Proveedor de Certificados PROCERT ITFB, C. A.
Política de Certificado Electrónico para OCSP

Fecha	Diciembre 2023
Edición	2
Elaborado por	Operaciones
Aprobado	Alta Dirección diciembre 2023
Descripción	Política de Certificado Electrónico para OCSP

Índice

1. Control De Versiones

Versión	Motivo de Cambio	Publicación	Vigencia
Edición 01	**Emisión**	**08/12/2023**	**No**
Edición 02	**Control, Revisión y Ajuste Semestral (Actualización – CURVA ELIPTICA)**	**13/09/2024**	**Si**

2. Título: Política de certificado electrónico para OCSP.

3. Código: AC-D-0012.

4. Introducción: El PSC PROCERT procede a la emisión y publicación de presente documento de la política de certificado electrónico para OCSP, el cual tiene como fin, documentar, informar a la alta dirección, personal, y parte interesada del PSC PROCERT, cerca del uso autorizado y soporte técnico del certificado para servicio OSCP. El certificado para el servicio OCSP es para uso interno de la plataforma tecnológica de certificación del PSC PROCERT. La presente política se encuentre ajustada a los mandatos impuestos por el Decreto Ley de Mensajes de Datos y Firmas Electrónicas (LSMDFE), su Reglamento y marco normativo que regula la materia dentro de la República Bolivariana de Venezuela

5. Objetivo: La presente política de certificado para OCSP, se constituye en la guía de mejores principios de gestión y operación del PSC PROCERT aplicables a la generación y uso del certificado electrónico para OCSP; los cuales deben ser documentados e informados a todos los clientes, proveedores y parte interesada contratantes de certificados electrónicos. Las actividades desarrolladas por el PSC PROCERT en el área de certificación electrónica, se encuentran reguladas por el Decreto Ley de Mensajes de Datos y Firmas Electrónicas y su Reglamento, como marco normativo y de referencia. La supervisión por parte del Estado Venezolano será ejercida por la SUSCERTE. Los certificados para OCSP no tendrán un fin comercial y se generan para el cumplimiento del estándar legal y técnico aplicable a las plataformas de certificación electrónica abiertas.

6. Alcance: La presente política de certificado electrónico para OCSP del PSC PROCERT, aplica a la alta dirección, empleados y consultores de la AC del PSC PROCERT, conforme a los lineamientos impuestos por la SUSCERTE.

7. Limitaciones: La presente política de certificado electrónico para OCSP del PSC PROCERT se constituye en el marco referencial acerca del PSC PROCERT, suministrando la información requerida para la compresión y documentación de los procesos asociados a la generación de certificados para OCSP.

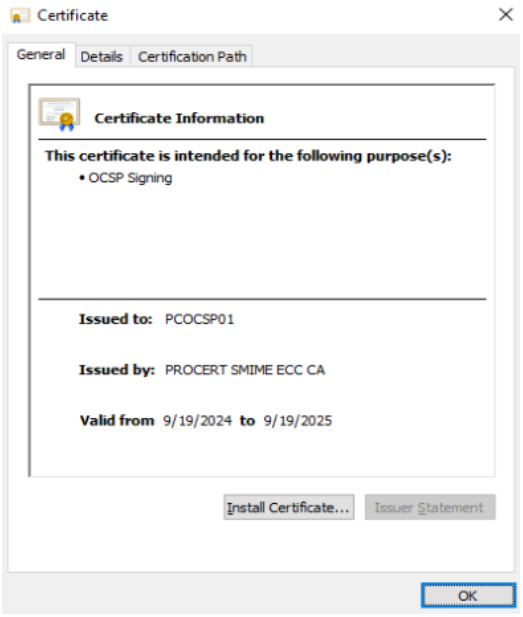
8. Usos de los certificados: La AC tiene la capacidad de generar certificados de firma electrónica con clave desde 2048 hasta 4096, según corresponda el tipo de certificado a emitir. Se describe a continuación el certificado electrónico para OCSP.

