DECLARACIÓN DE PRÁCTICAS DE PRESTACIÓN DEL SERVICIO DE GENERACIÓN O GESTIÓN DE DATOS DE CREACIÓN DE FIRMA ELECTRÓNICA DEL PCSC VIT S.A.

DOC-DPF3-VITSA-V1.0

Versión 1.0

CONTROL DOCUMENTAL

Documento	
Título: DECLARACIÓN DE PRÁCTICAS DE PRESTACIÓN DEL SERVICIO DE GENERACIÓN O GESTIÓN DE DATOS DE CREACIÓN DE FIRMA ELECTRÓNICA DEL PCSC VIT S.A.	**Nombre Fichero:** DOC-DPF3-VITSA-V1.0
Código: DOC-DPF3-VITSA-V1.0	**Soporte Lógico:** https://www. efirma.com.py
Fecha: 12/10/2022	**Versión:** 1.0

Registro de Cambios		
Versión	**Fecha**	**Motivo de Cambio**
1.0	12/10/2022	Versión Inicial

Distribución del documento	
Nombre	**Área**
Ministerio de Industria y Comercio (MIC)	Dirección General de Comercio Electrónico (DGCE)
Autoridad Certificadora (AC)	Prestadores Cualificados de Servicios de Confianza (PCSC)
Documento Público	https://www.efirma.com.py

Control del documento	
Elaborado por: ***WALTER CORREA*** ***ALEJANDRO TORALES***	
Verificado por: ***RAQUEL VILLALBA***	
Aprobado por: ***JOSE LUIS CASTILLO***	

Contenido

1. INTRODUCCIÓN

1.1 DESCRIPCIÓN GENERAL

Este documento es parte de un conjunto de normativas creadas para regular al Prestador Cualificado de Servicios de Confianza (PCSC) VIT S.A. dentro del alcance de la Infraestructura de Claves Públicas de Paraguay (ICPP). Dicho conjunto consta de los siguientes documentos:

a) DOC-ICPP-07 (este documento); y

b) DOC-ICPP-08 [1].

El PCSC VIT S.A. es una entidad habilitada y supervisada por el Ministerio de Industria y Comercio (MIC) y se encuentra autorizada a prestar servicios de generación o gestión de datos de creación de firma electrónica en el marco de la ICPP en los términos establecidos en el documento POLITICA DE CERTIFICACIÓN F3 VIT S.A.

Las claves privadas de los usuarios finales almacenadas en dispositivos estandarizados conforme lo establecido en el documento POLITICA DE CERTIFICACIÓN F3 VIT S.A. [1], y las firmas electrónicas hechas por la clave privada del usuario en otros sistemas son válidas de conformidad a la Ley N° 6822/2021.

Este documento establece los requisitos mínimos que obligatoriamente deben ser observados por la PCSC VIT S.A. integrante de la ICPP, para la prestación de servicios de generación o gestión de datos de creación de firma electrónica en nombre del firmante. Esta DP es el documento que describe las prácticas, procedimientos operativos y técnicos empleados por el PCSC VIT S.A. para la prestación de sus servicios.

El PCSC VIT S.A. utiliza sistemas y productos fiables, incluidos canales de comunicación electrónicos seguros, aplicando procedimientos y mecanismos técnicos y organizativos adecuados, para garantizar que el entorno sea confiable y que los datos de creación de firma se utilicen bajo el control exclusivo del titular del certificado. Además, deben custodiar y proteger los datos de creación de firma frente a cualquier alteración, destrucción o acceso no autorizado, así como garantizar su continua disponibilidad.

Este documento se basa en los estándares de la ICPP, RFC 4210, 4211, 1305, 2030, 3447, 3647 de IETF y Reglamento (UE) 910/2014.

Las regulaciones previstas en los otros documentos de la ICPP también se aplican al PCSC VIT S.A. como integrantes de la referida ICPP, según corresponda:

a) NORMA ISO/IEC 27002:2022. Tecnologías de la información - Técnicas de seguridad - Código de prácticas para los controles de seguridad de la información;

b) DOC-ICPP-03 [3];

c) DOC-ICPP-04 [2];

d) DOC-ICPP-06 [4]; y

e) DOC-ICPP-12 [5].

Esta DP cumple con el RFC 3647 de Internet *Engineering Task Force* (IETF) y puede someterse a actualizaciones periódicas.

1.2 NOMBRE E IDENTIFICACIÓN DEL DOCUMENTO

Documento: DECLARACIÓN DE PRACTICAS DE PRESTACIÓN DEL SERVICIO DE GENERACIÓN O GESTIÓN DE DATOS DE CREACIÓN DE FIRMA ELECTRÓNICA CUALIFICADO EN EL MARCO DE LA ICPP DE VIT S.A.

Versión: 1.0

Estado: APROBADO

Fecha de emisión: 12 de octubre del 2022

URL del documento: https://www.efirma.com.py/repositorio/DPF3-PCSC-VITSA.pdf

Sitio de internet oficial: https://www. efirma.com.py

Referencia de la DP/ OID de la DP: 1.3.6.1.4.1.44234.1.1.1.11

1.3 PARTICIPANTES Y APLICABILIDAD

1.3.1. PRESTADORES CUALIFICADOS DE SERVICIOS DE CONFIANZA

En la URL https://efirma.com.py/productos-y-servicios-i4 están publicadas los servicios prestados por el PCSC VIT S.A.

El PCSC VIT S.A. es una entidad autorizada por la CA Raíz-Py para prestar servicios de generación o gestión de datos de creación de firma en nombre del firmante, los mismos se pueden clasificar en tres categorías, según el tipo de actividad prevista:

a) Almacenamiento de claves privadas de usuarios finales; o

b) servicio de firma electrónica cualificada, verificación de firma electrónica cualificada; o

c) ambos.

El PCSC VIT S.A. mantiene actualizada en todo momento la información anterior.

Entiéndase el servicio de firma cualificada indicado en el literal b), como el proceso de firma electrónica cualificado realizado por medio de la clave privada del titular de un certificado electrónico emitido por el PCSC VIT S.A. cuya clave privada se encuentra almacenada en un dispositivo HSM en custodia del PCSC VIT S.A.

1.3.2. SUSCRIPTORES

En contexto de esta DP y en relación al PCSC VIT S.A., es suscriptor toda persona física o jurídica que protege su clave privada y el uso de su correspondiente certificado digital en forma centralizada en la PCSC VIT S.A.

Los suscriptores deberán manifestar plenamente la aprobación de los servicios de la PCSC VIT S.A., así como el nivel de monitoreo que el PCSC VIT S.A. deberá informar, para fines exclusivos de protección de la clave privada del titular, ya sea en la provisión de almacenamiento de claves privadas, servicios de firma y verificación de firmas electrónicas cualificadas.

Los Titulares de Certificados podrán revocar la autorización otorgada al PCSC VIT S.A. para la prestación de los servicios, para lo cual deberá solicitar la revocación de su certificado al PCSC VIT S.A. que lo emitió. Formalizada la revocación, el PCSC VIT S.A. procederá de manera inmediata a la eliminación de la clave privada del Titular del Certificado almacenada en el dispositivo criptográfico por éste custodiado.

1.3.3. APLICABILIDAD

a) **CUSTODIA CENTRALIZADA:** El resguardo de las credenciales de identidad se realiza en un repositorio virtual centralizado de alta seguridad y accesible desde cualquier entorno. El suscriptor se autentica y accede de forma remota, vía red o internet a las claves custodiadas por un prestador cualificado de servicios de confianza, que puede ser un tercero o la propia organización.

b) **FIRMA CUALIFICADA Y AUTENTICACION:** El suscriptor accederá a una

plataforma en el cual tendrá acceso a su certificado cualificado resguardado de forma centralizada, donde se autentica y accede a su certificado digital y de esta forma poder realizar la firma digital de los documentos electrónicos.

1.4. DATOS DE CONTACTO

1.4.1. ORGANIZACIÓN QUE ADMINISTRA EL DOCUMENTO

Nombre: VIT S.A.

RUC: 80080099-0

Dirección: España N° 2028 c/ Brasilia.

Teléfono: (595-21) 229 350

Dirección de correo electrónico: info@efirma.com.py

Página Web: https://www.efirma.com.py

1.4.2. PERSONA DE CONTACTO

Nombre: Raquel Villalba

Teléfono: 021-229-350

Página web: https://www. efirma.com.py

Dirección de correo electrónico: info@efirma.com.py

Dirección: España N° 2028 c/ Brasilia

1.5 PROCEDIMIENTOS DE CAMBIO DE ESPECIFICACIÓN

1.5.1. POLITICAS DE PUBLICACION Y NOTIFICACIÓN.

La PCSC VIT S.A. distribuye y pone a disposición su DP del servicio de generación o gestión de creación de datos en nombre del firmante mediante el repositorio público de efirma.com.py

1.5.2. PROCEDIMIENTOS DE APROBACIÓN.

El directorio y el personal autorizado de VIT S.A. conforme a los Estatutos de la empresa, aprobaran el contenido de la DP y sus posteriores enmiendas o modificaciones, y luego será puesta a consideración de la Dirección General Comercio Electrónico y autoridades pertinentes del Ministerio de Industria y Comercio para su aprobación.

