7ma. avenida 5-45 zona 4 edificio XPO1
nivel 9, Guatemala, Guatemala
info@dsigner.online
+(502) 2424 9280

Declaración de prácticas de certificación (CPS)

DSIGNER, S.A.

Código	DE-PRAC-CPS-01
Versión	01
Fecha de la versión	28-09-2021

7ma. avenida 5-45 zona 4 edificio XPO1
nivel 9, Guatemala, Guatemala
info@dsigner.online
+(502) 2424 9280

Contenido

7ma. avenida 5-45 zona 4 edificio XPO1
nivel 9, Guatemala, Guatemala
info@dsigner.online
+(502) 2424 9280

7ma. avenida 5-45 zona 4 edificio XPO1
nivel 9, Guatemala, Guatemala
info@dsigner.online
+(502) 2424 9280

1. Introducción

La presente declaración de prácticas de certificación -CPS- está relacionada a la infraestructura de clave pública PKI por sus siglas en inglés (Public Key Infraestructure) y que comprende todos aquellos servicios que están relacionados a los certificados digitales de firma electrónica avanzada que DSIGNER S.A. gestione para sus usuarios, suscriptores y titulares.

Este documento describe los procedimientos bajo los cuales se emite un certificado digital de firma electrónica avanzada a cualquier titular que genere una solicitud dentro del sistema.

Adicionalmente aborda las prácticas técnicas, de los procesos y procedimientos, así como el ciclo de vida en la emisión de los diferentes tipos de certificados de firma electrónica avanzada y su operatividad dentro del alcance de las actividades de acuerdo con su AC Raíz (Autoridad de Certificación Raíz).

Para todos los titulares, este documento será vinculante y efectivo al aceptar un acuerdo de suscriptor o términos de uso. Para las partes que confían, esta –CPS– es vinculante al basarse en un certificado emitido bajo esta –CPS– y los suscriptores están obligados por el acuerdo de suscriptores a informar a las partes que confían que la –CPS– es en sí misma vinculante para las partes que confían.

Los titulares o suscriptores de certificados de la infraestructura PKI de DSIGNER S.A. deberán de entender de qué manera están identificados y autenticados sus datos y la necesidad de sus documentos acreditativos, así como sus obligaciones al respecto del resguardo de su información.

Los certificados de DSIGNER S.A. pueden utilizarse únicamente para firmar documentos electrónicos reemplazando las firmas manuscritas.

El propósito de este documento es presentar las prácticas y procedimientos utilizados por DSIGNER S.A. en la gestión de los certificados digitales para firma electrónica avanzada a fin de demostrar el cumplimiento ante cualquier entidad regulatoria o entidad con necesidad de conocer.

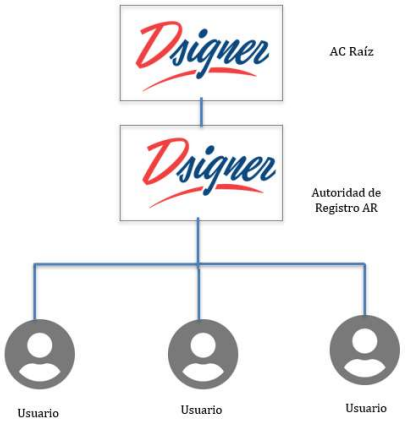
7ma. avenida 5-45 zona 4 edificio XPO1
nivel 9, Guatemala, Guatemala
info@dsigner.online
+(502) 2424 9280

2. Consideraciones Generales

A continuación, se describen las consideraciones generales que aplican a todos los servicios, procesos, sistemas tecnológicos y participantes dentro del entorno de DSIGNER, S.A.

2.1 Partes involucradas

A continuación, se encuentra un diagrama macro de todo el contexto y partes interesadas del sistema DSIGNER, S.A.



2.1.1 Autoridad certificadora raíz (CA)

Dsigner fungirá como Autoridad Certificadora Raíz, siendo responsable de la gestión de todos los certificados dentro del PKI de GlobalSign administrada por Dsigner.

Dsigner tiene el control final sobre el ciclo de vida y la gestión de Dsigner CA raíz y cualquier CA emisora subordinada posterior, Dsigner asegura la disponibilidad y seguridad de todos los servicios relacionados con la gestión de certificados, que incluyen, entre otros, la emisión, la revocación y el estado de verificación de un certificado, dichas políticas pueden revisarse bajo el sitio web de Dsigner (https://www.dsigner.online).

Dsigner utiliza el nombre de la raíz como propietario, este esta definido como “Autoridad Certificadora raíz – DSIGNER, S.A.”

2.1.2 Autoridad de registro (RA)

DSIGNER S.A. es una autoridad de certificación subordinada con su respectiva autoridad de registro que depende de la infraestructura de clave pública PKI de su autoridad de certificación raíz y emite certificados de acuerdo cona los procedimientos establecidos en este documento y regida por su política de certificación – CP DSIGNER.S.A.

Como autoridad de certificación subordinada y de registro, DSIGNER S.A. realiza todas las funciones relacionadas con la gestión del ciclo de vida de los certificados siendo este la emisión, renovación, distribución y revocación de certificados.

DSIGNER S.A. También proporciona información sobre el estado del certificado mediante un repositorio en forma de un punto de distribución de lista de revocación de certificados (CRL); Así mismo tiene un respondedor de protocolo de estado de certificado (OCSP).

2.1.3 Suscriptor (Titular)

Los suscriptores o titulares son entidades legales o personas físicas que solicitan y reciben un certificado de firma electrónica avanzada para sustentar su uso en el portal del servicio de DSIGNER, S.A.