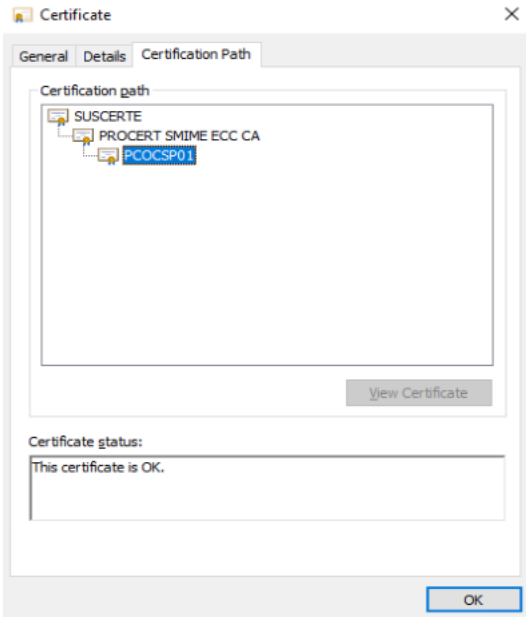
8.1. Certificado electrónico para OCSP: Los Certificados para OCSP se utilizan dentro de la Plataforma Tecnológica de Certificación del PSC PROCERT, a los fines de dar cumplimiento al estándar nacional e internacional y nos permiten validar el estado de los certificados emitidos por el PSC PROCERT. Comprobando que es correcto y que no está revocado, permitiendo una mayor

seguridad en las transacciones. El uso asignado al certificado para OCSP es el siguiente:

- Determinar el estado de vigencia de un certificado digital X.509 usando otros medios que no sean el uso de CRL.
- Brindar confianza en el usuario de los certificados emitidos por el PSC PROCERT.

8.2. Vista del certificado para OSCP





8.3. Estructura del certificado electrónico para OCSP

Nombre del campo	Valor
Versión	**V3** (Número de versión).
Serial number	550000000318d927bbbe7a8e3600000000000 3
Algoritmo de Firma	sha384ECDSA
Algoritmo del hash de Firma	sha384
Datos del emisor	
CN	PROCERT SMIME ECC CA
C	VE
O	Proveedor de Certificados PROCERT ITFB
Período de validez	
Valid From	Fecha de emisión del Certificado
Valid To	Fecha de vencimiento del certificado
SUJETO	
CN	PCOCSP01

O	Proveedor de Certificados PROCERT ITFB
C	VE
Clave Pública	RSA (2048 Bits)
Uso Extendido de la llave	OCSP SIGNING
OCSP non revocation cheking	05 00
Identificados de la llave del sujeto	317e81418e30a53e5c7f4c43dc946688978697ef (Identificador de las subject key en el certificado)
Identificador de la llave de la autoridad	
Key ID	Id. de clave=bf431617e0356fce635b859bed5174263a7680b8
Basic Constraitns	
Subject Type	End Entity
Path Length Constraint	None
Key Usage	Digital Signature

8.4. Usos permitidos: El uso del certificado subordinado del PSC PROCERT estará limitado a la firma de certificados electrónicos para autoridades subordinadas, firma de las listas de certificados revocados y la firma de todos los certificados establecidos en el presente documento. El uso del certificado electrónico para OCSP emitido por el PSC PROCERT es el siguiente:

Tipo de certificado	Uso	Uso mejorado
Certificado electrónico para OCSP	Firma electrónica	Firma OCSP

8.5. Usos no permitidos: La generación del certificado para OCSP corresponde a requerimientos técnicos y legales. Solo será utilizado para la plataforma de certificación del PSC PROCERT**.** La Alta Dirección, empleados, consultores y parte interesada del PSC PROCERT se obligan a utilizarlos conforme a los usos permitidos y señalados en la sección anterior y los establecidos por el Decreto con Fuerza de Ley Sobre Mensajes de Datos y Firmas Electrónicas, sus Reglamentos y otras normas de carácter sub-legal vigentes o cualquier texto normativo que los sustituya y regule la actividad de certificación electrónica dentro de la República Bolivariana de Venezuela y para el uso para el cual fue emitido, quedando expresamente indicado que cualquier violación a las normas, usos y/o leyes de la República Bolivariana de Venezuela queda bajo la responsabilidad del empleado del PSC PROCERT que cometa el acto o ejecute la acción, así como los daños y perjuicios que ocasionare y en un todo le serán aplicable las previsiones que al efecto estén contenidas en la Ley de ilícitos

Informáticos y supletoriamente el Código Penal y Procesal Penal venezolano. Adicionalmente le será revocado el certificado electrónico.