1.6 DEFINICIONES, SIGLAS Y ACRÓNIMOS

1.6.1 DEFINICIONES

1. **Autenticación:** proceso técnico que permite determinar la identidad de la persona física o jurídica.
2. **Autenticación electrónica:** un proceso electrónico que posibilita la identificación electrónica de una persona física o jurídica, o del origen y la integridad de datos en formato electrónico.
3. **Autoridad de Aplicación:** Ministerio de Industria y Comercio a través de la Dirección General de Comercio Electrónico, dependiente del Viceministerio de Comercio y Servicios.
4. **Autoridad de Certificación:** entidad que presta servicios de emisión, gestión, revocación u otros servicios de confianza basados en certificados cualificados. En el marco de la ICPP, son Autoridades de Certificación, la AC Raíz-Py y el PCSC VIT S.A.
5. **Autoridad de Certificación Raíz del Paraguay:** órgano técnico, cuya función principal es coordinar el funcionamiento de la ICPP. La AC Raíz-Py tiene los certificados de más alto nivel, posee un certificado autofirmado y es a partir de allí, donde comienza la cadena de confianza. Las funciones de la AC Raíz-Py son ejercidas por la AA.
6. **Gestión de datos de creación de firma:** El PCSC VIT S.A. podrá, en nombre del firmante, gestionar los datos de creación de firma electrónica cualificada a los que hayan prestado sus servicios, este servicio deberá ser provisto por el PCSC VIT S.A. siempre y cuando cuente con la debida habilitación.
7. **Certificado cualificado de firma electrónica:** un certificado de firma electrónica que ha sido expedido por un PCSC y que cumple los requisitos establecidos en el artículo 43 de la ley Nº 6822/2021.
8. **Certificado cualificado de sello electrónico:** un certificado de sello electrónico que ha sido expedido por un PCSC y que cumple los requisitos establecidos en el artículo 53 de la ley Nº 6822/2021.
9. **Claves criptográficas:** valor o código numérico que se utiliza con un algoritmo criptográfico para transformar, validar, autenticar, cifrar y descifrar datos.
10. **Clave pública y privada:** la criptografía en la que se basa la ICPP, es la

criptografía asimétrica. En ella, se emplean un par de claves: lo que se cifra con una de ellas, sólo se puede descifrar con la otra y viceversa. A una de esas claves se la denomina pública y está incorporada en el certificado electrónico, mientras que a la otra se le denomina privada y está bajo exclusivo control del titular o responsable del certificado.

11. **Compromiso:** violación de la seguridad de un sistema a raíz de una posible divulgación no autorizada de información sensible.
12. **Data center (Centro de Datos):** infraestructura compuesta por espacio físico para la instalación de equipos informáticos y de comunicación con adecuados sistemas de energía, aire acondicionado y seguridad. Es parte de una AC, constituye un recinto seguro que alberga, entre otras cosas, los módulos criptográficos de hardware, protege la infraestructura tecnológica y es el lugar donde se ejecutan servicios del ciclo de vida del certificado. La importancia del data center radica en la protección que brinda a la clave privada y asegura la confianza en los certificados electrónicos emitidos por la AC.
13. **Datos de activación:** valores de los datos, distintos al par de claves, que son requeridos para operar los módulos criptográficos y que necesitan estar protegidos.
14. **Declaración de Prácticas de Certificación:** documento en el cual se determina la declaración de las prácticas que emplea una AC al emitir certificados y que define la infraestructura, políticas y procedimientos que utiliza la AC para satisfacer los requisitos especificados en la PC vigente.
15. **Emisión de certificado:** es la autorización de la emisión del certificado en el sistema del PCSC VIT S.A. previa comprobación de la concordancia de los datos de solicitud del certificado con los contenidos en los documentos presentados.
16. **Firma electrónica cualificada:** una firma electrónica que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica, la cual deberá estar vinculada al firmante de manera única, permitir la identificación del firmante, haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede

utilizar, con un alto nivel de confianza, bajo su control exclusivo y estar vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable.

17. **Firmante:** una persona física que crea una firma electrónica.
18. **Generador:** máquina encargada de generar electricidad a partir de un motor de gasolina o diésel. La instalación de este equipo deberá ser de tal forma que, al interrumpirse el suministro de energía eléctrica del proveedor externo, el mismo debe arrancar automáticamente tomando la carga de las instalaciones del data center de la AC, incluyendo los circuitos de iluminación, de los equipos informáticos, equipos de refrigeración, circuitos de monitoreo, prevención de incendios; en fin de todos los circuitos eléctricos críticos para el funcionamiento de las instalaciones tecnológicas.
19. **Habilitación:** autorización que otorga el MIC, una vez cumplidos los requisitos y condiciones establecidos en la norma.
20. **Infraestructura de Claves Públicas del Paraguay:** conjunto de personas, normas, leyes, políticas, procedimientos y sistemas informáticos necesarios para proporcionar una plataforma criptográfica de confianza que garantiza la presunción de validez legal para actos electrónicos firmados o cifrados con certificados electrónicos cualificados y claves criptográficas emitidas por esta infraestructura.
21. **Integridad:** característica que indica que un mensaje de datos o un documento electrónico no ha sido alterado desde la transmisión por el iniciador hasta su recepción por el destinatario.
22. **Módulo criptográfico**: software o hardware criptográfico que genera y almacena claves criptográficas.
23. **Módulo de Seguridad de Hardware:** dispositivo basado en un módulo criptográfico tipo hardware que genera, almacena y protege claves criptográficas.
24. **Normas Internacionales:** requisitos de orden técnico y de uso internacional que deben observarse en la prestación de los servicios mencionados en la presente DP.
25. **Organismo de Evaluación de Conformidad:** organismo que desempeña

actividades de evaluación de la conformidad a un prestador de servicios de confianza y de los servicios de confianza que este presta conforme a la Ley Nº 6822/2021.

26. **Parte usuaria:** persona física o jurídica que confía en el servicio de confianza.
27. **Prestador Cualificado de Servicios de Confianza:** prestador de servicios de confianza que presta uno o varios servicios de confianza cualificados y al que el organismo de supervisión ha concedido la habilitación.
28. **Política de Seguridad:** es un conjunto de directrices destinadas a definir la protección del personal, seguridad física, lógica y de red, clasificación de la información, salvaguarda de activos de la información, gerenciamiento de riesgos, plan de continuidad de negocio y análisis de registros de eventos de una AC.
29. **Registro de Auditoría:** registro cronológico de las actividades del sistema, el cual es suficiente para permitir la reconstrucción, revisión e inspección de la secuencia de los ambientes y de las actividades que rodean o que conducen a cada acontecimiento en la ruta de una transacción desde su inicio hasta la salida de los resultados finales.
30. **Solicitud de certificado:** documento que se instrumenta mediante un formato autorizado de solicitud de certificado o como parte de documento específico denominado Contrato de Prestación de Servicios de Confianza, suscripto por el solicitante en nombre propio en el caso de certificados cualificados de firma electrónica para persona física, o bien en nombre del titular en el caso de certificados cualificados de sello electrónico para persona jurídica.
31. **Solicitud de revocación**: documento que se instrumenta mediante un formato autorizado de solicitud para la revocación de un certificado.
32. **Verificación y validación de firma o sello:** determinación y validación de que la firma o sello electrónico fue creado durante el periodo operacional de un certificado válido, por la clave privada correspondiente a la clave pública que se encuentra en el certificado y que el mensaje no ha sido alterado desde que su creación.

1.6.2 SIGLAS Y ACRÓNIMOS

Tabla Nº 1 - Siglas y Acrónimos

Sigla/Acrónimo	Descripción
AA	Autoridad de Aplicación
AC	Autoridad de Certificación (CA por sus siglas en inglés, Certificate Authority)
AC Raíz-Py	Autoridad Certificadora Raíz del Paraguay
DP	Declaración de Prácticas
DGCE	Dirección General de Comercio Electrónico dependiente del Viceministerio de Comercio y Servicios.
HSM	Módulo de Seguridad Criptográfico basado en Hardware (HSM por sus siglas en inglés, Hardware Security Module)
ICPP	Infraestructura de Clave Pública del Paraguay
IDS	Sistema de Detección de Intrusos
ISO	Organización Internacional para la Estandarización (ISO por sus siglas en inglés, International Organization for Standardization).
MIC	Ministerio de Industria y Comercio
OEC	Organismo de Evaluación de la Conformidad
PC	Política de certificación (CP por sus siglas en inglés, Certificate Policy)
PCN	Plan de Continuidad del Negocio
PCSC	Prestador cualificado de servicios de confianza
PS	Política de Seguridad
PSS	Prestador de Servicios de Soporte

Py	Paraguay
RFC	Petición de Comentarios (RFC por sus siglas en inglés, Request For Comments)
UPS	Sistemas de alimentación ininterrumpida (UPS por sus siglas en inglés, uninterruptible power supply)
URL	Localizador uniforme de recursos (URL por sus siglas en inglés, Uniform Resource Locator).

2. RESPONSABILIDAD DEL REPOSITORIOY PUBLICACIÓN

2.1. PUBLICACIÓN

2.1.1. PUBLICACIÓN DE INFORMACIÓN DE PCSC

El PCSC VIT S.A. dispone en su sitio principal de un Repositorio público de información, en la dirección URL con protocolo seguro: https://www.efirma.com.py/repositorio/

El PCSC VIT S.A. es responsable de las funciones de su Repositorio, el servicio de Repositorio referido no contiene ninguna información de naturaleza confidencial.

El PCSC VIT S.A. tiene disponible las siguientes informaciones en su sitio web:

a) capacidad de almacenamiento de las claves privadas de los Titulares de Certificados que opera;

b) su DP;

c) los servicios que implementa.

d) las condiciones generales mediante la cual son prestados los servicios de almacenamiento de claves privadas o servicio de firma electrónica cualificada y verificación de firma electrónica cualificada.

2.1.2. FRECUENCIA DE PUBLICACIÓN

Se realizan revisiones anuales al presente documento y cuando surjan cambios

en la normativa vigente. De existir cambios en el mismo, se publicará la nueva versión luego de su aprobación.

2.1.3. CONTROLES DE ACCESO

El PCSC VIT S.A. brinda acceso irrestricto a toda la información contenida en el repositorio público y establece controles adecuados para restringir la posibilidad de escritura y modificación de la información publicada, garantizando su integridad

3. IDENTIFICACIÓN Y AUTORIZACIÓN

En el contexto de la presente DP, la Identificación y Autenticación comprende el proceso que se aplica cuando el suscriptor persona física desea obtener su certificado cualificado custodiada, para lo cual se presenta en la AR, quien a través de sus funcionarios valida su identidad y habilita la emisión de su certificado.

4. REQUERIMIENTOS OPERACIONALES

4.1. ALMACENAMIENTO Y ACCESO A LAS CLAVES PRIVADAS DEL TITULAR DEL CERTIFICADO

El PCSC VIT S.A. almacena las claves privadas de los usuarios finales, para los certificados del Tipo F3 en hardware criptográficos tipo HSM (debidamente homologado por el MIC).