Un suscriptor o titular, como se usa en este documento, se refiere tanto al sujeto del certificado como a la entidad que ha contratado a DISGNER S.A.

Para todas las categorías de suscriptores, se requiere información por tipo de certificado para la verificación y emisión de cada certificado.

2.1.4 Partes Interesadas

Para verificar la validez de un certificado, las partes interesadas pueden utilizar el portal en línea de DSIGNER, S.A. (https://portal.dsigner.online) para validar si ese documento electrónico es válido y emitido por un titular vigente.

Adicionalmente pueden consultar la revocación de información en forma de un punto de distribución CRL o un respondedor OCSP, como también consultar la vigencia de un certificado dentro “Consulta de Certificados” dentro del portal web (https://www.dsigner.online).

Los destinatarios de cualquier documento que deseen validar de manera fuera de línea los documentos firmados por DSIGNER, S.A. pueden descargar los certificados RAIZ(CA) e Intermediario (RA) para su instalación en sitio y así poder validar los documentos dentro de su ordenador.

2.2 Obligaciones

A continuación, se encuentran las obligaciones por participante.

2.2.1 Autoridad certificadora raíz (CA)

- Proveer el servicio de CA raíz velando la confidencialidad, integridad y disponibilidad del servicio.
- Proveer interfaces seguras para la solicitud de certificados digitales.
- Proveer todos los controles requeridos en el ámbito regulatorio.

2.2.2 Autoridad de registro (RA)

- Proveer el servicio de RA velando la confidencialidad, integridad y disponibilidad del servicio.
- Proveer todos los controles requeridos en el ámbito regulatorio.
- Proveer los servicios necesarios para el ciclo de vida de los certificados digitales de firma electrónica avanzada para los suscriptores del sistema en Guatemala.
- Proveer los controles necesarios para la correcta verificación de datos y emisión de firmas electrónicas avanzadas.
- Proveer los sistemas y canales electrónicos para el uso de la firma electrónica avanzada.

2.2.3 Suscriptor (Titular)

- Proveer la información legal, verdadera y fehaciente necesaria para la validación correcta de su certificado de firma electrónica avanzada.

2.2.4 Partes Interesadas

- Utilizar únicamente los medios y canales electrónicos provistos por Dsigner para la validación de los documentos firmados electrónicamente dentro del sistema y plataforma Dsigner.

2.3 Responsabilidades

A continuación, se encuentran las responsabilidades por participante.

2.3.1 Autoridad certificadora raíz (CA)

- Debe brindar confidencialidad, integridad y disponibilidad del servicio de CA.
- Debe brindar confidencialidad, integridad y disponibilidad del servicio en el almacenamiento de llaves privadas.
- Debe brindar todas las evidencias de la correcta gestión de controles a los reguladores del sistema.

2.3.2 Autoridad de registro (RA)

- Debe brindar confidencialidad, integridad y disponibilidad del servicio de RA.
- Debe validar de manera exhaustiva mediante todas las practicas detalladas la veracidad de la información provista en la solicitud de certificados de firma electrónica avanzada.
- Debe brindar todas las evidencias de la correcta gestión de controles a la Entidad Autorizadora.
- Debe mantener activas las certificaciones ISO9001, ISO27001 y la póliza de responsabilidad civil.
- Debe brindar todos los canales electrónicos necesarios para que cualquier suscriptor pueda solicitar una gestión de soporte.

2.3.3 Suscriptor (Titular)

- Debe mantener su información confidencial (Contraseñas, PIN, Usuario, Token) en estricta confidencialidad.
- Debe firmar únicamente documentos que él tenga pleno conocimiento consciente de plasmar su firma electrónica avanzada.

2.3.4 Partes Interesadas

- Debe revisar que los documentos entregados por suscriptores se encuentren vigentes y hayan sido firmados por una firma electrónica avanzada autorizada por un prestador de servicios de certificación autorizado por el RPSC.

2.4 Cumplimiento y Auditoria

Las prácticas que se indican en estas –CPS– tienen el propósito de cumplir o superar los requisitos de las normas nacionales e internacionales generalmente aceptadas y en desarrollo, incluyendo el sistema ISO 27001 así como la legislación nacional vigente y documentos técnicos emitidos por el RPSC (Registro de Prestadores de Servicios de Certificación).

En base a los controles establecidos por DSIGNER, S.A. se generan las siguientes auditorias dentro del sistema:

- Prueba de intrusión anual a todos los sistemas públicos con cara a Internet.
- Revisión anual por el ente certificador de ISO27001 como auditoria de seguimiento.
- Revisión anual por el ente certificador de ISO9001 como auditoria de seguimiento.
- Revisión anual por el ente regulador(RPSC) como auditoria de seguimiento.
- Escaneo de vulnerabilidades mensual en busca de vulnerabilidades tecnológicas.
- Revisión anual por un tercero verificando los procesos y procedimientos operativos en base al cumplimiento de estándares ISO.

2.5 Confidencialidad y Propiedad Intelectual

Las políticas de confidencialidad de DSIGNER, S.A. se encuentran definidas dentro de la política de privacidad y protección de datos.

DSIGNER, S.A. tiene la propiedad intelectual de todos sus sistemas utilizados dentro del contexto de firma electrónica avanzada, siendo estos:

- https://www.dsigner.online
- https://portal.dsigner.online
- SmartVerify (Sistema Interno).

