Declaración de Prácticas de certificación

Código:	SIG-RE-020
Versión:	2.1
Fecha de Versión:	15 de Julio, 2024
Nivel de Confidencialidad:	Público

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
06l de junio de 2023	2	Oficial de Seguridad de la Información	Creación de documento
15 de julio 2024	2.1	Gestor de Calidad	Revisión anual sin cambio alguno

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

El presente documento constituye una manifestación y declaración expresa de CYBERSIGN, Sociedad Anónima (en adelante CYBERSIGN) sobre sus prácticas de certificación, las cuales son objetivas y no discriminatorias y las cuales oportunamente serán comunicadas a sus usuarios de manera sencilla y en idioma español.

Mediante el presente documento se da cumplimiento a los requisitos establecidos en la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas (Decreto 47-2008) y su Reglamento, respecto a la declaración de prácticas de certificación.

En este sentido, como primer punto, CYBERSIGN declara cumplir con los requisitos señalados en el artículo 23 del Reglamento de la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas (Acuerdo 135-2009), en el sentido que cumple con los siguientes requisitos:

a) Demostrar la Habilidad necesaria de sus servicios;
b) Garantizar la existencia de un servicio seguro de consulta del registro de certificados emitidos;
c) Emplear personal calificado para la prestación de los servicios ofrecidos y los procedimientos de seguridad y de gestión adecuados;
d) Utilizar sistemas y productos confiables que garanticen la seguridad de sus procesos de certificación;
e) Contar con la capacidad tecnológica necesaria para el desarrollo de la actividad de certificación; y,
f) Cumplir con todas las regulaciones emitidas por el Registro de Prestadores de Servicios de Certificación.

1. INTRODUCCIÓN

Las prácticas de certificación serán llevadas a cabo por CYBERSIGN, S.A. (en adelante CYBERSIGN) conforme al tipo de usuario que resulte aplicables.

En este sentido, los tipos de usuario son:

a) Persona natural a título individual

2. CONSIDERACIONES GENERALES.

2.1. De las partes involucradas en la prestación de los servicios de certificación.

Las partes involucradas en los servicios de certificación son los siguientes:

a) Prestador de Servicios de Certificación: es la entidad que expide certificados y puede prestar otros servicios relacionados con las firmas electrónicas. El prestador de servicios tiene tanto las funciones de Autoridad Certificadora (CA) como las de Autoridad de Registro (RA), las cuales puede delegar en terceros siempre y cuando se garantice que cumpla con lo establecido en este documento. La CA es la encargada de gestionar las solicitudes y emitir, renovar, revocar y suspender los certificados que emite. La RA es encargada de recibir las solicitudes de certificados, validar la información, si así lo establece su relación con la CA, y trasladar una solicitud completa hacia la CA para su procesamiento.

b) Entidad autorizadora: es el Registro de Prestadores de Servicios de Certificación adscrito al Ministerio de Economía -RPSC

c) Suscriptor: son las entidades o personas que adquieren los certificados de firma electrónica avanzada, quienes a su vez obtienen una licencia de uso del certificado de firma electrónica para los fines que le convengan siempre y cuando no sean usos prohibidos por la regulación, estas CPS (Declaración de Prácticas de Certificación) o las CP (Políticas de Certificación) asociadas.

d) Firmante: es la persona que posee los datos de creación de la firma y que actúa en nombre propio o del suscriptor al que representa.

e) Tercero que confía: son personas y organizaciones que reciben archivos firmados con certificados de firma electrónica avanzada emitidas por CYBERSIGN. Dichas personas, tienen la obligación de verificar la validez y vigencia de los certificados antes de confiar en los mismos.