El acceso a las claves privadas de los usuarios es de uso, conocimiento y control exclusivo del titular del certificado, sin la posibilidad de ingreso por parte de otros titulares en el mismo HSM, cualquier empleado/funcionario del PCSC VIT S.A. o dependiente de otras claves criptográficas, El PCSC VIT S.A. proporciona mecanismos de doble factor de autenticación al titular del certificado para el acceso a su clave privada

El PCSC VIT S.A. informa como los componentes de software se comunican entre la aplicación del Titular del Certificado y el acceso al certificado y sus claves, describiendo:

a) el lenguaje de programación utilizado por el PCSC VIT S.A. para la construcción de la plataforma de acceso es Java

b) Se pone a disposición del Titular del Certificado una plataforma web accesible desde cualquier navegador, disponible desde "https://ag.chefirma.com.py/user/auth";

c) todas las comunicaciones viajan a través del canal seguro de transporte TLS;

d) la arquitectura de red de la aplicación de acceso.

4.2. SERVICIO DE CREACIÓN Y VERIFICACIÓN DE FIRMA ELECTRÓNICA CUALIFICADA

El PCSC VIT S.A. antes de procesar la petición de firma electrónica cualificada garantiza que el usuario titular del certificado sea autenticado y debe verificar la validez de dicho certificado.

El firmante electrónico que quiere crear una firma en un documento electrónico; se conecta mediante una aplicación conductiva que representa un ambiente de usuario que el titular del certificado usa para acceder a la funcionalidad de firma electrónica; y por medio de un sistema de creación de firma electrónica, procede a la firma electrónica aplicando el pin de firma correspondiente

El proceso de validación de una firma electrónica es realizado conforme una política de firma explícita, que consiste en un conjunto de restricciones de validación, denominada Política de firma, y genera un informe que indica el estado de validación (Válido, Inválido o Indeterminado), que proporciona los detalles de la validación técnica de cada una de las restricciones aplicables, que pueden ser relevantes para la aplicación exigente en la interpretación de los resultados.

El firmante crea una firma de acuerdo con una política de firma y el verificador evalúa la validez de una firma utilizando la misma política de firma utilizada en la creación de esa firma.

4.3. PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD

En los siguientes ítems de la DP, son descriptos los aspectos relacionados a los sistemas de auditoría y de registro de eventos implementados por el PCSC VIT S.A. con el objetivo de mantener un ambiente seguro.

4.3.1. TIPOS DE EVENTOS REGISTRADOS

El PCSC VIT S.A. registra en archivos de auditoría todos los eventos relacionados con la seguridad de su sistema. Entre otros, los siguientes eventos están obligatoriamente incluidos en los archivos de auditoría:

a) arranque y apagado de los sistemas del PCSC VIT S.A.;

b) tentativas de crear, eliminar, establecer contraseñas o cambiar los privilegios de los Sistemas Operativos del PCSC VIT S.A.;

c) cambios en la configuración de los sistemas del PCSC VIT S.A.;

d) tentativas de acceso (*login*) y de salida del sistema (*logoff*);

e) tentativas de acceso no autorizados a los archivos del sistema;

f) registros de almacenamiento de claves privadas y/o certificados electrónicos;

g) tentativas de iniciar, eliminar, habilitar y deshabilitar a usuarios de sistemas;

h) operaciones fallidas de escritura o lectura, cuando sea aplicable;

i) todos los eventos relacionados sincronizados con una fuente confiable de tiempo ajustados a la fecha y hora oficial paraguaya;

j) registros de las firmas electrónicas cualificadas creadas y verificaciones realizadas;

k) registros de acceso a los documentos de los Titulares de Certificados;

l) registros de acceso o tentativas de acceso a la clave privada del Titular de Certificado.

El PCSC VIT S.A. también registra, electrónica o manualmente, informaciones de seguridad no generada directamente por sus sistemas, tales como:

a) registros de accesos físicos;

b) el mantenimiento y cambios en la configuración de sus sistemas;

c) los cambios en el personal y de perfiles cualificados;

d) los informes de discrepancia y compromiso; y

e) el registro de destrucción de medios de almacenamiento que contienen claves criptográficas, datos de activación de certificados o información personal de

los Titulares de Certificados.

La DP prevé que todos los registros de auditoría deberán contener la identidad del agente que los causó, así como la fecha y hora del evento. Los registros de auditoría electrónicos contienen la hora *Universal Time Coordinated* (UTC). Los registros manuales en papel contienen la hora local siempre que se especifique la ubicación.

Para facilitar los procesos de auditoría, toda la documentación relacionada con los servicios del PCSC VIT S.A. esta almacenada, ya sea de forma electrónica o manual, en una única ubicación, conforme a lo establecido en la norma ISO 27002/2022.

4.3.2. FRECUENCIA DE AUDITORÍA DE REGISTRO (LOGS)

La DP establece la periodicidad, que no exceda de una semana, con la cual los registros de auditoría del PCSC VIT S.A. son analizados por su personal operacional. Todos los eventos significativos son explicados en un informe de auditoría de registros. Tales análisis involucran una breve inspección de todos los registros, con la verificación de que no hayan sido alterados, seguida de una investigación más detallada de cualquier alerta o irregularidad en esos registros. Todas las acciones tomadas como resultado de este análisis deberán ser documentadas.

4.3.3. PERIODO DE CONSERVACIÓN DE REGISTROS (LOGS) DE AUDITORÍA

El PCSC VIT S.A. mantiene localmente sus registros de auditoría durante al menos 2 (dos) meses y posteriormente los almacena de la manera descripta en el ítem 4.5.

4.3.4. PROTECCIÓN DEL REGISTRO (LOG) DE AUDITORÍA

El sistema de registro de eventos de auditoría incluye mecanismos para proteger los archivos de auditoría contra lectura, modificación y eliminación no autorizadas a través de la funcionalidad de los sistemas operativos nativos. A las herramientas disponibles en el sistema operativo brindan acceso lógico a los registros de auditoría solo a los usuarios o aplicaciones autorizadas, mediante permisos otorgados por el administrador del sistema de acuerdo con la función de los usuarios o aplicaciones y orientación del departamento de seguridad.

El propio sistema operativo también registra el acceso a los archivos donde se almacenan los registros de auditoría.

La información de auditoría manual también está protegida contra lectura, modificación y eliminación no autorizadas mediante controles de acceso a los entornos físicos donde se almacenan estos registros.

Los mecanismos de protección descriptos en este ítem obedecen a lo dispuestoen el ítem 12 “seguridad en la operativa” de la norma ISO 27002/2022.

4.3.5. PROCEDIMIENTOS PARA COPIA DE SEGURIDAD (*BACKUP*) DE REGISTRO (*LOG*) DE AUDITORÍA

Los registros de auditoría y los resúmenes de auditoría de todos los equipos utilizados por el PCSC VIT S.A. tienen copias de respaldo (copia de seguridad) diario realizada, automáticamente por una herramienta de backup.

4.3.6. SISTEMA DE RECOPILACIÓN DE DATOS DE AUDITORÍA

El sistema de recopilación de datos de auditoría interna del PCSC VIT S.A. es una combinación de procesos automatizados y manuales, realizados por su personal operativo y sus sistemas.

4.3.7. NOTIFICACIÓN DE AGENTES CAUSANTES DE EVENTOS

Cuando un evento es registrado por el conjunto de sistemas de auditoría del PCSC VIT S.A., ninguna notificación es enviada a la persona, organización, dispositivo o aplicación que causó el evento.

4.3.8. EVALUACIONES DE VULNERABILIDAD

Los eventos que indiquen posibles vulnerabilidades, detectados en el análisis periódico de los registros de auditoría del PCSC VIT S.A., serán analizados detalladamente y, dependiendo de su gravedad, registrados por separado. Las acciones correctivas resultantes serán implementadas por el PCSC VIT S.A. y registradas para fines de auditoría.

4.4. ARCHIVO DE REGISTROS

En los ítems siguientes de esta DP es descripta la política general de archivo de registros, para uso futuro, implementada por el PCSC VIT S.A.

4.4.1. TIPOS DE REGISTROS ARCHIVADOS

La PCSC VIT S.A. archiva los siguientes tipos de registros entre otros:

a) notificaciones de compromiso de las claves privadas de los Titulares de Certificados por cualquier motivo;

b)

c) informaciones de auditoría previstas en este ítem.

La PCSC VIT S.A. establece como período de retención para cada registro archivado, señalando que los registros de almacenamiento de claves privadas y/o certificados electrónicos, de firmas electrónicas cualificados creados, de verificaciones de firmas electrónicas cualificados y, tal vez, de los documentos almacenados, incluidos los archivos de auditoría, deberán conservarse durante al menos5 (cinco) años.

4.4.2. PROTECCIÓN DE ARCHIVOS

La PCSC VIT S.A. establece que todos los registros archivados son clasificados y almacenados con los requisitos de seguridad consistentes con esa clasificación, conforme a lo establecido en la norma ISO 27002/2022.

4.4.3. PROCEDIMIENTOS PARA LA COPIA DE SEGURIDAD(BACKUP) DE ARCHIVO

La PCSC VIT S.A. establece que una segunda copia de todo el material archivado se almacena en un ambiente diferente a las instalaciones principales, recibiendo el mismo tipo de protección utilizada por él, en el archivo principal.

Las copias de respaldo siguen períodos de retención definidos para los registros de los cuales son copias.

El PCSC VIT S.A. verifica la integridad de esas copias de seguridad, al menos, cada 6 (seis) meses.

4.4.4. REQUISITOS PARA FECHADO DE REGISTROS

La información de fecha y hora en los registros se basa en la hora oficial de la república del Paraguay incluidos los segundos (en el formato AAMMDDHHMMSS), inclusosi el número de segundos es cero.

4.4.5. SISTEMA DE RECOPILACIÓN DE DATOS DE ARCHIVOS

El PCSC VIT S.A. cuenta con un sistema para la recopilación de datos de

archivos.

4.4.6. PROCEDIMIENTOS PARA OBTENER Y VERIFICAR INFORMACIÓN DE ARCHIVO

El PCSC VIT S.A. implementa un procedimiento para obtener y verificar la información de archivo, esta se lleva cabo mediante un personal de confianza autorizado, el mismo realiza pruebas de restauración de la información archivada al menos 1 vez al año. La integridad de la información debe ser verificada cuando es restaurada.

4.5. LIBERACIÓN DE ESPACIO DEL SUSCRIPTOR

Una vez que el certificado del suscriptor expira o se revoca, se procede a la liberación del espacio (*slot*) destinado. La liberación se realiza con un mecanismo que impide la recuperación de la clave privada. Los HSM utilizados proveen funciones para la liberación segura.

