GUÍA DE ESTÁNDARES TECNOLÓGICOS Y LINEAMIENTOS DE SEGURIDAD PARA LA ACREDITACIÓN Y RENOVACIÓN COMO PROVEEDOR DE SERVICIOS DE CERTIFICACIÓN Ó CASOS ESPECIALES

CONTROL DE VERSIONES

VERSIÓN (EDICIÓN)	MOTIVO DEL CAMBIO	PUBLICACIÓN
1	Creación	Agosto- 2006
2	Actualización General (incluido estándares)	Julio- 2007
2.1	Actualización General	Abril- 2008
3	Actualización General (incluido estándares)	Agosto- 2011
3.1	Actualización General (Inclusión de Casos Especiales)	Enero - 2012

ÍNDICE

TRÁMITE	
NOMBRE	**CARGO SUSCERTE**
	Superintendente Superintendente Adjunto
	Director de Registro y Acreditación Directora de Inspección y Fiscalización Director de Investigación y Desarrollo Tecnológico Directora de la Oficina de Gestión Administrativa Asesora Legal

GRUPO DE TRABAJO:			**COMISIÓN ESPECIAL:**		
COORDINADOR:					
MIEMBROS PERMANENTES:			**CARGO:**		
NOMBRE	**UNIDAD**	**CARGO**			
			ESPECIALISTA(S) INVITADO(S):		
			NOMBRE	**ENTIDAD**	**CARGO**

OBSERVACIONES	**RESPONSABLE DE LA EDICIÓN**
	COORDINADOR: FECHA: FIRMA:
	SUPERINTENDENTE: FECHA: FIRMA:
	APROBACIÓN APLICACIÓN EN: FECHA: FIRMA:

1. OBJETO Y CAMPO DE APLICACIÓN

El propósito de esta guía es orientar al solicitante de acreditación acerca de la aplicación de los estándares desarrollados para el análisis de los requisitos tecnológicos, seguridad y confianza que debe cumplir para obtener la acreditación como Proveedor de Servicios de Certificación y Caso Especial.

2. REFERENCIAS NORMATIVAS

2.1 Decreto con Fuerza de Ley 1.204 (LSMDFE).

2.2 Reglamento Parcial de la LSMDFE.

2.3 Norma SUSCERTE No 027. Guía para la Acreditación de Proveedores de Servicios de Certificación. (2007).

2.4 ISO/IEC 27002:2007 Tecnología de la Información. Técnicas de Seguridad – Sistema de Gestión de la Información. (2007).

2.5 ISO/IEC 15408: Common Criteria for Information Technology Security Evaluation, Versión 3 (2009)

2.6 FIPS PUB 140-2: Security Requirements for Cryptographic Modules, (Diciembre 2002).

2.7 ETSI TS 102 042: “Policy requirements for certification authorities issuing public key certificates”. V2,1,1 (2009-5)

2.8 RFC 3280, “Internet X.509 Public Key Infrastructure Certificate and Certificate. Revocation List (CRL) Profile”. Abril 2002.

2.9 ISO/IEC 9594-8:2005 Information Tecnology – Open Systems Interconnection – The Directory: Public-key and Attribute Certificate Frameworks.

2.10 ITU-T Rec. X.509 Tecnología de la información. Interconexión de sistemas abiertos – El directorio – Marco de autenticación. (1997).

2.11 ITU-T Rec. X.690 (1997) / ISO/IEC 8825-1:2008. ASN.1 Basic Encoding Rules

2.12 RFC 2559 Boeyen, S. et al. "Internet X.509 Public Key Infrastructure. Abril 2002.

2.13 RFC 3647. “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework“. Noviembre 2003.

2.14 NIST SP800-18, Guide for Developing Security Plans for Information Technology Systems. Diciembre 1998.

2.15 NIST SP800-26 Self Assessmen Guide IT System Review. Noviembre 2001.

3. DEFINICIONES Y TERMINOLOGÍAS

A los efectos de esta norma, se establecen las siguientes definiciones y terminologías:

ACREDITACIÓN	Titulo que otorga la Superintendencia de Servicios de Certificación Electrónica a los Proveedores de Servicios de Certificación para proporcionar certificados electrónicos, una vez cumplidos los requisitos y condiciones establecidos en el Decreto-Ley 1.204.
AUDITOR REGISTRADO	Persona natural que actúa en forma propia o como representante de una persona jurídica que se encuentra registrado en SUSCERTE y avalado por esta para efectuar las evaluaciones y auditorías técnicas de los solicitantes PSC o CE.
AUDITORÍA TÉCNICA	Proceso sistemático que consiste en obtener y evaluar objetivamente evidencias concernientes al cumplimiento de las políticas, planes, procedimientos de seguridad y requisitos técnicos, orientados a garantizar la prestación continua de los servicios de certificación, para luego comunicar los resultados a las personas o entes interesados.
CASO ESPECIAL	Casos Especiales son entidades de Certificación excepcionales para Proyectos de Interés Nacional que son acreditados por SUSCERTE, siempre y cuando se de alguno de los extremos del art. 11 de la Providencia Administrativa N°016 del 05 de febrero del 2007. Para los cuales aplica a los efectos de la presente Norma las mismas obligaciones y derechos que los PSC, con las excepciones establecidas en las respectivas Providencias de Creación.
SUPERINTENDENCIA DE SERVICIOS DE CERTIFICACIÓN ELECTRÓNICA (SUSCERTE)	Servicio Autónomo, integrado a la estructura orgánica del Ministerio del Poder Popular para la Ciencia, Tecnología e Industrias Intermedias, según Gaceta Oficial de la República Bolivariana de Venezuela No 5.836 Extraordinario de fecha 08 de Enero de 2007.

4. SÍMBOLOS Y ABREVIATURAS

A los efectos de esta norma, se establecen los siguientes símbolos y abreviaturas:

AC	Autoridad de Certificación
AR	Autoridad de Registro
DIF	Dirección de Inspección y Fiscalización
DPC	Declaración de Prácticas de Certificación.
DRA	Dirección de Registro y Acreditación
LCR	Lista de Certificados Revocados
LSMDFE	Ley Sobre Mensajes de Datos y Firmas Electrónicas.
OCSP	On - line Certificate Status Protocol (Protocolo de estado de certificados en línea)
PC	Política de Certificados.
PSC	Proveedor de Servicios de Certificación.
CE	Casos Especiales
SUSCERTE	Superintendencia de Servicios de Certificación Electrónica.

5. PROCEDIMIENTO

5.1. Principio Básico

Con el uso de esta guía de evaluación se pueden recolectar y analizar, con el detalle y rigurosidad que exige el Decreto-Ley 1.204, los aspectos que deben ser revisados en el área tecnológica, seguridad y confianza del solicitante, los cuales permitirán definir un criterio preciso sobre su capacidad para lograr y mantener en el tiempo la acreditación como Proveedor de Servicios de Certificación o Caso Especial.

5.2. Consideraciones Generales

5.2.1 El objetivo de la acreditación para los Proveedores de Servicio de Certificación (PSC) o Caso Especial (CE) es asegurar la existencia de un sistema de certificación de firma electrónica confiable, que garantice su continuidad en el tiempo y que sirva de base para el desarrollo tecnológico del país

5.1.2 Como criterios generales de la acreditación, se tienen:

5.2.2.1 Los criterios de acreditación están definidos con base en el cumplimiento del conjunto de requisitos y obligaciones definidas por la Ley Sobre Mensajes de Datos y Firmas Electrónicas (LSMDFE), su Reglamento Parcial y las Normas y Resoluciones emitidas por SUSCERTE.

5.2.2.2 El proceso de acreditación coloca a disposición pública los requisitos que se

deben cumplir para ser acreditado por el Gobierno de la República Bolivariana de Venezuela, a través de SUSCERTE, con el propósito de proveer confianza a los usuarios y generar las condiciones y los acuerdos necesarios para el desarrollo de la actividad.

5.2.2.3 Los requerimientos del proceso de acreditación deben garantizar la compatibilidad de la Infraestructura Nacional de Certificación Electrónica con los estándares internacionales, permitiendo así la interoperabilidad entre los sistemas.

5.2.2.4 Los niveles de exigencia del proceso de acreditación deben ajustarse a las mejores prácticas y los estándares internacionales.

5.2.2.5 Se considera fundamental promover el desarrollo tecnológico de los servicios de certificación electrónica, sin preferencia hacia una tecnología en particular. Además los PSC o CE podrán introducir cambios tecnológicos siempre que estos cumplan con la normativa establecida, se notifique a SUSCERTE y sean aprobados por ella.

5.2.2.6 La realización de un proceso de acreditación riguroso requiere de información estratégica o altamente sensible de parte de los PSC o CE. Por lo anterior, SUSCERTE se compromete a no usar ni divulgar la información entregada por el PSC o CE, clasificada como confidencial, más que para los fines propios del procedimiento de acreditación. Este compromiso es extensible a todo organismo y persona que intervenga en el proceso de acreditación.

5.2.2.7 El contenido de estos criterios puede cambiar en el tiempo, dependiendo de los avances de la tecnología y consideraciones de seguridad nacional. Si el cambio es considerado significativo, el proceso de revisión incorporará consultas con la industria y debe ser validado por SUSCERTE.

5.2.2.8 Cualquier PSC o CE acreditado debe ser notificado de los cambios de este documento. Si existiera alguna duda respecto a la actualización de estos criterios, deberá contactarse con la Superintendencia.

5.2.2.9 Los lineamentos establecidos en este documento corresponden al cumplimiento de los estándares internacionales para ofrecer de forma segura y confiable servicios de certificación electrónica. Los estándares tecnológicos utilizados a lo largo del documento son los siguientes:

a) En cuanto a Prácticas de Certificación:

- ETSI TS 102 042: “Policy requirements for certification authorities issuing

public key certificates". V2,1,1 (2009-5)

- RFC 3647. "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework". Noviembre 2003.

b) Respecto a Seguridad:

- ISO/IEC 27002:2007 Tecnología de la Información. Técnicas de Seguridad – Sistema de Gestión de la Información. (2007)
- ISO/IEC 15408: Common Criteria for Information Technology Security Evaluation, Versión 3 (2009)
- FIPS PUB 140-2: (2009) Security Requirements for Cryptographic Modules, (Diciembre 2002)

c) Referentes a Estructura de Certificados:

- ITU-T Rec. X.509 (1997) Tecnología de la información. Interconexión de sistemas abiertos – El directorio – Marco de autenticación (2001)
- ITU-T Rec. X.690 (1997) / ISO/IEC 8825-1:1998. ASN.1 Basic Encoding Rules

d) Para Repositorio de Información:

- [RFC 2559] Boeyen, S. , "Internet X.509 Public Key Infrastructure. Abril 2002
- [RFC 4386] Boeyen, S. , "Internet X.509 Public Key Infrastructure repository locator services. Febrero 2006

e) En cuanto a criptografía

- [RFC 3280] "Internet X.509 Public Key Infrastructure Certificate and Certificate. Revocation List (CRL) Profile". Abril 2002.

5.2.3 Con base en la LSMDFE y su Reglamento Parcial, es posible establecer un sistema de acreditación para PSC o CE que involucra los siguientes elementos:

5.2.3.1 SUSCERTE

El proceso de acreditación de PSC o CE es desarrollado por SUSCERTE quien puede apoyarse en expertos (auditores), para realizar la evaluación de dichas entidades.

Además, debe velar porque los requisitos y obligaciones que se observaron al momento de otorgarse la acreditación se mantengan durante la vigencia de la acreditación. (LSMDFE Art. 22). Para ello puede requerir información y ordenar Auditorías a las instalaciones del PSC o CE inspeccionado, sin previo aviso, ya sea con su personal o por medio de los auditores.

5.2.3.2 Auditores

Corresponde a una o más personas que cuentan con la capacidad técnica para realizar el proceso de evaluación, las cuales son inscritas en un registro que lleva la Superintendencia, una vez comprobada su capacidad.

El proceso de evaluación y Auditoría es el procedimiento por el cual la Superintendencia verifica el cumplimiento de la LSMDFE y sus reglamentos, tanto para los PSC o CE acreditados como para los que solicitan acreditación, respectivamente.

5.2.3.3 Proveedores de Servicios de Certificación (PSC)

Corresponde a la entidad emisora de certificados de firma electrónica, la cual solicita ser acreditada.

5.2.3.4 Casos Especiales

Corresponde a la entidad de certificación extraordinaria que por motivos de proyectos de interés nacional son acreditados ante SUSCERTE.

5.2.3.5 Registro de PSC Acreditados

Registro público que mantiene la Superintendencia, en el cual están identificados los PSC acreditados (Articulo 22 LSMDFE).

5.2.3.5 Registro de Auditores

Registro público que mantiene la Superintendencia, en el cual están identificados los Auditores autorizados a realizar las auditorías a PSC o CE.

5.2.3.6 Estándares Técnicos

Conjunto de estándares internacionales vigentes que debe cumplir el PSC o CE para ser acreditado por la Superintendencia, además de los requisitos y obligaciones establecidas explícitamente en el Articulo 31 de la LSMDFE y los establecidos en el presente Documento.

5.2.4 Los estándares tecnológicos y lineamientos de seguridad a aplicar para la acreditación como PSC o CE, se resumen en el Anexo No 1 y se detallan a continuación en las consideraciones específicas.

5.3. Consideraciones Específicas

5.3.1 Estructura e información del Certificado de Firma Electrónica

5.3.1.1 Objetivo

Comprobar los aspectos mínimos que dispone la LSMDFE con relación a la conformidad con el estándar ITU-T Rec. X.509, contenidos mínimos, incorporación de los requisitos mínimos obligatorios, límites y atributos del certificado de firma electrónica.

5.3.1.2 Descripción

1. La estructura de datos que conforma el certificado de firma electrónica emitido por el PSC o CE debe estar en conformidad al estándar ITU-T Rec. X.509.
2. El certificado de firma electrónica emitido por el PSC o CE debe contener al menos los siguientes datos:
   a) Un código de identificación único del certificado.
   b) Identificación del PSC o CE, con indicación de su nombre o razón social, RIF, dirección de correo electrónico, y, en su caso, los antecedentes de su acreditación y su propia firma electrónica.
   c) Los datos de la identidad del signatario, entre los cuales deben necesariamente incluirse su nombre, dirección de correo electrónico y cédula de identidad.
   d) Plazo de vigencia (fecha de inicio y de vencimiento).
3. El PSC o CE debe incorporar en sus certificados el RIF propio y la identificación del signatario de acuerdo a la estructura e identificadores que se especifica por la Superintendencia de acuerdo al caso.
4. Los PSC o CE deben indicar en forma explícita, que el certificado emitido corresponde a una política de certificados con los límites de uso (ej. de firma electrónica). Esta indicación debe quedar inserta en el campo Certificate Policies de las extensiones del certificado del formato X.509 versión 3.
5. El PSC o CE interesado debe estructurar los certificados que emite, de forma que los atributos adicionales que introduce, así como la incorporación de límites al uso del certificado, no impidan la lectura del mismo ni su reconocimiento por terceros de la Infraestructura Nacional de Certificación Electrónica.
6. Los límites de uso que se incorporen en los certificados, deben ser

reconocibles por terceros de la Infraestructura Nacional de Certificación Electrónica.