2.2. De las obligaciones, responsabilidades y cumplimiento de auditorías

CYBERSIGN se obliga a lo siguiente:

a) Emitir certificados conforme a lo solicitado o acordado con el firmante.

b) Implementar los sistemas de seguridad para garantizar la emisión y creación de firmas electrónicas avanzadas, la conservación y archivo de certificados y documentos en soporte de mensaje de datos.

c) Garantizar la protección, confidencialidad y debido uso de la información suministrada por el firmante.

d) Garantizar la prestación permanente del servicio de entidad de certificación.

e) Atender oportunamente las solicitudes y reclamaciones hechas por los firmantes.

f) Suministrar la información que le requieran las entidades administrativas competentes o judiciales en relación con las firmas electrónicas y certificados emitidos y en general sobre cualquier comunicación electrónica que se encuentre bajo su custodia y administración.
g) Permitir y facilitar la realización de las auditorías por parte del Registro de Prestadores de Servicios de Certificación.
h) Elaborar los reglamentos que definen las relaciones con el firmante y la forma de prestación del servicio.
i) Llevar un registro de los certificados.
a) Comprobar la identidad de los solicitantes y cualesquiera circunstancias pertinentes para la emisión de un certificado, en los términos establecidos por la ley, su reglamento y las regulaciones pertinentes
b) A no alterar, modificar o destruir los certificados que emita sin que medie resolución de la Entidad Autorizadora o de autoridad judicial competente
c) A permitir a la Entidad Autorizadora efectuar las auditorías a que se refiere la ley, su reglamento y las regulaciones pertinentes
d) A no revelar los datos de creación de firma electrónica que correspondan a su propio certificado.
e) A no difundir sin autorización la información que le ha sido confiada o cualquier otra conducta que vulnere la confidencialidad de la misma.

El SUSCRIPTOR se obliga a lo siguiente:

a) Proporcionar a CYBERSIGN información precisa, exacta y completa en sus solicitudes de certificado.
b) Proteger sus credenciales de acceso y uso de la clave privada de uso no autorizado, asegurando que se mantengan bajo su control exclusivo.
c) Notificar a CYBERSIGN cuando los datos incluidos en su certificado de firma electrónica avanzada sean incorrectos.
d) Notificar a CYBERSIGN cuando tenga sospecha o descubra que sus credenciales de acceso y/o uso su clave privada han sido comprometidas.
e) Solicitar la revocación de su certificado cuando las circunstancias descritas en la sección de revocación de certificados de estas CPS se cumplan.
f) Informar a los terceros que confían en archivos firmados con su certificado de las maneras de verificar la validez de dicha firma.
g) Utilizar el certificado y la clave privada de acuerdo a lo establecido en estas CPS, las CP asociadas y el contrato de suscriptor.
h) Notificar a CYBERSIGN cuando los datos incluidos en el certificado hayan sido objeto de cambio, debiendo realizar dicha notificación de manera inmediata o lo más pronto posible, bajo su responsabilidad.
i) Notificar a CYBERSIGN cuando se tenga conocimiento de cualquier situación que ponga en riesgo la confiabilidad del certificado.
j) Abstenerse de monitorear, alterar, realizar ingeniería inversa, o interferir en cualquier otra forma con la prestación del servicio de certificación por parte de CYBERSIGN.

k) Hacer uso de programas informáticos para descarga masiva de información del repositorio de información de CYBERSIGN.

El FIRMANTE se obliga a lo siguiente:

a) Contar la autorización debida por parte del SUSCRIPTOR al constar sus datos de identificación personal en el certificado.
b) Proteger sus credenciales de acceso y uso de la clave privada de uso no autorizado, asegurando que se mantengan bajo su control exclusivo.
c) Utilizar el certificado y la clave privada de acuerdo a lo establecido en estas CPS, las CP asociadas y el contrato de suscriptor.

El TERCERO QUE CONFÍA se obliga a lo siguiente:

a) Verificar la validez y vigencia de los certificados de firma electrónica en los que desea confiar antes de darlos por válidos, utilizando alguno de los medios descritos en estas CPS.
b) Revisar que el certificado en el que desea confiar, se utiliza dentro de los límites permitidos para su uso según estas CPS, las CP asociadas y la regulación aplicable.
c) Informar a CYBERSIGN y al SUSCRIPTOR cuando sospeche que un certificado esté siendo utilizado de manera irregular o sin autorización del SUSCRIPTOR.
d) Abstenerse de monitorear, alterar, realizar ingeniería inversa, o interferir en cualquier otra forma con la prestación del servicio de certificación por parte de CYBERSIGN.
e) Hacer uso de programas informáticos para descarga masiva de información del repositorio de información de CYBERSIGN.