9. Políticas de administración de la AC: Las políticas de administración de la AC son las señaladas en el aparte 11 de la declaración de prácticas de certificación (DPC) (AC-D-0003).

10. Publicación de información del PSC y repositorios de los certificados.

10.1. Repositorios: A fin de garantizar la completa disponibilidad de este documento de la política de certificado de firma electrónica para OCSP, el PSC PROCERT mantiene un repositorio dentro de su Página Web:

- http://www.procert.net.ve/.
- Para el certificado de la AC Subordinada PROCERT, los certificados emitidos por dicha AC y la DPC**:** http://www.procert.net.ve/ac.html
- Para la lista de certificados revocados: http://www.procert.net.ve/ecc-crl/smime-ca.crl
- Para el servicio de validación en línea (OCSP): ocspsmime.procert.net.ve/ocsp

El repositorio público del PSC PROCERT, no contiene ninguna información confidencial o privada.

10.2. Publicación: Es obligación para el PSC PROCERT publicar la información relativa a sus prácticas, sus certificados y el estado actualizado de dichos certificados. Las publicaciones que realice el PSC PROCERT, de toda la información clasificada como pública, se anunciara en su respectiva página web de la siguiente forma:

- La lista de certificados revocados (LCR), se encuentra disponible en formato CRL V2, en: http://www.procert.net.ve/ecc-crl/smime-ca.crl
- El presente documento se encuentra disponible en: http://www.procert.net.ve/ac.html
- El certificado de la AC Subordinada PROCERT se encuentra disponible en: http://www.procert.net.ve/ac.html
- Los certificados emitidos por la AC Subordinada PROCERT se encuentran en https://www.procert.net.ve/ConsultaPublica/index.aspx
- Los datos de contacto del PSC PROCERT en la dirección: https://www.procert.net.ve/index.html#contacto
- La documentación técnica del PSC Procert en la dirección: http://www.procert.net.ve/ac.html

10.3. **Frecuencia de publicación**.

10.3.1. Certificados del PSC: EL periodo de validez es de diez (10) años.

10.3.2. Lista de certificados revocados (LCR): La publicación de la lista de certificados revocados se realizará cada 24 horas.

10.3.3. Declaración de prácticas de certificación: A menos que explícitamente se indique lo contrario en este documento de la política de certificado para OCSP, se publicarán en la página web del PCS PROCERT (www.procert.net.ve), las nuevas versiones de este documento, inmediatamente tras la aprobación de estas.

11. Identificación y autenticación: Las características de la identificación señalados en el numeral 16 y procedimientos para la validación son las señaladas en los apartes 14 y 15 de la declaración de prácticas de certificación (DPC) (AC-D-0003).

12. Controles de acceso al repositorio de certificados: El acceso a la información publicada por el PSC PROCERT será de consulta y no podrá ser modificada por personas no autorizadas. La información pública solo será actualizada por el personal encargado de esa función que labora en el PSC PROCERT; además se garantiza la consulta de la LCR y al OCSP.

13. Tramitación de solicitud de un certificado.

13.1. Solicitud de emisión: Al ser un certificado no comercial, la generación, trámite y emisión del certificado para OCSP, debe cumplir los procesos internos del PSC PROCERT, respecto a su debido trámite, configuración y emisión, conforme a las normas legales y técnicas aplicables dentro y fuera de la República Bolivariana de Venezuela.

14. Emisión de Certificado.

14.1. Acciones de la AC durante la emisión de un certificado: Para la emisión del certificado para OCSP se deberá cumplir el control de cambios previamente documentado y aprobado por las instancias correspondientes dentro del PSC PROCERT

14.2. Emisión del certificado para OCSP: Una vez sea emitido el certificado para OCSP, el mismo será instalado en la plataforma Tecnológica de Certificación del PSC PROCERT, debiendo cumplir con el protocolo de acceso al centro de datos.

