POLÍTICA DE CERTIFICACIÓN.

Código:	**POL-DSIG-SGI-003**
Versión:	1.2
Fecha de la versión:	18/02/25
Nivel de confidencialidad:	Interno

Elaborado por: **Pablo García -Oficial de Seguridad**
Revisado y Autorizado: **Silvia Valerio – Coordinadora Dsigner**

DSIGNER S.A.

Tabla de Contenido

1. Objetivo.

Establecer los criterios y procedimientos necesarios para garantizar que todos los procesos de certificación dentro de Dsigner, se realicen de manera consistente, imparcial y en cumplimiento con los estándares establecidos en la guía de requisitos establecida por el registro de prestadores de servicios de certificación (RPSC), asegurando la calidad y la credibilidad de los productos, servicios o procesos certificados.

2. Alcance.

Este documento declara las Políticas de Certificación de DSIGNER S.A., las cuales dan cumplimiento a los requisitos establecidos en el Decreto 47-200, Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas y su reglamento, así como las normas técnicas que establece el Registro de Prestadores de Servicios de Certificación.

3. Documentos de Referencia.

Guía de evaluación RPSC: ME-VAR-RPSC-IN-01 Versión 1. R4-24
Decreto 47-200, Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas.

4. Glosario.

Registro de prestadores de servicios de certificación -RPSC: Adscrito al Ministerio de Economía, ejerce las funciones que legalmente le han sido asignadas respecto a los Prestadores de Servicios de Certificación.

Certificado digital: Es el único medio que permite garantizar técnica y legalmente la identidad de una persona a través del Internet y las diferentes comunicaciones electrónicas. El certificado digital es el que nos permite ofrecer una firma electrónica avanzada para firmar documentos, el receptor de un documento firmado puede tener la seguridad de que éste es el original y no ha sido manipulado; por lo tanto, el autor de la firma electrónica avanzada no podrá negar la autoría de esta firma.

Llave pública y privada: Un certificado digital contiene una pareja de claves criptográficas, una pública y una privada, creadas con un algoritmo matemático, de forma que aquello que se cifra con una de las claves sólo se puede descifrar con su clave pareja. El titular del certificado debe mantener bajo su poder la clave privada, ya que, si ésta es sustraída, el sustractor podría suplantar la identidad del titular. La clave pública forma parte de lo que se denomina certificado digital en sí, que es un documento digital que contiene la clave pública junto con los datos del titular, todo ello firmado electrónicamente por una autoridad de certificación (CA), la cual es un tercero de confianza que asegura que la clave pública corresponde con los datos del titular.

CA - Certification-Authority: Autoridad certificadora raíz, es una entidad de confianza, que expide los certificados digitales, con toda la seguridad y es quién posee la infraestructura PKI para dicha emisión de certificados.

RA - Registration-Authority: Autoridad de registro. La función de las autoridades de registro es controlar y registrar la generación de certificados digitales que se emiten a los usuarios. Previa identificación, la autoridad de registro se encarga de realizar la petición del certificado y de guardar los datos pertinentes que identifican al titular.

PIN Secreto: Contraseña secreta que únicamente el titular debe conocer, el sistema digital se la solicitará cada vez que desee firmar un documento electrónico con su certificado de firma electrónica avanzada.

GLOBALSIGN: Proveedor internacional de certificados digitales el cual provee los servicios de gestión de los certificados como autoridad certificadora raíz de DSIGNER, S.A.

OTP - One-Time-Password: Código de validación que llega al teléfono móvil como mensaje de texto para confirmar el número de teléfono y seguir el proceso de validación digital.

PDF - Portable-Document-Format: Formato de documento portátil; es un formato de almacenamiento para documentos digitales independiente de plataformas de software o hardware.

5. Política de certificación.

5.1. Titulares que pueden solicitar certificados de firma electrónica avanzada

A continuación, se especifican los titulares que pueden adquirir por nuestro servicio, un certificado de firma electrónica avanzada:

- Persona Individual.
- Profesional titulado.
- Relación con la entidad.
- funcionario Público.
- Representante Legal.
- Persona Jurídica.

Cualquier persona nacionalizada en Guatemala que tenga su identificación oficial guatemalteca con la documentación necesaria puede solicitar un certificado de firma electrónica avanzada.

5.2. Requisitos por tipo de certificado.

Persona Individual:

- Nombre completo; nombres, apellidos.
- Correo electrónico (Correo válido).
- Fecha de Nacimiento. o Número de DPI.
- Municipio de nacimiento
- Dirección de residencia; Dirección; zona, Municipio, Departamento.
- Fecha de nacimiento o Número de Identificación Tributaria. (NIT)
- Teléfono de contacto; Residencia y Celular.
- País
- Código postal

- Departamento
- Documento Personal de Identificación (DPI) – formato imagen.