2.3. De la confidencialidad

La Entidad Autorizadora, así como el personal que actúe bajo su dependencia o por cuenta de ella, de conformidad con la ley, deberá guardar la confidencialidad y custodia de los documentos y la información que le entreguen los prestadores de servicios de certificación autorizados o que hayan presentado solicitud para calificación y autorización.

El Prestador de Servicios de Certificación emplea los elementos técnicos disponibles para brindar seguridad y privacidad a la información aportada, y los usuarios tendrán derecho a que se les informe, previamente al inicio de la prestación del servicio, de las características generales de dichos elementos, debiéndose siempre cumplir con las Políticas de Privacidad y Protección de datos.

2.4. De los derechos de Propiedad Intelectual

CYBERSIGN manifiesta que se reserva el registro, derecho, uso y licenciamiento de todas las marcas, nombres comerciales, señales de publicidad, derechos de autor y o patentes registrados o no ante el Registro de Propiedad Intelectual. Lo anterior bajo el entendido que los suscriptores y/o firmantes sí están autorizados a hacer uso de los certificados y

llaves asociadas que les fueren asignadas, por lo que el uso o licenciamiento de cualquiera de éstos derechos o activos fuera de lo recién establecido, deberán ser debidamente autorizados por CYBERSIGN.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1. Proceso de la solicitud de certificado

CYBERSIGN mantiene procesos de identificación y autenticación del solicitante a través del correo electrónico, evidencias recogidas en el formulario de solicitud de certificado, tecnologías que verifican la identidad del solicitante por medio de audio/video en cumplimiento con lo establecido en la Guía de identificación virtual publicada por el RPSC y autenticación multifactor. La información proporcionada en el formulario de solicitud puede ser validada con bases de datos confiables tales como registros públicos del gobierno, o en entidades privadas cuando estas estén disponibles y se cuente con la autorización correspondiente.

3.2. Proceso de la suspensión de certificado

CYBERSIGN realizará el proceso de suspensión de certificado posterior a la identificación del solicitante por el correo electrónico y autenticación multifactor, para las solicitudes que se hagan llegar por medio del sitio web de CYBERSIGN.

3.3. Proceso de la revocación de certificado.

CYBERSIGN realizará el proceso de revocación del certificado posterior a determinar la razón de revocación del certificado, la identificación del solicitante mediante el correo electrónico y la autenticación multifactor, para las solicitudes que se hagan llegar por medio del sitio web de CYBERSIGN.
Los pasos a seguir se detallan en el Manual **SIG-RE-027**

4. REQUERIMIENTOS OPERACIONALES.

Los requerimientos operacionales para los procesos a continuación enumerados son los siguientes:

a) Solicitud de certificado
   La solicitud de certificado de usuario requiere del ingreso de información en el formulario de solicitud, presentación de un documento válido de identificación

b) Emisión de certificados
   La emisión de certificados requiere el uso de la plataforma de CYBERSIGN para poder realizar dicha solicitud, el administrador de usuarios para la autentificación de éstos a partir de credenciales, el uso de un método multifactor y la disponibilidad de las claves para emitir certificados.

c) Suspensión y revocación de certificados
La suspensión y revocación de certificados requiere el uso de la plataforma de CYBERSIGN y el uso de un método multifactor como autenticación.

d) Procesos de auditoría de seguridad,
El proceso de auditoría de seguridad requiere del personal designado como oficial de Seguridad para su realización.

e) Almacenamiento de información relevante,
El proceso de almacenamiento de información relevante requiere tener una bitácora de esta información y tener personal designado para filtrar y almacenar la información.

f) Cambio de datos de creación de firma electrónica,
El proceso de cambio de datos de creación de firma electrónica requiere realizar el proceso de revocación de certificado y emisión de uno nuevo con los nuevos datos.

g) Superación de situaciones críticas,
El proceso para la superación de situaciones críticas requiere poner en práctica el plan de incidencias y continuidad del negocio, y realizar una actualización al plan de análisis de riesgos.

h) Casos de fuerza mayor y caso fortuito,
El proceso para casos de fuerza mayor y caso fortuito requiere poner en práctica el plan de contingencia y respaldos (“backup”) y recuperación ante desastres, así como realizar una actualización al plan de análisis de riesgos.

i) Procedimiento de término del usuario del servicio de certificación
El procedimiento para el término del usuario del servicio de certificación requiere el uso de la plataforma de CYBERSIGN para poder realizar la solicitud de revocación de certificado, el administrador de usuarios para la autentificación de estos a partir de credenciales, el uso de un método multifactor y la disponibilidad de OCSP y CRL.