7. Los datos de creación de firma del PSC o CE acreditado para emitir certificados, no deben ser utilizados más allá de lo establecido en la DPC aprobada por SUSCERTE.

5.3.1.3 Estándares de Evaluación

- ITU-T Rec. X.509 / ISO/IEC 9594-8
- ITU-T X.690

5.3.1.4 Documentación Solicitada

Modelos de Certificado tipo de firma electrónica, emitido por el PSC o CE en evaluación y el Modelo de la solicitud de firma del certificado (CSR)

5.3.1.5 Detalles de la Evaluación

Aspectos	Evaluación
Conformidad con el estándar ITU-T Rec. X.509	Se verificará que la estructura básica del certificado esté en conformidad a la norma y que la gramática utilizada tanto en la estructura básica como en las extensiones obligatorias para incluir el RIF o CI, puedan ser leídos por cualquier aplicación que cumpla dicho el estándar.
Contenido básico del certificado de firma electrónica emitido por el PSC o CE	Se confirmará que el certificado contiene la siguiente información: a) Un código de identificación único del certificado b) Identificación del PSC o CE, con indicación de su nombre o razón social, RIF, dirección de correo electrónico, y, en su caso, los antecedentes de su acreditación y su propia firma electrónica c) Los datos de la identidad del signatario, entre los cuales deben necesariamente incluirse su nombre, dirección de correo electrónico, su RIF O CI, y d) El tiempo de vigencia.
Método de incorporación de identificación del signatario	Se verificará que el PSC o CE incorpore en sus certificados el identificador que venga al caso, como por ejemplo en caso de que el signatario sea persona jurídica se debe incluir el RIF.
Lectura y	Se validará que el PSC o CEPSC o CE estructure sus

reconocimiento del contenido mínimo cuando existen atributos adicionales en el certificado	certificados, de forma que los atributos adicionales que introduzca con el fin de incorporar límites al uso del certificado, si los hay, no impidan la lectura ni su reconocimiento por terceros.
Reconocimiento de límites de uso del certificado de firma electrónica por terceros	Se verificará que el PSC o CE estructure sus certificados de manera que los límites de uso, si los hay, sean reconocibles por terceros.
Uso de clave pública acreditada	Se verificará que los datos de creación de firma del PSC o CE acreditado para emitir certificados no sean utilizados más allá de lo establecido en la DPC aprobada por SUSCERTE.
Algoritmos de firma	Se validará que el PSC o CE utilice algoritmos de firma estándares de la industria (establecidos por el RFC 3280) que provean el adecuado nivel de seguridad aprobado por SUSCERTE tanto para su propia firma como para la firma del signatario.
Tamaño de las claves	Se comprobará que el PSC o CE utilice el tamaño de clave pública y privada, de mínimo 4096 para su propia firma y 2048 para la firma del signatario; o en su defecto cualquier tamaño de clave que sea elegido debida y formalmente por SUSCERTE.
Funciones Hash	Se verificará que el PSC o CE utilice funciones Hash de última generación para el proceso de firma, debidamente elegidas a través de un estudio de factibilidad por la Superintendencia, que provean el nivel de seguridad, tanto para su propia firma como para la firma del signatario. El uso de funciones de hash debe actualizarse cada año, posterior a la creación de este documento, ya que al cumplirse el lapso se debe haber superado cualquier problema de interoperabilidad de algoritmos de mayor complejidad.

5.3.2 Estructura de la Lista de Certificados Revocados (LCR)

5.3.2.1 Objetivo

Verificar que las listas de certificados revocados tengan el formato y contenido

especificado en el estándar, y permita al signatario identificar plenamente al PSC o CE emisor de la LCR.

5.3.2.2 Descripción

La lista de certificados revocados (LCR) debe contener la información y estructura que especifica el estándar ISO/IEC 9594-8.

Este estándar especifica que la lista debe contener al menos la identificación del emisor, fecha de su emisión e identificación de los certificados revocados a dicha fecha.

Ya que la lista podría ser almacenada y enviada en medios inseguros, debe estar debidamente firmada por el PSC o CE emisor.

5.3.2.3 Estándares de Evaluación

- ISO/IEC 9594-8

5.3.2.4 Documentación Solicitada

- DPC y PC del PSC o CE.

- LCR emitida por el PSC o CE en evaluación y el certificado de firma electrónica de la AC que la emite.

5.3.2.5 Detalles de la Evaluación

Aspectos	Evaluación
Contenido Mínimo	Se verificará que la LCR contenga al menos la siguiente información: • Versión. Debe tener el valor 2 • Algoritmo de firma. Este campo debe contener la identificación del algoritmo de firma utilizado, siguiendo el RFC 3280. • Nombre del emisor. Este campo debe contener el nombre de la entidad que emitió y firmó la lista de certificados revocados. • Fecha actual. Este campo debe contener la fecha y hora en que fue emitida la lista de certificados revocados (LCR). • Próxima actualización. Se deberá incluir en este campo la fecha en que se emitirá la próxima lista de certificados revocados. • Certificados revocados. En este campo se deben

	incluir los números de serie de los certificados revocados por el emisor, indicando además la fecha y hora de revocación correspondiente.
Comprobación de firma	Se comprobará que la lista de certificados revocados esté debidamente firmada por el PSC o CE emisor.
Mecanismo de suspensión de certificados	Se verificará que la lista de certificados revocados incluya la información necesaria para indicar el estado de suspensión de un certificado.

5.3.3 Registro de Acceso Público. (Servicios, contenido y accesibilidad electrónica del sistema público de información del PSC o CE)

5.3.3.1 Objetivo

Asegurar el acceso a información relevante descriptiva del sistema por parte de los signatarios y terceros.

5.3.3.2 Descripción

Se verificará que el PSC o CE:

- Garantice la existencia de un servicio seguro de consulta remota de un registro de certificados emitidos, en el que quede constancia de los certificados emitidos indicando si el mismo se encuentra vigente, revocado o suspendido, si le ha sido traspasado de otro PSC o CE acreditado o si es homologado.
- Provea acceso al registro público de certificados a los signatarios y partes interesadas por medios electrónicos de manera continua y regular.
- Use sistemas y productos confiables que garanticen la seguridad de su sistema de difusión de información.
- Cuente con procedimientos para informar a los signatarios las características generales de los procesos de creación y verificación de firma electrónica, así como de las reglas sobre prácticas de certificación que el PSC o CE se comprometa a utilizar en la prestación del servicio.
- Tenga procedimientos para dejar sin efecto temporal o definitivamente (suspender o revocar) los certificados.

- Cuente con procedimientos para publicar y actualizar en su(s) sitio(s) la información de acceso electrónico, las resoluciones de la Superintendencia que le afecten. Esto debe realizarse como mínimo en los sitios de dominio público registrados durante el proceso de acreditación. Además, debe incluirse la DPC y PC.

5.3.3.3 Estándares de Evaluación

Este apartado no aplica

5.3.3.4 Documento Solicitado

Documento descriptivo que contenga al menos la siguiente información:

- Detalle del sitio Web donde publicara la información.
- Descripción de la tecnología.
- Disponibilidad, accesibilidad, conexión, esquemas y diagramas de funcionamiento.
- Medidas de seguridad.
- Sitio Web de prueba con las funcionalidades requeridas.

5.3.3.5 Detalles de la Evaluación

Aspectos	Evaluación
Existencia y contenido mínimo del Sitio Web de información pública	El PSC o CE debe mantener un sitio de acceso electrónico, con información relevante para los signatarios y las partes que confían. Al menos debe contener los siguientes documentos: • Registro de certificados emitidos, indicando código de identificación único del certificado y su estado (vigente, suspendido o revocado). • Copia de la LCR actualizada cada 24 horas. • Indicar si el certificado ha sido traspasado de otro PSC o CE acreditado o ha sido homologado. • Acceso seguro a los signatarios para realizar revocación o suspensión de certificados vigentes. • Declaración de Prácticas de Certificación (DPC) y Política de Certificados (PC).
Disponibilidad de la Información y servicio	Se debe asegurar una disponibilidad del sitio no menor al

	99%. Para esto se verificará la existencia de mecanismos redundantes o alternativos de conexión y sitios de emergencia que se levanten manual o automáticamente en caso de desastres.
Seguridad	Se debe proteger la integridad y disponibilidad de la información mediante el uso de tecnología y medidas de seguridad tanto físicas como lógicas que reduzcan los riesgos y consecuencias de ataques maliciosos tanto internos como externos en contra del sitio.

5.3.4 Modelo de Confianza

5.3.4.1 Objetivo

Verificar que el PSC o CE provea a los signatarios de certificados de firma electrónica emitidos por él, un mecanismo de confianza que le permita comprobar la validez de cualquier certificado que reciba.

5.3.4.2 Descripción

El certificado de firma electrónica emitido por un PSC o CE acreditado debe permitir a su receptor verificar, en forma directa o mediante consulta electrónica, todos los certificados que reciba, con la finalidad de comprobar la validez del mismo.

De esta forma es factible asegurar la interoperabilidad en el sistema y la propagación de la confianza depositada por el signatario en su PSC o CE hacia el resto del sistema.

5.3.4.3 Estándares de Evaluación

Este apartado no aplica

5.3.4.4 Documento Solicitado

Documento en el que se describe el modelo de confianza utilizado por el PSC o CE para lograr el objetivo o alternativamente la DPC y PC si contiene dicho punto.

5.3.4.5 Detalles de la Evaluación

Aspectos	Evaluación
Modelo	Se evalúa que el modelo de confianza adoptado permite

de confianza	cumplir con el objetivo planteado (Anexo No 2)
Efectividad	Se verifica el mecanismo utilizado para implementar el modelo de Confianza en forma práctica en la Infraestructura Nacional de Certificación Electrónica.

5.3.5 Inclusión de Certificado Raíz de PSC o CE en Herramientas Tecnológicas

5.3.5.1 Objetivo

Verificar el cumplimiento por parte del PSC o CE en la inclusión del Certificado Raíz en herramientas y aplicaciones tecnológicas, que permita establecer confianza en la identidad de los certificados utilizados.

5.3.5.2 Descripción

Dado que el producto principal de un PSC o CE es la confianza en la identidad digital, esta se debe garantizar en el ámbito nacional al momento del empleo de herramientas y aplicaciones para navegar en páginas web, procesamiento de palabras, correo electrónico, entre otras; que implementen certificados emitidos por los PSC o CE.

La inclusión del Certificado Raíz en herramientas y aplicaciones tecnológicas requiere lo siguiente:

1. Estudio de factibilidad de inclusión en las distintas herramientas y aplicaciones tecnológicas, tanto privativas como no privativas, garantizando así el cumplimiento del Decreto 3.390 en materia de Tecnologías Libres.
2. Contar con la validación de SUSCERTE, para continuar con el proceso de incorporación en las herramientas y aplicaciones validadas.
3. Crear la petición de solicitud de inclusión en cada herramienta o aplicación requerida.
4. Someterse a un proceso de verificación de las políticas, estándares y documentación relacionada con el Certificado Raíz del PSC o CE, por parte de la organización donde se desea incluir el Certificado de la AC.
5. Reunir los requisitos exigidos por parte de la organización donde se solicita la inclusión, tales como:
    1. **Generales**. Información sobre el PSC o CE: creación, naturaleza,

misión, visión, objetivos, sector atendido, entre otros.

2. **Técnicos.** Información sobre el Certificado Raíz, Nombre del Certificado, Nombre Común, Resumen, URL del Certificado, Huella, Validez, Versión, Parámetros de las llaves de firma, URL página web, Certificados de ejemplo, CRL, OCSP, Solicitud de bits de confianza, Validación SSL, Jerarquía, Firmas Cruzadas, entre otros.
3. **Documentación de políticas y prácticas.** Información referente a la operación del PSC o CE, disponible tanto en idioma nativo como en idioma inglés que incluye: DPC, PC, acuerdos para firmas cruzadas, auditorías, procedimientos de verificación de SSL y de correo electrónico, procedimientos de firma de código, entre otros; así como cualquier otro que sea requerido por la organización donde se procese la inclusión.

4. **Informar mensualmente a SUSCERTE** sobre el estatus del reporte, a partir de la creación de la petición de inclusión.
5. **Disponer del recurso humano y tecnológico**, para el logro de la meta en el tiempo mínimo dispuesto por la organización referente para la inclusión; así como para la consecución de los objetivos del Estado, en materia de certificación electrónica.
6. **Cumplir con todas las condiciones** que no se encuentren en este apartado, pero que sean exigidas por la organización a quien se solicita la inclusión, siempre y cuando no se contradiga lo dispuesto en las normativas legales y sublegales que apliquen en materia de certificación electrónica.

5.3.5.3 Estándares de Evaluación

1. X.509v3
2. RFC 2560
3. RFC 4346

5.3.5.4 Documentación Solicitada

- Copia electrónica del documento correspondiente a la evaluación de la documentación del PSC o CE y pruebas técnicas requeridas.
- Copia electrónica de la tramitación, aprobación o negación, tal sea el

caso, de la inclusión del Certificado Raíz en los Navegadores Web.

5.3.5.5 Detalles de la Evaluación

Aspectos	Evaluación
Generales	• Verificar la información propia del PSC o CE facilitada a los Navegadores Web. • Validar la petición o solicitud de inclusión en los navegadores web.
Técnicos	• Verificar la información del Certificado Raíz suministrada por el PSC o CE a la organización que provee el navegador web. • Validar la disponibilidad de LCR y el servicio de OCSP del PSC o CE.
Documentación	• Verificar que la documentación relacionada con el Certificado Raíz del PSC o CE requerida por el Navegador Web este en idioma ingles.
Personal	• Verificar que exista un personal asignado al seguimiento de la solicitud de inclusión.

5.3.6 Revisión de la Evaluación de Riesgos y Amenazas

5.3.6.1 Objetivo

Determinar la consistencia del análisis de riesgos y amenazas del plan de negocios del PSC o CE

5.3.6.2 Descripción

Dado que el producto principal de un PSC o CE es la "confianza", el requerimiento fundamental para un PSC o CE es demostrar una clara comprensión de las amenazas de seguridad enfrentadas por el negocio y poder mostrar planes efectivos para reducir el riesgo a un nivel aceptable.

La Evaluación de Riesgos es parte de un proceso más amplio denominado Administración del Riesgo. El objetivo principal de un proceso de administración del riesgo en una organización debe ser proteger la organización y su capacidad de cumplir con su misión, y no sólo sus activos IT.

La Administración del Riesgo incluye tres procesos:

1. **Valoración de los riesgos,** incluye la identificación y evaluación de los riesgos e impactos de los riesgos, y medidas recomendadas para reducirlos.
2. **Tratamiento de los riesgos,** se refiere a la priorización, implementación y mantenimiento de las medidas de reducción de riesgo apropiadas recomendadas por el proceso de valoración de riesgos. Este proceso conduce a la definición de un Plan de Seguridad.
3. **Mantenimiento,** corresponde al proceso de evaluación continua para adecuar la valoración de riesgos a condiciones cambiantes del entorno o del negocio.

