GUIA PARA LA ACREDITACIÓN, ESTÁNDARES TECNÓLOGICOS Y LINEAMIENTOS DE SEGURIDAD PARA LA ACREDITACIÓN DE PROVEEDORES DEL SERVICIO DE ESTAMPADO DE TIEMPO (PSET)

CONTROL DE VERSIONES

VERSIÓN (EDICIÓN)	MOTIVO DEL CAMBIO	PUBLICACIÓN
1	Creación	Agosto 2011
2	Actualización General	Octubre 2011
2.2	Actualización (Estándares y Auditoría)	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 AMBITO DE APLICACIÓN

La finalidad de la presente norma consiste en regular y establecer los mecanismos y procedimientos para acreditar a los PROVEEDORES DEL SERVICIO DE ESTAMPADO DE TIEMPO **(PSET)**, en el Sistema Nacional de Certificación Electrónica de la República Bolivariana de Venezuela, de conformidad con lo señalado en la LSMDFE, su Reglamento Parcial y demás Normas de carácter sublegal.

2. REFERENCIAS NORMATIVAS

2.1 Decreto 1.204 con Fuerza de Ley Sobre Mensaje de Datos y Firmas Electrónicas, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela N° 37.148 del 28 de febrero de 2001.(LSMDFE).

2.2 Reglamento Parcial de la Ley Sobre Mensajes de Datos y Firmas Electrónicas, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela N° 38.086 del 14 de diciembre de 2004.ISO 8601. Elementos de datos y formatos intercambiables — Intercambio de información Representación de fechas y horas, 3era Edición. Diciembre 2004.

2.3RFC 1305. Protocolo de Tiempo en Redes (NTP).

2.4RFC 3161. Protocolo para el Estampado de Tiempo (TSP).

2.5RFC 3280. Internet X.509 Public Key Infrastructure Certificate. Abril 2002.

2.6RFC 3628. Requerimiento para las Autoridades de Estampado de Tiempo. Noviembre 2003.

2.7ETSI TS 102 023 V1.2.1. Firmas Electrónicas e Infraestructuras. Políticas de requerimientos para Autoridades de Estampado de Tiempo.

2.8ISO / IEC 18014. information Technology – Security Techniques – Time Stamping Services

3. DEFINICIONES Y TERMINOLOGÍAS

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

ACREDITACIÓN	Licencia que otorga la Superintendencia de Servicios de Certificación Electrónica a las personas que expresan su voluntad de ser Proveedores de Servicios de Estampado de Tiempo, a los fines de proporcionar este servicio, todo conforme a lo establecido en la Providencia N°003-2011, de gaceta N° 39174 del 15 de julio de 2011.
PROVEEDOR DE SERVICIO DE ESTAMPADO DE TIEMPO	Persona Jurídica que actúa como tercera parte de confianza y certifica la existencia de unos datos electrónicos en una fecha y hora concreta. Esta dedicada a proporcionar el Servicio de Estampado de Tiempo y demás actividades previstas en la normativa sublegal vigente.
CERTIFICADO ELECTRÓNICO	Mensaje de Datos emitido por la Autoridad de Estampado de Tiempo, que le atribuye certeza y validez al Estampado de Tiempo.

HASH	Resultado de aplicar un algoritmo de hasshing o resumen sobre un documento. Son funciones en un sólo sentido, es decir, conociendo el resultado es prácticamente imposible conocer el dato original.
IDENTIFICADOR DE OBJETO	Valor universal único asociado a un objeto para identificarlo inequívocamente.
ESTAMPADO DE TIEMPO	Documento electrónico emitido por la Autoridad de Estampado de Tiempo, que sirve como evidencia de que una información digital existió en una determinada fecha y hora en el pasado.
TOKEN DE TIEMPO	Objeto o cadena de caracteres que vincula una serie de datos a un momento determinado de tiempo, estableciendo así la evidencia de que esos datos existen desde cierto instante de tiempo.
SERVIDOR DE ESTAMPADO DE TIEMPO	Servidor de red que criptográficamente emite tokens de tiempo asociado a un conjunto de datos electrónicos, los cuales son firmados electrónicamente.
USUARIO	Toda persona que utilice un sistema de información, y utilice la Infraestructura de Servicio de Estampado de Tiempo.
SOLICITANTE	Cualquier Persona Jurídica que solicite su acreditación como PSET ó ya este Acreditado ante SUSCERTE.
TIEMPO UNIVERSAL COORDINADO (UTC)	Escala del tiempo adoptada como el estándar de tiempo oficial internacional, utilizada para el sistema de Metrología Internacional, Convención del Metro, determinada y distribuida por la BIPM.
PROTOCOLO DE TIEMPO DE RED	Es un protocolo de internet utilizado para sincronizar los relojes de los sistemas informáticos a través de paquetes en redes.