4.6. COMPROMISO Y RECUPERACIÓN ANTE DESASTRES

4.6.1. DISPOSICIONES GENERALES

El PCSC VIT S.A. garantiza, en caso de que su operación se vea comprometida por cualquiera de los motivos enumerados en los ítems situados más abajo, que las informaciones relevantes son disponibilizadas a los Titulares de Certificados y a las terceras partes.

El PCSC VIT S.A. disponibiliza a todos los Titulares de Certificados y terceras partes una descripción del compromiso que se ha producido.

En caso de compromiso de una operación de almacenamiento y acceso a las claves de uno o más Titulares de Certificados, el PCSC VIT S.A. ya no provee ese servicio, hasta que la AC Raíz-Py tome las medidas administrativas correspondientes, informando a los Titulares de Certificados sobre el problema y las derivaciones a tomar como consecuencia del suceso.

En el caso de compromiso de una operación de servicio de firma electrónica o verificación de la firma electrónica de los documentos firmados o sellados, siempre que sea posible, el PCSC VIT S.A. disponibiliza a todos los Titulares de Certificados y las

terceras partes las informaciones que puedan ser utilizadas para identificar cuáles documentos pudieron haber sido afectados, a menos que viole la privacidad de los Titulares de Certificados o comprometa la seguridad de los servicios del PCSC VIT S.A.

4.6.2. RECURSOS COMPUTACIONALES, SOFTWARE Y DATOS CORROMPIDOS.

Posterior a una corrupción de recursos computacionales, software o datos el PCSC VIT S.A. realizará en forma oportuna, un reporte del incidente y una respuesta al evento.

4.6.3. SINCRONISMO DEL PCSC

La PCSC VIT S.A. mantiene sincronizado su conjunto de sistema de cómputo con el horario oficial de la República del Paraguay mediante protocolo NTP (Network Time Protocol).

4.6.4. SEGURIDAD DE LOS RECURSOS DESPUÉS DE UN DESASTRE NATURAL O DE OTRA NATURALEZA

La PCSC VIT S.A. tiene definidos planes de continuidad del negocio y recuperación ante desastres, que le permiten continuar con su operativa en la eventualidad de fallas de equipamiento y/o siniestros. Estos planes contienen análisis de riesgos de interrupción del servicio y las estrategias de recuperación propuestas, así como también ventanas máximas de interrupción aceptables.

4.7. EXTINCIÓN DE SERVICIOS DE UN PCSC

El PCSC VIT S.A. garantiza que las posibles interrupciones con los Titulares de Certificados y terceras partes, como resultado del cese de los servicios de almacenamiento de claves privadas o del servicio de firmas y/o sellos electrónicos cualificados y de verificación de las firmas y/o sellos electrónicos cualificados, serán mínimos y, en particular, asegurar el mantenimiento continuo de la información necesaria para que no haya perjuicio para sus Titulares de Certificados y terceras partes.

Antes del cese de sus servicios, el PCSC VIT S.A. ejecutara, como mínimo los siguientes procedimientos:

a) Disponibilizar a todos los Titulares de Certificados y parte usuaria, informaciones

respecto a su extinción;

b) Transfer a otro PCSC, después de la aprobación de AC Raíz-Py, las obligaciones relativas con el mantenimiento del almacenamiento de las claves, de certificados y documentos firmados o sellados, si fuera el caso, y de auditoría necesarios para demostrar el correcto funcionamiento del PCSC, por un periodo razonable;

c) mantendrá o transferirá a otro PCSC, después de la aprobación de AC Raíz-Py, sus obligaciones relativas con la disponibilidad de sus sistemas y hardware, por un período razonable;

d) notificará a todas las entidades afectadas.

El PCSC VIT S.A. proporcionará los medios para cubrir los costos de cumplimiento de estos requisitos mínimos en caso de quiebra o por otras razones que impidan cubrirlos.

5. CONTROLES DE SEGURIDAD FÍSICA, DE PROCEDIMIENTO Y PERSONAL

A continuación se describen los controles de seguridad implementados por el PCSC VIT S.A para ejecutar de modo seguro sus funciones, de conformidad con el DOC-ICPP-08 [1].

5.1. SEGURIDAD FÍSICA

La PCSC VIT S.A. mantiene controles de seguridad no técnicos (esto es, controles físicos, procedimientos y de personal) para asegurar la ejecución de las funciones de generación de clave del certificado, servicios de firma digital, autenticación y revocacióndel certificado, auditoría y almacenamiento seguro.

5.1.1 CONSTRUCCIÓN Y LOCALIZACIÓN DE LAS INSTALACIONES DEL PCSC.

LA PCSC VIT S.A. cuenta con un sitio con la infraestructura adecuada para brindar con seguridad los servicios de almacenamiento de claves privadas requeridas en la normativa vigente. Las operaciones del PCSC VIT S.A. están dentro de un ambiente de protección física que impide y previene usos o accesos no autorizados o divulgación de información sensible. Las instalaciones del PCSC VIT S.A. cuentan con seis perímetros de seguridad física:

La generación de claves criptográficas de los suscriptores se realizan en un centro de datos (Data center) situado en una infraestructura de alta seguridad conformelos perímetros de seguridad señalados.

Las instalaciones del PCSC VIT S.A. cuentan con las siguientes medidas de protección:

- Servicio de vigilancia las 24 horas;
- Ambiente alejado de sótanos para prevenir posibles inundaciones;
- El edificio está situado en un sitio de fácil y rápido acceso en caso de necesidad, por parte de los servicios de orden público y bomberos.
- El edificio está situado en una zona sin antecedentes de catástrofesnaturales y de baja actividad sísmica.
- El edificio está situado en zona de bajo nivel de delincuencia.
- EL PCSC VIT S.A. cuenta con sistema de energía y aire acondicionado redundantes;
- EL PCSC VIT S.A. cuenta mecanismos de prevención y protección contra incendios.

EL PCSC VIT S.A. cuenta con cables protegidos contra daños o interceptación electromagnética, o interceptación de la transmisión tanto de datos como de telefonía.

5.1.2. ACCESO FÍSICO EN LAS INSTALACIONES DE PCSC.

El PCSC VIT S.A. implementa un sistema de control de acceso físico que garantiza la seguridad de sus instalaciones, conforme con lo establecido en la norma ISO 27002/2022, y los requisitos que siguen.

5.1.2.1. NIVELES DE ACCESO

El PCSC VIT S.A. cuenta con un sitio con la infraestructura adecuada para brindar con seguridad los servicios de almacenamiento de claves requeridos en la normativa vigente. Las operaciones del PCSC VIT S.A. están dentro de un ambiente de protección física que impide y previene usos o accesos no autorizados o divulgación de información sensible.

Las instalaciones del PCSC VIT S.A. cuentan con seis perímetros de seguridad física:

- **Primer perímetro:** Acceso al edificio corporativo sito en España 2028 casi Brasilia, cada persona deberá ser identificada y registrada por el personal de seguridad, a partir de ese nivel personas extrañas a la operativa del PCSC VIT S.A. deberán transitar debidamente identificadas y acompañadas. A partir de este nivel, equipos de grabación, fotografía, vídeo, sonido o similares, así como los ordenadores portátiles, será controlado su ingreso y sólo pueden ser utilizados mediante la autorización formal y supervisada.
- **Segundo perímetro:** Oficina Administrativa PCSC VIT S.A.: acceso al piso donde está ubicada la oficina del PCSC VIT S.A. con recepción personal con un factor de autenticación electrónica y tarjeta de identificación visible, previa comunicación del personal de Seguridad.
- **Segundo perímetro:** Data center PCSC VIT S.A.: Esta área es un Data center con la seguridad requerida de dos factores de autenticación: lector biométrico + contraseña.
- **Tercer perímetro:** corresponde a una área interna que cuenta con dos factores de autenticación: lector biométrico + contraseña, ubicado dentro del segundo perímetro correspondiente al data center de ubicación de equipamientos tecnológicos, dividida en tres sectores (Servidores, Comunicaciones, Energía).
- **Cuarto perímetro:** corresponde al área de máxima seguridad ubicado dentro del tercer perímetro, delimitado a través de una jaula de máxima seguridad de suelo a techo con dos factores de autenticación: lector biométrico + contraseña.
- **Quinto perímetro:** Caja fuerte de máxima seguridad ubicada dentro del cuarto perímetro y para acceder al mismo se debe contar con la llave de la cerradura.
- **Sexto perímetro:** Gabinete reforzado ubicado en el interior de jaula de

máxima seguridad con cerradura antirrobo

5.1.2.2. SISTEMAS FÍSICOS DE DETECCIÓN

La seguridad de todos los ambientes del PCSC VIT S.A. deberá llevarse a cabo bajo un régimen de vigilancia 24 x 7 (veinticuatro horas al día, siete días a la semana).

La seguridad se puede lograr mediante:

a) guardia armado, uniformado, debidamente entrenado y apto para la tarea de vigilancia; o
b) circuito interno de TV, sensores de intrusión instalados en todas las puertas y ventanas, y sensores de movimiento, monitoreados local o remotamente por una compañía de seguridad especializada.

El ambiente de nivel 3 deberá ser dotado, adicionalmente, de un circuito interno de TV conectado a un sistema local de grabación 24x7. El posicionamiento y la capacidad de estas cámaras no deberían permitir la captura de contraseñas ingresadas en los sistemas.

Los medios resultantes de esta grabación deben almacenarse durante al menos 1 (un) año, en un ambiente de nivel 2.

El PCSC VIT S.A cuenta con mecanismos que permitan, en caso de falta de energía:

a) iluminación de emergencia en todos los ambientes, activada automáticamente;
b) continuidad y funcionamiento de los sistemas de alarma y del circuito interno de TV.

5.1.2.3. SISTEMA DE CONTROL DE ACCESO

El PCSC VIT S.A. cuenta con un sistema de control de acceso instalado en un ambiente de nivel 3.