5. CONTROLES DE PROCEDIMIENTO PERSONAL Y FÍSICOS

CYBERSIGN dispone de controles de seguridad los cuales aseguran las funciones de:

a) Generación de datos de creación de firma electrónica: Se tiene un control basado en roles donde solamente los usuarios autorizados poseen un rol específico para poder monitorear y dar mantenimiento previo, posterior y durante la generación de datos de creación de firma electrónica. Este acceso se brinda por medio del uso de credenciales.

b) El centro de datos principal donde se encuentran los equipos criptográficos en los que se generan, almacenan y respaldan las claves de las CA y RA de CYBERSIGN cumplen con estándares reconocidos internacionalmente. Esto garantiza que los equipos cuentan con controles de acceso físico, protección frente a desastres naturales, soporte contra fallos en sistemas de apoyo (energía eléctrica, telecomunicaciones, etc), tratamiento de residuos, prevención y protección contra incendios. El sitio alterno cuenta con las mismas características que el sitio principal.
c) Los empleados de confianza que participan en el esquema de *M of N* cuentan con autenticación multifactor para dichos procedimientos.
d) Todo el personal de CYBERSIGN cuenta con la experiencia y/o ha sido capacitado para llevar a cabo las funciones que le han sido asignadas.
e) CYBERISGN garantiza que sus empleados de confianza no tienen conflictos de interés en las tareas relacionadas con el desarrollo de sus funciones, además se cuentan con procedimientos disciplinarios internos en caso de detectar un caso de este tipo.
f) CYBERSIGN solicita a cualquier candidato a ser un empleado de confianza la información que considere necesaria (referencias laborales, referencias personales, antecedentes penales, policiacos, constancias de estudios, etc) para garantizar cumple con lo establecido en los incisos anteriores.
g) CYBERSIGN cumple con capacitar de manera periódica a sus empleados para el desarrollo de sus funciones.
h) Auditoría y almacenamiento de información relevante
   El control del almacenamiento de información importante para su auditoría se llevará a cabo por personal designado por CYBERSIGN.

   Se cuenta con una persona designada como Oficial de Seguridad, el cual se encargará de llevar este control.

6. CONTROLES DE SEGURIDAD TÉCNICA

Controles de seguridad técnica para la autoridad de certificación raíz.
Las medidas de seguridad adoptadas por CYBERSIGN para proteger los datos de creación de su propia firma electrónica avanzada, se listan a continuación:

a) Uso de métodos de encriptación para manejo, transporte de datos y almacenamiento.
b) Aislamiento del servicio de generación de certificados de usuarios finales con respecto al sistema para administrar la CA.
c) Uso de plataforma web única para la solicitud y gestión de certificados para firmas electrónicas.
d) Las interacciones con la clave privada de CYBERSIGN se llevan a cabo en redes aisladas del resto de sistemas de producción.

e) Uso de *M of N* con un valor de M con mínimo de 3 personas para operaciones que requieran el uso de la clave privada de la CA de CYBERSIGN.
f) Los empleados de confianza que participan en el esquema de *M of N* cuentan con autenticación multifactor para dichos procedimientos.
g) El tamaño de las claves de la CA de CYBERSIGN es de 4096 bits, dichas claves son generadas y almacenadas en HSM que cumple con los estándares requeridos por la normativa aplicable.
h) Para las claves de autoridades de certificación intermedias, estas son de 4096 bits como mínimo y podrán aumentarse conforme la regulación lo requiera o CYBERSIGN lo decida.
i) CYBERSIGN mantiene copias de respaldo de su clave privada de acuerdo con los planes de recuperación de desastre. Estas copias de respaldo son accedidas únicamente por el personal autorizado cuando sea necesario, dicho personal consta del administrador del sistema PKI, el administrador de sistemas informáticos.
j) El acceso al sistema cuando se utiliza la clave privada se hace únicamente desde equipos designados por CYBERSIGN para este propósito y con los controles de seguridad apropiados para protegerlos contra códigos maliciosos.
k) Todo el desarrollo hecho por CYBERSIGN es tratado de acuerdo con las políticas internas de desarrollo seguro de sistemas.
l) CYBERSIGN cuenta con políticas y procedimientos para manejar los incidentes de seguridad de la información.