Los titulares o suscriptores son propietarios de toda documentación utilizada dentro de sus perfiles, estos son custodios y responsables de sus propios documentos, así como de sus credenciales de acceso y firma.

3. Identificación y Autenticación

A continuación, se describe el procedimiento de identificación y autenticación de suscriptores y/o titulares de una firma electrónica avanzada.

Toda gestión, acceso, solicitud se centraliza dentro del portal del servicio: (https://portal.dsigner.online).

Para el uso del sistema, el usuario debe ingresar al sitio del servicio y generar su usuario electrónico, completando la información solicitada en el apartado "**Crear una cuenta**".

Al terminar su registro este podrá ingresar al sistema utilizando su correo electrónico y la contraseña definida en la creación de su cuenta. Si el usuario olvida su contraseña, este podrá ingresar al índice del portal y solicitar recuperar su contraseña en el apartado "**Recuperar Contraseña**". Esta opción le brindará una contraseña temporal a su correo electrónico registrado en donde al ingresar le pedirá cambiar su contraseña temporal por una definitiva.

Una vez creado el usuario, este podría utilizar nuestro sistema de manera gratuita para firma y cargar documentos con la "**firma simple**" brindada por DSIGNER, S.A. Dicha firma carece de legalidad y no puede presentarse como firma legal ante documentos que requieran algún tipo de validez legal.

Si el usuario desea adquirir una "**Firma Electrónica Avanzada**" con validez legal, este podrá ir dentro de su perfil y cambiar la suscripción a:

- Plan Personal; plan básico de firma electrónica avanzada de persona natural.
- Plan Profesional; plan para firma electrónica de profesionales titulados, con beneficios adicionales.
- Plan PYME; plan para pequeñas y medianas empresas para utilizar la plataforma y programa Dsigner dentro de sus organizaciones con beneficios de firma electrónica avanzada para sus colaboradores, empleados y representantes.

Al seleccionar la suscripción requerida, este adquirirá la suscripción deseada y se le habilitará la opción de "**Solicitar Firma Avanzada**" el cual iniciará el proceso de "**Verificación Digital**" definido dentro de la guía de verificación digital de identidad que se encuentra en la sección de Tutoriales del programa Dsigner.

Dentro del proceso de verificación digital de identidad el titular se identificará y de ser aprobada su solicitud, aceptará el contrato de "términos y condiciones de uso" y finalmente tendrá que generar su "**PIN Secreto**" el cual únicamente el titular tiene conocimiento. Este será requerido cada vez que el titular desee firmar un documento con su certificado de firma avanzada.

Este "**PIN Secreto**" puede cambiarse dentro del sistema, si este pierde dicha información, el certificado de firma avanzada no podrá utilizarse y deberá solicitarlo nuevamente.

3.1 Proceso de autenticación al sistema

El titular o usuario registrado deberá colocar su usuario (correo electrónico) y su contraseña de acceso dentro del portal oficial.

Si el titular o usuario no recuerda su contraseña, este puede solicitar "**Restaurar su Contraseña**" dentro del inicio del portal. Esta estará llegando a su correo asignado.

3.2 Proceso de revocación y renovación de firma avanzada

Este proceso aplica a cualquiera de las siguientes acciones:

- Revocación: Invalidar el certificado electrónico de firma avanzada.
- Renovación: Renovar el certificado electrónico de firma avanzada.

Todos los certificados emitidos por DSIGNER, S.A. cuentan con una validez de 365 días, las 24 horas al día.

El titular o suscriptor podrá **revocar** su certificado electrónico dentro del portal electrónico ingresando al sistema, navegando hacia su perfil en el apartado "certificado electrónico" seleccionar el certificado que desea revocar y seleccionar en la acción requerida. Dicha acción le solicitará un motivo de su revocación, así como una confirmación que esta acción no puede deshacerse por lo cual perderá su certificado de firma electrónica avanzada.

El titular o suscriptor podrá **renovar** su certificado electrónico dentro del portal electrónico ingresando al sistema, navegando hacia su perfil y luego en el apartado "certificado electrónico" seleccionar el certificado que desea renovar y darle clic en la acción requerida. Dicha acción le enviara a la página de suscripciones, pago y nuevamente le habilitara la opción de "Solicitar Firma Electrónica Avanzada" para que inicie el proceso nuevamente de verificación digital.

3.3 Proceso de verificación digital de identidad

El titular o suscriptor una vez adquirida su suscripción, este deberá iniciar su proceso de verificación digital de identidad. Dicho proceso se encuentra debidamente documentado dentro de la "**Guía de verificación digital de identidad**".

La guía de verificación digital de identidad se encuentra en el apartado de Tutoriales de la plataforma de Dsigner, la misma se encuentra en concordancia a los requerimientos del RPSC (Registro de Presentación de Servicios de certificación) del Ministerio de Economía en Guatemala.

Dicho sistema permite la verificación digital de la identidad del titular y solicita todos los requerimientos necesarios por tipo de certificado que el titular desea poseer.

Si hubiese alguna incongruencia con la documentación solicitada, el personal de validación de DSIGNER, S.A. podrá solicitar pruebas de vida, documentación o una entrevista con el suscriptor, por medio de videoconferencia con el titular, una entrevista física en las Instalaciones de Dsigner o por el medio que se indique al suscriptor.

3.4 Proceso de soporte técnico telefónico, chat u correo electrónico.

Si el titular o suscriptor desea un apoyo o gestión específica, podrá comunicarse por medio de los canales electrónicos siguientes:

- Llamada al PBX de DSIGNER, S.A.
- Chat oficial de WhatsApp Business de DSIGNER, S.A.
- Correo electrónico a soporte@dsigner.online.