15. Uso del par de claves y del certificado.

15.1. Uso de la clave privada del certificado: El equipo técnico genera el CSR para la emisión del certificado de OCSP, quedando almacenado en el servidor desde donde se ejecutará el servicio de OSCP.

15.2. Uso de la clave pública y del certificado por los terceros de buena fe: El certificado de raíz de certificación de la AC se hace público a los efectos de la validación de la ruta. La huella del certificado y los certificados de la infraestructura de clave pública (ICP) de la AC del PSC PROCERT están disponibles en la página web del PSC PROCERT (www.procert.net.ve). Los usos asignados a los certificados se encuentran definidos en el aparte 9.7.1 de la declaración de prácticas de certificación (DPC) y política de certificados (PC) de PROCERT.

16. Renovación del certificado con cambio de clave.

16.1. Causas para la renovación de un certificado: Todo certificado electrónico generado por el PSC PROCERT para OCSP podrá ser renovado, siempre y cuando sean cumplidas las condiciones siguientes:

16.1.1. Que se haya cumplido el término de vigencia de la firma o certificado electrónico del cual es propietario.

16.1.2. Que la firma o certificado electrónico no haya sido revocado por el PSC PROCERT por razones de uso ilícito de la firma o certificado electrónico, según corresponda.

16.1.3. Que el solicitante cumpla con el proceso de interno del PSC PROCERT para la emisión de los certificados de la Plataforma Tecnológica de Certificación.

16.2. Entidad que puede solicitar la renovación del certificado OCSP: El gerente General, el coordinador de Tecnología y el encargado de PKI del PSC PROCERT actuarán de forma conjunto en el proceso de trámite, generación, aprobación de emisión y emisión del certificado electrónico de OCSP.

16.3. Procedimiento de solicitud para renovación de un certificado: El Consultor de tecnología o el encargado de PKI, solicitaran al Gerente General la emisión del certificado OSCP**.** La emisión del certificado para OCSP será sometido al Comité de Seguridad del PSC PROCERT y luego de su aprobación se procederá con el trámite, gestión y emisión correspondiente.

16.4. Notificación de la instalación del certificado OCSP: El Consultor de tecnología o el encargado de PKI, informarán al Gerente General acerca de la emisión e instalación conforme del certificado OCS dentro de la Plataforma Tecnológica de Certificación.

16.5. Publicación del certificado renovado por la AC: La AC PROCERT, posee un repositorio de todos los certificados emitidos y renovados tanto en su servidor de certificación como en una base de datos redundante. El acceso al repositorio de los certificados emitidos es público y puede ser realizado por los clientes, proveedores o parte interesada a través de la página web del PSC PROCERT (www.procert.net.ve), accediendo al vínculo de "Certificados Emitidos" e ingresando los datos correspondientes al tipo de firma o certificado electrónico y el nombre o apellido del cliente propietario de la firma o certificado electrónico.

16.6. Notificación de la emisión del certificado por la AC a otras autoridades: La operación con AC externas al PSC PROCERT no se encuentra normada o desarrollada por la SUSCERTE. No obstante, el Decreto Ley Sobre Mensajes de Datos y Firmas Electrónicas, si contempla dicha posibilidad, quedando abierta la posibilidad de establecer esquemas de operación con Autoridades de Certificación externas una vez se cuente con la normativa que regule la materia.

17. Modificación de certificados: El certificado electrónico para OCSP generado por el PSC PROCERT, debe mantener su integridad durante su período de vigencia y no podrá ser objeto de modificación o cambio alguno.

18. Revocación y suspensión de un certificado.

18.1. Circunstancias para la revocación del certificado: Las circunstancias para la revocación del certificado son las señaladas en el aparte 23.1 de la declaración de prácticas de certificación (DPC) (AC-D-0003).

18.2. Entidad que puede solicitar la revocación: La entidad que puede solicitar la revocación del certificado electrónico para OCSP es el Coordinador de tecnología, el encargado de PKI o el Gerente General. Se debe contar con la autorización del Comité de Seguridad del PSC PROCERT.