Controles de seguridad técnica para la autoridad de certificación intermedia.

a) Uso de métodos de encriptación para manejo y transporte de datos y almacenamiento.
b) Aislamiento del servicio de generación de certificados de usuarios finales con respecto al sistema para administrar la CA.
c) Uso de plataforma web única para la solicitud y gestión de certificados para firmas electrónicas.
d) Las interacciones con la clave privada de CYBERSIGN se llevan a cabo en redes aisladas del resto de sistemas de producción.
e) Uso de usuario y sistema automatizado para operaciones que requieran el uso de la clave privada de la CA de CYBERSIGN.
f) Los sistemas de autenticación del usuario automatizado utilizan credenciales de corta duración para mitigar el riesgo de filtración de dichas credenciales.
g) El tamaño de las claves de la CA de CYBERSIGN es de 4096 bits, dichas claves son generadas y almacenadas en HSM que cumple con los estándares requeridos por la normativa aplicable.
h) CYBERSIGN mantiene copias de respaldo de su clave privada de acuerdo con los planes de recuperación de desastre. Estas copias de respaldo son accedidas únicamente por el personal autorizado cuando sea necesario, dicho personal

consta del administrador del sistema PKI, el administrador de sistemas informáticos.

i) El acceso al sistema cuando se utiliza la clave privada se hace únicamente desde equipos designados por CYBERSIGN para este propósito y con los controles de seguridad apropiados para protegerlos contra códigos maliciosos.
j) Todo el desarrollo hecho por CYBERSIGN es tratado de acuerdo con las políticas internas de desarrollo seguro de sistemas.
k) CYBERSIGN cuenta con políticas y procedimientos para manejar los incidentes de seguridad de la información.

Controles de seguridad técnica para las llaves privadas de los suscriptores:

a) Las claves privadas de los clientes se almacenan dentro de la infraestructura de CYBERSIGN en el datacenter seguro, dichas llaves cuentan con restricciones para que no puedan ser extraídas hacia un sistema externo, dichos llaves son accesibles solamente desde la infraestructura segura de CYBERSIGN. Estas llaves cuentan con varias capas de cifrado. Siendo la primera cifrado del sistema de almacenamiento. Segundo, encriptación con AAD específico del cliente dueño de la llave. Tercero, cifrado con llave no extraíble dentro del HSM, en conjunto con vector único aleatorio específico por operación
b) Para autorizar el uso de la llave privada es necesario contar con la autenticación multifactor que está bajo el control exclusivo del cliente, no pudiendo Cybersign autorizar el uso de dicha llave.
c) Las llaves privadas solamente existen sin cifrado, dentro del HSM y una vez la operación de firma es completada, las llaves sin cifrar son eliminadas del HSM.
d) Para las claves de usuarios finales, estas son de 2048 bits como mínimo y podrán aumentarse conforme la regulación lo requiera o CYBERSIGN lo decida.