5.1.3. ENERGÍA Y AIRE ACONDICIONADO DE NIVEL 3 DEL PCSC

Las áreas donde se ubican los equipos de la infraestructura tecnológica de la PCSC VIT S.A., cuentan con suministros de electricidad y aire acondicionados

adecuados a los requisitos de los equipos en ellas instalados. Los equipos del PCSC VIT S.A. se protege contra fallas en el fluido eléctrico corriente y otras anomalías en la energía: las instalaciones están equipadas con sistemas de energía primario y de respaldo para asegurar continuidad del fluido eléctrico. Las instalaciones del PCSC VIT S.A. cuentan con sistemas de aire acondicionado de precisión redundantes. El equipo instalado para climatizar el recinto es capaz de controlar la humedad relativa del mismo. Las instalaciones del PCSC VIT S.A. disponen de:

1. Sistemas de alimentación ininterrumpida (UPS por sus siglas en inglés Uninterruptible Power Supply).
2. Sistemas de UPS redundante
3. Grupo electrógeno con potencia suficiente para soportar la carga del centro de datos (Data Center), incluido los equipos informáticos y equipos de refrigeración.
4. Sistemas redundantes de aire acondicionado.

5.1.4. EXPOSICIÓN AL AGUA EN LAS INSTALACIONES DEL PCSC

El ambiente de nivel 3 del PCSC VIT S.A. está instalado en un lugar protegido contrala exposición al agua, filtraciones e inundaciones.

5.1.5. PREVENCIÓN Y PROTECCIÓN CONTRA INCENDIO EN LAS INSTALACIONES DEL PCSC

Las instalaciones del PCSC VIT S.A. donde se encuentra la infraestructura tecnológica dispone de sistemas inteligentes de detección y extinción de incendios para la protección de su contenido. El cableado está situado en un falso suelo o techo y dispone de los medios adecuados (detectores en suelo y techo) para la protección del mismo contra incendios. Las instalaciones de la PCSC VIT S.A. deberán ser construidas y equipadas para prevenir, detectar y suprimir incendios o daños producidos por la exposición a llamas o humo, y contar con procedimientos implementados para la prevención y protección al fuego

El PCSC VIT S.A. implementa mecanismos específicos para garantizar la seguridad de su personal y de sus equipamientos en situaciones de emergencia. Estos

mecanismos permiten que las puertas se desbloqueen mediante accionamiento mecánico, para l a salida de emergencia de todos los ambientes con control de acceso. La salida efectuada a través de estos mecanismos accionan inmediatamente las alarmas de apertura de las puertas.

5.1.6. ALMACENAMIENTO DE MEDIOS EN LAS INSTALACIONES DEL PCSC

La información relacionada a la infraestructura del PCSC VIT S.A. se almacena de forma segura en armarios ignífugos y cofres de seguridad, según la clasificación de la información en ellos contenida. Los cofres de seguridad son de acero o material deresistencia equivalen, y ofrece tolerancia:

- Al fuego por al menos 60 minutos.
- Aberturas forzadas.
- Posee tranca con llave manual o electrónica.
- Es suficientemente pesado, de forma a dificultar su retiro o deberá ser fijado alpiso.

El PCSC VIT S.A. se asegura el adecuado manejo y protección de los medios de almacenamiento de información, que contengan datos críticos o sensibles del sistema, contra daños accidentales (agua, fuego, electromagnetismo) y debe impedir, detectar yprevenir su uso no autorizado, acceso o su divulgación

5.1.7. ELIMINACIÓN DE RESIDUOS EN LAS INSTALACIONESDEL PCSC

El PCSC VIT S.A. implementa controles y procedimientos para la eliminación de residuos (papel, medios, equipos y cualquier otro desecho), con el fin de prevenir el uso no autorizado, el acceso o divulgación de información privada y confidencial contenida en los desechos. Los documentos y materiales sensibles son triturados antes de su eliminación. Los medios utilizados para capturar o transmitir información sensible deben ser dejados ilegibles antes de su eliminación. Los dispositivos criptográficos deben ser destruidos físicamente o su contenido dejado en cero de acuerdo a la guía del fabricante antes de su eliminación. Otros desechos deberán ser eliminados de acuerdo a los requerimientos de eliminación de desechos normales definidos por la PCSC.

5.1.8. ARCHIVO EXTERNO (OFF-SITE) DEL PCSC

La PCSC VIT S.A. cuenta con una instalación alterna, con niveles de

protección física y ambiental similar al sitio principal y con una separación física adecuada y mantiene respaldo de los datos críticos del sistema y de cualquier otra información sensible, incluyendo los datos de auditoría, en la instalación alterna y segura fuera del sitio principal. Las copias de seguridad externa deben ser establecidas y mantenidas de conformidad con la política de continuidad del negocio y el plan de recuperación frente a desastres de manera compatible con los estándares internacionales.

5.2. CONTROLES PROCEDIMENTALES

En los ítems siguientes de la DP se describen los requisitos para la caracterización y el reconocimiento de perfiles cualificados en el PCSC VIT S.A., con las responsabilidades definidas para cada perfil. Para cada tarea asociada con los perfiles definidos, son establecidos el número de personas requeridas para su ejecución.

5.2.1. PERFILES CUALIFICADOS

El PCSC VIT S.A. garantiza la segregación de tareas para las funciones críticas, a fin de evitar que un empleado o funcionario utilice indebidamente los servicios del ambiente sin ser detectado. Las acciones de cada empleado o funcionario deberán estar limitadas de acuerdo con su perfil.

El PCSC VIT S.A. deberá establecer un mínimo de 3 (tres) perfiles distintos para su operación:

a) Administrador del sistema: autorizado para instalar, configurar y mantener los sistemas de confianza, así como para administrar la implementación de las prácticas de seguridad del PCSC;
b) Operador del sistema: responsable del funcionamiento diario de los sistemas de confianza del PCSC. Autorizado para realizar copias de seguridad y recuperación del sistema.
c) Auditor del sistema: autorizado para ver archivos y auditar los registros de los sistemas de confianza del PCSC.

Todos los empleados o funcionarios del PCSC VIT S.A. deberán recibir capacitación específica antes de obtener cualquier tipo de acceso. El tipo y nivel de acceso son determinados, en un documento formal, en función de las necesidades de cada perfil.

Cuando un empleado o funcionario deja de pertenecer al plantel del PCSC VIT S.A., sus derechos de acceso deberán ser revocados de inmediato. Cuando hay un cambio en la posición o función que el empleado o funcionario ocupa dentro del PCSC, deberán ser revisados sus permisos de acceso. La PCSC mantiene una lista de revocación, con todos los recursos, antes disponibilizados, que el empleado o funcionario deberá devolver al PCSC al momento de su desvinculación.

5.2.2. NÚMEROS DE PERSONAS REQUERIDAS POR TAREA

Todas las tareas realizadas en el cofre o gabinete donde se localizan los servicios del PCSC VIT S.A. requieren la presencia de al menos 2 (dos) empleados o funcionarios con perfiles cualificados. Para los casos de copias de las claves de los usuarios, se requieren al menos 3 (tres) empleados o funcionarios con perfiles distintos y cualificados. Las otras tareas del PCSC VIT S.A. pueden ser realizadas por un solo empleado ofuncionario.

5.2.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA PERFIL

El PCSC VIT S.A. garantiza que todo empleado o funcionario tendrá su identidad y perfil verificados antes de:

a) ser incluido en una lista de acceso físico a las instalaciones del PCSC;

b) ser incluido en una lista de acceso lógico a los sistemas de confianza del PCSC;

c) ser incluido en una lista para el acceso lógico a los demás sistemas del PCSC.

Los certificados, cuentas y contraseñas utilizados para identificar y autenticar a los empleados o funcionarios deberán:

a) ser asignados directamente a un solo empleado o funcionario;

b) no ser compartidos; y

c) estar restringidos a acciones asociadas con el perfil para el que fueron creadas.

El PCSC VIT S.A. implementa un estándar para el uso de "contraseñas seguras", definido en su Política de Seguridad y de acuerdo con el correspondiente de la norma ISO 27002/2022, con procedimientos para validar esas contraseñas.

5.3. CONTROLES DE PERSONAL

LA PCSC VIT S.A. cumple con controles y procedimientos asociados a la gestión del personal involucrado en su funcionamiento como PCSC. Dichos controles y procedimientos tienen carácter de reservado para preservar su confidencialidad y evitar así revelar a terceros información del funcionamiento interno que pueda viabilizar un ataque al servicio. No obstante, son parte del alcance de las auditorías realizadas periódicamente, para garantizar a los terceros aceptantes y suscriptores el cumplimiento con la normativa vigente y los estándares internacionales de seguridad que aplican para el almacenamiento centralizado de claves. Sin perjuicio de lo anterior, la PCSC VIT S.A. declara que dichos controles y procedimientos incluyen requerimientos de calificaciones y experiencia del personal, requerimientos de capacitación continua en seguridad de la información en general y sobre servicios de almacenamiento centralizado de claves en forma específica, mecanismos de sanción por acciones no autorizadas o contravenciones a los procedimientos establecidos y requerimientos específicos para la relación con proveedores independientes, entre otros.

El PCSC VIT S.A. garantiza que todos los empleados a cargo de las tareas operativas, hayan registrado en un documento formal los siguientes términos de responsabilidad:

a) los términos y condiciones del perfil que ocuparán;

b) el compromiso de observar las políticas y reglas aplicables en el marco de la ICPP; y

c) el compromiso de no divulgar información confidencial a la que tengan acceso.

5.3.1. ANTECEDENTES, CUALIFICACIÓN, EXPERIENCIA Y REQUISITOS DE IDONEIDAD

Todo el personal del PCSC VIT S.A. involucrado en actividades directamente relacionadas con los procesos de gerenciamiento de los sistemas de almacenamiento de claves privadas, firmas o sellos electrónicos cualificados y verificaciones de firmas o sellos electrónicos cualificados deberán son admitidos de acuerdo con el ítem correspondiente de la norma ISO 27002/2022. Y además deberán:

- Haber demostrado capacidad para ejecutar sus deberes
- Haber suscripto un acuerdo de confidencialidad y disponibilidad
- No poseer otros deberes que puedan interferir o causar conflictos con los de la PCSC VIT S.A.
- No tener antecedentes de negligencia o incumplimiento de labores
- No tener antecedentes judiciales ni penales.