El resultado debe ser un compromiso razonable entre los costos económicos y operacionales de las medidas de protección, y obtener mejoras en la capacidad de lograr la misión de la organización.

Se debe seguir un proceso similar al descrito en los documentos indicados en las referencias, para realizar el proceso de evaluación de riesgos.

El reporte de la valoración de los riesgos debe tener lineamientos dados en la siguiente estructura, un ejemplo se muestra en el Anexo No 3.

5.3.6.3 Estándares de Evaluación

Este apartado no aplica

5.3.6.4 Documentación Solicitada

Copia del documento correspondiente a la Evaluación de Riesgos o documento equivalente.

5.3.6.5 Detalles de la Evaluación

Aspectos	Evaluación
Reporte de la valoración de riesgos [1]	• Verificar que los riesgos considerados sean reales. • Validar que riesgos relevantes no hayan sido omitidos. • Verificar la valoración adecuada de los riesgos. • Constatar si hay un plan de mantenimiento de la valoración .
Estructura del proceso de valoración de riesgos	Verificar si el proceso de valoración ha sido realizado o auditado por un ente externo, independiente y calificado.

5.3.7 Política de Seguridad de la Información (Documentación y mantenimiento)

5.3.7.1 Objetivo

Comprobar a través de este documento que la organización tiene claros los objetivos de seguridad relevantes para el negocio y que las instancias de gestión del PSC o CE apoyan formalmente esta política.

5.3.7.2 Descripción

La política de seguridad es una declaración de objetivos de seguridad. Solo contiene objetivos de seguridad que son factibles de lograr a través de acciones, procedimientos y mecanismos implementados por el PSC o CE. Si el PSC o CE tiene en otra organización algún aspecto de seguridad o confianza, entonces debe indicarse claramente.

La política de seguridad debe cumplir al menos con los siguientes requerimientos:

1. Los objetivos de seguridad deben ser consecuencia de la Evaluación

1 * Risk Management Guide for information Technology Systems, Special Publication 800-30, Recommendations of the National Institute of Standards and Technology, October 2001
* Handbook 3, Risk Management, Version 1.0, Australian Communications Electronic Security Instruction 33 (ACSI 33)

de Riesgos y Amenazas, de forma tal que los objetivos de la política de seguridad y sus defensas asociadas correspondan al nivel de riesgo requerido para que un PSC o CE sea un ente de confianza.

2. Debe estar basada en las recomendaciones del estándar ISO 27002:2007 sección 5, los cuales se transcriben en el Anexo No 4 de este documento de evaluación.
3. Los objetivos de la política son de alto nivel y no técnicos, por tanto debe ser lo suficientemente general para permitir alternativas de implementación tecnológica.
4. Si la complejidad de los objetivos así lo requieren, la política puede estar conformada por más de un documento; esto es, puede haber una política general soportada por políticas específicas.
5. En esta política de seguridad deben estar incluidos los elementos contenidos en la DPC y PC
6. Este documento debe identificar los objetivos de seguridad relevantes y las amenazas potenciales relacionadas a los servicios suministrados, así como las medidas tomadas para evitar o limitar los efectos de estas amenazas.
7. Adicionalmente, la documentación debe describir las reglas, directivas y procedimientos que indican como son provistos los servicios específicos y las medidas de seguridad asociadas.

En el Anexo No 6 de este documento se describen los principales aspectos que una política de seguridad debe considerar.

Para los propósitos de la acreditación de un PSC o CE, algunos de los aspectos más relevantes han sido incorporados en criterios separados para así facilitar el proceso de evaluación y donde estos se detallan completamente. Por ello, este documento puede expresar en forma general aquellos aspectos de la seguridad organizacional que se tratan en documentos específicos.

5.3.7.3 Estándares de Evaluación

- ISO/IEC 27002:2007

5.3.7.4 Documentación Solicitada

Copia del documento correspondiente a la política de seguridad de la organización.

Documento en el cual se describa formalmente la estructura organizativa del PSC o CE, aprobada por las autoridades de la Institución.

5.3.7.5 Detalles de la Evaluación

Aspectos	Evaluación
Conformidad con el estándar ISO 27002:2007 sección 5.1.1	Verificar que los requerimientos de la sección 5.1.1 descritos en el Anexo No 4, están incorporados.
Conformidad con el estándar ISO 27002:2007 sección 5.1.2	Verificar que se ha incluido un procedimiento de revisión y evaluación periódico de la política de seguridad.
Consistencia entre la política de seguridad y la DPC y PC	Constatar la consistencia de la política de seguridad con la DPC y PC .
Relación entre la Evaluación de Riesgos y la política de seguridad	Verificar que los principales aspectos de la política de seguridad son coherentes con los niveles de riesgo determinados en la evaluación formal de riesgos.
Inclusión de lo indicado en el Anexo 6	Chequear que los elementos fundamentales de una política de seguridad (que apliquen al PSC o CE) están incluidos en el documento.
Claridad de los objetivos de seguridad	Verificar que se establecen objetivos de seguridad claros relacionados con la protección de los procesos de negocios, activos y servicios del PSC o CE.

5.3.8 Plan de Continuidad del Negocio y Recuperación ante Desastres

5.3.8.1 Objetivo

Comprobar a través de este documento que la organización tiene planes establecidos para disminuir a un nivel aceptable el efecto de interrupciones del servicio del PSC o CE, mediante una combinación de controles preventivos y planes de contingencia.

5.3.8.2 Descripción

El Plan de Continuidad del Negocio y de Recuperación de Desastres, debe describir cómo los servicios serán restaurados en el evento de desastre, una

caída de los sistemas o fallas de seguridad.

Dicho plan debe ser mantenido y probado periódicamente y debiera ser parte integral de los procesos de la organización.

En particular, el documento describe la prioridad de restauración para asegurar la continuidad de los negocios de terceros que sean dependientes de la operación del PSC o CE.

Este documento debe seguir los lineamientos brindados por:

- Estándar ISO 27002:2007 en su sección 14 y
- Estándar ETSI TI 102 042 en su sección 7.4.8

Este documento también debe describir los procedimientos de emergencia a ser seguidos en al menos los siguientes eventos:

- Desastre que afecte el funcionamiento de los productos de software en el cual el PSC o CE basa sus servicios.
- Incidente o posible incidente de seguridad que afecte la operación del sistema en el cual el PSC o CE basa sus servicios.
- Compromiso de la clave privada de firma del PSC o CE.
- Falla de los mecanismos de Auditoría.
- Falla en el hardware donde se ejecuta el producto en el cual el PSC o CE basa sus servicios, este debe incluir los servidores, dispositivos criptográficos, dispositivos de seguridad y dispositivos de comunicaciones.

Se debieran identificar los eventos que pueden causar interrupciones a los procesos comerciales y operacionales, junto con la probabilidad y el impacto de dichas interrupciones y sus consecuencias para la seguridad de la información, esto según la ISO 27002:2007.

El plan debe además incluir mecanismos para la preservación de evidencia de mal uso de los sistemas, cuyo propósito es proporcionar evidencia admisible en una corte judicial en alguna fecha posterior.

5.3.8.3 Estándares de Evaluación

- ISO 27002:2007
- ETSI TI 102 042

5.3.8.4 Documentación Solicitada

- Documento de Planes de Continuidad del Negocio y Recuperación de Desastres.
- Documento de Evaluación de Riesgo.

5.3.8.5 Detalles de la Evaluación

Aspectos	Evaluación
Conformidad con el estándar ISO 27002:2007 sección 14.1.1 al 14.1.4	Verificar que los requerimientos de la sección 14 indicados en el Anexo No 4, están incorporados.
Conformidad con el estándar ISO 27002:2007 sección 14.1.5	Comprobar que se ha incluido un procedimiento de revisión y evaluación periódico de la política de seguridad.
Conformidad con el estándar ETSI TI 102 042 sección 7.4.8	Verificar que el plan incorpora procedimientos especialmente detallados para el caso de compromiso de la clave privada de firma tal como lo indica el estándar ETSI, reproducido en el Anexo No 7 de este documento.
Evaluación del riesgo	Esta evaluación debiera considerar los procedimientos comerciales y operacionales y no se debieran limitar a los medios de procesamiento de la información. También se debe verificar que la evaluación del riesgo identifique, cuantifique y establezca prioridad de los riesgos en comparación con los criterios y objetivos relevantes para la organización, incluyendo los recursos críticos, impactos de las interrupciones, tiempos de desabastecimiento permitidos y prioridades de recuperación.
Viabilidad de las facilidades computacionales alternativas	Chequear que las facilidades computacionales alternativas consideradas en el plan, cumplen con los requerimientos mínimos para la operación del PSC o CE.
Elementos de Auditoría	Verificar que el sistema en el cual el PSC o CE basa sus servicios provee mecanismos de preservación de los elementos de Auditoría.

5.3.9 Plan de Seguridad de la Información

5.3.9.1 Objetivo

Comprobar a través de este documento que la organización tiene un plan de seguridad coherente con su Política de Seguridad, que permita mostrar un nivel de confianza consistente con los objetivos del negocio.

5.3.9.2 Descripción

El Plan de Seguridad de la información tiene como propósito describir los requerimientos de seguridad de la información y los controles desplegados o planificados para satisfacer dichos requerimientos. Adicionalmente, debe delinear las responsabilidades y conductas esperadas de los individuos que acceden a los sistemas.

Por lo tanto, el Plan de Seguridad de la información debe describir las acciones operacionales, procedimientos y mecanismos que permitan lograr los objetivos indicados en la Política de Seguridad del PSC o CE.

El plan de seguridad debe considerar al menos las secciones 6 a 13 del estándar ISO 27002:2007. Sin embargo, en este requisito se evalúan en particular los siguientes aspectos:

- Organización de la Seguridad de la Información
- Gestión de activos
- Seguridad en Recursos Humanos
- Seguridad Física y Ambiental
- Gestión de las comunicaciones y operaciones
- Control del acceso
- Adquisición, desarrollo y mantenimiento de los sistemas de información

En el anexo No. 8 se mencionan otros elementos a considerar para la evaluación del plan de seguridad de la información

Se considera que este Plan es una declaración de intenciones del PSC o CE, por lo que la evaluación bajo este requisito no es una certificación de su nivel de seguridad. El proceso de evaluación bajo este requisito indica el nivel de confiabilidad del PSC o CE si este cumple con el plan de seguridad de la información.

El PSC o CE debe asegurar que el acceso físico a los servicios que manejan información sensible esté controlado y los riesgos físicos para los activos estén reducidos a su valor residual.

En el Anexo No 11, se explican los niveles de seguridad que debe contener un sistema de control de acceso físico al centro de datos de la AC del PSC o CE.

5.3.9.3 Estándares de Evaluación

ISO/IEC 27002:2007

5.3.9.4 Documentación Solicitada

Copia del documento correspondiente al Plan de Seguridad de Información.

5.3.9.5 Detalles de la Evaluación

Aspectos	Evaluación
Relación entre el Plan de Seguridad y los recursos asignados	Verificar que el PSC o CE puede justificar la disponibilidad de los recursos y capacidades para implementar los mecanismos y los recursos asignados procedimientos de seguridad (según el NIST SP800-18 y el NIST SP800-26)
Relación entre el Plan de Seguridad y Evaluación de Riesgos	Comprobar que los procedimientos y mecanismos de seguridad permiten lograr el riesgo residual determinado en la Evaluación de Riesgos.
Relación entre Plan de Seguridad y Política de Seguridad	Confirmar que los procedimientos y mecanismos de seguridad permiten lograr los objetivos de la Política de Seguridad.
Mantenimiento del Plan de seguridad	Verificar que el Plan de Seguridad incluye los procedimientos que garanticen que la seguridad del PSC o CE se mantiene en el tiempo ante cambios en: amenazas, personal, servicios, componentes tecnológicos, etc.
Relación del Plan de Seguridad con las prácticas y política de certificación	Verificar que los objetivos de seguridad enunciados en la DPC y PC del PSC o CE se logran a través del Plan de Seguridad.
Requerimientos ISO 27002:2007, sección 6	Confirmar que los controles de Organización de la Seguridad de la información del estándar ISO 27002:2007 están considerados (indicados en el Anexo No 4 de este documento).
Requerimientos ISO 27002:2007, sección 7	Verificar que se han tomado en cuenta los controles de Gestión de Activos del estándar ISO 27002:2007 (ver Anexo No 4)
Requerimientos ISO 27002:2007, sección 8	Comprobar que los controles de Seguridad de Recursos

	Humanos del estándar ISO 27002:2007 están incluidos (indicados en el Anexo No 4 de este documento)
Requerimientos ISO 27002:2007, sección 9	Verificar que los controles de Seguridad Física y Ambiental del estándar ISO 27002:2007 están presentes (ver Anexo No 4)
Requerimientos ISO 27002:2007, sección 10	Rectificar que los controles de Gestión de Comunicaciones y Operaciones del estándar ISO 27002:2007 están considerados (ver Anexo No 4)
Requerimientos ISO 27002:2007, sección 11	Verificar la inclusión de los controles de la cláusula de Control de Acceso del estándar ISO 27002:2007 (indicados en el Anexo No 4 de este documento)
Requerimientos ISO 27002:2007, sección 12	Comprobar que se han tomado en cuenta los controles de Adquisición, Desarrollo y Mantenimiento de Sistemas del estándar ISO 27002:2007 (ver Anexo No 4)
Requerimientos ISO 27002:2007, sección 13	Verificar que los controles de Gestión de un incidente en la seguridad de la información estén considerados (ver Anexo No 4)
Administración de claves Criptográficas	Verificar que el Plan de Seguridad contiene un Plan de Administración de Claves Criptográficas para todo el ciclo de vida de estas claves.
Protección del repositorio de acceso público	Verificar que el Plan de Seguridad contiene medidas especiales de protección del repositorio público de certificados.
Protección de información privada	Asegurarse de que el plan incluye medidas de protección de información privada recaudada durante el proceso de registro.

5.3.10 Implementación del Plan de Seguridad de la Información

5.3.10.1 Objetivo

Comprobar que la organización tiene implementado un plan de seguridad coherente con su Política de Seguridad, que permita mostrar un nivel de confianza consistente con los objetivos del negocio.

5.3.10.2 Descripción

El PSC o CE debe mostrar que sus procedimientos de administración de la

seguridad y la capacidad de disponer de las instalaciones, están de acuerdo con el Plan de Seguridad.

Se evalúan:

- Acciones operacionales, procedimientos y mecanismos que permiten lograr los objetivos indicados en el Plan de Seguridad del PSC o CE.
- Controles desplegados o planificados para satisfacer dichos requerimientos.
- Que estos controles sean coherentes con los requerimientos del estándar ISO 27002:2007. En particular los planes correspondientes a los siguientes aspectos:
    1. Organización de la seguridad de la información .
    2. Gestión de activos .
    3. Gestión de las comunicaciones y operaciones .
    4. Control del acceso .
    5. Adquisición, desarrollo y mantenimiento de los sistemas de información .

La evaluación combinará entrevistas con el personal del PSC o CE y Auditorías que incluirán visitas a las instalaciones del PSC o CE para verificar la implementación práctica del plan.