DSIGNER, S.A. no puede brindar información de ningún usuario y/o certificado de firma electrónica avanzada por medio de los anteriores canales electrónicos.

DSIGNER, S.A. únicamente guiara al titular o suscriptor a la acción para que reinicie su contraseña para que pueda ingresar al sistema. Si dicho suscriptor no posee acceso al correo registrado previamente, DSIGNER, S.A. no podrá modificar dicho usuario y únicamente podrá la realizar la acción de "**Suspensión de Usuario**" el cual invalida el acceso a la plataforma y al certificado digital correspondiente.

3.5 Proceso de suspensión o eliminación de usuario.

Este proceso aplica a cualquiera de las siguientes acciones:

- Suspensión: suspende el usuario electrónico para que este no pueda realizar ninguna acción dentro del sistema.

- Eliminación: elimina completamente el perfil del usuario dentro del sistema, no existe forma de recuperar la información de un usuario que haya sido eliminado. Esta acción también revoca un certificado de firma electrónica avanzada si se encontraba vigente.

DSIGNER, S.A. podrá suspender o eliminar usuarios que encuentre dentro del sistema que hayan sido identificados como fraudulentos o no respeten las políticas de uso del sistema.

DSIGNER, S.A. únicamente podrá suspender o activar un usuario electrónico si este es validado de manera digital contrarrestando toda la información que se encuentre en el perfil del usuario. El operador de PKI debe validar cada dato dentro del perfil y si esta es comprobada se emite la acción de suspensión o activación.

DSIGNER, S.A. no modificará ni actualizará los datos del perfil del usuario bajo ninguna circunstancia.

DSIGNER, S.A. podrá eliminar la información de un usuario cuando haya recibido una declaración jurada de la solicitud de eliminación de datos debidamente autenticada por un notario en Guatemala en su dirección oficial física. La eliminación de información de usuario no puede solicitarse de manera digital, sino que se deberá tener la declaración jurada del solicitante, validando previamente su información de registro.

4. Requerimientos Operacionales

DSIGNER, S.A. pone a disposición los siguientes procedimientos operacionales en donde se definen las actividades desarrolladas en el ciclo de vida de los certificados de firma avanzada, así como mejores prácticas de operación.

4.1 Proceso de solicitud, emisión, revocación y renovación de certificados

Dichos procesos y su detalle se encuentran definidos en el inciso #3 "identificación y Autenticación" de este -CPS-.

DSIGNER, S.A. utiliza un sistema centralizado gestionado en su totalidad por el suscriptor o titular, ingresando al sistema el titular puede realizar lo necesario para la solicitud, emisión, revocación y renovación de su firma avanzada. Dentro de dichas actividades, se encuentran las siguientes:

- Creación de cuenta de usuario.
- Adquisición de certificado de firma avanzada.
- Solicitud para la verificación digital de su firma avanzada.
- Firma de documentos electrónicos.
- Cambio de su "Pin Secreto" utilizado para firmar.
- Revocación de su firma avanzada.
- Renovación de su firma avanzada.

Dentro del sistema se encuentran los tutoriales técnicos que le permiten realizar cada actividad dentro del sistema.

DSIGNER, S.A. cuenta con un operador PKI únicamente para la validación digital en la emisión del certificado de firma avanzada, así como la suspensión o activación del usuario previamente identificado.

DSIGNER, S.A. no puede modificar, eliminar, editar, reemplazar ninguna información de un usuario o suscriptor. Dicha información únicamente la puede cambiar el usuario dentro de su perfil dentro del sistema tecnológico provisto.

4.2 Proceso de Auditoría de Seguridad

DSIGNER, S.A. y todos los sistemas que lo conforman fueron creados desde un inicio con los más altos estándares de ciberseguridad, así como la aplicación de controles de seguridad de la información.

A continuación, se establece un calendario de actividades de auditoria con su periodicidad, los cuales fueron descritos en el apartado 2.4 de Cumplimiento y Auditoría, la calendarización se realizará durante la planificación anual de actividades de Dsigner.

Auditoria	Periodicidad
Prueba de intrusión interna y externa.	1 vez / Anual.
Revisión por ente certificador ISO27001.	1 vez / Anual.
Revisión por ente certificador ISO9001.	1 vez / Anual.
Revisión por ente regulador del RPSC.	1 vez / Anual.
Escaneo de vulnerabilidades interno y externo.	4 veces / Trimestral.
Revisión por un tercero verificando los procesos y procedimientos operativos.	1 vez / Anual.

4.3 Almacenamiento de información confidencial o sensible.

DSIGNER, S.A. restringe la visualización y operación de la información dentro del perfil de usuario del suscriptor, así como sus documentos, firma electrónica y cualquier otro dato que este contenga dentro de su perfil.

DSIGNER, S.A. únicamente permite al operador PKI visualizar la información provista por el usuario en el formulario de la solicitud de firma avanzada. Dicha información es utilizada únicamente para fines de emisión del certificado de firma avanzada.

DSIGNER, S.A. utiliza estándares de ciberseguridad y de los más altos controles de seguridad para el acceso a sus sistemas, así como la gestión y almacenamiento de su información, dicha revisión de controles esta definida en el apartado 4.2 de este inciso.

5. Controles de procedimiento y procesos

A continuación, se describe los controles de procedimientos y procesos para la verificación de las funciones de todo el personal interno de DSIGNER, S.A.