Persona Profesional:

- Nombre completo; nombres, apellidos.
- Correo electrónico (Correo válido).
- Número de DPI.
- Municipio
- Dirección de residencia; Dirección; zona, Municipio, Departamento.
- Fecha de Nacimiento.
- Número de Identificación Tributaria. (NIT)
- Teléfono de contacto; Residencia y Celular.
- Profesión.
- Título
- Departamento
- No. De Colegiado
- Código postal
- Documento RTU actualizado
- Constancia de Colegiado Profesional (activo)
- Documento Personal de Identificación (DPI) – formato imagen.
- Documento RTU actualizado.
- Constancia de Colegiado Profesional (activo).

Persona con relación a entidad:

- Nombre completo; nombres, apellidos. ○ Correo electrónico (Correo válido). ○ Número de DPI.
- Municipio residencia
- Dirección de residencia; Dirección; zona, Municipio, Departamento.
- Fecha de Nacimiento.
- Número de Identificación Tributaria (NIT)
- Teléfono de la empresa
- Empresa donde labora.
- Área de empresa donde pertenece.
- Cargo desempeñado.
- Supervisor inmediato
- País
- Departamento de residencia
- Dirección de la empresa
- Vigencia del cargo
- Código postal
- Documento RTU actualizado

- Documento de relación con la empresa con cargo desempeñado.
- Documento Personal de Identificación (DPI) – formato imagen.
- Documento RTU actualizado.
- Documento de relación con empresa con cargo desempeñado

Funcionario Público:

- Nombre completo; nombres, apellidos.
- Correo electrónico (Correo válido).
- Número de DPI. o Lugar de Nacimiento; municipio.
- Dirección de residencia; dirección; zona, municipio, departamento.
- Fecha de Nacimiento.
- Número de identificación tributaria (NIT)
- Teléfono de contacto; Residencia y Celular.
- Documento RTU actualizado
- Carta de solicitud firmada por la máxima autoridad de la institución
- Cargo
- Vigencia del cargo
- Entidad
- Dirección de Entidad
- Dependencia
- Código postal
- Departamento
- Documento Personal de Identificación (DPI) – formato imagen.
- Documento RTU actualizado del funcionario
- Nombramiento por parte de la institución
- Carta de autorización de la máxima autoridad de la institución a la que pertenece.

Representante legal:

- Nombre completo; nombres, apellidos.
- Correo electrónico (Correo válido).
- Número de DPI.
- Municipio de nacimiento
- Dirección de residencia; Dirección; zona, Municipio, Departamento.
- Fecha de Nacimiento.
- Número de Identificación Tributaria. (NIT)
- Teléfono de contacto; Residencia y Celular.
- Nombre de la compañía
- Dirección de la compañía
- Número de representación
- Vigencia de representación

- Patente de la compañía
- Número de identificación tributaria NIT de la compañía ○ Código postal
- Departamento
- RTU actualizado de la institución
- Nombramiento vigente como representante legal
- Patente de Sociedad
- Patente de comercio
- Documento Personal de Identificación (DPI) – formato imagen.
- RTU actualizado de la Institución.
- Nombramiento vigente como Representante Legal.
- Patente de sociedad
- Patente de comercio

Representante legal:

- Nombre completo; nombres, apellidos de Representante Legal
- Correo electrónico (Correo válido representante legal).
- Número de DPI representante legal.
- Lugar de Nacimiento; municipio.
- Dirección de residencia; Dirección; zona, Municipio, Departamento.
- Fecha de nacimiento
- Número de identificación tributaria (NIT) de la empresa
- Número de Identificación Tributaria representante legal
- Teléfono de contacto; Residencia y Celular
- Nombre de la Entidad
- RTU actualizado del representante legal
- RTU actualizado de la institución
- Nombramiento vigente del representante legal
- Patente de Comercio
- Patente de sociedad anónima
- Acta de constitución de la empresa
- Número de representación, registro, finca, folio y libro
- Vigencia de representación
- Número de registro, folio y libro de la sociedad
- Dirección Empresa, Zona, Municipio, Departamento (Comprobable)
- Acta de Constitución de Entidad o Sociedad. – PDF
- RTU actualizado de la Institución. – PDF
- Nombramiento vigente como Representante Legal – PDF
- RTU actualizado del representante legal
- Patente de Comercio. – PDF
- Patente de Sociedad – PDF
- Documento Personal de Identificación (DPI) Representante legal – formato imagen.