5.3.10.3 Estándares de Evaluación

ISO 27002:2007

5.3.10.4 Documentación Solicitada

Documento descriptivo de la implementación del Plan de Seguridad de la Información del solicitante a PSC o CE, el cual será validado al momento de la auditoría.

5.3.10.5 Detalles de la Evaluación

Aspectos	Evaluación
Relación entre el Plan de Seguridad y los recursos asignados	Verificar que el PSC o CE dispone de los recursos y capacidades para implementar los mecanismos y procedimientos de seguridad (según el NIST SP800-18 y el NIST SP800-26)
Relación entre el plan de seguridad y política de seguridad	Comprobar que los procedimientos y mecanismos de seguridad implementados permiten lograr los objetivos de la política de seguridad.

Relación entre Plan de Seguridad y Evaluación de Riesgos	Verificar que los procedimientos y mecanismos de seguridad implementados permiten lograr el riesgo residual determinado en la Evaluación de Riesgos.
Mantenimiento del Plan de Seguridad	Confirmar que la implementación del Plan de Seguridad incluye los procedimientos que garanticen que la seguridad del PSC o CE se mantiene en el tiempo ante cambios en: amenazas, personal, servicios, componentes tecnológicos, etc.
Relación del Plan de Seguridad con prácticas y la Política de Certificados	Verificar que los objetivos de seguridad enunciados en la DPC y PC del PSC o CE se logran a través del Plan de Seguridad.
Requerimientos ISO 27002:2007, sección 6	Verificar que los controles de Organización de la Seguridad de la información recomendados por el estándar ISO 27002:2007 están implementados (indicados en el Anexo No 4)
Requerimientos ISO 27002:2007, sección 7	Comprobar que los controles de Gestión de Activos recomendados por el estándar ISO 27002:2007 están implementados (ver Anexo No 4)
Requerimientos ISO 27002:2007, sección 8	Verificar que los controles de Seguridad de Recursos Humanos recomendados por el estándar ISO 27002:2007 están implementados (ver Anexo No 4)
Requerimientos ISO 27002:2007, sección 9	Confirmar la implementación de los controles de Seguridad y Física y Ambiental recomendados por el estándar ISO 27002:2007 (ver Anexo No 4)
Requerimientos ISO 27002:2007, sección 10	Validar que los controles de Gestión de las Comunicaciones y Operaciones recomendados por el estándar ISO 27002:2007 están implementados (ver Anexo No 4)
Requerimientos ISO 27002:2007, sección 11	Verificar la implantación de los controles de la cláusula de Control del Acceso recomendados por el estándar ISO 17 27002:2007 799 (ver Anexo No 4)
Requerimientos ISO 27002:2007, sección 12	Confirmar que los controles de adquisición, desarrollo y mantenimiento de los sistemas de información recomendados por el estándar ISO 27002:2007 están implementados (ver Anexo No 4)

Protección del repositorio de acceso público	Verificar que la implementación del Plan de Seguridad contiene medidas especiales de protección del repositorio público de certificados.
Protección de información privada	Comprobar que la implementación del plan incluye medidas de protección de información privada recolectada durante el proceso de registro.

5.3.11 Plan de Administración de Claves Criptográficas. (Implementación y Mantenimiento)

5.3.11.1 Objetivo

Comprobar que la organización implementa un plan de administración del ciclo de vida de sus claves criptográficas coherente con su política de seguridad, que permita mostrar un nivel de confianza consistente con los objetivos del negocio.

5.3.11.2 Descripción

Las claves criptográficas son la base de una infraestructura de claves públicas (PKI), siendo el elemento principal a resguardar y administrar por el PSC o CE, y por lo tanto requiere de un plan especifico para su administración (ETSI TS 102 042 sección 7.2) Contenido de este plan:

- Documentación del ciclo de vida completo de las claves criptográficas, esto es:
  1. Generación de las claves de la Autoridad de Certificación de firma electrónica del PSC o CE
  2. Almacenamiento, respaldo y recuperación de la clave privada de la AC de firma electrónica.
  3. Distribución de la clave pública de la AC de firma electrónica.
  4. Uso de la clave privada por parte de la AC de firma electrónica.
  5. Término del ciclo de vida de la AC de firma electrónica .
- Administración del ciclo de vida del hardware criptográfico utilizado por la AC.
- Servicios de administración de las claves de los signatarios suministradas por la AC (generación de clave y renovación después de vencimiento)

- Preparación de los dispositivos seguros de los signatarios.
- A su vez el plan debe ser consistente con la PC.

5.3.11.3 Estándares de Evaluación

- ETSI TS 102 042

- FIPS 140-2

5.3.11.4 Documentación Solicitada

Documento descriptivo de la implementación del Plan de Administración de Claves Criptográficas de la Organización.

5.3.11.5 Detalles de la Evaluación

Aspectos	Evaluación
Relación entre el Plan de Administración de Claves y los recursos asignados	Verificar que el PSC o CE dispone de los recursos y capacidades adecuados para implementar el plan de administración de claves.
Relación entre Plan de Administración de Claves y Evaluación de Riesgos	Verificar que los procedimientos y mecanismos de administración de claves implementados permiten lograr el riesgo residual determinado en la Evaluación de Riesgos.
Mantenimiento del Plan de Administración de Claves	Confirmar que los procedimientos implementados de acuerdo al Plan de Administración de Claves posibilitan que la seguridad de las claves se mantiene en el tiempo ante cambios en: amenazas, personal, servicios, componentes tecnológicos, etc.
Relación del Plan de Administración de Claves con las prácticas y Política de Certificados	Comprobar que los objetivos de seguridad enunciados en la DPC y PC del PSC o CE se logran a través de la implementación del Plan de Administración de Claves.
Requerimientos ETSI TS 102 042, sección 7.2.1	Verificar que los requerimientos de Generación de Claves de la AC, del estándar ETSI TS 102 042 están considerados.
Requerimientos ETSI TS 102 042, sección 7.2.2	Verificar que los requerimientos de Almacenamiento, Respaldo y Recuperación, del estándar ETSI TS 102 042 están considerados.
Requerimientos ETSI TS 102 042, sección 7.2.3	Confirmar que los requerimientos de Distribución de la clave pública de la AC, del estándar ETSI TS 102 042 están considerados.
Requerimientos ETSI TS 102 042, sección 7.2.5	Verificar que los requerimientos de Uso de Clave de la AC, del estándar ETSI TS 102 042 están considerados.

Requerimientos ETSI TS 102 042, sección 7.2.6	Comprobar que los requerimientos de Fin del Ciclo de Vida de la Clave de la AC, del estándar ETSI TS 102 042 están considerados.
Requerimientos ETSI TS 102 042, sección 7.2.7	Verificar que los requerimientos de Administración del hardware criptográfico del estándar ETSI TS 102 042 están considerados.
Nivel de seguridad del dispositivo seguro de los signatarios	Verificar que el dispositivo seguro de los signatarios cumple como mínimo con los requerimientos del estándar FIPS 140-2 nivel 3 (o Common Criteria EAL 3) en sus elementos de seguridad e implementación de los algoritmos criptográficos estándares.

5.3.12 Evaluación de la Plataforma Tecnológica

5.3.12.1 Objetivo

Evaluar los elementos de seguridad de la plataforma tecnológica utilizada para la generación, publicación y administración de certificados de firma electrónica y LCR.

5.3.12.2 Descripción

Evaluar la seguridad de los elementos que constituyen la plataforma tecnológica del PSC o CE. Se debe considerar componentes hardware y software que conforman la infraestructura PKI del PSC o CE, así como, todos los elementos de apoyo a su operación e interrelación, como protocolos y servicios.

Los elementos a considerar son:

- Módulo criptográfico.
- Módulo AC (Autoridad de Certificación)
- Módulo AR (Autoridad de Registro)
- Módulo de Almacenamiento y Publicación de Certificados.
- Protocolos de comunicación entre AC y AR.
- Elementos de administración de logs y Auditoría.

5.3.12.3 Estándares de Evaluación

FIPS 140-2, ISO/IEC 15408 o equivalente.

5.3.12.4 Documentación Solicitada

Documento descriptivo de la implementación de la infraestructura tecnológica.

Este documento debe incluir al menos, planos de interconexión de sistemas, cableado de red de datos, cableado de poder principal y auxiliar, dispositivos de seguridad y control de acceso, y todo aquello relevante que permita demostrar la confiabilidad de la infraestructura tecnológica.

Manuales del fabricante de los productos hardware y software relevantes.

Documentación del fabricante que acredite el correspondiente nivel de seguridad.

5.3.12.5 Detalles de la Evaluación

Aspectos	Evaluación
Módulo criptográfico	1. Funcionalidad y operación: • Generar pares de clave privada y pública con claves de al menos 4096 bits • Capacidad de firma y cifrado 2. Seguridad • Existencia de sistema de control de acceso para acceder a la clave privada • Existencia de controles de acceso para acceder a funcionalidades de firma y cifrado 3. Ciclo de vida • Capacidad de respaldar la clave privada, en forma segura • Capacidad de recuperar la clave privada de respaldo (back-up) 4. Auditoría • Capacidad de generar log auditable para administración de contingencia y accesos maliciosos 5. Documentación • Manuales de operación, configuración y puesta en marcha • Procedimiento de recuperación ante contingencia
Módulo AC (Autoridad de Certificación)	1. Funcionalidad y operación: • Capacidad para generar certificados con claves de al menos 2048 / 4096 bits, según corresponda al tipo de certificado

	emitido. • Capacidad de suspensión y revocación de certificados • Capacidad para generar LCRs • Indicar fecha de publicación y de nueva renovación de la LCR. • Capacidad para generar certificados de firma electrónica • Capacidad de generar certificados de comunicación segura, entre AC y AR, si corresponde a la arquitectura (CC P2 FTP_ITC.1). • Capacidad de entregar certificados y LCR a directorios públicos X500. 2. Seguridad. • Existencia de sistema control de acceso para acceder a la generación de certificados (CC P2 FIA_SOS.2) • Existencia de sistema de control de acceso para acceder a los sistemas de administración y Auditoría (CC P2 FIA_UAU.2) 3. Ciclo de vida. • Capacidad de emitir, suspender y revocar certificados • Capacidad de revocar certificado raíz y generar uno nuevo 4. Auditoría. Capacidad de generar log auditable para administración de contingencia. Actividades del personal autorizado y accesos maliciosos. 5. Documentación. • Manuales de operación, configuración y puesta en marcha. • Procedimiento de Recuperación ante contingencia.
Módulo de AR (Autoridad de Registro)	1. Funcionalidad y operación: • Capacidad de recibir requerimientos de certificados (CC P2 FCS_CKM.2). • Solicitar certificado a la AC. 2. Seguridad: • Existencia de sistema control de acceso para acceder a la generación de certificados.

	• Existencia de sistema de control de acceso para acceder a los sistemas de administración y Auditoría. 3. Ciclo de vida: • Capacidad de validación de datos de los certificados y solicitud de certificados a la AC. 4. Auditoría: • Capacidad de generar log auditable para administración de contingencia y accesos maliciosos. 5. Documentación: • Manuales de operación, configuración y puesta en marcha. • Procedimiento de Recuperación ante contingencia.
Módulo de Almacenamiento y Publicación de Certificados	Almacenamiento de certificados en base de datos X500, y publicación a través de protocolos LDAP v2.0 y/o OCSP V1.0.
Protocolos de comunicación entre AR y AC	Capacidad de generar certificados de comunicación segura, entre AC y AR, si corresponde a la arquitectura, utilizando un protocolo estándar de la industria (CC P2 FTP_ITC.1)
Elementos de administración de log y Auditoría	Deben existir módulos de log y de Auditoría, que permitan verificar los intentos de acceso, los accesos y las operaciones dañinas, sean estas intencionadas o no.

5.3.13 Declaración de Prácticas de Certificación (DPC) y Política de Certificados (PC)

5.3.13.1 Objetivo

Verificar que el PSC o CE disponga de un documento, que señale los procedimientos de gestión de certificados y los diferentes tipos de certificados a otorgar, según se establece en la LSMDFE y su Reglamento Parcial.

5.3.13.2 Descripción

Los elementos principales que debe contener la DPC, son las delimitaciones de responsabilidad y las obligaciones tanto del PSC o CE, como del signatario.

Además debe quedar explícito, tanto el ciclo de vida de los certificados, desde su solicitud hasta el término de su vida útil, como el ciclo de vida del PSC o CE, desde el inicio hasta el fin del mismo.

Este requisito es relevante no sólo para el signatario del certificado sino para

todas las entidades involucradas, incluyendo quienes reciben un documento firmado electrónicamente.

La DPC y PC se presentan en un solo documento, en el cual se verificará al menos: que permita la interoperabilidad con otro PSC o CE y entregue la confianza necesaria para que los documentos firmados en forma electrónica por el signatario de un certificado, se ciñan a la forma de operar recomendada y sean equivalentes a una firma autógrafa en las circunstancias que indica la LSMDFE

5.3.13.3 Estándares de Evaluación

- RFC 3647
- ETSI TS 102 042

5.3.13.4 Documentación Solicitada

Documento de la Declaración de Prácticas de Certificación (DPC) y Política de Certificados (PC) con los diferentes tipos de estructura de campos de certificados. Ver anexo No 5.

5.3.13.5 Detalles de la Evaluación

Aspectos	Evaluación
Verificar estructura	Verificar que la DPC contiene al menos los tópicos indicados en el Anexo No 5 de este documento.
Signatarios	Se debe indicar a quien se le puede otorgar un certificado de firma electrónica.
Usos del certificado	Se debe indicar los propósitos para el cual fue emitido el certificado y sus limitaciones, indicando cuales usos son permitidos y cuales no.
Publicación de información de la AC y Repositorios de los Certificados	Se debe verificar la publicación de los certificados, LCR, y DPC, su frecuencia de publicación, así como la disponibilidad de los repositorios y sus controles de acceso.
Identificación y Autenticación	Se debe comprobar el registro del nombre del signatario, la validación inicial de su identidad, así como la identificación y autenticación de las solicitudes de renovación y revocación de la clave.
Ciclo de vida de los certificados	Confirmar que para cada etapa del ciclo de vida de los certificados (emisión/revocación/suspensión/renovación)

	estén establecidos los procedimientos y deberes del PSC o CE.
Controles de seguridad física, de gestión y de operaciones	Se debe comprobar la existencia de los controles de seguridad física, funcionales, de seguridad personal, los procedimientos de control de seguridad, los archivos de informaciones y registros. Además se debe contemplar que exista la documentación de procedimientos de la recuperación en caso de desastre y en caso del cese de la actividad del PSC o CE, que incluyan los procedimientos de término y de traspaso a otro PSC u organismo que asuma la responsabilidad de mantener la continuidad de los servicios, en tanto existan certificados vigentes.
Controles de Seguridad técnica	Comprobar la existencia de las medidas de seguridad adoptadas por el PSC o CE para la generación e instalación de las claves privada y pública, la protección de la clave privada, los datos de activación. Además se debe verificar los siguientes controles de seguridad: del computador, del ciclo de vida y de la red, así como los controles de ingeniería de los módulos criptográficos.
Perfiles de certificados, OSCP y LCR	Se verificará que el perfil de los certificados cumpla con los estándares internacionales vigentes, aplicables para las infraestructuras de claves públicas y los certificados electrónicos. En forma similar se verificará que el perfil de la LCR y el OCSP se adapten al estándar correspondiente.
Auditoría de conformidad	Se debe verificar que el PSC o CE cumpla con la frecuencia de la realización de auditorías internas.
Aranceles y responsabilidad financiera	Se refiere a las tasas establecidas para la emisión, renovación y revocación de certificados.
Confidencialidad de la información de los signatarios /protección de datos	Existencia de procedimientos de protección de la información de los signatarios.