5.1 Control de acceso físico

DISGNER, S.A. tiene sus oficinas centrales dentro de la región de Guatemala, en la dirección (7 avenida 5-45 Zona 4, edificio XPO1 nivel 6 oficina 603 en la ciudad de Guatemala.) En dicha ubicación se encuentra el personal de la compañía.

DISGNER, S.A. tiene implementada la identificación física de cada colaborador por medio de gafetes visuales los cuales son otorgados desde su ingreso. Estos identifican al colaborador verificando su puesto dentro de la compañía. Adicionalmente que estos deben de acceder mediante su huella biométrica para ingresar a las instalaciones físicas.

DISGNER, S.A. contiene todos sus sistemas electrónicos del sistema principal en la nube de Microsoft Azure, no existe ningún centro de datos en donde se almacene información de suscriptores y/o titulares.

DISGNER, S.A. se rige bajo las políticas de seguridad y los controles de acceso provistos por su casa matriz - DEVEL. Dicho contrato entre empresas define los servicios que DEVEL le brinda a DSIGNER.

DISGNER, S.A. restringe el acceso al sistema de SmartVerify, sistema utilizado por el operador PKI, el cual, únicamente puede ser utilizado dentro de las instalaciones físicas de la compañía.

5.2 Control de acceso lógico

Todo personal dentro de DSIGNER, S.A. contiene su usuario identificativo dentro del directorio activo de la compañía, dicho usuario le permite el uso de los servicios básicos del sistema, siendo estos:

- Acceso a su computador asignado.
- Acceso al correo electrónico.

DISGNER, S.A. establece la política de “Need-to-Know” la cual especifica que cada usuario únicamente tiene la autenticación y autorización de ver y utilizar los sistemas que su perfil amerita, sin tener mayor acceso a otros sistemas.

DSIGNER S.A. garantiza que todos los operadores y administradores, incluidos los agentes de verificación, actúan en la capacidad de un rol de confianza. Los roles de confianza son tales que no es posible crear ningún conflicto de intereses, y los roles se distribuyen de manera que ninguna persona pueda eludir la seguridad del sistema.

DSIGNER S.A ha identificado, de acuerdo con su política de seguridad, las siguientes funciones o roles con la condición de fiables:

- **Auditor Interno:** responsable del cumplimiento de los procedimientos operativos. Se trata de una persona externa al departamento de sistemas de información. Las tareas de Auditor interno son incompatibles en el tiempo con las tareas de certificación e incompatibles con Sistemas.
- **Administrador de Sistemas**: responsable del funcionamiento correcto del hardware y software soporte de la plataforma de certificación.
- **Operador PKI:** Persona responsable de aprobar las peticiones de certificación realizadas por el suscriptor y de la emisión de certificados digitales.
- **Responsable de Seguridad:** Encargado de coordinar, controlar y hacer cumplir las medidas de seguridad definidas por las políticas de seguridad. Debe encargarse de los aspectos relacionados con la seguridad de la información: lógica, física, redes, organizativa, etc. Las personas que ocupan los puestos anteriores se encuentran sometidas a procedimientos de investigación y control específicos.
- **Desarrollador:** responsable del desarrollo de sistemas.
- **Oficial de seguridad / jefe de seguridad de la información:** Responsabilidad general de administrar la implementación de las prácticas de seguridad de la RA.

DISGNER, S.A. contiene controles de “PAM”, registro de acceso privilegiado para todos los sistemas en producción los cuales contienen bitácoras, acceso único y resguardo de las contraseñas de todos los sistemas en producción.

5.3 Revisión y bitácoras de los sistemas

DISGNER, S.A. ha implementado bitácoras dentro de todos los sistemas de SmartVerify, sistema que recibe las solicitudes de suscriptores, así como del portal web, en donde se identifican y registran todas las acciones que cualquier usuario del sistema realiza.

DISGNER, S.A. de manera mensual con alta gerencia realizara un muestreo y verificación de controles de todas las solicitudes recibidas, así como la verificación del número de solicitudes rechazadas, emitidas, revocadas o renovadas.

DISGNER, S.A. de manera mensual con alta gerencia revisara bitácoras de errores, tickets de soporte y cualquier incidente que haya sucedido dentro de las plataformas tecnológicas en línea.

6. Controles de seguridad de la cadena de certificados

Dsigner, entidad de autoridad de certificación raíz, mantiene los estándares y controles de ciberseguridad más altos de la industria y esta protege el acceso a sus certificados privados con los controles de ciberseguridad mas rigurosos del mercado. Dicha definición de cambio de llaves, renovación de CA's y demás funcionalidades se encuentran acorde y en cumplimiento a los estándares Fips 140-2

Para poder utilizar los servicios de PKI, los servidores de DSIGNER, S.A. deben contar con listas de acceso por direcciones IP, así como credenciales de acceso (API KEY) para poder utilizar los servicios de certificación.