5.3. Procedimiento de registro (Solicitud de Firma Electrónica Avanzada)

A continuación, se describe el proceso a utilizar para el registro de cualquier firma electrónica avanzada proveniente de DSIGNER, S.A.

5.3.1. Procedimiento digital de identificación

Nuestro procedimiento de registro y solicitud de certificados de firma electrónica avanzada es única y exclusivamente digital. El titular podrá utilizar nuestro portal para iniciar su procedimiento de adquisición, registro y verificación digital, el cual se encuentra completamente descrito en el apartado de "Tutoriales" del portal web.

Dichos procedimientos, se inician desde la adquisición o compra de una suscripción por el titular hasta la verificación y aprobación de la identidad de los solicitantes. La suscripción que se da dentro de la plataforma definirá el tipo de certificado de firma avanzada digital que el usuario solicite.

Luego de adquirir su suscripción, el titular podrá iniciar el proceso de verificación digital dentro de nuestro portal; nuestra plataforma Dsigner, enviará un correo electrónico con un enlace, hacia el proceso de verificación en donde el solicitante realizara los pasos que se indican tales como el llenado de los datos que se solicitan en el formulario en línea, la incorporación de los documentos solicitados, así como la prueba de vida y la validación de su número telefónico mediante un token OTP.

Al concluir su solicitud, esta es enviada hacia nuestros servicios de verificación digital en donde nuestro Operador PKI, estará respondiendo cada solicitud validando la información del titular en línea y si hubiese necesidad de algo adicional tendrá la facultad de solicitarle documentos adicionales para la corroboración de sus datos e identidad.

Luego de terminada la validación digital, el Operador PKI procederá a aprobar el certificado digital de acuerdo con la firma electrónica avanzada solicitada, el solicitante recibirá una notificación por correo electrónico con el resultado. Si esta es favorable, el solicitante, podrá ingresar nuevamente al sistema Dsigner, confirmando el contrato de "Términos y Condiciones" el cual firmará electrónicamente, a través de la configuración del "PIN" de su certificado digital el cual le servirá para certificar y validar legalmente cada uno de los documentos que firme electrónicamente. Este PIN es único y secreto y solo puede ser utilizado por el titular y responsable de la firma electrónica avanzada.

Finalmente, el solicitante, tendrá disponible su firma electrónica avanzada dentro de su perfil con la que podrá iniciar la firma de documentos digitales con validez legal.

5.3.2. Generación de llaves privadas

Un certificado digital consta de una pareja de claves criptográficas, una pública y una privada, creadas con algoritmos matemáticos, de forma que aquello que se cifra con una de las claves sólo se puede descifrar con su clave pareja. El titular del certificado debe mantener bajo su poder la clave privada, ya que, si ésta es sustraída, el sustractor podría suplantar la identidad del titular. La clave pública, es un documento digital que contiene, los datos del titular, validado y certificado por una autoridad de certificación (CA), que es una tercera entidad de confianza que asegura que la clave pública corresponde con los datos del titular.

Esta solicitud es enviada por medio de canales seguros a los servicios web de GlobalSign en donde el resultado, de la solicitud es la recepción de la llave pública de nuestra solicitud.

Esta llave pública es configurada en el perfil del titular para el uso de su firma electrónica avanzada desde el portal o sistema de DSIGNER.

Cuando el titular desea firmar un documento dentro de nuestro sistema o plataforma, este debe colocar su "PIN / Contraseña" para poder utilizar su llave privada dentro de la custodia de GlobalSign.

DSIGNER, S.A. no entrega ninguna llave privada al titular, ni credenciales para el uso de su certificado en otro sistema. Los certificados emitidos en DSIGNER, S.A. únicamente pueden ser utilizados dentro de nuestro sistema. Los términos y condiciones se encuentran establecidos en el contrato firmado por el titular a la hora de la adquisición de nuestros servicios.

5.3.3. Uso del certificado de firma electrónica avanzada

DSIGNER, S.A. no se hace responsable del contenido de los documentos firmados dentro del sistema.

DSIGNER, S.A. provee una solución en la nube para que el titular pueda utilizar su firma electrónica avanzada, con la cual podrá firmar la documentación que él requiera, el contenido de dichos documentos es ajeno a DSIGNER, S.A.

El uso de la firma electrónica avanzada de DSIGNER, S.A. es de uso único, dentro del sistema Dsigner (https://portal.dsigner.online), y tanto la suscripción del servicio en la nube como la validez del certificado digital, deberán estar vigentes para que el titular pueda utilizar el servicio sin interrupción.