18.3. Procedimiento de solicitud de la revocación: El Coordinador de tecnología, el encargado de PKI o el Gerente General. Podrán solicitar y deberán fundamente en el Comité de Seguridad su solicitud de revocación de certificado.

18.4. Disponibilidad de compromiso on-line de revocación y estado de los certificados: La AC tiene la capacidad de entregar la lista de certificados revocados utilizando el OCSP a través del enlace http://ocspsmime.procert.net.ve/ocsp

18.5. Requisitos de comprobación on-line de revocación: El cliente del PSC PROCERT podrá acceder en línea a la verificación del estado de un certificado a los fines de verificar si se encuentra suspendido o revocado. El cliente deberá ingresar en la página web de PROCERT (www.procert.net.ve) y acceder el módulo “AC PROCERT” seguidamente buscar la opción *Publicación de los certificados revocados AC Procert* y seleccionar la opción OCSP.

19. Servicio de Comprobación de estado de certificados.

19.1. Características operativas: El PSC PROCERT posee servicios de comprobación de estado de la firma o certificado electrónico. Dichos servicios son la LCR y el acceso OCSP para acceso en línea a la comprobación del estado de las firmas y certificados electrónicos generados por el PSC PROCERT. El funcionamiento de la LCR se encuentra establecido en el apartado 32.7 de la declaración de prácticas de certificación (DPC) y política de certificados (PC) (AC-D-0003). El funcionamiento del acceso vía OCSP se encuentra establecido en los apartes 23.9 y 23.10 de la declaración de prácticas de certificación (DPC) (AC-D-0003).

19.2. Disponibilidad del servicio: El PSC PROCERT mantiene disponibles los servicios de la LCR y acceso OCSP a través de su página web (www.procert.net.ve). La Autoridad de Certificación (AC) PROCERT mantiene en operación su portal web, cumpliendo con un alto porcentaje de disponibilidad.

19.3. Características adicionales: Características adicionales a los servicios de LCR y acceso OCSP se encuentran señaladas de forma precedente en este documento de la política de certificado electrónico para servidor seguro SSL, en los puntos 18.8 y 18.9.

19.4. Custodia y recuperación de la clave: La clave privada del PSC PROCERT se custodia en un dispositivo criptográfico HSM. Para el acceso al repositorio de claves privadas es necesario el uso de tarjetas inteligentes. El esquema de operación del PSC PROCERT y su plataforma tecnológica de certificación, se encuentran configurados para que el cliente genere su par de claves (pública y privada). Siempre y en todo caso el compromiso de clave del certificado de OCSP, se deberá proceder a la emisión de un nuevo certificado y deberá cumplir el proceso de interno asignado dentro del PSC PROCERT.

20. Controles de seguridad física, de gestión y de operaciones: Los controles de seguridad física de gestión y de operaciones son los señalados en el aparte 27 de la Declaración de Prácticas de Certificación (DPC) (AC-D-0003).

21. Controles de seguridad técnica: Los controles de seguridad técnica son los señalados en el aparte 31 de la declaración de prácticas de certificación (DPC) (AC-D-0003).

22. Perfiles de Certificados, LCR / OCSP.

22.1. Perfil del certificado: Los certificados del PSC PROCERT son emitidos conforme a las siguientes normas:

- RFC 6818: Internet X.509 V3 Public Key Infrastructure - Certificate and CRL Profile, January 2013.
- ITU-T Recommendation X.509 (2016): Information Technology – Open. System Interconnection - The Directory: Authentication Framework.
- ETSI TS 101 862 V1.3.3 (2006-01): Qualified Certificate Profile, 2006.
- RFC 3739: Internet X.509 Public Key Infrastructure – Qualified Certificate. Profile, 2006 (prevaleciendo en caso de conflicto la TS 101 862).

22.2. Número de Versión: Como se indicó en el aparte 8.1., que precede, el número de versión del certificado es V3.

22.3. Extensiones del Certificado: Las extensiones de los certificados del PSC PROCERT permiten codificar información adicional en los certificados. Las extensiones estándar X.509 definen los siguientes campos:

- Subject Key Identifier.
- AuthorityKeyIdentifier
- BasicConstraints.
- Certificate Policies.
- KeyUsage.
- LCRDistribucionPoint.
- SubjectAlternativeName.
- AuthorityInformationAccess.

