentes del solicitante y futuros titulares, dependiendo del tipo de certificado requerido.

4.4 Aceptación de Certificados

El sólo hecho de acceder a la dirección URL antes indicada y bajar el certificado implica la aceptación de éste.

4.5 Revocación de Certificados

4.5.1 Circunstancias de Revocación

Son causales de Revocación del certificado los siguientes motivos:

- Pérdida del certificado
- Pérdida del dispositivo
- Pérdida de la clave de acceso (pin) al certificado y/dispositivo
- Cesación en el cargo

Paperless S.A
Av. Andrés Bello 2687- Piso 25,
Las Condes, Santiago
56-2-5589 5400

- Solicitud del titular o solicitante
- No pago de la renovación
- Revocación por parte de Paperless S.A

4.5.2 Solicitud de Revocación

Sólo podrán solicitar la revocación de un certificado el titular de éste o el solicitante en aquellos casos que se trate de empresas. Tratándose de certificados de representantes legales, el nuevo representante legal podrá solicitar la revocación de los certificados de sus dependientes conforme las normas generales de derecho.

4.5.3 Procedimiento de Revocación

Dependiendo de la causal invocada, el interesado, y facultado para solicitar dicha revocación, deberá enviar un correo electrónico a Paperless S.A, a la casilla comunicaciones@pkichile.cl o a través de la página Web http://www.pkichile.cl, para solicitar la revocación, con expresa indicación de los datos del titular, el motivo de la revocación. Paperless S.A se reserva el derecho de verificar los antecedentes invocados para la revocación.

4.5.4 Listado de Certificados Revocados

La Frecuencia de Emisión del Listado de Certificados Revocados - CRL de Paperless S.A se genera y actualiza cada 24 horas. Los Requisitos para Comprobar la CRL es a través de la dirección https://www.pkichile.cl, y no tiene requisitos de comprobación.

Paperless S.A no contempla otras formas de aviso de revocación más que la publicación en la CRL, salvo acuerdos específicos con grupos de usuarios. Paperless S.A tiene contemplados procedimientos adecuados de seguridad y auditoria. Paperless S.A dará cumplimiento a las exigencias legales en materia de término de su actividad como RA y CA.

Paperless S.A
Av. Andrés Bello 2687- Piso 25,
Las Condes, Santiago
56-2-5589 5400

5 Controles de Personas, Físicos y de Procedimientos

5.1 General

Paperless S.A cuenta con políticas de control de su personal, de sus equipos y de los procedimientos para la actividad de certificación electrónica. Estos controles han sido diseñados conforme a los requerimientos de esta actividad.

5.2 Data Center

Paperless S.A para la prestación de sus servicios, integra a sus políticas y procedimientos los servicios de seguridad que brinda GTD.

GTD es un centro de datos de clase mundial con el máximo nivel de seguridad para resguardar el equipo y la información de los clientes de Paperless S.A, incorporando múltiples medidas para su protección, combinando varios mecanismos restrictivos y procesos para aumentar al máximo la seguridad.

En GTD, las áreas y los servicios en los cuales se manejan información confidencial cuentan con procedimientos de control de acceso, supervisados continuamente a efecto de reducir al mínimo los riesgos, estos procedimientos se describen en la "Política de Seguridad Física de Paperless S.A". Los controles implementados evitan riesgos, daño o pérdida de los activos, alteración o sustracción de la información.

Mientras que los servicios compartidos por otra entidad distinta a Paperless S.A, o por personal de éste no dedicado al servicio de certificación, se encuentra fuera del perímetro de seguridad.

5.2.1 Seguridad Física Data Center

GTD brinda los siguientes aspectos de seguridad física

- Un solo punto de acceso al Centro de Datos, protegido por personal de seguridad las 24 horas del día.
- Acceso a visitantes con escolta y sólo con cita previa autorizada del Oficial de Seguridad de Paperless S.A.
- Muro perimetral.
- Más de 100 cámaras de vigilancia ubicadas en los exteriores e interiores del Edificio.
- Sistemas de monitoreo continuo en sitio para controlar la seguridad física de las instalaciones.
- Acceso restringido al Centro de Datos a través de tarjetas de proximidad, sensores biométricos de huella y temperatura corporal, vidrios anti-balas nivel 7 y puertas con esclusas de acero.

5.2.2 Sistema de Energía Eléctrica

GTD cuenta con un avanzado esquema de redundancia de suministro de energía que supera los estándares tradicionales de los Centros de Datos en el mundo.
En el remoto caso de un corte, tiene implementado un sistema de respaldo que consiste en equipos generados que son alimentados por múltiples tanques de diesel.