Los certificados de firma electrónica avanzada se utilizarán para firmar, documentos electrónicos, con validez legal o que requieran de una autorización. El sistema Dsigner permitirá la firma electrónica avanzada en documentos que hayan sido convertidos en formato PDF.

A continuación, se encuentran los usos de cada tipo de certificado de firma electrónica avanzada:

- Persona Individual: Identifica legalmente a una persona natural (Ej: Carlos Pérez).
- Persona Profesional titulado: Identifica legalmente a un titular con título profesional y su colegiado activo. (EJ: Arquitecto Carlos Pérez).
- Persona en Relación con la entidad: Identifica legalmente a un titular que es colaborador activo de una institución privada. (EJ: Licenciado Carlos Pérez, Gerente General).
- Funcionario Público: Identifica legalmente a un titular en calidad de funcionario público de una institución gubernamental. (EJ: Ingeniero Carlos Pérez, ministro de Comunicaciones).
- Representante Legal: Identifica legalmente a un titular que posee un nombramiento como representante legal vigente, de una institución privada. (EJ: Arquitecto Carlos Pérez, Representante Legal de X Empresa).

- Persona Jurídica: Identifica legalmente a una institución privada que se encuentre activa y registrada por el registro mercantil en el territorio de Guatemala. (EJ: MiEmpresa, S.A.); o de una institución pública a efecto de firmar documentos electrónicos en los que se desea identificar a la empresa o institución que los firma.

5.3.4. Limitaciones y prohibiciones del uso de la firma electrónica avanzada

A continuación, se describen limitaciones del servicio y prohibiciones de uso de los certificados de firma electrónica avanzada provistos por DSIGNER, S.A.

Limitaciones del servicio:

- DSIGNER, S.A. no brinda o entrega ninguna llave privada de los certificados digitales emitidos por nuestra CA, así como ninguna tarjeta criptográfica o dispositivo USB de certificado digital.

- Las firmas electrónicas avanzadas, se utilizarán dentro del sistema electrónico de DSIGNER, S.A. (https://portal.dsigner.online).

- Los certificados de firma electrónica avanzada son únicamente legales dentro del territorio de Guatemala, DSIGNER, S.A. se encuentra autorizada por el Registro de Prestadores de Servicios de Certificación del Ministerio de Economía, dichas resolución de autorización puede ser validada en el sitio web; del Registro de prestadores de servicios de certificación, (https://www.rpsc.gob.gt/index.php/prestadores-autorizados/).

Prohibiciones del uso del certificado digital:

- Los certificados digitales de firma electrónica se emiten por tipo de necesidad y uso; Se encuentra prohibido utilizar un tipo de certificado (EJ: Personal Individual) para legalizar o firmar un documento electrónico como representante legal. Cada certificado digital de firma electrónica avanzada es exclusivo según su tipo y para su propio fin, así como también para la institución a la que pertenece si fuera el caso.

5.3.5. Obligaciones de los participantes en los servicios de Certificación

A continuación, se describen las obligaciones de las partes involucradas dentro de todo el sistema de DSIGNER, S.A.

Entidad autorizadora de certificación (CA) – DSIGNER, S.A.:

Es una entidad de confianza, responsable de emitir y revocar los certificados digitales, de firma electrónica avanzada, empleando la criptografía de clave pública. Jurídicamente, se trata de un caso particular de Prestador de Servicios de Certificación autorizado como raíz que posee la infraestructura tecnológica que se conoce como infraestructura de Clave pública PKI. GLOBALSIGN como proveedor de servicio de confianza internacional brinda los servicios de "Autoridad Certificadora", y nos permite generar certificados de firma electrónica avanzada a través de su infraestructura. Dicha CA es operada en su

totalidad por la entidad internacional GLOBALSIGN, su función es la generación de certificados digitales solicitados por nuestra entidad legal guatemalteca DSIGNER, S.A. Su obligación es proveer los servicios de CA para toda la cadena de confianza y certificados digitales emitidos por DSIGNER, S.A.

Entidad autorizadora de registro (RA) - DSIGNER, S.A.:

Entidad jurídica guatemalteca, que brinda los servicios de generación y emisión de certificados de firma electrónica avanzada dentro del territorio de Guatemala. Dicha entidad tiene la obligación de validar las identidades de todos los titulares que se presenten por el servicio de certificación de una firma electrónica avanzada.