22.4. Identificadores de Objeto (OID) de los Algoritmos: El OID del algoritmo criptográfico utilizado por el PSC PROCERT es: SHA384withECDSAEncryption (1.3.132.0.34).

22.5. Formatos de Nombres: El formato y significado asignado a los nombres en cada uno de las firmas y certificados electrónicos generados por el PSC PROCERT se

encuentran detallados en los numerales 32.5 y 14 de la declaración de prácticas de certificación (DPC) (AC-D-0003).

22.6. Identificador de Objeto (OID) de la PC: PSC PROCERT, utilizará la definición de política de asignación de OID's según el árbol privado de numeración asignado por la SUSCERTE.

22.7. Perfil de LCR / OCSP: La LCR es una lista de firmas y certificados electrónicos, en la cual concretamente, se muestran los números de serie de las firmas o certificados electrónicos revocados por una AC, los números de serie que han sido revocados, ya no son válidos, y por ende el usuario no debe confiar en ningún certificado incluido en la (LCR) del sistema. Una (LCR) es un archivo que contiene:

- Nombre del emisor de la LCR
- Números de serie de la firma o certificado
- Fecha de revocación de las firmas o certificados.
- La fecha efectiva y la fecha de la próxima actualización.

Dicha lista está firmada electrónicamente por la propia AC que la emitió. Cuando un usuario desea comprobar la validez de un certificado debe descargar e instalar la LCR actualizada desde los servidores de la misma AC que emitió la firma o certificado, al realizar esto, las firmas o certificados que se encuentren instalados en el computador en donde se halla instalado la LCR, automáticamente se validan, si los mismos se encuentran revocados, se invalidan; también se puede comprobar a través del número de serie ubicado en la LCR el status de algún otro certificado. Se comprueba la autenticidad de la lista gracias a la firma electrónica de la autoridad de certificación.

Nombre del campo	Valor
Versión	V2 (Número de versión del certificado).
Algoritmo de Firma:	Sha-256ECDSA (Algoritmo de Firma)
Datos del emisor	
CN	PSCPROCERT.
O	Sistema Nacional de Certificación Electrónica
OU	PROCERT
C	VE (VENEZUELA)
E	contacto@procert.net.ve
L	Av. Libertador Multicentro Empresarial del Este piso 13 Oficina B-132 Torre Libertador Núcleo B
ST	MIRANDA
Período de Validez	
Última Actualización :	Contiene la fecha y hora en que fue emitida la lista de certificados revocados (LCR).
Próxima Actualización :	Fecha en que se emitirá la próxima lista de certificados revocados.
Lista de certificados revocados	
Certificados Revocados	Contiene la lista de certificados revocados indicados por su

	número de serie y su fecha de revocación.
Extensiones	
Identificación de clave de la autoridad certificadora	Proporciona un medio para identificar la clave pública que corresponde a la clave privada utilizada para firmar una LCR (ID DE CLAVE)
Nombre alternativo del emisor	
DNSName	**procert.net.ve**
Número de LCR	Número de Identificación de la LCR
Punto de distribución LCR	http://www.procert.net.ve/ecc-crl/smime-ca.crl

El perfil correspondiente al OCSP se encuentra detallado en el aparte 32 de la Declaración de Prácticas de Certificación (DPC).

22.8. Auditoría de conformidad: En el caso de la raíz de certificación de la AC del PSC PROCERT es supervisada y auditada anualmente por la SUSCERTE. La SUSCERTE en cualquier momento y con la frecuencia que considere apropiada puede realizar auditorías exhaustivas o parciales para determinar si el manejo de la Clave Criptográfica de la AC PROCERT cumple con las directrices de Ley para operar como PSC.