Para poder acceder a los servicios PKI, únicamente existe la forma de servicios web (Web Services) por lo cual se tiene centralizado únicamente el acceso por un canal electrónico debidamente asegurado y custodiado

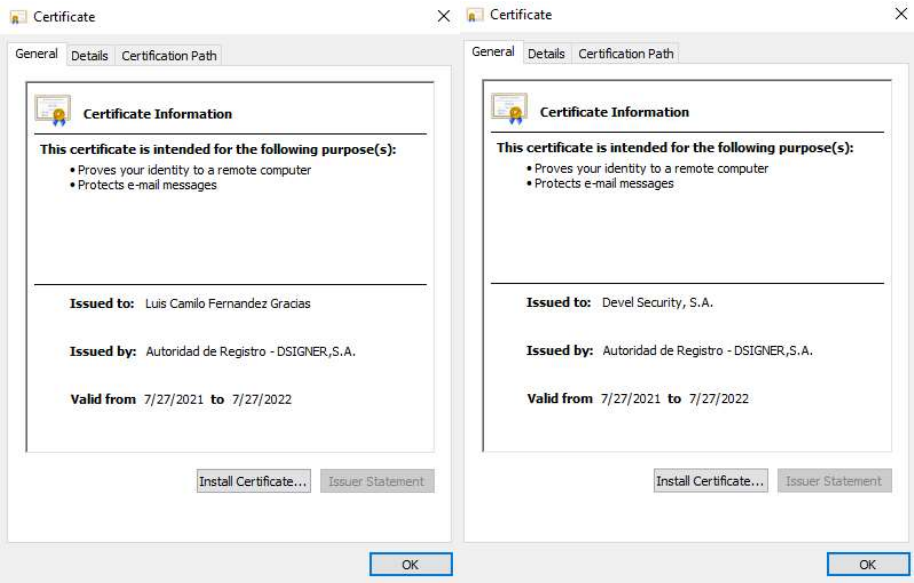
DSIGNER, S.A. no tiene acceso a su llave privada (RA), esta únicamente puede utilizarla para la emisión de certificado de firma electrónica avanzada.

7. Perfiles de certificados de firma avanzada

A continuación, se describe los diferentes tipos de firma avanzada que pueden ser provistos por DSIGNER, S.A. Dichos certificados son emitidos y utilizados dentro del sistema de DSIGNER, S.A.

Para la validación externa, fuera de línea de los documentos firmados por cualquier certificado de firma avanzada, ver el inciso 7.9 "Certificado intermediario y raíz".

Los requerimientos de cada perfil de certificado los pueden identificar dentro del portal informativo (https://www.dsigner.online/).



Ejemplos de certificados emitidos por DSIGNER, S.A.

7.1 Persona individual

Certificado que valida a una persona individual como firmante. (Ejemplo: Juan Pérez)

OU = Persona Individual C = GT L = Guatemala S = Ciudad de Guatemala PostalCode = 01010 STREET = 10 avenida 14-92 zona 10 E = cfernandez@develsecurity.com OU = FECHA_NACIMIENTO:19-06-83 OU = NIT:37262165 OU = DPI:2400037560101 CN = Luis Camilo Fernandez Gracias

7.2 Persona profesional

Certificado que valida que una persona es un profesional colegiado en su profesión como firmante. (Ejemplo: Lic. Juan Pérez)

OU = Profesional Colegiado C = GT L = Guatemala S = Ciudad de Guatemala PostalCode = 01010 STREET = 10 avenida 14-92 zona 10 E = cfernandez@develsecurity.com OU = TITULO:Ingeniero en Sistemas OU = COLEGIADO:18871 OU = PROFESION:Ingeniero OU = FECHA_NACIMIENTO:19-06-83 OU = NIT:37262165 OU = DPI:2400037560101

CN = Luis Camilo Fernandez Gracias

7.3 Persona en relación con entidad

Certificado que valida que una persona posee una relación actual contractual como colaborador de una empresa como firmante. (Ejemplo: Gerente de producto. Juan Pérez)

OU = Empleado Privado C = GT L = Guatemala S = Ciudad de Guatemala PostalCode = 01010 STREET = 10 avenida 14-92 zona 10 E = cfernandez@develsecurity.com OU = VIGENCIA_CARGO: Indefinida OU = DEPARTAMENTO: Administracion OU = CARGO: Gerente General OU = TELEFONO_ENTIDAD: 23075700 OU = DIRECCION_ENTIDAD: 12 avenida 1-2 zona 4 OU = ENTIDAD: Devel Security, S.A. OU = FECHA_NACIMIENTO:19-06-83 OU = NIT:37262165 OU = DPI:2400037560101 CN = Luis Camilo Fernandez Gracias

7.4 Funcionario público

Certificado que valida que una persona es colaborador activo de una institución de gobierno. (Ejemplo: Ministro. Juan Pérez)

OU = Funcionario Publico C = GT L = Guatemala S = Ciudad de Guatemala PostalCode = 01010 STREET = 10 avenida 14-92 zona 10 E = cfernandez@develsecurity.com OU = VIGENCIA_CARGO: 31-12-2025 OU = DEPENDENCIA: Administracion OU = CARGO: MINISTRO OU = TELEFONO_ENTIDAD: 23075700 OU = DIRECCION_ENTIDAD: 12 avenida 1-2 zona 4 OU = ENTIDAD: Ministerio de Relaciones Publicas OU = FECHA_NACIMIENTO:19-06-83 OU = NIT:37262165 OU = DPI:2400037560101 CN = Luis Camilo Fernandez Gracias

7.5 Representante legal

Certificado que valida que una persona es representante legal activo de una empresa como firmante. (Ejemplo: Representante Legal. Juan Pérez)

OU = Representante Legal C = GT L = Guatemala S = Ciudad de Guatemala PostalCode = 01010 STREET = 10 avenida 14-92 zona 10 E = cfernandez@develsecurity.com OU = VIGENCIA_REPRESENTACION: Indefinida OU = NUMERO_REPRESENTACION: 43902-2020 OU = PATENTE_EMPRESA: 879615-708-1094 OU = TELEFONO_EMPRESA: 23075700 OU = DIRECCION_EMPRESA: 7ave. 5-45 Zona 4 OU = NIT_EMPRESA: 7680854-8 OU = EMPRESA: Devel Security, S.A. OU = FECHA_NACIMIENTO:19-06-83 OU = NIT:37262165 OU = DPI:2400037560101 CN = Luis Camilo Fernandez Gracias

7.6 Persona jurídica

Certificado que valida a una empresa como firmante. (Ejemplo: Empresa, S.A.)