Titulares de un certificado digital de firma electrónica avanzada en calidad de: (Persona individual/ Profesional titulado/ Representante legal/ funcionario público/ Relación con la entidad y Persona jurídica):

Persona o suscriptor autorizado, tras la validación de su identidad, para la adquisición de su certificado digital de firma electrónica avanzada, a través de la obtención de su suscripción y enrolamiento en el sistema Dsigner, es responsabilidad y obligación del titular de dichas firmas electrónicas, la correcta gestión de sus accesos al sistema, para utilizar su certificado digital de firma electrónica avanzada, con el fin de certificar y validar su documentación electrónica firmada por el mismo. Es responsabilidad del titular, el resguardo de sus contraseñas de acceso, pin y códigos enviados por SMS. Adicionalmente, se hace saber que queda bajo la responsabilidad del titular, la notificación de la renovación, anulación o revocación de su certificado de firma electrónica avanzada.

DSIGNER, S.A. proveerá todos los canales electrónicos necesarios en el horario de 24 horas al día, los 7 días de la semana, para el soporte técnico, de cualquier requerimiento que surja; de un titular, dicha información puede consultarse en (https://www.disgner.online). Adicionalmente DSIGNER, S.A. cuenta con una póliza activa de responsabilidad civil por cualquier agravio identificado como responsabilidad de DSIGNER, S.A. en la región de Guatemala.

5.3.6. Políticas de privacidad y protección de datos

DSIGNER S.A. establece los más altos niveles de confidencialidad y protección de datos, los cuales se someten anualmente a una revisión de controles cibernéticos por medio de su certificación ISO 27001:2013.

DSIGNER S.A. no divulgará, comercializará, ni venderá los datos personales de los solicitantes o suscriptores de los certificados u otra información de identificación acerca de ellos de conformidad con las cláusulas de confidencialidad de los contratos con sus titulares, así como por las regulaciones pertinentes dentro de la región de Guatemala.

DSIGNER S.A. ha establecido una política de privacidad para la gestión de certificados de firma electrónica avanzada, así como la gestión de información confidencial.

5.3.7. Circunstancias de generación, renovación y revocación del certificado

DSIGNER, S. A. cuenta con el control necesario para la Revocación de los Certificados Digitales de firma electrónica avanzada; que se revoquen al finalizar el tiempo de vigencia; por lo que Dsigner comunicará con la antelación suficiente al usuario o suscriptor o solicitante, a fin de que el mismo cuente con dicha información, para realizar el proceso necesario a efecto de continuar o no con el servicio de firma electrónica, de continuar con el servicio se procederá a una Renovación del certificado digital a través de la realización, de una nueva solicitud, donde deberá presentar la información requerida de acuerdo al tipo de Certificado Digital y Firma electrónica avanzada que solicite.

DSIGNER, S.A. establece los siguientes lineamientos en base al correcto uso de su sistema y gestión de certificados de firma electrónica avanzada:

- DSIGNER, S.A. podrá emitir un certificado electrónico de firma electrónica avanzada una vez, el titular solicitante cumpla con todos los requerimientos necesarios para que dicho certificado sea concedido. Estos requerimientos podrán ser digitales o físicos dependiendo del requerimiento o caso.

- DSIGNER, S.A. podrá cancelar la solicitud, así como revocar o no generar un certificado de firma electrónica avanzada, cuando existan indicios de fraude o falsedad de identidad y no esté sujeto a brindar resultados, opiniones ni descripciones de la decisión, en tal caso DSIGNER, S.A. se reserva el derecho de admisión y gestión de certificados de cualquier titular.

- DSIGNER, S.A. proveerá los canales electrónicos necesarios para que cualquier titular las 24 horas al día los 7 días de la semana, pueda solicitar su renovación o revocación de su firma avanzada de manera automática dentro del portal (https://portal.dsigner.online).

- DSIGNER, S.A. y sus Operadores PKI, podrán realizar una llamada telefónica cuando el titular a revocado su certificado a efecto de comprobar que efectivamente sea una revocación o bien se haya solicitado la misma por error involuntario.

5.3.8. Vigencia de la política de certificación

La presente política de certificación; entra en vigor desde el inicio de operaciones de DSIGNER, S.A. y su resolución aprobada por el Registro de Prestadores de Servicios de Certificación del Ministerio de Economía.

Dicha política está sujeta a una revisión anual y puede actualizarse periódicamente en base a cambios en los requerimientos técnicos, regulatorios o de procesos que surjan en el servicio o leyes aplicables.

6. Historial de Modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
13/06/2023	1.0	Coordinador Dsigner	Primera Versión
22/02/2024	1.1	Coordinador Dsigner	Se realizo actualización anual, se cambio formato y modificaron los requisitos para solicitud de certificados
18/02/2025	1.2	Oficial de seguridad	Se realizo actualización, se cambió formato.