7. PERFILES CERTIFICACIONES Y DE REGISTRO DE ACCESO PÚBLICO

Todos los certificados emitidos por CYBERSIGN se generan de acuerdo a lo establecido en X.509 versión 3, así como el RFC 5280.
Los certificados incluyen como mínimo los siguientes datos:
Un certificado emitido por un prestador de servicio de certificación autorizada, además de estar firmado electrónicamente por este, debe contener por los menos lo siguiente:

a) Nombre, dirección y domicilio del firmante
b) Identificación del firmante nombrado en el certificado
c) Número de serie del certificado
d) Nombre del Emisor
e) Fecha de emisión del certificado
f) Fecha de vencimiento del certificado
g) Identificadores del algoritmo criptográfico
h) Formularios utilizados para los nombres de la autoridad certificadora, autoridad de registro y el nombre del firmante.

i) Extensiones de restricciones de políticas

Los OID que se han asignado a los certificados que CYBERSIGN emite son los siguientes:

Tipo de certificado	OID
Persona natural	1.3.6.1.4.1.58088.1.1.1

Para los casos en donde los datos indiquen o se expresen en palabras donde denotan su invalidez (ej. “TEST”, “PRUEBA” o “INVÁLIDO”), se considerarán certificados sin validez legal y por tal razón sin responsabilidad por parte de CYBERSIGN. Estos certificados se emiten con el fin de realizar pruebas técnicas y permitir la evaluación de los servicios y certificados emitidos.

Certificado de persona natural: Estos certificados tienen el OID 1.3.6.1.4.1.58088.1.1.1 y son emitidos para cumplir con la autenticación de acuerdo a las disposiciones del Decreto No. 47-2008 de Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas. Este certificado garantiza la vinculación entre la identidad del firmante y el suscriptor de manera única. Además el firmante cuenta con el control de exclusivo de sus credenciales de uso. La firma electrónica avanzada generada a través de este certificado tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio conforme a las previsiones del artículo 33 de la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas.

Información requerida al solicitante:

a) Nombre, dirección y domicilio del firmante
b) teléfono de contacto del solicitante
c) Documento de identificación del solicitante nombrado en el certificado
d) correo electrónico del solicitante

Información contenida en el certificado:

a) Nombres del firmante
b) Apellidos del firmante
c) Dirección del firmante
d) correo electrónico del firmante
e) Identificación del firmante
f) El nombre, la dirección y el lugar donde realiza actividades la prestadora de servicios de certificación.
g) La clave pública del firmante
h) El número de serie del certificado.
i) Fecha de emisión y expiración del certificado.

Uso de un certificado: Durante una transacción electrónica, un certificado permite a una entidad autenticarse frente a otros participantes dentro de la transacción.

Uso apropiado de un certificado: Los certificados pueden utilizarse en transacción de dominio público que exigen

a) Compromisos de no repudio
b) Autenticación
c) Confidencialidad
d) Integridad
e) Firma electrónica

Uso prohibido de certificados: Los certificados emitidos por CYBERSIGN no pueden utilizarse en estas condiciones

a) Uso en aplicaciones que requieran un rendimiento a prueba de fallos.
b) Uso en aplicaciones en las cuales los problemas de certificado puedan generar un riesgo de seguridad.
c) En situaciones en las que su uso lo prohíba la ley.
d) En situaciones en las que el traslado de información pueda resultar en encarcelamiento si el certificado se ve comprometido o falsificado.
e) En situaciones en las que la transferencia de datos se considere ilegal.
f) En operaciones de instalaciones nucleares.
g) En operaciones de navegación aérea o sistemas de comunicaciones.
h) En sistemas de control de armas.
i) En operaciones cuya falla conlleva directamente a la muerte, lesiones corporales o daños ambientales graves.

CYBERSIGN mantiene un repositorio público con los controles de acceso físicos y lógicos adecuados para evitar modificaciones no autorizadas de la información publicada, en este repositorio se publica la siguiente información:

a) Lista de certificados revocados (CRL) publicadas al menos cada 24 horas y con una vigencia de 48 horas.
b) Certificados de toda la cadena de confianza de su PKI.
c) Consulta del estado de un certificado específico
d) Protocolo de consulta en línea del estado de un certificado (OCSP).

CYBERSIGN no pone a disposición del público materiales sensibles y/o confidenciales, incluidos controles de seguridad, procedimientos operativos y políticas de seguridad interna. En el caso de que surja la necesidad de su uso en una auditoría, estos documentos están disponibles para auditores calificados.