Obligaciones AC, AR, signatario	Descripción de las obligaciones que contraen las entidades involucradas en la emisión y utilización de un certificado.
Las obligaciones y responsabilidades del PSC o CE	Comprobar que exista una declaración de las obligaciones y deberes del PSC o CE.
Las obligaciones y responsabilidades del signatario	Verificar que existan definiciones de los deberes y obligaciones de los signatarios.
Renuncias de garantías y limitación de responsabilidades	Concordancia de la DPC y PC con los procedimientos operacionales.
Modificaciones	Entre los requisitos comerciales y legales, todo PSC o CE debe tener procedimientos que especifiquen una autoridad que apruebe los cambios aplicables a su DPC, así como su publicación y notificación.

5.3.14 Modelo de Operación de la Autoridad de Certificación (AC) del PSC o CE

5.3.14.1 Objetivo

Comprobar a través de la documentación presentada que el Modelo de Operación cumple con los requerimientos y obligaciones que dispone la LSMDFE y su Reglamento Parcial en relación con la confiabilidad e interoperabilidad en la forma de operar y prestar los servicios de la AC en un PSC o CE.

5.3.14.2 Descripción

El Modelo de Operación debe responder al menos a las siguientes preguntas:

- ¿Cuáles son los servicios prestados por la AC del PSC o CE?.
- ¿Cómo se interrelacionan los diferentes servicios?
- ¿En qué lugares opera?.
- ¿Qué tipos de certificados se entregan?
- ¿Cómo se pretende hacer esto, incluyendo servicios con terceros?.
- ¿Cómo se protegerán los activos?

5.3.14.3 Estándares de Evaluación

Este apartado no aplica

5.3.14.4 Documentación Solicitada

Descripción del Modelo de Operación de la AC del PSC o CE

5.3.14.5 Detalles de la Evaluación

Aspectos	Evaluación
Consistencia del documento	Se verificará que el documento incluya todas las partes mencionadas en el documento tipo descrito en el Anexo No 9.
Resumen Ejecutivo	Se verificará que el resumen incluya: a) Un resumen coherente del contenido del documento b) La historia de la empresa. c) Relaciones comerciales con proveedores de insumos o servicios para sus operaciones.
Componentes del sistema	Se verificará que el modelo comprenda los siguientes aspectos: a) Interfaces con AR b) Implementación de elementos de seguridad c) Procesos de administración d) Sistema de directorios para los certificados e) Procesos de Auditoría y respaldo f) Bases de Datos g) Privacidad h) Entrenamiento del personal
Proceso de Certificación	Se verificará que el modelo considere la generación de claves para el signatario de acuerdo a la PC.
Plan de Auditoría	Se verificará que el modelo considere en el plan de Auditoría lo siguiente: a) Seguridad y dispositivos de seguridad b) Restricciones del personal c) Interfaces de administración d) Procedimientos de recuperación de desastres e) Procedimientos de respaldo
Seguridad	Se verificará que el modelo incluya los requerimientos de: a) La seguridad física y ambiental de las instalaciones. b) Seguridad de recursos humanos. c) Nivel de seguridad del módulo criptográfico.

5.3.15 Modelo de Operación de la Autoridad de Registro (AR) del PSC o CE

5.3.15.1 Objetivo

Comprobar los aspectos mínimos que disponen la LSMDFE y su Resoluciones con relación a conformidad con los requisitos de confiabilidad e interoperabilidad en la forma de operar y prestar sus servicios.

5.3.15.2 Descripción

El Modelo de Operación debe responder a:

- ¿Cuales son los servicios de registro prestados por el PSC o CE?.
- ¿En qué lugares se ofrece dichos servicios?.
- ¿Que tipos de certificados se entregan?.
- ¿Cómo se pretende hacer esto, incluyendo los servicios prestados por terceros?.

Según la norma técnica ETSI TS 102 042 se entiende que el PSC o CE tiene la obligación de generar y entregar en forma segura la clave privada del signatario de un certificado de firma electrónica emitido por él, asegurar la fiabilidad del dispositivo seguro y de los mecanismos que el signatario utiliza para firmar.

5.3.15.3 Estándares de Evaluación

ETSI TS 102 042

5.3.15.4 Documentación Solicitada

Descripción del Modelo de Operación de la AR

5.3.15.5 Detalles de la Evaluación

Aspectos	Evaluación
Consistencia del documento	Se verificará que el documento incluya todas las partes requeridas del documento tipo descrito en el Anexo No 10 de este documento.
Resumen ejecutivo	Se valida que el resumen ejecutivo sea coherente con el contenido del documento.
Componentes del sistema	Se verificará que el modelo comprenda los siguientes aspectos: a) Interfaces con la AC b) Implementación de dispositivos de seguridad c) Procesos de administración d) Procesos de Auditoría y respaldo e) Bases de Datos f) Privacidad

	g) Entrenamiento del personal
Proceso de Certificación	Se valida que el modelo de registro del signatario provea una identificación unívoca del signatario y el modelo de uso de la clave privada provea la confianza requerida en el sistema.
Plan de auditoría	Se verificará que el modelo de la AR incluya auditoría de lo siguiente: a) Dispositivos de seguridad b) Seguridad c) Restricciones del personal d) Interfaces de administración e) Procedimientos de recuperación de desastres f) Procedimientos de respaldo
Seguridad	Se verificará que el modelo de la AR incluya lo siguiente: a) Descripción de la seguridad física y ambiental de las instalaciones b) Seguridad de recursos humanos

5.3.16 Manual de Operación de la Autoridad de Certificación (AC)

5.3.16.1 Objetivo

Comprobar a través de la documentación presentada, el cumplimiento de los aspectos operacionales mínimos que dispone la LSMDFE y su Reglamento parcial, con relación a los requisitos de confiabilidad e interoperabilidad en la forma de operar y prestar los servicios de la AC de un PSC o CE.

5.3.16.2 Descripción

El propósito del manual es describir la administración diaria y las prácticas operacionales de la AC y garantizar que las directrices primarias de la DPC y PC estén implementadas operacionalmente; con el fin de facilitar al personal (de operaciones, consultores y/o auditores), la comprensión de esta información, se permite el uso de gráficos, diagramas de flujo, funcionales, líneas de tiempo, etc.

El Manual de Operación de la AC deberá tener al menos las siguientes características:

- Ser consistente con la Política de Certificados.
- Incluir la interacción entra la AC y la AR.

- Describir los controles de seguridad física, de red, de recursos humanos y de procedimientos.
- Incluir los procedimientos adoptados para el manejo de claves públicas y privadas

5.3.16.3 Estándares de Evaluación

ETSI TS 102 042

RFC 3647

5.3.16.4 Documentación Solicitada

Manual de operación de la AC del PSC o CE

5.3.16.5 Detalles de la Evaluación

Aspectos	Evaluación
Nómina y descripción de cargos	Nómina de los cargos de personal, con la descripción de las responsabilidades y los procedimientos en que los empleados realizan sus funciones.
Referencias de los cargos en los planes de la PSC o CE	Referencia del personal en los planes de continuidad del negocio y los planes de recuperación de desastres y emergencia.
Descripción de las Operaciones	Descripción detallada de los siguientes procedimientos: **1.** Generación de pares de claves **2.** Publicación de la LCR **3.** Publicación de la información del certificado **4.** Distribución de claves y certificados **5.** Renovación de certificados **6.** Renovación de certificados luego de una revocación **7.** Medidas de control de acceso **8.** Procedimientos de respaldo y recuperación
Actualización de DPC y PC	Procedimiento de actualización de la DPC y PC de firma electrónica.
Servicios de la AC	Descripción de los servicios de la AC
Interacción AC - AR	El documento cubre la interacción entre la AC y AR

5.3.17 Manual de Operación de la Autoridad de Registro (AR)

5.3.17.1 Objetivo

Comprobar a través de la documentación presentada los aspectos operacionales mínimos que dispone la LSMDFE y su reglamento parcial con relación a los requisitos de confiabilidad e interoperabilidad de la operación del PSC o CE para realizar las funciones de Autoridad de Registro.

5.3.17.2 Descripción

El Manual de Operación deberá describir como operará el servicio de registro del PSC o CE y su administración diaria. Entre otros aspectos debería tener las siguientes características:

- Ser consistente con la PC.
- Describir el plan de entrenamiento de los empleados.
- Incluir la forma en que se verifica la identidad de las personas.
- Incluir procedimientos de entrega y uso de la clave privada por los signatarios de los certificados. Según la norma ETSI TS 102 042, se entiende que el PSC o CE tiene la obligación de generar y entregar en forma segura la clave privada del signatario de un certificado de firma electrónica emitido por él, asegurar la fiabilidad del dispositivo seguro y los mecanismos que el signatario utiliza para firmar.
- Contener la metodología adoptada para manejar los temas de:
  - Análisis de riesgos
  - Plan de recuperación de desastres
  - Plan de seguridad
- Incluir la interacción entre las unidades internas que cumplen la función de AC y AR.

5.3.17.3 Estándares de Evaluación

RFC 3647

5.3.17.4 Documentación Solicitada

Manual de Operación de la AR

Manual técnico de los dispositivos seguros de firma electrónica

5.3.17.5 Detalles de la Evaluación

Aspectos	Evaluación
Nómina y descripción de cargos	Nómina de los cargos de personal empleado, con la descripción de los procedimientos operacionales y la forma en que los empleados realizan sus funciones.
Proceso de registro	Se verifica el registro del signatario. La autenticación,

	confirmación de su identidad y forma de política para comprobar el nombre del signatario.
Entrega segura de los datos de creación de firma	El PSC o CE debe tener implementados procedimientos y prácticas que permitan entregar en forma personal y segura los datos de creación de firma al signatario del certificado.
Dispositivo seguro y mecanismos de firma del signatario	El PSC o CE debe tener implementados procedimientos y prácticas que aseguren que una vez entregados los datos de creación de firma sólo el signatario tenga control de ellos. El dispositivo seguro entregado al signatario debe firmar internamente el documento sin ser jamás accesible la clave privada del signatario. El mecanismo de control de acceso a la clave privada sólo debe ser conocido por el signatario al momento de la entrega del dispositivo y en lo posible modificable por el mismo signatario, antes de ser utilizado por primera vez. El dispositivo seguro debe contar con mecanismos que inhabiliten el dispositivo en caso de reiterados intentos fallidos de acceso. El PSC o CE debe entregar al signatario herramientas, aplicaciones e instrucciones para que el signatario pueda firmar en forma segura.
Capacitación y servicio al signatario	El PSC o CE debe implementar procedimientos de capacitación que permitan al signatario manejar en forma segura e informada el dispositivo de firma, y además mantener un servicio de atención para responder y solucionar dudas de los signatarios.
Referencias de los cargos en los planes de continuidad de negocios del PSC o CE	Referencia del personal en los planes de continuidad del negocio y los planes de recuperación de desastres y contingencia
Planes de contingencia	Descripción de planes de emergencia
Descripción de las operaciones	Descripción detallada de los siguientes eventos: **1.** Procedimiento certificados seguro de suspensión y revocación de Medidas de control de acceso **2.** Procedimientos de respaldo y recuperación

Interacción entre AR del PSC o CE	El documento cubre los procedimientos que involucren la interacción entre la AC y AR

5.3.18 Evaluación del Personal.

5.3.18.1 Objetivo

Verificar que el PSC o CE emplea personal calificado para la prestación de los servicios ofrecidos, en el ámbito de la firma electrónica y los procedimientos de seguridad y de gestión, con el fin de minimizar los riesgos de errores humanos, robos o mal uso de los atributos del cargo.

5.3.18.2 Descripción

Se evaluará en conformidad al análisis de riesgos del PSC o CE que el personal que maneja o tiene acceso a sistemas e información sensible cumpla al menos con las siguientes condiciones:

a) Que tenga la calificación técnica o profesional requerida para el cargo o función que desempeña.
b) Que tenga la experiencia mínima requerida para el cargo y función que desempeña.
c) Que esté instruido en los procedimientos mínimos de seguridad que debe guardar en su función.

Se evalúa el procedimiento que utiliza el PSC o CE para reclutar, seleccionar, evaluar y contratar personal crítico.

El personal de operaciones y sistemas no debería tener acceso a funciones de confianza, hasta que todos sus antecedentes hayan sido razonablemente verificados.

Los empleados que manejen información sensible, deben ser personal fijo, y deben existir contratos de confidencialidad que se extiendan más allá de la vigencia del contrato del empleado y/o empresa externa.

5.3.18.3 Estándares de Evaluación

- ISO 27002:2007
- ETSI TS 102 042

5.3.18.4 Documentación Solicitada

Perfiles de los cargos del personal que maneja información o sistemas sensibles Currículos de las personas que ocupan los cargos y funciones sensibles.

Evidencia de Identificación del personal calificado como crítico, durante la visita del experto designado por la Superintendencia, en la forma que él lo solicite (Presentación de CV, foto, huella biométrica, etc.)

5.3.18.5 Detalles de la Evaluación

Aspectos	Evaluación
Experiencia profesional del personal crítico	Se valida la experiencia del personal crítico que trabaja para el PSC o CE, verificando la concordancia de los perfiles en cada cargo y función, con el análisis de riesgos.
Capacitación del personal crítico en aspectos de seguridad acorde a su función y cargo.	Se confirma que el personal crítico esté capacitado en las prácticas de seguridad que debe observar de acuerdo a su cargo y función.
Procedimiento de contratación del personal crítico	Se valida el procedimiento definido por el PSC o CE para la contratación del personal crítico.

5.4 Descripción del Procedimiento

Ver Norma SUSCERTE No 027, la cual presenta una Guía para la Acreditación de Proveedores de Servicios de Certificación.