22.8.1. Frecuencia de los controles de conformidad para cada entidad: Las auditorias de control y seguimiento ordenas por Ley e impuestas por mandato de la SUSCERTE serán efectuadas anualmente; y mediante dichas auditorias se establecerá el nivel de cumplimiento del PSC PROCERT acerca de la normativa de Ley y técnica, nacional e internacional aplicable a todo PSC en operación. Todo PSC acreditado ante SUSCERTE debe realizar la auditoria anual de seguimiento si opta a la renovación de su acreditación para operación durante el año siguiente al proceso de auditoría.

22.8.2. Auditores: Las auditorias anuales serán efectuadas por el auditor seleccionado por el PSC PROCERT. El auditor seleccionado deberá estar acreditado ante el Registro de Auditores que mantiene la SUSCERTE.

22.8.3. Relación entre el auditor y la autoridad auditada: Entre el PSC PROCERT y el auditor seleccionado, solamente existe una relación comercial que no causa dependencia. El PSC PROCERT contratará la auditoría de seguimiento ordenada por la SUSCERTE y el auditor prestará el servicio con la obligación de generar un informe de cumplimiento, el cual entregará al PSC PROCERT y a la SUSCERTE y de mantener en todo momento la confidencialidad de la información a la cual tuvo acceso durante el proceso de auditoría.

22.8.4. Tópicos cubiertos por el control de conformidad: Los tópicos cubiertos por la auditoria de cumplimiento incluyen:

22.8.4.1. Seguridad física.
22.8.4.2. Evaluación de tecnología.
22.8.4.3. Administración de servicios CA.
22.8.4.4. Investigación de personal.

22.8.4.5. Documento de la declaración de prácticas de certificación (DPC) y la política de certificados (PC) y otras políticas y documentos aplicables.
22.8.4.6. Contractos.
22.8.4.7. Protección de datos y consideraciones sobre privacidad.
22.8.4.8. Planificación de recuperación ante desastres.

22.8.5. Acciones que tomar como resultado de una deficiencia: Todo punto u observación generado por el auditor acreditado ante la SUSCERTE respecto a la operación y generación de certificados del PSC PROCERT y que sea considerado como "disconformidad", será sometido a plan de remediación y cumplimiento, el cual deberá establecer el cronograma y tiempo fijado para superar la "disconformidad", en el supuesto que la misma sea declarada. Si el PSC PROCERT no supera o cumple con el proceso de remediación de la "disconformidad", no podrá optar a la renovación de su acreditación como PSC y cesará operación.

22.8.6. Comunicación del resultado: Los resultados de las auditorias se consideran información comercial sensitiva. A menos que esté estipulado en el contrato, serán protegidos como información confidencial de acuerdo con la sección 32.8.6 de la declaración de prácticas de certificación (DPC) (AC-D-0003).

23. Marco legal y normativo.

- Decreto Ley de Mensaje de Datos y Firmas Electrónicas y su Reglamento.
- Normativa de la SUSCERTE.
- Normativa PROCERT.
- Estándar internacional ITU- T X.509 V3.
- Estándar Internacional ITU-T X.609.
- Norma ISO 9000:2005.
- Norma ISO/IEC 9594-8.
- Norma ISO/TR 10013:2001.
- Norma ISO/IEC 27001:2006.

24. Funciones y responsabilidades dentro de la AC: Las funciones y responsabilidades de los distintos niveles de la AC del PSC PROCERT respecto al manejo, control y resguardo del presente Documento, se encuentran definidos dentro del documento para el establecimiento de funciones y responsabilidades (AC-PO-0003).

25. Actores sujetos al cumplimiento del presente documento: El presente documento política de certificado electrónico para servidor seguro SSL, emitido por la AC del PSC PROCERT, conforme a los lineamientos de la SUSCERTE se constituye en norma de obligatorio cumplimiento y sujeción por parte de los actores que se indican a continuación:

- Alta Dirección de la AC PROCERT.
- Empleados de la AC PROCERT.
- Clientes usuarios de certificados electrónicos emitidos por la AC PROCERT ITFB.

- Parte Interesada usuaria de los certificados electrónicos emitidos por la AC PROCERT ITFB.

26. Revisión, Aprobación y Modificación: Los procesos asociados a la revisión, aprobación, modificación o ajuste de la documentación de la AC del PSC PROCERT, serán regulados por la política de documentación y gestión documental (AC-PO-0002).