5.2.3 Sistema de Control Ambiental

El sistema ambiental de GTD funciona a través de un control automatizado que regula tanto la temperatura como las condiciones de humedad del Centro de Datos a través de unidades de aire acondicionado.

Paperless S.A
Av. Andrés Bello 2687- Piso 25,
Las Condes, Santiago
56-2-5589 5400

La distribución del aire brinda circulación ininterrumpida bajo el piso falso anti-estático, y le ofrece flujo preferente a los racks para prolongar el periodo de vida útil de los equipos. GTD utiliza también aires de precisión en los componentes críticos de la infraestructura de energía eléctrica.

5.2.4 Sistema de Extinción y Control de Incendios

Como primera línea de defensa ante un incendio, GTD ha incorporado un sistema de detección de incendios capaz de identificar sensibles incrementos en la temperatura del cableado y otros componentes críticos de la infraestructura del Centro de Datos. De esta manera, el personal puede tomar acciones preventivas para eliminar un posible foco de siniestro.

No obstante, en el lejano caso de un siniestro, GTD cuenta con un eficiente sistema de extinción vía gas, ya que no crea neblina al ser expulsado, para no disminuir la visibilidad de las salidas de emergencia y no deja residuos que afecten los equipos de cómputo.

5.2.5 Seguridad Lógica Data Center

GTD brinda los siguientes aspectos de seguridad lógica:

- Múltiple tecnología de firewall
- Sistema de detección de intrusos
- Sistemas de análisis de seguridad activos

Paperless S.A
Av. Andrés Bello 2687- Piso 25,
Las Condes, Santiago
56-2-5589 5400

6 Controles de Seguridad Técnica

6.1 General

Paperless S.A cuenta con políticas de seguridad técnica para la actividad de certificación electrónica. Estos controles han sido diseñados conforme los requerimiento de esta actividad. A modo de garantizar la seguridad en la emisión de certificados, a continuación se explica los procedimientos inherentes a la creación de llaves.

6.2 Instalación y Generación de Pares de Llaves

Paperless S.A para sus aspectos de instalación y generación de pares de llaves los relaciona con las siguientes actividades:

- **Generación del par de Llaves**

  Las llaves inherentes al certificado emitido por Paperless S.A se generan en el momento que el solicitante completa el procedimiento para la solicitud del certificado. A su vez, junto a la entrega del certificado electrónico a su titular se activan las llaves y el certificado.

- **Entrega de la Llave Privada**

  La llave privada se entrega al solicitante junto con el certificado electrónico.

- **Entrega de la Llave Pública al Emisor del Certificado**

  La llave pública se entrega al solicitante junto con el certificado electrónico.

- **Entrega de la Llave Pública de la PSC**

  La llave pública de la PSC se entrega al solicitante junto con el certificado electrónico.

- **Largo de Llaves**

  Las llaves proporcionadas por Paperless S.A tienen la capacidad de generar llaves de 2048 bits.

- **Generación de Parámetros para la Llave Pública**

  Las llaves públicas se generan y entregan al comprobarse los requisitos necesarios para la solicitud de un certificado digital.

- **Verificación de la Calidad de los Parámetros**

  Los parámetros de verificación se revisan a través de la comprobación de los antecedentes proporcionados por el solicitante y la aprobación del otorgamiento de un certificado electrónico.

Paperless S.A
Av. Andrés Bello 2687- Piso 25,
Las Condes, Santiago
56-2-5589 5400

- **Generación de Llave por Hardware/Software**

El par de llaves se genera en el browser del solicitante al momento de enviar la solicitud de un certificado electrónico. Estas llaves son generadas en un dispositivo definido en el Proveedor de Servicios Criptográficos. De esta manera se define si las llaves se generaran en un dispositivo interno del equipo o externo (token, smartcard u otro).

- **Propósitos de la Llave (como X.509 v3)**

El par de llaves y el certificado electrónico tienen por propósito identificar al titular y permitirle firmar electrónicamente documentos electrónicos (asociado a otro software), así como cifrar tales documentos.

7 Administración de las DPC

7.1 Procedimientos para Modificar las DPC

Estas Prácticas de Certificación Digital Avanzada han sido generadas en consideración a la actividad de la certificación electrónica, la Ley y el Reglamento Chileno sobre la materia. En caso de requerirse modificaciones a ésta, serán publicadas, en lo pertinente, con anticipación de 30 días a su implementación.

Paperless S.A
Av. Andrés Bello 2687- Piso 25,
Las Condes, Santiago
56-2-5589 5400