6 ANEXOS NORMATIVOS

Anexo No 1 Resumen de Recaudos Técnicos para la Acreditación

N°	Nombre de Recaudo	Normas y Guías	Documentación Solicitada
T01 Infraestructura de Claves Públicas			
T01.1	Certificado tipo de firma electrónica	- ISO/IEC 9594-8 - ITU-T X.690	Modelo de Certificado tipo de firma electrónica emitido por el solicitante a PSC o CE
T01.2	Lista de certificados revocados y el certificado de firma electrónica de la AC que la emite	- ISO/IEC 9594-8	- DPC y PC del solicitante a PSC o CE - LCR y certificado de firma electrónica de la AC que la emite
T01.3	Registro de acceso público	Este apartado no aplica	Documento descriptivo que contenga al menos: detalle del sitio web donde se publicará la información, descripción de la tecnología, disponibilidad, accesibilidad, conexión, esquemas y diagramas de funcionamiento, medidas de seguridad y sitio web de prueba con funcionalidades requeridas
T01.4	Modelo de confianza	Este apartado no aplica	Modelo de confianza utilizado por el PSC o CE o alternativamente la DPC y PC, si contiene dicho punto.
T02 Seguridad			
T02.1	Evaluación de riesgos	Este apartado no aplica	Evaluación de riesgos o documento equivalente .
T02.2	Política de seguridad de la información	- ISO/IEC 27002:2007	Política de seguridad de la información.
T02.3	Plan de continuidad del negocio y recuperación ante desastres.	- ISO/IEC 27002:2007 - ETSI TI 102 042	-Plan de continuidad del negocio y plan de recuperación ante desastres
T02.4	Plan de seguridad de la información	- ISO/IEC 27002:2007	Plan de seguridad de la información.
T02.5	Implementación del plan de seguridad de la información.	- ISO/IEC 27002:2007	Documento descriptivo de la implementación del plan de seguridad de la información. Esto es validado en la auditoria al PSC o CE

T02.6	Plan de administración de claves criptográficas.	- ETSI TI 102 042 - FIPS 140-2	Documentación de la implantación del plan de administración de claves criptográficas.
T03 Plataforma Tecnológica			
T03.1	Evaluación de la plataforma tecnológica	- FIPS 140-2 - ISO/IEC 15408	Documento descriptivo de la implementación de la infraestructura tecnológica
T04 Políticas de Certificación			
T04.1	Declaración de prácticas de certificación y políticas de certificados	- ETSI TI 102 042 - RFC 3647	Debe seguirse las recomendaciones del estándar RFC 3647 y ETSI TS 102 042. Incluir la estructura de campos de los diferentes tipos de certificados a emitir. Debe presentar las PC para cada tipo de certificado.
T04.2	Modelo de Operación de la Autoridad de Certificación (AC) del PSC o CE	Este apartado no aplica	Descripción del Modelo de Operación de la AC del solicitante a PSC o CE
T04.3	Modelo de Operación de la Autoridad de Registro (AR)	- ETSI TI 102 042	Descripción del Modelo de Operación de la AR del solicitante a PSC o CE
T05 Administración de los Servicios de Certificación Electrónica			
T05.1	Manual de Operación de la Autoridad de Certificación (AC) del PSC o CE	- ETSI TI 102 042 - RFC 3647	Manual de Operación de la Autoridad de Certificación (AC) del PSC o CE
T05.2	Manual de Operación de la Autoridad de Registro (AR)	- RFC 3647	- Manual de Operación de la AR - Manual técnico de los dispositivos seguros de firma electrónica
T06 Modelo Organizacional			
T06.1	Estructura organizativa	- ISO/IEC 27002:2007 - ETSI TI 102 042	Estructura organizativa
T06.2	Evaluación del personal	- ISO/IEC 27002:2007 - ETSI TI 102 042	Perfiles de los cargos del personal que maneja información o sistemas sensibles - Currículos de las personas que ocupan los cargos y funciones sensibles - Procedimientos de seguridad aplicados en la contratación - Identificación del personal calificado como crítico, durante la visita del experto designado por SUSCERTE.

Anexo N° 2 Modelo de Confianza

El modelo de confianza es el esquema por el cual un signatario de un certificado de firma electrónica emitido por un PSC o CE acreditado puede confiar en dicho certificado.
El esquema definido en la LSMDFE y su reglamento parcial, deja en manos del PSC implementar el mecanismo por el cual un signatario que confíe en él, pueda confiar en cualquier otro PSC o CE acreditado.
El mecanismo propuesto consiste en que cada PSC o CE mantenga en su repositorio de acceso público los certificados de todos los Proveedores acreditados, de tal manera que los signatarios que confíen en él puedan instalar en sus aplicaciones estos certificados.
El método debe incluir mecanismos de seguridad para evitar que se puedan reemplazar los certificados en el repositorio o durante su transmisión, sin que ello no pueda ser detectado por el signatario.

Anexo No 3 Ejemplo de Valoración de Riesgos

A continuación se presenta un cuadro de valoración solo como un ejemplo, para propósitos de guía.

Completar el siguiente cuadro de ejemplo de Valoración de Riesgo, identificando el activo, la posible amenaza, la posibilidad de que suceda, el daño en caso de ocurrir la amenaza, riesgo resultado, riesgo requerido y prioridad de la contramedida:

Identificación del activo	Amenaza al Activo	Posibilidad de ocurrencia de la Amenaza	Daño de ocurrir la amenaza	Riesgo resultado	Riesgo Requerido	Prioridad de la contra medida
Veracidad de la información pública disponible en el sitio web	Pérdida de confianza o buena fe debido a "hacking" de una página web	Alta	Menor	Medio	Bajo	1
Disponibilidad de servicio de correo externo	Ataque al servidor de correos tipo denegación de servicios	Extrema	Dañino	Crítico	Bajo	4

	(DoS)					
Confiabilidad de sitio web relacionado con comercio electrónico	Falla accidental de equipo o suministro electrónico	Media	Grave	Crítico	Nulo	4
Acceso seguro a los servicios de red interna por personal autorizado, desde redes externas.	Pérdida del token criptográfico o claves requeridas para acceder a los canales seguros	Muy baja	Serio	Medio	Bajo	1

Anexo N° 4 Controles del Estándar ISO/IEC 27002:2007, Secciones 5 a 14, Aplicables

SECCIÓN 5 Política de Seguridad

5.1 Política de Seguridad de la información

Objetivo: Dirigir y dar apoyo a la gestión de la seguridad de la información de acuerdo con los requisitos del negocio, las leyes y reglamentos pertinentes.

- Documento de la política de seguridad de la información (5.1.1)
- Revisión de la política de seguridad de la información (5.1.2)

SECCIÓN 6 Organización de la Seguridad de la información

6.1 Organización interna

Objetivo: Gestionar la seguridad de la información dentro de la organización.

- Compromiso de la gerencia para la seguridad de la información (6.1.1).
- Asignación de responsabilidades sobre seguridad de la información (6.1.3) .
- Proceso de autorización para los recursos de procesamiento de la información (6.1.4) .
- Acuerdos de confidencialidad (6.1.5) .

- Revisión independiente de la seguridad de la información (6.1.8) .

6.2 Grupos o personas externas

Objetivo: Mantener la seguridad de la información y los recursos de procesamiento de la información de la organización que son accesados, procesados, comunicados o gestionados por partes externas.

- Identificación de los riesgos relacionados a partes externas (6.2.1) .
- Tratamiento de la seguridad en las relaciones con clientes (6.2.2) .
- Tratamiento de la seguridad en los acuerdos de terceras partes (6.2.3) .

SECCIÓN 7 Gestión de activos

7.1 Responsabilidad por los Activos

Objetivo: Alcanzar y mantener la protección apropiada de los activos de la organización.

- Inventario de activos (7.1.1)
- Propiedad de los activos (7.1.2)
- Utilización aceptable de los activos (7.1.3)

7.2 Clasificación de la Información

Objetivo: Asegurar que la información reciba un apropiado nivel de protección.

- Directrices de clasificación (7.2.1)
- Etiquetado y manejo de la información (7.2.2)

SECCIÓN 8 Seguridad del recurso humano

8.1 Previo al empleo[2]

Objetivo: Asegurar que los empleados, los contratistas y usuarios de terceras partes comprendan sus responsabilidades, que sean apropiados para los roles considerados y reducir el riesgo de robo, fraude o mal uso de los recursos.

- Roles y responsabilidades (8.1.1)
- Investigación (8.1.2)

2 Explicación: La palabra “Empleo” significa cubrir todas las diferentes situaciones siguientes: empleo de personas (temporal o permanente), la asignación de roles de trabajo, cambio de roles de trabajo, asignación de contratos y la terminación de cualquiera de estos arreglos

• Términos y condiciones de empleo (8.1.3)

8.2 Durante el empleo

Objetivo: Asegurar que todos los empleados, contratistas y usuarios de terceras partes son conscientes de las amenazas y aspectos relacionados con la seguridad de la información, sus responsabilidades y obligaciones, y que estén equipadas para respaldar la política de seguridad de la organización en el curso de su trabajo normal, y reducir el riesgo de error humano.

• Responsabilidades de la Dirección (8.2.1)

• Toma de conciencia, educación y formación en la seguridad de la información (8.2.2)

• Proceso disciplinario (8.2.3)

8.3 Terminación o cambio de empleo

Objetivo: Asegurar que los empleados, contratistas y usuarios de terceras partes se retiran de una organización o cambian el empleo de una manera ordenada.

• Responsabilidades de terminación (8.3.1)

• Devolución de los activos (8.3.2)

• Retiro de los derechos de acceso (8.3.3)

SECCIÓN 9 Seguridad Física y Ambiental

9.1 Áreas Seguras

Objetivo: Prevenir el acceso físico no autorizado, daño e interferencia a las instalaciones e información de la organización.

• Perímetro de seguridad física (9.1.1)

• Controles físicos de entrada (9.1.2)

• Seguridad de oficinas, habitaciones e instalaciones (9.1.3)

• Protección contra las amenazas externas y ambientales (9.1.4)

• Trabajo en áreas seguras (9.1.5)

• Áreas de acceso público, entrega y carga (9.1.6)

9.2 Seguridad de los equipos

Objetivo: Prevenir pérdidas, daños, robo o comprometer los activos e interrupción de las actividades de la organización.

• Ubicación y protección del equipo (9.2.1)

- Servicio de Apoyo (9.2.2)
- Seguridad del cableado (9.2.3)
- Mantenimiento de equipos (9.2.4)
- Seguridad de equipos fuera de las instalaciones de la organización (9.2.5)
- Seguridad en la reutilización o eliminación de equipos (9.2.6)
- Retiro de la propiedad (9.2.7)

SECCIÓN 10 Gestión de Comunicaciones y operaciones

10.1 Procedimientos y Responsabilidades de Operación

Objetivo: Asegurar la operación correcta y segura de los recursos de tratamiento de información.

- Documentación de procedimientos operativos (10.1.1)
- Gestión de cambio (10.1.2)
- Separación de tareas (10.1.3)
- Separación de los recursos para el desarrollo, prueba y operación (10.1.4)

10.2 Gestión de entrega de servicio de tercera parte

Objetivo: Implementar y mantener el nivel apropiado de seguridad de la información y entrega del servicio en línea con los acuerdos de entrega del servicio tercera parte.

- Entrega del servicio (10.2.1)
- Seguimiento y revisión de los servicios de tercera parte (10.2.2)
- Gestión de cambios para los servicios de tercera parte (10.2.3)

10.3 Planeación y aceptación del sistema

Objetivo: Minimizar el riesgo de fallas de los sistemas.

- Gestión de la capacidad (10.3.1)
- Aceptación del sistema (10.3.2)

10.4 Protección contra código malicioso y movible

Objetivo: Proteger la integridad del software y de la información.

- Controles contra código malicioso (10.4.1)
- Controles contra código movible (10.4.2)

10.5 Copia de seguridad

Objetivo: Mantener la integridad y la disponibilidad de la información y los recursos de procesamiento de la información.

- Copia de seguridad de la información (10.5.1)

10.6 Gestión de seguridad de la Red

Objetivo: Asegurar la protección de la información en las redes y la protección de su infraestructura de soporte.

- Controles de redes (10.6.1)
- Seguridad de servicios de red (10.6.2)

10.7 Manejo de medios de información

Objetivo: Prevenir la divulgación, modificación, eliminación o destrucción no autorizada de los activos, e interrupción de las actividades del negocio.

- Gestión de medios removibles (10.7.1)
- Disposición de medios (10.7.2)
- Procedimientos de manejo de la información (10.7.3)
- Seguridad de la documentación del sistema (10.7.4)

10.8 Intercambio de Información

Objetivo: Mantener la seguridad de la información y el software intercambiado dentro de una organización y con cualquier entidad externa.

- Políticas y procedimientos de intercambio de información (10.8.1)
- Acuerdos de intercambio (10.8.2)
- Medios de información físicos en tránsito (10.8.3)
- Mensaje electrónico (10.8.4)
- Sistemas de información del negocio (10.8.5)

10.9 Servicios de comercio electrónico

Objetivo: Asegurar la seguridad de servicios de comercio electrónico, y su utilización segura.

- Comercio electrónico (10.9.1)
- Transacciones en línea (10.9.2)
- Información disponible públicamente (10.9.3)

10.10 Seguimiento

Objetivo: Detectar las actividades de procesamiento de la información no autorizadas.

- Registro de auditoría (10.10.1)
- Seguimiento de la utilización de los sistemas (10.10.2)
- Protección de la información de registro (10.10.3)
- Administrador y operador de registros (10.10.4)

• Registro de fallas (10.10.5)

• Sincronización de relojes (10.10.6)

SECCIÓN 11 Control de Accesos

11.1 Requisitos del negocio para el control de accesos

Objetivo: Controlar los accesos a la información.

• Política de control del accesos (11.1.1)

11.2 Gestión de Acceso de usuarios

Objetivo: Asegurar el accesos del usuario autorizado y prevenir el acceso no autorizado a los sistemas de información.

• Registro de usuarios (11.2.1)

• Gestión de privilegios (11.2.2)

• Gestión de contraseñas de usuario (11.2.3)

• Revisión de los derechos de acceso de usuario (11.2.4)

11.3 Responsabilidades de usuarios

Objetivo: Prevenir el acceso de usuarios no autorizados, y comprometer o robar la información y los recursos de procesamiento de información.

• Uso de contraseñas (11.3.1)

• Equipo desatendido del usuario (11.3.2)

• Políticas de escritorios y pantallas limpias (11.3.3)

11.4 Control de Acceso a la Red

Objetivo: Prevenir el acceso no autorizado a los servicios de red.

• Política de utilización de los servicios de red (11.4.1)

• Autenticación de usuarios para conexiones externas (11.4.2)

• Identificación de equipo en redes (11.4.3)

• Protección del diagnóstico remoto y de la configuración de puerto (11.4.4)

• Separación en redes (11.4.5)

• Control de conexión de redes (11.4.6)

• Control de direccionamiento en la red (11.4.7)

11.5 Control de acceso al sistema operativo

Objetivo: Prevenir el acceso no autorizado a los sistemas operativos.

• Procedimientos de conexión segura (11.5.1)

• Identificación y autenticación del usuario (11.5.2)

• Sistema de gestión de contraseñas (11.5.3)

- Utilización de las prestaciones del sistema (11.5.4)
- Sesión inactiva (11.5.5)
- Limitación del tiempo de conexión (11.5.6)

11.6 Control de acceso a las aplicaciones e información

Objetivo: Prevenir el acceso no autorizado a la información contenida en los sistemas de aplicación.

- Restricción de acceso a la información (11.6.1)
- Aislamiento de sistemas sensibles (11.6.2)

11.7 Computación móvil y trabajo a distancia

Objetivo: Asegurar la seguridad de la información cuando se utilizan recursos de computación móvil y de trabajo a distancia.

- Computación móvil y comunicaciones (11.7.1)
- Trabajo a distancia (11.7.2)

SECCIÓN 12 Adquisición, desarrollo y mantenimiento de sistemas de información

12.1 Requisitos de seguridad de los sistemas de información

Objetivo: Asegurar que la seguridad es una parte integral de los sistemas de información.