5.3.2. PROCEDIMIENTOS DE VERIFICACIÓN DE ANTECEDENTES

Con el propósito de resguardar la seguridad y la credibilidad de las entidades, todo el personal del PCSC VIT S.A. involucrado en actividades directamente relacionadas con los procesos de gerenciamiento de los sistemas de almacenamiento de claves privadas, firmas o sellos electrónicos cualificados y verificaciones de firmas o sellos electrónicos cualificados deberá ser sometido a:

a) verificación de antecedentes policiales y judiciales;

b) verificación del certificado de vida y residencia; y

c) comprobación de educación y del historial de trabajos anteriores.

El PCSC VIT S.A. puede definir requisitos adicionales para la verificación de antecedentes.

5.3.3. REQUISITOS DE ENTRENAMIENTO

Todo el personal del PCSC VIT S.A., involucrado en actividades directamente relacionadas con los procesos de gerenciamiento de los sistemas de almacenamiento de claves privadas, firmas o sellos electrónicos cualificados y verificaciones de firmas o sellos electrónicos cualificados deberán recibir capacitación documentada, suficiente para gestionar los siguientes temas:

a) principios y tecnologías de sistemas y hardware de almacenamiento de claves privadas, firmas o sellos electrónicos cualificadas y verificación de firmas o sellos electrónicos cualificados en uso en el PCSC;
b) ICPP;

c) principios y tecnologías para la certificación electrónica y las firmas o sellos electrónicos cualificados;

d) principios y mecanismos de seguridad de redes y seguridad del PCSC;

e) procedimientos de recuperación ante desastres y continuidad del negocio;

f) familiaridad con los procedimientos de seguridad, para las personas con responsabilidad de Oficial de Seguridad;

g) familiaridad con los procedimientos de auditoría en sistemas informáticos, para personas con la responsabilidad de Auditor de Sistemas;

h) otros asuntos relacionados con actividades bajo su responsabilidad.

5.3.4. FRECUENCIA Y REQUISITOS PARA CAPACITACIÓN TÉCNICA

Todo el personal del PCSC VIT S.A. que participe en actividades directamente relacionadas con los procesos de gerenciamiento de sistemas de almacenamiento de claves privadas, firmas o sellos electrónicos cualificados y verificaciones de firmas o sellos electrónicos cualificados deberá mantenerse actualizado ante eventuales cambios tecnológicos en los sistemas del PCSC. Como mínimo deberán recibir capacitación técnica al menos 1 (una) vez al año.

5.3.5. FRECUENCIA Y SECUENCIA DE ROTACIÓN DE CARGOS

El PCSC VIT S.A. efectúa una rotación de sus roles de confianza al menos una vez cada tres años.

Antes de asumir las nuevas labores, el personal recibe una nueva capacitación que le permita asumir las tareas satisfactoriamente.

5.3.6. SANCIONES POR ACCIONES NO AUTORIZADAS.

El PCSC VIT S.A. en la eventualidad de una acción no autorizada, real o sospechada, realizada por una persona encargada del proceso operacional del PCSC o de una AR vinculada de inmediato procederá a:

- suspender el acceso de esa persona a su sistema de certificación,
- iniciar un procedimiento administrativo para determinar los hechos y,
- si es necesario, tomar las medidas legales pertinentes.

El proceso administrativo referido en el párrafo anterior contempla, los siguientes puntos.

1. Relato de lo ocurrido con el modo de operación;
2. Identificación de los involucrados;
3. Eventuales perjuicios causados;
4. Las sanciones aplicadas, si fuere el caso.
5. Conclusiones.

Concluido el proceso administrativo, el PCSC VIT S.A. dependiendo del caso, comunicara sus conclusiones al CA Raíz. Las sanciones que podrían aplicarse como resultado de un procedimiento administrativo son:

a) Advertencia;

b) Suspensión por un plazo determinado; o

c) Impedimento definitivo de ejercer funciones en el ámbito de la ICP-Paraguay.

5.3.7. REQUISITOS PARA CONTRATAR PERSONAL.

Todo el personal del PCSC VIT S.A. involucrado en actividades directamente relacionadas con los procesos de gerenciamiento de los sistemas de almacenamiento de claves privadas, firmas o sellos electrónicos cualificados y verificación de firmas o sellos electrónicos cualificados deberá ser contratado según lo establecido en el ítem correspondiente de la norma ISO 27002/2022. Y bajo las siguientes condiciones mínimas.

- que exista un contrato con cláusulas propias de los roles de confianza y estipulasanciones para las acciones no autorizadas.
- que el PCSC VIT S.A. o RA vinculada no posea personal disponible para llenar losroles de confianza.
- que el personal a contratar cumpla con los mismos requisitos del ítem 5.3.1.
- que una vez finalizado el servicio contratado se revoquen los derechos de acceso

5.3.8. DOCUMENTACIÓN PROPORCIONADA AL PERSONAL.

EL PCSC VIT S.A. pone a disposición detodo supersonal:

a) su DP;

b) documentación operacional relacionada con sus actividades; y

c) contratos, normas y políticas relevantes para sus actividades.

Toda la documentación proporcionada al personal está clasificada de acuerdo con la política de clasificación de información definida por el PCSC VIT S.A. y debe mantenerse actualizada.

6. CONTROLES TÉCNICOS DE SEGURIDAD

En los siguientes ítems, el PCSC VIT S.A. define las medidas de seguridad implementadas para proteger las claves privadas de los Titulares de Certificados, mantener los servicios relacionados con las firmas y/o sellos electrónicos cualificados, así como el sincronismo de sus sistemas con la fuente de tiempo confiable. También son definidos otros controles técnicos de seguridad utilizados en el desempeño de sus funciones operacionales.

6.1. CONTROLES DE SEGURIDAD COMPUTACIONAL

6.1.1. DISPOSICIONES GENERALES

El PCSC VIT S.A. utiliza mecanismos de seguridad en sus estaciones de trabajo, servidores y otros sistemas y equipamientos, de conformidad con las disposiciones establecidas en los ítems correspondientes de la norma ISO 27002/2022.

6.1.2. REQUISITOS TÉCNICOS ESPECÍFICOS PARA LA SEGURIDAD COMPUTACIONAL

Los sistemas y los equipamientos del PCSC VIT S.A., utilizados en los procesos de gerenciamiento de los sistemas de almacenamiento de claves privadas, firmas o sellos electrónicos cualificados y verificaciones de firmas o sellos electrónicos cualificados, implementan, entre otras, las siguientes características:

a) control de acceso a los servicios y perfiles del PCSC VIT S.A.;

b) separación clara de tareas y atribuciones relacionadas con cada perfil cualificado del PCSC VIT S.A.;

c) uso de cifrado para la seguridad de la base de datos, cuando así lo requiera la

clasificación de sus informaciones;

d) generación y almacenamiento de registros de auditoría del PCSC VIT S.A.;

e) mecanismos internos de seguridad para garantizar la integridad de los datos y procesos críticos; y

f) los mecanismos de copia de seguridad (*backup).*

Estas características deberán ser implementadas por los sistemas operacionales del PCSC y con los mecanismos de seguridad física.

Cualquier equipamiento, o parte de él, cuando sea enviado para mantenimiento deberá tener la información sensible contenida en él, eliminado, además deberá ser controlado su número de serie, así como las fechas de envío y recepción del mismo. Al regresar a las instalaciones del PCSC VIT S.A., el equipamiento que pasó por mantenimiento deberá ser inspeccionado. De todo equipamiento que dejará de ser utilizado permanentemente y sujeto a las disposiciones del acto de eliminación, deberá ser destruida de manera definitiva toda información sensible almacenada relacionada con la actividad del PCSC VIT S.A. Todos estos eventos deberán ser registrados para fines de auditoría.

Cualquier equipamiento incorporado en el PCSC VIT S.A. deberá ser preparado y configurado según lo dispuesto en la Política de Seguridad implementada o en otro documento aplicable, a fin de preservar el nivel de seguridad necesario parasu propósito.

6.1.3. CLASIFICACIÓN DE SEGURIDAD COMPUTACIONAL

Los sistemas sensibles del PCSC VIT S.A. están en un ambiente informático dedicado y aislado, son de alta seguridad y confiabilidad, con procesos de auditoría de acuerdo a criterios tales como Trusted System Evaluation Criteria (TCSEC), Canadian Trusted Products Evaluation Criteria, European Information Technology Security Evaluation Criteria (ITSEC), Common Criteria e eIDAS.

6.2. CONTROLES TÉCNICOS DEL CICLO DE VIDA

La PCSC VIT S.A., mantiene procedimientos y controles implementados para el desarrollo de los sistemas y del gerenciamiento de la seguridad.

6.2.1. CONTROLES DE DESARROLLO DEL SISTEMA

Los requisitos de seguridad son exigibles, desde su inicio, tanto en la adquisición de sistemas informáticos como en el desarrollo de los mismos ya que puedan tener algún impacto sobre la seguridad de la PCSC VIT S.A. La PCSC mantiene controles que proporcionen una seguridad razonable de las actividades de desarrollo y mantenimiento de los sistemas de la PCSC.

Los nuevos sistemas o para la expansión de los sistemas existentes, se deben especificar los requisitos de control, seguir procedimientos de prueba y control de cambios para la implementación de software. Toda la documentación del ciclo de vida del sistema, debe estar disponible para su verificación.

La PCSC VIT S.A. mantiene los controles sobre el acceso a las bibliotecas fuente de programas.

6.2.2. CONTROLES DE GESTIÓN DE LA SEGURIDAD

EL PCSC VIT S.A. mantiene un inventario de todos los activos informáticos y realizará una clasificación de los mismos de acuerdo con sus necesidades de protección, coherente con el análisis de riesgos efectuado. La configuración de los sistemas se audita de forma periódica para asegurar el cumplimiento de los estándares de implementación deseguridad.

6.2.3. CICLO CLASIFICACIONES DE SEGURIDAD VIDA

Existen controles de seguridad a lo largo de todo el ciclo de vida de los sistemas con algún impacto en la seguridad de la ICPP.

El PCSC VIT S.A. realiza controles para proporcionar seguridad al dispositivo que realiza la generación de las claves de los suscriptores. Para evitar posibles incidencias en los sistemas se establecen los siguientes controles:

- El hardware de generación de claves es probado antes de su puesta enproducción.
- La generación de claves se producen dentro de los módulos criptográficos que cumplan los requisitos, técnicos, legales y del negocio.
- Los procedimientos para el almacenamiento seguro del hardware criptográfico y los materiales de activación después de

la ceremonia de generación de claves.