8. ESPECIFICACIONES DE ADMINISTRACIÓN DE LA POLÍTICA DE CERTIFICACIÓN

Organización que administra el documento: CYBERSIGN se identifica en el documento con su nombre comercial “CYBERSIGN”

Procedimiento para cambiar, publicar y comunicar este documento: CYBERSIGN administra este documento de acuerdo a sus políticas internas de gestión de documentos

que incluyen todo lo relativo a estas actividades. Dicho procedimiento incluye los mecanismos para editar, revisar y aprobar los cambios a este documento y está identificado con el código SIG-PR-001.
En estas se incluyen los involucrados, responsables y procedimientos para publicar y comunicar los cambios a estas CPS.

9. PROCEDIMIENTOS QUE DEFINEN EL CICLO DE VIDA DE LOS CERTIFICADOS

CYBERSIGN establece deberes y procedimientos requeridos para las siguientes etapas del ciclo de vida de los certificados:

a) Emisión certificados de firma electrónica
   Es necesario que la persona individual que desee realizar una solicitud de emisión de certificados de firma electrónica esté registrada en la plataforma de CYBERSIGN, siendo un suscriptor. Es responsabilidad de CYBERSIGN proveer un método de identificación y autenticación para validar las solicitudes de emisión de certificados.

   Por consiguiente, es necesario que el suscriptor realice la solicitud de emisión de certificado y que realice el proceso correspondiente brindando la información solicitada.

   Es responsabilidad del suscriptor brindar la información necesaria y verídica para realizar la validación de datos personales, mediante los sistemas utilizados por CYBERSIGN, y así poder aplicar a la emisión del certificado.

   CYBERSIGN, como autoridad certificadora, tiene la responsabilidad de manejar la información del usuario de manera adecuada y segura para poder realizar la emisión del certificado solicitado, siempre y cuando la solicitud no haya sido rechazada a lo largo del proceso.

   Es necesario que los solicitantes posean un método multifactor para poder validar que la solicitud haya sido realizada por la persona individual registrada y continuar con el proceso de emisión de certificados.

   CYBERSIGN notificará al solicitante mediante correo electrónico cuando el certificado haya sido emitido y pueda ser utilizado para firmas electrónicas, o bien cuando su solicitud haya sido rechazada.

   El proceso de emisión de certificados comienza con el registro del sitio web de cybersign y requiere de la validación del correo electrónico provisto para tal efecto. Una vez validado, se procede a llenar el formulario de solicitud de certificado en el cual el solicitante indica sus datos personales así como el resto de datos a ser incluidos en el certificado. Posteriormente se procede a validar de manera virtual la

identidad del solicitante, esto por medio de validaciones a su documento de identidad así como al factor de coincidencia biométrica entre el solicitante y el documento presentado. Una vez se haya llevado a cabo este proceso un operador de registro de CYBERSIGN procederá a validar la información provista por el solicitante para validarla.

b) Revocatoria de certificados de firma electrónica

Las circunstancias en las cuales un certificado puede ser revocado incluyen: la elección del solicitante, compromiso de la clave privada, detección de una vulnerabilidad y/o confirmación de que dicho certificado ha sido falsificado. La terminación de las actividades del prestador de servicios de certificación u otros que el suscriptor decida.

El solicitante, la autoridad de registro y la autoridad certificadora son los participantes capaces de realizar una solicitud de revocación de un certificado.

El período de tiempo para realizar la solicitud de revocación de un certificado finaliza posterior a la fecha de vencimiento del certificado. Una vez realizada esta solicitud, el proceso de revocación es irreversible.

La solicitud de revocación de un certificado se realiza en la plataforma de CYBERSIGN, quien solicita una razón para la solicitud de revocación y autenticación multifactor. El suscriptor debe identificarse en la plataforma con las credenciales que tiene bajo su control e ingresar al apartado de certificados donde podrá elegir su certificado y solicitar su revocación. El tiempo de vigencia que reste al certificado al momento de su revocación no será reembolsado por CYBERSIGN al suscriptor.

c) Suspensión de certificados de firma electrónica

La solicitud de suspensión de un certificado debe realizarse en la plataforma de CYBERSIGN y requiere de autenticación multifactor.

La suspensión de un certificado puede realizarse por el solicitante y la autoridad de registro.