- Análisis y especificación de los requisitos de seguridad (12.1.1)

12.2 Procesamiento correcto en las aplicaciones

Objetivo: Prevenir los errores, pérdida, modificación no autorizada o mal uso de la información en las aplicaciones.

- Validación de datos de entrada (12.2.1)
- Control del procesamiento interno (12.2.2)
- Integridad de mensaje (12.2.3)
- Validación de los datos de salida (12.2.4)

12.3 Controles Criptográficos

Objetivo: Proteger la confidencialidad, autenticidad o integridad de la información por los medios criptográficos.

- Política sobre la utilización de controles criptográficos (12.3.1)
- Gestión de claves (12.3.2)

12.4 Seguridad de los archivos del sistema

Objetivo: Asegurar la seguridad de los archivos del sistema.

• Control del software operativo (12.4.1)
• Protección de los datos de prueba del sistema (12.4.2)
• Control de acceso al código fuente del programa (12.4.3)

12.5 Seguridad en los procesos de desarrollo y soporte

Objetivo: Mantener la seguridad del software y la información del sistema de aplicación .

• Procedimientos de control de cambios (12.5.1)
• Revisión técnica de aplicaciones después de los cambios de sistema operativo (12.5.2)
• Restricciones en los cambios a los paquetes de software. (12.5.3)
• Fuga de información (12.5.4)
• Desarrollo de software contratado externamente (12.5.5)

12.6 Gestión de vulnerabilidad técnica

Objetivo: Reducir los riesgos que resultan de la explotación de las vulnerabilidades técnicas publicadas.

• Control de las vulnerabilidades técnicas (12.6.1)

SECCIÓN 13 Gestión de incidente de seguridad de la información

13.1 Reportar los eventos y debilidades de seguridad de la información

Objetivo: Asegurar que los eventos y debilidades de seguridad de la información asociadas con los sistemas de información sean comunicados de una manera tal que permita que la acción correctiva sea tomada oportunamente.

• Reporte de los eventos de seguridad de información (13.1.1)
• Reporte de debilidades de seguridad (13.1.2)

13.2 Gestión de los incidentes y mejoras de seguridad de la información

Objetivo: Asegurar que un enfoque coherente y eficaz es aplicado a la gestión de los incidentes de seguridad de la información. • Responsabilidades y procedimientos (13.2.1)

• Aprendizaje de los incidentes de seguridad de la información (13.2.2)

• Recolección de evidencias (13.2.3)

SECCIÓN 14 Gestión de la Continuidad del Negocio

14.1 Aspectos de seguridad de la información de la gestión de la continuidad del negocio

Objetivo: Contrarrestar las interrupciones de las actividades del negocio y proteger los procesos críticos del negocio de los efectos de fallas significativas o desastres de los sistemas de información y asegurar su reanudación oportuna.

• Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio (14.1.1)

• Continuidad del negocio y evaluación de riesgo (14.1.2)

• Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información (14.1.3)

• Marco de planificación para la continuidad del negocio (14.1.4)

• Prueba, mantenimiento y reevaluación de los planes de continuidad del negocio (14.1.5)

Anexo N° 5 Contenido de la Declaración de Prácticas de Certificación (DPC) y Política de Certificados (PC)

1. DPC y PC del PSC o CE

1.1 PRESENTACIÓN

1.2 NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN

1.3 COMUNIDAD DE USUARIO Y APLICABILIDAD

1.3.1 Autoridad de Aprobación de Políticas (AAP)

1.3.2 Autoridad de Certificación AC

1.3.3 Autoridad de Registro (AR)

1.3.4 Certificados Electrónicos

1.3.5 Terceros de buena fe

1.4 USO DE LOS CERTIFICADOS

1.4.1 Usos permitidos

1.4.2 Usos no permitidos

4. EL CICLO DE VIDA DE LOS CERTIFICADOS DEL PSC o CE

4.1 SOLICITUD DE CERTIFICADOS

4.1.1 Proceso de generación de la solicitud de certificados y responsabilidades

4.1.2 Proceso de firma del certificado

4.1.3 Proceso de generación de la solicitud de renovación de las claves del certificado

4.1.4 Procedimiento para realizar una solicitud de revocación de un certificado

4.1.5 Procedimiento para realizar una solicitud de suspensión de un certificado

4.2 TRAMITACIÓN DE SOLICITUD DE UN CERTIFICADO

4.2.1Realización de las funciones de identificación y autenticación

4.2.2 Aprobación o denegación de un certificado

4.2.3 Plazo para la tramitación de un certificado

4.3 EMISIÓN DE CERTIFICADO

4.3.1 Acciones de la AC durante la emisión de un certificado

4.3.2 Notificación al solicitante por parte de la AC acerca de la emisión de su certificado

4.4 ACEPTACIÓN DE CERTIFICADOS

4.4.1 Forma en la que se acepta el certificado

4.4.2 Publicación del certificado por la AC

4.4.3 Notificación de la emisión del certificado por la AC a otras autoridades

4.5 USO DEL PAR DE CLAVES Y DEL CERTIFICADO

4.5.1 Uso de la clave privada del certificado

4.5.2 Uso de la clave pública y del certificado por los terceros de buena fe

4.6 RENOVACIÓN DEL CERTIFICADO CON CAMBIO DE CLAVE

4.6.1 Causas para la renovación de un certificado

4.6.2 Entidad que puede solicitar la renovación de un certificado

4.6.3 Procedimiento de solicitud para la renovación de un certificado

4.6.4 Notificación de la emisión de un nuevo certificado a la AR

Anexo N° 6 Documento Estándar de una Política de Seguridad

Según la ISO 27002:2007: una política de seguridad debe contener enunciados relacionados con:

- Una definición de seguridad de la información, sus objetivos y alcance generales y la importancia de la seguridad como un mecanismo facilitador para intercambiar información

- Un enunciado de la intención de la gerencia, fundamentando sus objetivos y los principios de la seguridad de la información en línea con la estrategia y los objetivos comerciales.

- Un marco referencial para establecer los objetivos de control y los controles, incluyendo la estructura de la evaluación del riesgo y la gestión de riesgo.

- Una explicación breve de las políticas, principios, estándares y requerimientos de conformidad de la seguridad de particular importancia para la organización.

- Una definición de las responsabilidades generales y específicas para la gestión de la seguridad de la información .

- Referencias a la documentación que fundamenta la política

Aunque cada organización debe crear su política y destacar los aspectos que le apliquen, a continuación se mencionan algunos de los considerados más relevantes:

Organización de la seguridad de la información

- Se debe establecer un marco referencial gerencial para iniciar controlar la implementación de la seguridad de la información.

- La gerencia debe aprobar la política de seguridad de la información,asignar los roles de seguridad y coordinar y revisar la implementación de la seguridad en toda la organización.

- Si fuese necesario, se debe establecer una fuente de consultoría sobre seguridad de la información.

- Se debe fomentar un enfoque multi-disciplinario para la seguridad de la información.

Gestión de Activos

- Todos los activos debieran ser inventariados y contar con un propietario nombrado.

- Los propietarios debieran identificar todos los activos y se debiera asignar la responsabilidad por el mantenimiento de los controles apropiados.

Seguridad de recursos humanos

- Especifica los requerimientos de selección del personal de seguridad y como estos serán logrados.

- En caso de no ser necesaria una selección formal por un departamento de seguridad, esta sección detalla la política de verificación indirecta de antecedentes del personal, para asegurar que sea empleado en posiciones de confianza sólo personal adecuado.

- Proveer directrices bajo las cuales personal, contratistas, consultores y/o auditores pueden acceder a las dependencias de la organización, darle acceso a información de los sistemas internos, etc.

- También es importante un plan mediante el cual al personal se le da acceso privilegiado a los sistemas críticos.

- Esta sección también debe detallar las responsabilidades asociadas con el uso de los sistemas de la organización y los requerimientos que permitan asegurar que los signatarios estén conscientes de sus responsabilidades y efectos de las violaciones.

Seguridad ambiental y física

- Especifica los objetivos de seguridad física incluyendo, pero no limitado a, eliminación de elementos en desuso, guardias, alarmas de seguridad física, tiempos de respuesta, claves físicas, y estructura de la seguridad física de todas las dependencias relevantes.

- Los medios de procesamiento de información crítica o confidencial debieran ubicarse en áreas seguras, protegidas por los perímetros de seguridad definidos, con las barreras de seguridad y controles de entrada apropiados.

- Deben estar físicamente protegidos del acceso no autorizado, daño e interferencia.

Gestión de las comunicaciones y operaciones

- Se deben establecer las responsabilidades y procedimientos para la gestión y operación de todos los medios de procesamiento de la información.

- Chequear la implementación de los acuerdos, monitorear su cumplimiento con los estándares y manejar los cambios para asegurar que los servicios sean entregados para satisfacer los requerimientos acordados por la tercera persona .
- Realizar proyecciones de los requerimientos de la capacidad futura para reducir el riesgo de sobrecarga en el sistema.

- Establecer, documentar y probar los requerimientos operacionales de los sistemas nuevos antes de su aceptación y uso

- Tomar precauciones para evitar y detectar la introducción de códigos maliciosos y códigos móviles no-autorizados.

- Establecer los procedimientos de rutina para implementar la política de respaldo

acordada y la estrategia para tomar copias de respaldo de la data y practicar su restauración oportuna.

- Los medios se deben controlar y proteger físicamente.

- Se debe establecer los procedimientos de operación apropiados para proteger los documentos, medios de cómputo (por ejemplo, cintas y discos), input/output de data y documentación del sistema de una divulgación no-autorizada, modificación, eliminación y destrucción .

- Considerar las implicaciones de seguridad asociadas con el uso de servicios de comercio electrónico, incluyendo las transacciones en línea, y los requerimientos de controles.

- También se debe considerar la integridad y la disponibilidad de la información publicada electrónicamente a través de los sistemas públicamente disponibles .

- Monitorear los sistemas y se debieran reportar los eventos de seguridad de la información. Utilizar bitácoras de operador y registrar las fallas para asegurar que se identifiquen los problemas en los sistemas de información.

Control de Acceso

- Controlar el acceso a la información, medios de procesamiento de la información y procesos comerciales sobre la base de los requerimientos comerciales y de seguridad.

- Especifica los niveles de clasificación de la confidencialidad e importancia de la información que será manipulada o que podría ser accesada por el personal autorizado de los sistemas de información de la organización.

Adquisición, desarrollo y mantenimiento de los sistemas de información

- Identificar y acordar los requerimientos de seguridad antes del desarrollo y/o implementación de los sistemas de información .

- Desarrollar una política sobre el uso de controles criptográficos .

- Controlar el acceso a los archivos del sistema y el código fuente del programa, y los proyectos TI y las actividades de soporte se debieran realizar de una manera segura .

- Controlar estrictamente los ambientes del proyecto y soporte.

- Los gerentes responsables por los sistemas de aplicación también deben asegurar que todos los cambios propuestos para el sistema, sean revisados para chequear que no comprometan la seguridad del sistema o el ambiente de operación.

- Implementar una gestión de la vulnerabilidad técnica de una manera efectiva, sistemática y respetable .

Gestión de un incidente en la seguridad de la información

• Establecer procedimientos formales de reporte y de la identificación de un evento.

• Establecer las responsabilidades y procedimientos para manejar de manera efectiva los eventos y debilidades en la seguridad de la información una vez que han sido reportados. Se debiera aplicar un proceso de mejoramiento continuo para la respuesta a, monitoreo, evaluación y la gestión general de los incidentes en la seguridad de la información .

Gestión de la continuidad del negocio

• Desarrollar e implementar planes para la continuidad del negocio para asegurar la reanudación oportuna de las operaciones esenciales .

• Debe incluir controles para identificar y reducir los riesgos, además del proceso general de evaluación de riesgos, debe limitar las consecuencias de incidentes dañinos y asegurar que esté disponible la información requerida para los procesos comerciales y operacionales.

• La evaluación del riesgo de la continuidad el negocio se debiera llevar a cabo con la participación total de los propietarios de los recursos y procesos comerciales y operacionales.

Cumplimiento

• El diseño, operación, uso y gestión de los sistemas de información pueden estar sujetos a requerimientos de seguridad estatutarios, reguladores y contractuales.

• Durante las auditorías de los sistemas de información deben existir controles para salvaguardar los sistemas operacionales y herramientas de auditoría.

• Los gerentes deberán asegurar que se lleven a cabo correctamente todos los procedimientos de seguridad dentro de su área de responsabilidad para asegurar el cumplimiento de las políticas y estándares de seguridad.

Anexo N° 7 Estándar ETSI TS 102 042 Sección 7.4.8: Administración de la Continuidad

El PSC o CE debe asegurar que las operaciones deben restaurarse tan pronto como sea posible ante la ocurrencia de un desastre, incluyendo el caso del compromiso de la clave privada utilizada para la firma de certificados.

NOTA 1: Otras situaciones de desastre incluyen la falla de componentes críticos de los sistemas del PSC o CE, incluyendo hardware y software.

En particular:

a) El plan de continuidad de negocios del PSC o CE deberá considerar como un desastre el compromiso o sospecha de compromiso de la clave privada de firma del PSC o CE y los procesos de recuperación deben estar disponibles y probados.

b) A continuación de un desastre el PSC o CE deberá, en la medida que sea posible, tomar las medidas que eviten su repetición.

c) En el caso de compromiso de su clave privada, el PSC o CE deber como mínimo tomar las siguientes medidas:

1. Informar del compromiso a todos los subscriptores y sus contrapartes así como a los otros PSC o CE con quienes tiene acuerdos de interoperabilidad, certificación cruzada u otras formas de colaboración.
2. Indicar que los certificados e información del estado de revocación emitidos usando la clave del PSC o CE puede no ser válida, porque ha sido comprometida.

NOTA 2: Se recomienda que cuando otro PSC o CE, con la cual se tiene un acuerdo de colaboración, es informado del compromiso de la clave privada, este debiera revocar cualquier certificado de CA que ha sido emitido por el PSC o CE comprometido.

Anexo No 8 Elementos de Evaluación de un Plan de Seguridad

La evaluación es una valoración de los siguientes aspectos:

- ¿Existe un administrador de la seguridad IT in situ?
- ¿Tiene el administrador de seguridad IT un conocimiento adecuado de su rol, consistente con aquel descrito en el Plan de Seguridad y el Manual de Operación?
- ¿Está el personal de soporte que se identifica en el Plan de Seguridad disponible?
- ¿Tiene el personal de soporte un conocimiento adecuado de su rol, consistente con aquel descrito en el Plan de Seguridad y el Manual de Operación?
- ¿Es el conjunto de signatarios privilegiados del sistema AC o AR consistente con el conjunto de signatarios privilegiados descritos en el plan de seguridad?
- ¿Está la infraestructura computacional y de red instalada y operando de acuerdo a lo descrito en: el Plan de Seguridad, el Manual de Operación, la DPC y PC y el Plan de Continuidad de Negocios y Recuperación ante Desastres?
- ¿Están los mecanismos de seguridad y procedimientos descritos en el Plan de Seguridad instalados y configurados o implementados de acuerdo con el Plan? Se verificará principalmente:

  1. Mecanismos de control de acceso
  2. Captura y revisión de datos de Auditoría
  3. Monitoreo de incidentes de seguridad
  4. Administración de incidentes y procedimientos de respuesta ante incidentes

5. Mantenimiento y uso de la información acerca de vulnerabilidades de las instalaciones de la AC o AR

6. Plan de administración de claves criptográficas

7. Administración de cuentas de signatarios

8. Control de media removible

9. Respaldo y recuperación de datos y sistemas, incluyendo almacenamiento de segundas copias fuera de las instalaciones

10. Control de inventario, incluyendo procedimientos de registro para controlar ubicación y acceso de los activos críticos.