6.3. CONTROLES DE SEGURIDAD DE REDES

6.3.1. DISPOSICIONES GENERALES

La PCSC VIT S.A. mantiene los controles relacionados con la seguridad de la red, incluyendo el firewall y recursos similares, observando las disposiciones establecidas en el ítem 13. "seguridad en las telecomunicaciones" de la norma ISO 27002/2012.

Todos los servidores y elementos de la infraestructura y protección de red, tales como: enrutadores, hubs, switches, firewalls y sistemas de detección de intrusos (IDS), localizados en el segmento de red que aloja los sistemas del PCSC, deberán estar ubicados y en funcionamiento al menos en el nivel 3.

Las versiones más recientes de los sistemas operacionales y las aplicaciones de los servidores, así como las correcciones (*parches*) disponibilizados por los respectivos fabricantes deberán ser implementadas inmediatamente después de las pruebas en un ambiente de desarrollo o de homologación.

El acceso lógico a los elementos de la infraestructura y protección de red deberá ser restringido a través de un sistema de autenticación y autorización de acceso. Los enrutadores conectados a redes externas deberán implementar filtros de paquetes de datos, que permitan solamente conexiones a los servicios y servidores previamente definidos como sujeto a acceso externo.

El acceso a Internet es proporcionado por al menos dos líneas de comunicación desde diferentes sistemas autónomos.

El acceso vía red a los sistemas del PCSC es permitido para los siguientes servicios:

a) por el PCSC VIT S.A., para la administración de los sistemas de gestión desde equipos conectados por una red interna o por VPN establecida por medio de una direcciónIP fija previamente registrada.

b) por el Titular del Certificado, para el almacenamiento y acceso a la clave privada y servicios de firma electrónica cualificada y verificación de la firma electrónica

cualificada.

6.3.2. FIREWALL

Los mecanismos de *firewall* son implementados en equipos para usos específicos, configurados exclusivamente para esa función. Los *firewalls* deberán estar dispuestos y configurados de forma a promover el aislamiento, en sub-redes específicas, los equipos servidores con acceso externo (denominada "zona desmilitarizada" (DMZ)) en relación a los equipos con acceso exclusivamente interno al PCSC.

El *software* de firewall, entre otras características, deberá implementar registros de auditoría.

El oficial de seguridad deberá verificar periódicamente las reglas del *firewall*, para garantizar que solo se permita el acceso a los servicios realmente necesarios y permitidos, y que se bloquee el acceso a puertos innecesarios o no utilizados.

6.3.3. SISTEMA DE DETECCIÓN DE INTRUSOS (IDS)

El IDS deberá tener la capacidad de ser configurado para reconocer ataques en tiempo real y responder automáticamente, con medidas tales como: enviar trampas SNMP, ejecutar programas definidos por la administración de la red, enviar correos electrónicos a los administradores, enviar mensajes de alerta al *firewall* o terminal de administración, para desconectar automáticamente conexiones sospechosas o para reconfigurar el *firewall.*

El IDS deberá ser capaz de reconocer diferentes patrones de ataque, inclusive contra el propio sistema, presentando la posibilidad de la actualización de su base de reconocimiento.

El IDS debe proporcionar el registro de eventos en *logs*, recuperables en archivos de tipo texto, además de implementar la gestión de la configuración.

6.3.4. REGISTRO DE ACCESO NO AUTORIZADO A LA RED.

Las tentativas de acceso no autorizado en ruteadores, Firewall o IDS, deberán ser registradas en archivos para posterior análisis, que podrá ser automatizada. La frecuencia

de examen de los archivos de registro deberá ser, como mínimo, diario y todas las acciones tomadas como resultado de este examen deben ser documentadas.

6.3.5. OTROS CONTROLES DE SEGURIDAD DE RED

El PCSC implementa un servicio *proxy*, restringiendo el acceso, desde todas sus estaciones de trabajo, a servicios que puedan comprometer la seguridad del ambiente del PCSC.

Las estaciones de trabajo y servidores deberán estar equipados con antivirus, *antispyware* y otras herramientas de protección contra las amenazas que emanan de la red a la que están vinculados.

6.4. CONTROLES DE INGENIERÍA DEL MÓDULO CRIPTOGRÁFICO

El Módulo criptográfico de generación de claves asimétricas para el suscriptor de la PCSC VIT S.A. cumple con los requerimientos y estándar definidos en el documento **NORMAS DE ALGORITMOS CRIPTOGRAFICOS DE LA ICPP** del Ministerio De Industria Y Comercio.

7. POLÍTICAS DE FIRMA

Adicionalmente a la gestión y almacenamiento de claves privadas de personas físicas o jurídicas, el PCSC VIT S.A. brinda el servicio de firma que facilite a los suscriptores la utilización de su clave privada de firma digital en custodia centralizada. El servicio de firma ofrecido por el PCSC VIT S.A. establece mecanismos seguros para realizar firmas digitales únicamente por orden del firmante. A continuación, se definen una serie de consideraciones técnicas para el servicio de firma que permite el uso de la clave de firma digital en custodia centralizada.

7.1 SERVICIO DE FIRMA

El servicio es desarrollado tomando en cuenta estándares internacionales para el desarrollo seguro. El PCSC VIT S.A. dispone de documentación para desarrolladores para la integración a su servicio de firma, quedando a criterio del PCSC la definición de las condiciones para su uso y/o integración. Independientemente de la implementación del servicio de firma, en todo momento se asegura el exclusivo control del firmante sobre su clave privada de firma digital en custodia

7.2 AUTENTICACIÓN DEL SUSCRIPTOR

La autenticación del suscriptor durante el proceso de solicitud del certificado se asocia al mismo los medios de identificación digital necesarios para la autenticación electrónica requerida por el servicio de firma.

El PCSC VIT S.A. garantiza un nivel de fortaleza en el proceso de autenticación electrónica equivalente o superior a AAL2 definido por el NIST y por tanto proporcionar un alto grado de confianza, en que la persona solicitante de una autenticación electrónica para el uso de su clave privada en custodia centralizada, es poseedora de los medios de identificación digital que le fueron asociados durante el registro de identificación presencialen la solicitud del certificado.

7.3 FORMATOS DE FIRMAS

La generación de firmas cualificadas resultantes de uso del servicio de firma está en conformidad a lo dispuesto en el documento **NORMAS DE ALGORITMOS CRIPTOGRAFICOS DE LA ICP-PARAGUAY** del Ministerio De Industria Y Comercio.

8. AUDITORÍAS Y EVALUACIONES DE CONFORMIDAD

8.1 INSPECCIÓN DE CUMPLIMIENTO Y AUDITORÍA

El PCSC VIT S.A. será auditado, al menos cada veinticuatro (24) meses, corriendo con los gastos que ello genere, por un OEC. La finalidad de la auditoría es confirmar que el PCSC VIT S.A., como los servicios de confianza cualificados que presta, cumplen con los requisitos establecidos en esta DP y en la normativa vigente. El PCSC VIT S.A. enviará un informe de evaluación de la conformidad correspondiente a la AC Raíz-Py en el plazo de 3 (tres) días hábiles tras su recepción.

Sin perjuicio de lo dispuesto en el párrafo anterior, la AC Raíz-Py podrá en cualquier momento auditar o solicitar a un OEC que realice una evaluación de conformidad al PCSC VIT S.A. que correrá con los gastos de la misma., para confirmar que tanto el PCSC como los servicios de confianza cualificados que presta cumplen los requisitos de esta DP y de la normativa vigente.

La PCSC VIT S.A., implementa un programa de auditorías internas conforme a lo estipulado en el ítem correspondiente de la norma ISO 27002/2022 para la

verificación de su sistema de gestión.

Cuando la AC Raíz-Py requiera al PCSC VIT S.A. que corrija el incumplimiento de requisitos de esta DP o de la normativa vigente, y el mismo no actúe en consecuencia, en su caso, en el plazo fijado por la AC Raíz-Py, la AC Raíz-Py, teniendo en cuenta en particular el alcance, la duración y las consecuencias de este incumplimiento, puede retirar la cualificación al prestador o al servicio que este presta y actualizar la lista de confianza. La AC Raíz-Py comunicará al PCSC la retirada de su cualificación o de la cualificación del servicio de que se trate.

Tales supervisiones son efectuadas conforme a las disposiciones en materia de auditoría, reglamentadas por la AC Raíz-Py.

El PCSC VIT S.A. está obligado al cumplimiento de las auditorías, éstas permiten establecer una confianza razonable en el marco de la ICPP.

La disposición o resolución que ordena una Auditoría o evaluación no es recurrible.

9. OTROS ASUNTOS COMERCIALES Y LEGALES

9.1. OBLIGACIONES Y DERECHOS

En los siguientes ítems son incluidas las obligaciones generales de las entidades involucradas. Si se implementan obligaciones específicas, las mismas deben son descritas.

9.1.1. OBLIGACIONES DEL PCSC

El PCSC VIT S.A. es responsable de la DP, contendiendo, al menos, las que se enumeran a continuación:

a) operar de acuerdo con su DP y la descripción de los servicios que realiza;

b) gestionar y garantizar la protección de las claves privadas de los Titulares de Certificados;

c) mantener el PCSC sincronizado con una fuente confiable de tiempo ajustado con la fecha y hora oficial paraguaya;

d) tomar las medidas apropiadas para garantizar que los Titulares de Certificados y

demás entidades involucradas conozcan sus respectivos derechos y obligaciones;

e) supervisar y controlar el funcionamiento de los servicios prestados;

f) notificar al Titular del Certificado, cuando su clave privada se ve comprometida y solicitar la revocación inmediata del certificado correspondiente o la finalización de sus actividades;

g) publicar en su sitio web la DP y las Políticas de Seguridad (PS) aprobadas que implementa;

h) publicar, en su sitio web, la información definida en el punto 2.1.1 de este documento;

i) identificar y registrar todas las acciones realizadas, de acuerdo con las normas, prácticas y reglas establecidas en el marco de la ICPP por la AC Raíz-Py;

j) adoptar las medidas de seguridad y control previstas en la DP, en el Procedimiento Operativo y Política de Seguridad que implementa, involucrando sus procesos, procedimientos y actividades, observando los estándares, criterios, prácticas y procedimientos de la ICPP;

k) mantener la conformidad de sus procesos, procedimientos y actividades con las normas, prácticas y reglas de la ICPP, y con la legislación vigente;

l) mantener y garantizar la integridad, confidencialidad y seguridad de la información tratada por ella;

m) mantener y probar anualmente su PCN;

n) mantener un seguro que cubra la responsabilidad civil derivada de la actividad y el almacenamiento de claves privadas para usuarios finales, con cobertura suficiente y compatible con el riesgo de estas actividades;

o) informar a los Titulares de Certificados que contratan sus servicios sobre la cobertura, las condiciones y las limitaciones estipuladas por la póliza de seguro de responsabilidad civil contratada en los términos anteriores; y

p) informar a AC Raíz-Py, mensualmente, el número de claves privadas o los certificados electrónicos correspondientes almacenados y las firmas realizados y verificados.