OU = Empresa C = GT L = Guatemala S = Ciudad de Guatemala PostalCode = 01004 STREET = 7 avenida 5-45 Zona 4, Edificio XPO1 - Nivel 9 E = info@develsecurity.com OU = NOMBRE_COMERCIAL: Devel OU = PATENTE_EMPRESA: 879615-708-1094 OU = TELEFONO_EMPRESA: 23075700 OU = NIT_EMPRESA: 7680854-8 OU = FECHA_CONSTITUCION:01-01-11 CN = Devel Security, S.A.

7.7 Consulta de certificados

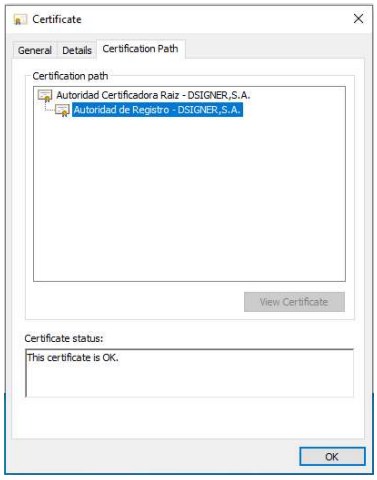
DSIGNER S, A. pone a disposición la "Consulta de certificados" la cual se encuentra dentro del portal informativo (https://www.dsigner.online) en donde cualquier persona puede consultar la validez de un certificado de firma avanzada por medio de la búsqueda del número serial del certificado.

7.8 Validación de documentos

DSIGNER S, A. pone a disposición la "Validación de Documentos" la cual se encuentra dentro del portal informativo (https://www.dsigner.online) en donde cualquier persona puede subir un documento digital y el validador le devolverá si este fue firmado por Dsigner que es Prestador de Servicios de Certificación autorizado por el RPSC, si la firma sigue vigente y si este fue firmado por el sistema de DSIGNER, S.A.

7.9 Cadena de confianza – Certificado intermediario y raíz

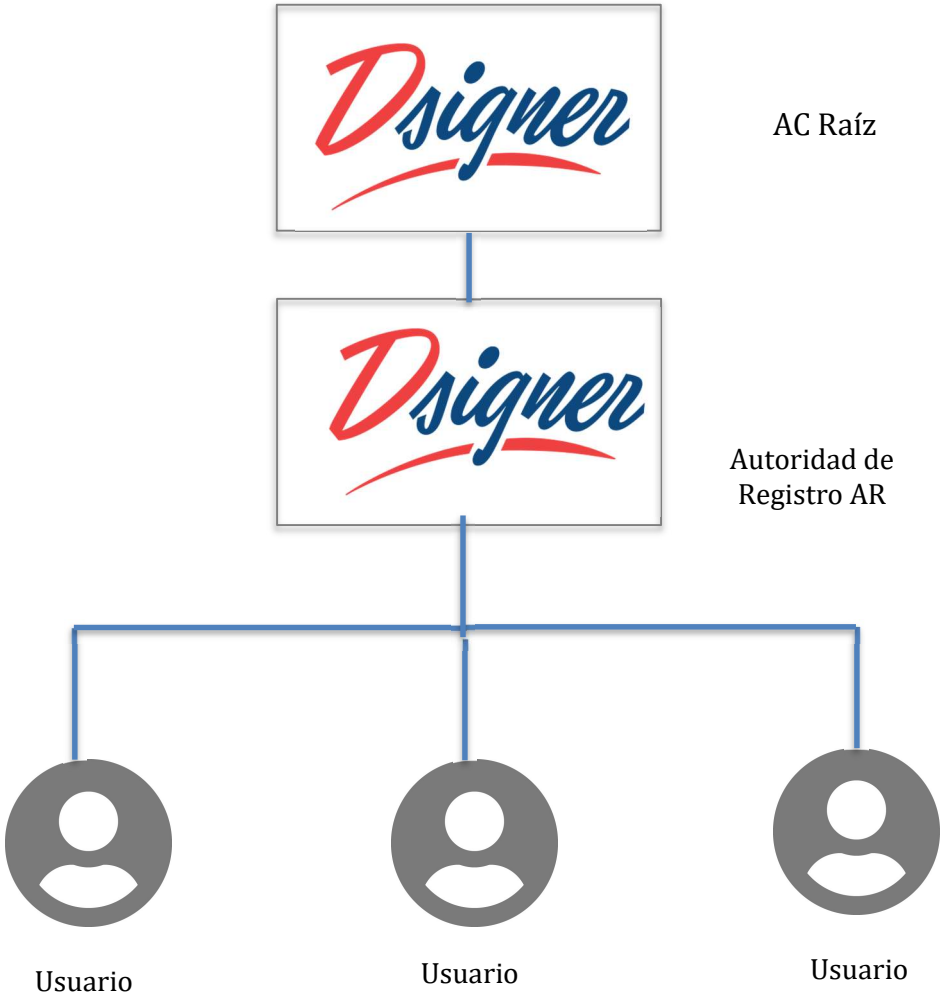
DSIGNER S, A. desglosa a continuación la cadena de confianza de sus certificados digitales de firma avanzada, en donde se encuentra especificada la cadena de confianza con la entidad de autoridad de certificación raíz y la autoridad de registro. Cada certificado emitido por DSIGNER, S.A. contendrá la siguiente cadena de confianza.