La solicitud de suspensión de un certificado se realiza en la plataforma de CYBERSIGN, quien solicita la autenticación multifactor. El suscriptor debe identificarse en la plataforma con las credenciales que tiene bajo su control e ingresar al apartado de certificados donde podrá elegir su certificado y solicitar su suspensión. Si el certificado llegara a expirar mientras el certificado se encuentra suspendido, este pasará automáticamente a un estado de expirado y no podrá reactivarse nuevamente.

El período de tiempo para realizar la solicitud de suspensión de un certificado finaliza posterior a la fecha de vencimiento del certificado. El proceso de suspensión y remoción de la suspensión de un certificado puede realizarse cuantas veces quiera realizarlo el solicitante.

d) Renovación certificados de firma electrónica
Esta solicitud se podrá hacer efectiva siempre y cuando el certificado que se solicite sea renovado, no haya expirado previamente.

Para que se realice el proceso de renovación de certificados, es necesario que el suscriptor sea el responsable de realizar la solicitud de renovación mediante la plataforma de CYBERSIGN y mediante su usuario registrado.

Este procedimiento requiere el uso del método multifactor del suscriptor para poder hacer efectiva la solicitud y renovación del certificado. Por otro lado, CYBERSIGN deberá realizar el procedimiento para la renovación del certificado y la publicación del mismo para su uso.

CYBERSIGN notificará al solicitante mediante correo electrónico cuando el certificado haya sido renovado y pueda ser utilizado para firmas electrónicas, o bien cuando su solicitud haya sido rechazada.

e) Pérdida de vigencia de los certificados de firma electrónica
La pérdida de vigencia de los certificados puede ocurrir de dos maneras. La primera es por medio de la revocación del certificado en donde el suscriptor es responsable de realizar la solicitud de revocación de éste por medio de la plataforma de CYBERSIGN y su usuario registrado. Esto implica que CYBERSIGN realizará dicho procedimiento, y el certificado será marcado como revocado en los sistemas de consulta de certificados.

f) El estado de la vigencia de los Certificados se puede comprobar por medio del protocolo OCSP en la siguiente dirección

http://ocsp.cybersign.gt

Por otro lado, está la expiración de los certificados de manera natural. Esto implica que CYBERSIGN es responsable de marcar el certificado según la fecha de expiración indicada en el certificado. Una vez expira un certificado este no tendrá validez y no deberá ser utilizado.

CYBERSIGN deberá publicar la revocación de estos certificados por medio de OCSP y CRL. Teniendo estos de forma pública en:

https://cybersign.gt/certificates-crl

g) CYBERSIGN pone a disposicion de los terceros interesados el sitio web https://cybersign.gt/ en el cual se puede consultar la información pública relevante a los certificados asi como a estas practicas de certificación.

10. FINALIZACIÓN DE ACTIVIDADES DE CERTIFICACIÓN

Conforme el artículo 45 del Decreto Número 47-2008, Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas , las sociedades de certificación autorizadas pueden cesar en el ejercicio de actividades, siempre y cuando hayan recibido autorización por parte del Registro de Prestadores de Servicios de Certificación.

En caso que CYBERSIGN finalice sus actividades de certificación, esta tendrá la responsabilidad de notificar esto a sus suscriptores. De esta forma se procederá a revocar los certificados según las solicitudes de los usuarios, o dejar que éstos expiren de forma natural. Cuando Cybersign así lo considere necesario podrá revocar el certificado y reembolsar al cliente el valor proporcional al tiempo restante en el certificado para culminar el cierre de actividades durante el periodo establecido.

11. GLOSARIO

CPS: Declaración de Prácticas de Certificación.
CP: Políticas de Certificación.
HSM: Hardware Security Module
CA: Autoridad Certificadora
RA: Autoridad de Registro
FIPS: Federal Information Processing Standards
OCSP: Online Certificate Status Protocol
CRL: Certificate Revocation List
PKI: Public Key Infrastructure
M of N: M de N
OID: Object Identifier

Rolando Haroldo Alonso Ordoñez

Firmado digitalmente por Rolando Haroldo Alonso Ordoñez
Fecha: 2024.10.17 09:08:28 -06'00'