9.1.2. OBLIGACIONES DEL SUSCRIPTOR

El Titular del Certificado debe asegurarse, a través de las aplicaciones disponibles al aceptar el servicio de la PCSC VIT S.A., que su par de claves y/o certificados electrónicos se hayan almacenado correctamente y que la clave privada utilizada para firmar o sellar esté funcional.

9.1.3 DERECHOS DEL TERCERO (RELYING PARTY)

Se considera que el tercero es la parte usuaria que confía en el contenido, la validez y la aplicabilidad del servicio de firma electrónica, y de la verificación de la firma electrónica.

Constituyen derechos de tercera parte:

a) rehusarse a utilizar el servicio de firma electrónica cualificada y de verificación de la firma electrónica cualificada de documentos electrónicos prestados por el PCSC para fines distintos de su propósito de uso en el marco de la ICPP.

b) verificar, en cualquier tiempo, la validez de firma electrónica cualificado. Una firma electrónica cualificada en el marco de la ICPP se considera válido cuando:

i. el certificado electrónico no aparece en la CRL del PCSC emisor;
ii. la clave privada utilizada para firmar electrónicamente no ha sido comprometida en el momento de la verificación;
iii. puede ser verificada utilizando la cadena de certificados que lo generó;
iv. el propósito del uso está de acuerdo con lo definido en la política del certificado electrónico de los firmantes.

El incumplimiento de estos derechos no elimina la responsabilidad del PCSC VIT S.A. y del titular del certificado.

9.2. RESPONSABILIDADES

9.2.1. RESPONSABILIDADES DEL PCSC

El PCSC VIT S.A. responderá por cualquier daño causado en perjuicio del titular del certificado. En cambio puede rechazar todas las garantías del servicio que no se encuentren vinculadas a obligaciones de los Prestadores de Servicios de Almacenamiento habilitados bajo subordinación de la CA RAÍZ, establecidas por la legislación vigente en materia.

9.3. RESPONSABILIDAD FINANCIERA

9.3.1. INDEMNIZACIONES A TERCEROS (RELYING PARTY)

Se establece la inexistencia de responsabilidad del tercero (*relying party*) ante el PCSC VIT S.A., excepto en el caso de un acto ilegal.

9.3.2. RELACIONES FIDUCIARIAS

La PCSC VIT S.A. indemniza íntegramente los daños que se demuestre causar, cuando el titular del certificado es una persona física.

En situaciones justificables, la indemnización puede ser limitada cuando el titular del certificado es una persona jurídica.

9.3.3. PROCEDIMIENTOS ADMINISTRATIVOS

El suscriptor que sufre daños resultantes de las operaciones de la PCSC VIT S.A. tiene derecho a notificar al mismo que quiere la indemnización prevista en el punto 9.3.2 anterior que ha sido acreditada mediante examen pericial realizado por experto especializado e independiente.

9.4. INTERPRETACIÓN Y EJECUCIÓN

9.4.1. LEGISLACIÓN

Esta DP se rige por la ley 6822/21, así como las resoluciones y normativas vigentes de la ICPP.

9.4.2. FORMA DE INTERPRETACIÓN Y NOTIFICACIÓN.

Se realizarán notificaciones o cualquier otra comunicación necesaria con respecto a las prácticas descritas en esta DP a través de mensaje electrónico firmado digitalmente, con clave pública certificada por la ICP-Paraguay, o por escrito y

entregado a PCSC VIT S.A.

9.4.3. PROCEDIMIENTOS DE RESOLUCIÓN DE DISPUTAS

En la eventualidad de cualquier disputa que implique los servicios o prestaciones que incluye esta DP y normativa vigente, la parte afectada notificará primero al PCSC VIT S.A. y a todas las partes interesadas con relación a la disputa. El PCSC VIT S.A. asignará al personal adecuado para resolver el litigio extrajudicialmente.

La DP del PCSC VIT S.A. no prevalece sobre las reglas, criterios, prácticas y procedimientos establecidos por el MIC.

Los casos omitidos deberán ser remitidos para su consideración a la CA Raíz-Py.

9.5. LAS TASAS DE SERVICIO

El PCSC VIT S.A. define una política tarifaria variable conforme a la definición comercial y de reembolso aplicable, si fuera el caso, así como los costos asociados al servicio de:

a) almacenamiento de claves privadas para los usuarios finales;

b) de firma electrónica cualificado y de verificación de firma electrónica cualificada;

c) otras tarifas.

9.6. CONFIDENCIALIDAD

9.6.1. DISPOSICIONES GENERALES

La clave privada de los Titulares de Certificados será mantenida por el PCSC VIT S.A., que será responsable de su confidencialidad, manteniendo registros de auditoría con la hora y fecha de acceso disponibles para el Titular del Certificado.

Las firmas electrónicas cualificadas como las verificaciones de firmas electrónicoa cualificadas podrán ser realizados por el PCSC VIT S.A., quien será responsable de su confidencialidad, manteniendo los registros de auditoría sincronizados con la hora y fecha una fuente UTC confiable ajustados a la fecha y hora

paraguaya, inclusive pudiendo identificar cuál documento, IP o URL, entre otros, que deben ser previamente autorizados por el Titular del Certificado, fueron firmados o sellados con la clave privada del Titular del Certificado.

Los documentos firmados o sellados electrónicamente por los Titulares de Certificados podrán ser conservados por el PCSC VIT S.A., siempre que se acuerde expresamente con el Titular del Certificado y de conformidad con la legislación vigente.

9.6.2. TIPOS DE INFORMACIONES CONFIDENCIALES

Como principio general, cualquier documento, información o registro proporcionado a PCSC VIT S.A. por los suscriptores es confidencial.

Como principio general, no se divulga ningún documento, información o registro proporcionado por el suscriptor al PCSC VIT S.A., excepto cuando se llega a un acuerdo con el titular del certificado para su publicación más amplia.

9.6.3. TIPOS DE INFORMACIÓN NO CONFIDENCIALES

En este ítem, son indicados los tipos de informaciones consideradas no confidenciales por el PCSC VIT S.A., las cuales deberán comprender, entre otros:

a) los certificados del Titular del Certificado;

b) la DP del PCSC VIT S.A.;

c) versiones públicas de su Política de Seguridad; y

d) la conclusión de los informes de auditoría.

9.6.4. INCUMPLIMIENTO DE LA CONFIDENCIALIDAD POR RAZONES LEGALES

El PCSC VIT S.A. proporciona documentos, información o registros bajo su custodia, por orden judicial.

9.6.5. INFORMACIÓN A TERCEROS

No se proporcionará a ninguna persona ningún documento, información o registros en poder de la PCSC VIT S.A., excepto cuando la persona que lo solicite, por medio de un instrumento debidamente constituido, esté autorizado para hacerlo y esté correctamente identificado.

9.6.6. OTRAS CIRCUNSTANCIAS DE DIVULGACIÓN DE INFORMACIÓN

No aplica.

9.7. DERECHOS DE PROPIEDAD INTELECTUAL

LA PCSC VIT S.A. es la propietaria de la presente Declaración de Prácticas, de sus Políticas de Certificación y de las aplicaciones de su sistema de almacenamiento centralizado de certificados. Quedan excluidos los derechos de propiedad intelectual e industrial derivados de aplicaciones que integran el sistema de almacenamiento centralizado y que sean propiedad de un tercero. Para elaboración de la DP de la PCSC VIT S.A. se han recogido las exigencias de las DIRECTIVAS OBLIGATORIAS PARA LA FORMULACION Y ELABORACION DE PRACTICAS DE CERTIFICACIÓN DE LOS PRESTADORES DE SERVICIO DE ALMACENAMIENTO DE LA ICP PARAGUAY, y se ha hecho referencia directa y uso de especificaciones, términos y en algunos casos contenido de la misma para asegurar plena subordinación y concordancia con la CA RAÍZ.

10. DOCUMENTOS DE REFERENCIA

10.1 REFERENCIAS

- Ley Nº 6822/2021 “De los servicios de confianza para las transacciones electrónicas, del documento electrónico y los documentos transmisibles electrónicos.”
- RFC 4210: Internet X.509 Public Key Infrastructure. Certificate Management Protocol (CMP).
- RFC 4211: Internet X.509 Public Key Infrastructure. Certificate Request Message Format (CRMF).
- RFC 2030: Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI.
- RFC 3447: Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography. Specifications Version 2.1.
- RFC 3647: Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework.

- Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo del 23 de julio de 2014 - relativo a la identificación electrónica y los servicios de confianza para transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.
- NORMA ISO/IEC 27002:2022

10.2. REFERENCIAS A DOCUMENTOS QUE COMPONEN LA ICPP

Tabla Nº2 – Documentos Referenciados

REF.	NOMBRE DEL DOCUMENTO	CÓDIGO
[1]	Procedimientos operacionales mínimos para el servicio de generación o gestión de datos de creación de firma electrónica y/o sello electrónico.	DOC-ICPP-08
[2]	Directivas obligatorias para la formulación y elaboración de la política de certificación de los Prestadores Cualificados de Servicios de Confianza de la ICPP.	DOC-ICPP-04
[3]	Directivas obligatorias para la formulación y elaboración de la declaración de prácticas de certificación de los prestadores cualificados de servicios de confianza de la ICPP.	DOC-ICPP-03
[4]	Normas de algoritmos criptográficos de la ICPP	DOC-ICPP-06
[5]	Criterios y procedimientos para realización de auditorías en las entidades miembros de la ICPP	DOC-ICPP-12