Ejemplo de cadena de confianza.

Si un usuario final o parte interesada desea validar los documentos emitidos por DSIGNER, S.A. este deberá de descargar los certificados intermedios y raíz (formato CRT) e instalarlos dentro de su computador, para esto puede consultar la "**Guía de instalación de certificados raíz**" dentro de la biblioteca del portal informativo (https://www.dsigner.online).

7.10 Modelo de Confianza, Autoridad de Certificación AC / Dsigner



Dsigner administra la estructura tecnológica PKI y funge como autoridad de certificación raíz, administrada por miembros del equipo de gestión de DSIGNER, S. A. con el soporte del equipo PKI correspondiente.

Dsigner, S. A. asegura la disponibilidad de los servicios relacionados a los Certificados Raíz administrados por Dsigner, que incluyen entre otros la emisión, revocación y renovación y el estado o verificación de un Certificado Digital.

Dsigner hace público el proceso y prácticas en la gestión de los certificados digitales con el fin de demostrar el cumplimiento de los requisitos relativos a la emisión y revocación como de la renovación de acuerdo con los requisitos establecidos y la normativa vigente.

8. Administración de la política de certificación

Las actualizaciones o cambios autorizados por el Registro de Prestadores de Servicios de Certificación del Ministerio de Economía a nuestra Política de Certificación será enviada por correo electrónico a todos los suscriptores o titulares que tengan vigente una firma electrónica avanzada con DSIGNER, S.A. Adicionalmente estas se encuentran publicadas dentro del portal informativo.

La política de certificación de DSIGNER, S.A. se encuentra respaldada y ejecutada mediante este documento de "Declaración de Practicas" en donde se especifican los lineamientos operaciones, técnicos y controles utilizados por el personal de la compañía para el correcto funcionamiento y operación del prestador de servicios de certificación que es DSIGNER, S.A.

La política de certificación y por consiguiente su declaración de prácticas es revisada de manera anual por la gerencia general de DSIGNER, S.A. identificando cualquier cambio o mejora necesaria y sometida al Registro de Prestadores de Servicios de Certificación del Ministerio de Economía de Guatemala.

9. Ciclo de vida de los certificados de firma electrónica avanzada

Los sistemas de DSIGNER S, A. no permiten la descarga de ningún certificado digital de firma avanzada, estos son utilizados dentro del propio sistema en línea que DSIGNER S, A. provee para todos sus suscriptores. (https://portal.dsigner.online).

DSIGNER, S.A. no provee ningún certificado de firma electrónica avanzada que pueda utilizarse de manera fuera de línea de su sistema central (Ej: Adobe Reader, Microsoft Office, etc.). No obstante, los documentos firmados con DSIGNER pueden ser validados por cualquier software de terceros.

DSIGNER, S.A. describe el funcionamiento y el ciclo de vida de sus certificados siendo esta la emisión, revocación, renovación de sus certificados en el apartado 4.1 de este documento.

DSIGNER, S.A. establece la expiración de cada certificado de firma avanzada emitido en un plazo de 365 días desde la emisión de este.

7ma. avenida 5-45 zona 4 edificio XPO1
nivel 9, Guatemala, Guatemala
info@dsigner.online
+(502) 2424 9280

10. Finalización de funciones como prestador de servicios de certificación

DSIGNER, S.A. establece que si por cualquier incidente, deba terminar las actividades de prestador de servicios de certificación, su impacto de la terminación de sus servicios deberá reducirse al mínimo posible.

Dsigner dará el aviso correspondiente al Registro de Prestadores de Servicios de Certificación del Ministerio de Economía de Guatemala previo a realizar cualquier notificación, anuncio o proceso relacionado.

Los procedimientos establecidos para dicho escenario son los siguientes:

- Comunicar la extinción mediante el envío de un correo electrónico dirigido a todos los suscriptores cuyos certificados digitales de firmas electrónicas avanzadas permanezcan en vigor y la publicación de un anuncio en dos diarios de amplia circulación nacional. La citada comunicación se llevará a cabo con una antelación mínima de dos meses al cese efectivo de la actividad.
- Procurar establecer, cuando ello fuera posible, acuerdos con terceras personas para transmitir todas sus obligaciones y derechos dentro del sistema de prestación de servicios de certificación, con la intención de continuar el servicio. Si se produce la subrogación, a la cual el suscriptor da su consentimiento de manera expresa, esta Declaración de Prácticas de Certificación seguirá siendo el documento que establece las relaciones entre las partes mientras no se establezca un nuevo documento por escrito.
- En caso de no haberse podido llevar a cabo transferencia de derechos y obligaciones a otra entidad, proceder a la revocación de todos los certificados digitales de firmas electrónicas avanzadas una vez transcurrido el plazo de dos meses desde la comunicación.
- Indemnizar adecuadamente a aquellos suscriptores que lo soliciten cuando sus firmas electrónicas sean revocadas con anterioridad al plazo previsto de vigencia, pactándose como tope para la indemnización el costo efectivo del servicio, descontando a prorrata el coste por los días transcurridos desde el inicio del contrato hasta la fecha de resolución.
- Cualquier otra obligación que establezca la legislación aplicable vigente y cualquier documento técnico emitido por el Registro de Prestadores de Servicios de Certificación del Ministerio de Economía de Guatemala.