11. Administración del FW Internet

12. Procedimientos y mecanismos que tengan un rol relevante en reducir las amenazas a las operaciones de la AC o AR.

13. Provee la confianza mediante la comprobación en terreno de que la seguridad operacional del PSC o CE se mantendrá en el tiempo dadas las condiciones siguientes:
    - ¿Después que el grupo evaluador se ha retirado?
    - ¿Después de cambios en las amenazas de seguridad, personal, servicios ofrecidos, tecnología e infraestructura?

Anexo N° 9 Pauta de Modelo de Operación de la AC de un PSC o CE

Este documento provee una guía para que un PSC o CE documente el modelo de operaciones de la AC.

El modelo de operaciones es uno de los primeros documentos que debieran ser preparados al iniciar sus actividades un PSC o CE. El cual debería presentar una visión general de cómo interaccionarán los diferentes elementos constituyentes de un PSC o CE.

Cubriendo aspectos operacionales, técnicos, legales, de seguridad y administración.

Algunas de las secciones de este documento pueden no aplicar a todos los PSC o CE y la organización postulante debería presentar en la documentación aspectos que reflejen su circunstancia particular.

Resumen Ejecutivo

Presentar una visión general de las operaciones del PSC o CE. Debiera responder a las siguientes preguntas:

¿Cuál es el producto y servicio?

¿Desde donde se operará?

¿A quien se proveerá de certificados?

¿Quién estará involucrado en las operaciones?

Historia de la Empresa

Descripción breve de los orígenes de la organización, relaciones con los proveedores de tecnología y otras empresas asociadas.

Relaciones Comerciales

Proveer un resumen de las relaciones comerciales del PSC o CE en relación con las operaciones de la PKI.

Si las operaciones involucran otras empresas, describir la relación con estas.

Prefacio del Documento

Describe el propósito y alcance del documento.
Descripción de los tópicos que cubre el documento y sus anexos.

Componentes del Sistema

Describe cuales son las partes funcionales del PSC o CE, en sus distintos modos de operación.
Los componentes que se describen son los necesarios para operar el PSC o CE y pueden incluir, pero no están limitados a: Interfaces entre la AC y AR, componentes de hardware y software.

Administración

Contiene las referencias a las políticas para los clientes, filosofía operacional, elementos estratégicos y de interrelación.
Se deben incluir detalles operacionales, como horarios de atención, personal requerido, infraestructura, etc.
Se puede incluir organigrama de la empresa.

Directorio

Describir brevemente: el estándar que utilice el directorio, por ejemplo x.500 LDAP, la información incluida en el directorio y como afectan las revocaciones al directorio.

Bases de Datos de la AC

Describir brevemente la información que incluyen las bases de datos de la AC. Por ejemplo:

- Registro de ingreso y egreso a los sistemas

- Registro de la creación de certificados
- Detalles de los certificados
- Detalles de las revocaciones

Otros Subsistemas

Cualquier otra información de subsistemas que pueda aplicar:

- Cuando se genera el par de claves, quien realiza esta función (AC/AR/ signatario) Si el signatario genera las claves, indicar por cual medio y describir la tecnología utilizada.
- Medios de comunicación entre la AC y AR. Cuales son las relaciones y dependencias entre ellas.
- Diagramas de los procesos pueden apoyar las descripciones.

Generación de Claves en la AC

Si aplica, describir el proceso de generación de claves. Detalle de los mecanismos de protección de acceso para la generación de claves.

Generación de Certificados

Mostrar como opera la cadena de jerarquía. Incluir referencias al certificado raíz y las relaciones con otras AC si aplica. Por ejemplo, en caso de existir AC subordinadas.

Operaciones de la AC

Este punto debiera describir brevemente otros aspectos sensibles a la seguridad o de naturaleza sensible a las operaciones de la PSC o CE y que no hayan sido descritos anteriormente.

Procedimientos de Recuperación de Datos

Presentar de manera breve la frecuencia de los respaldos y los procedimientos almacenamiento que se seguirán.

Planes de Auditoría

Describir cuales son los componentes del plan de Auditoría de la organización en, por ejemplo:

- Dispositivos de seguridad
- Seguridad

- Restricciones del personal
- Interfaces de administración

Recuperación de Desastres

Descripción de la estrategia para recuperación de desastres incluyendo:

- Definición de roles y responsabilidades
- Ejercicios de práctica para la recuperación de desastres, con cuanta frecuencia se realizan.
- Respaldos en cinta, frecuencia, tipo de respaldo (por ejemplo incremental o total).
- Reiniciar el sistema.
- Procesos de Auditoría y generación de reportes.

Seguridad

Esta sección debe presentar brevemente todos los aspectos de seguridad que están involucrados en las operaciones de la AC y AR. Los detalles de estos aspectos pueden ser referenciados a otros documentos presentados.

Seguridad de las Instalaciones

Provee la descripción física del lugar donde operara la AC y AR.
Puede incluir referencias a otros documentos o procesos de certificación con los cuales cumpla.

Seguridad del Personal

Provee descripción de los requerimientos de seguridad para el personal de la organización, como por ejemplo:

- Referencia a que puestos pueden entrar en zonas restringidas
- Plan de entrenamiento para el personal
- Zonas restringidas para el personal
- Registro de ingresos
- Control de ingreso

Nivel de Seguridad del Módulo Criptográfico

Describe los productos y tecnología que se está utilizando para realizar las operaciones de la PSC o CE, en particular el módulo criptográfico de la AC.

Anexo N° 10 Pauta de Modelo de Operación de la AR de un PSC o CE

Este documento provee una guía para que un PSC o CE documente el modelo de operación de la AR.
El modelo de operación es uno de los primeros documentos que debieran ser preparados por el PSC o CE al iniciar sus actividades. El cual debe presentar una visión general de cómo interaccionarán los diferentes elementos constituyentes de un PSC o CE.
Cubriendo aspectos operacionales, técnicos, legales, de seguridad y administración.
Algunas de las secciones de este documento pueden no aplicar a todos los PSC o CE y la organización postulante debe presentar en la documentación aspectos que reflejen su circunstancia particular.

Resumen Ejecutivo

Debe presentar una visión general de las operaciones de la AR. Debe responder a las siguientes preguntas:

- ¿Cuál es el producto y servicio?
- ¿Desde donde se operará?
- ¿A quien se proveerá de certificados?
- ¿Quién estará involucrado en las operaciones?

Historia de la Empresa

Descripción breve de los orígenes de la organización, relaciones con los proveedores de tecnología y otras empresas asociadas.

Relaciones Comerciales

Proveer un resumen de las relaciones comerciales del PSC o CE en relación con las operaciones de la PKI.
Si las operaciones involucran otras empresas, describir la relación con estas.

Prefacio del Documento

Detalla el propósito y alcance del documento.
Descripción de los tópicos que cubre el documento y sus anexos.

Componentes del Sistema

Describe cuales son los componentes funcionales de la AR, en sus distintos modos de operación.
Los componentes que se mencionen son los necesarios para operar el PSC o CE y pueden incluir, pero no están limitados a: Interfaces entre la AC y AR, componentes de hardware y software.

Administración

Contiene las referencias a las políticas para los clientes o usuarios, filosofía operacional,
elementos estratégicos y de interrelación.
Se deben incluir detalles operacionales, como horarios de atención, personal requerido, infraestructura, etc.
Se puede presentar organigrama de la empresa.

Bases de Datos de la AR.

Describir brevemente la información que incluyen las bases de datos de la AR. Por ejemplo:

- Registro de ingreso y egreso a los sistemas
- Registro de la creación de certificados
- Detalles de los certificados
- Detalles de las revocaciones

Otros Subsistemas

Cualquier otra información de subsistemas que pueda aplicar:

- Como se registran los usuarios para obtener un certificado
- El medio usado para registrar, por ejemplo: electrónico, cara a cara, etc.
- ¿Qué procesos se utilizan para registrar la identidad, y por quien.
- Cuando se genera el par de claves, quien realiza esta función (AC/AR/ signatario) Si el signatario genera las claves, indicar por cual medio y describir la tecnología utilizada.
- Medios de comunicación entre la AR y AC. Cuales son las relaciones y dependencias entre ellas.

Generación de Claves en la AC

Si aplica, describir el proceso de generación de claves. Cómo se comunica la AR y la AC una vez generadas las claves. Protección del mecanismo de generación de claves.

Operaciones de la AR

Este punto debe describir brevemente otros aspectos sensibles a las operaciones de la AR y que no hayan sido descritos anteriormente.

Procedimientos de respaldo y recuperación

Describir brevemente la frecuencia de los respaldos y los procedimientos de auditoría y almacenamiento que se seguirán.

Planes de Auditoría

Describir cuales son los componentes del plan de Auditoría de la organización en, por ejemplo:

- Dispositivos de seguridad
- Seguridad
- Restricciones del personal
- Interfaces de administración

Recuperación de Desastres

Descripción de la estrategia para recuperación de desastres incluyendo:

- Definición de roles y responsabilidades
- Ejercicios de práctica para la recuperación de desastres, con cuanta frecuencia se realizan.
- Respaldos en cinta, frecuencia, tipo de respaldo (por ejemplo incremental o total).
- Reiniciar el sistema.
- Procesos de Auditoría y generación de reportes.

Privacidad y entrenamiento

Describir brevemente:

- Las provisiones tomadas para proteger la información personal recolectada como evidencia de la identidad en el proceso de registro AR .
- Plan de entrenamiento del personal, en temas relacionados con el manejo

de información privada y confidencial .

Seguridad

Esta sección debe describir brevemente todos los aspectos de seguridad que están involucrados en las operaciones de la AR. Los detalles de estos aspectos pueden ser referenciados a otros documentos presentados.

Seguridad de las Instalaciones

Provee la descripción física del lugar donde operara la AR. Puede incluir referencias a otros documentos o procesos de certificación con los cuales cumpla.

Seguridad del Personal

Describe los requerimientos de seguridad para el personal de la organización, como por ejemplo:

- Referencia a que puestos pueden entrar en zonas restringidas
- Plan de entrenamiento para el personal
- Zonas restringidas para el personal
- Registro de ingresos
- Control de ingreso

Nivel de Seguridad del Módulo Criptográfico

Presenta los productos y tecnología que se está utilizando para realizar las operaciones del PSC o CE, incluyendo el módulo criptográfico de la AR, si lo hay, y el dispositivo donde almacenará las claves el signatario.

Anexo No 11. Controles físicos del centro de datos de las AC del PSC o CE

Ubicación de las instalaciones

La ubicación de los sistemas de certificación no debe estar públicamente identificada. No debe haber ambientes compartidos que permitan la visibilidad de las operaciones críticas de emisión o revocación de certificados. Esas operaciones deberán ser realizadas en compartimentos cerrados, que no permitan visibilidad desde el exterior y estar físicamente protegidos.

Los Proveedores de Servicios de Certificación deben detallar los aspectos de construcción

de las instalaciones de sus Autoridades de Certificación, referidos a los controles de seguridad física.

Acceso físico a las instalaciones

Todas las Autoridades de Certificación de los Proveedores de Servicios de Certificación que conforman la Infraestructura Nacional de Certificación Electrónica deben implementar un sistema de control de acceso físico que garantice la seguridad de sus operaciones, debiendo contar con por lo menos 4 zonas de acceso físico para llegar al ambiente donde residen los equipos de la Autoridad de Certificación.

Adicionalmente habrá zonas 5 y 6 relacionados con la protección de elementos sensitivos vinculados a la clave privada de firma de la Autoridad de Certificación.

Zona 1
Debe estar ubicada detrás de la primera barrera de control de las instalaciones en donde se encuentre alojada la Autoridad de Certificación. Para entrar a la Zona 1, todo individuo deberá ser identificado y su ingreso registrado por personal autorizado.
A partir de esta zona, toda persona debe transitar con una adecuada identificación a la vista. En esta zona no podrán realizarse operaciones ni procesos administrativos de la Autoridad de Certificación. A partir de aquí, los equipos de grabación, fotográficos, de video, o similares, así como computadoras portátiles, tendrán su entrada registrada y sólo podrán ser utilizadas mediante autorización formal y supervisión.

Zona 2
Debe ser interna a la Zona 1 y deberá requerir, de la misma forma que ésta, la identificación individual de las personas que ingresan en ella. Este es el mínimo nivel de seguridad requerido para la realización de cualquier proceso administrativo de la Autoridad de Certificación. El paso de la Zona 1 a la zona 2 deberá exigir identificación por medio electrónico y el uso de una tarjeta de identificación.

Zona 3
Debe estar comprendido dentro de la Zona 2 y será de uso exclusivo del Proveedor de Servicios de Certificación, en donde se podrán realizar actividades sensibles para las operaciones de la Autoridad de Certificación. Cualquier actividad relativa al ciclo de vida de los certificados digitales debe ser cumplida a partir de esta zona.

Las personas que no estén relacionadas con estas actividades no deben tener permiso de acceso a esta zona. Las personas que no posean permisos de acceso no podrán permanecer en esta zona sin estar acompañadas por personal autorizado.

En la Zona 3 deben ser controladas tanto las entradas como las salidas de cada persona. Para la identificación individual se requieren dos tipos distintos de mecanismos de control para la entrada y permanencia en este nivel, como

tarjeta de identificación electrónica, contraseña de ingreso y/o identificación biométrica.

Los teléfonos celulares, así como otros equipos portátiles de comunicación, excepto aquellos exigidos para las operaciones de la Autoridad de Certificación no deben ser admitidos en esta Zona.

Zona 4
Esta zona debe ser interior a la Zona 3, y aquí deben realizarse todas las actividades sensibles vinculadas a las operaciones de la Autoridad de Certificación tales como la emisión o revocación de certificados y la emisión de LCRs.

Todos los sistemas y equipamientos necesarios para estas operaciones deben estar ubicados a partir de este nivel.

La Zona 4 debe tener los mismos controles de acceso físico que la Zona 3. Adicionalmente se debe exigir que las personas ajenas a este nivel ingresen acompañadas por al menos 2 personas expresamente autorizadas del Proveedor de Servicios de Certificación.

Zona 5
Esta zona es interior a la Zona 4, y lo constituye una caja de seguridad o gabinete reforzado con cerradura antirrobo. El objetivo principal de este nivel es controlar el acceso a los compartimentos individuales que conforman la Zona 6.

Zona 6
Esta zona es interior a la Zona 5. Está constituido por compartimentos individuales localizados en el interior de la caja de seguridad o gabinete reforzado, cada uno de ellos con cerradura individual. Los datos de activación de la clave privada de la Autoridad de Certificación deben estar almacenados en ellos.