4. SÍMBOLOS Y ABREVIATURAS

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

AC	Autoridad de Certificación
AC Raíz	Autoridad de Certificación Raíz del Estado Venezolano
BIPM	Oficina internacional de pesos y medidas - Bureu International des Pois et Mesures -
DPC	Declaración de Prácticas de Certificación
LSMDFE	Ley sobre Mensajes de Datos y Firmas Electrónicas
OID	Identificador de Objeto.
PC	Política de Certificados
PSET	Proveedor de Servicio de Estampado de Tiempo
RPLSMDFE	Reglamento Parcial de la Ley sobre Mensajes de Datos y Firmas Electrónicas
SUSCERTE	Superintendencia de Servicios de Certificación Electrónica.

TSA	Autoridad de Estampado de Tiempo – Time Stamping Authority
TSS	Servidor de Estampado de Tiempo - Time Stamping Server
NTP	Protocolo de Tiempo de Red – Network Time Protocol

5. PROCEDIMIENTO

5.1. Principio Básico

Establecer el procedimiento que deben seguir los solicitantes a PSET para su acreditación ante SUSCERTE, así como los recaudos que deben acompañar la solicitud de acreditación, de conformidad con los requisitos establecidos en la LSMDFE, su Reglamento Parcial y demás Normas de carácter sublegal.

5.2. Consideraciones Generales

5.2.1 Los recaudos que deben ser presentados ante SUSCERTE para proceder a la Acreditación del solicitante a PSET son de tipo: legal, económico-financiero, técnico y de auditoría.

5.2.2 Los documentos deben entregarse en formato digital no editable firmado electrónicamente, según se especifica en la lista de recaudos (Punto 5.4 de esta norma), a excepción de los documentos que por su características requieran ser entregados en físico.

5.2.3 Los recaudos deben ser presentados ante SUSCERTE a través de medios electrónicos debidamente asegurados, contentivo además de la Planilla de Solicitud de Acreditación.

5.2.4 La información entregada a SUSCERTE debe contener los recaudos ordenados de acuerdo a las especificaciones de las Tablas No. 2, 3, 4 y 5, respectivamente identificadas en el punto 5.4 de esta norma.

5.2.5 Se aplicará la Guía de Estándares Tecnológicos y Lineamientos de Seguridad, establecidos en el Capitulo 7, de esta norma, para el servicio de Estampado de Tiempo.

5.2.6 La renovación de la acreditación a los PSET se realizará anual, tal como lo contempla el Reglamento Parcial del Decreto Ley sobre Mensaje de Datos y Firmas Electrónicas.

5.3. Procedimiento General Administrativo de Acreditación para PSET

Para que un Solicitante pueda prestar el servicio de estampado de tiempo, es necesario que cumpla con el procedimiento administrativo relacionado con la consignación y aprobación de los recaudos exigidos. A continuación se describe el procedimiento general administrativo de solicitud para el servicio de estampado de tiempo.

Tabla N° 1. Procedimiento General Administrativo.

RESPONSABLE	ACCIÓN
SOLICITANTE	**1.** CONSIGNACIÓN DE LA SOLICITUD: Entregará a SUSCERTE la solicitud de acreditación como PSET y los recaudos exigidos puntos 5.4 y 6.1.1, en el Capitulo 7 y Capitulo 8.
SUSCERTE	1. VERIFICACIÓN: Verificará que los documentos estén completos a)Si están conformes: i.Ir a paso 3 b)A falta de algún recaudo: i.Indicará al Solicitante sobre los documentos faltantes, y le otorgará en un lapso de diez (10) días hábiles para que consigne la información, cumpliendo con las indicaciones sugeridas por SUSCERTE. 2. ADMISIÓN: Notificará al solicitante que su solicitud ha sido admitida y en consecuencia se procederá a la evaluación. 3. EVALUACIÓN: en el ejercicio de sus atribuciones de supervisión y control, procederá a realizar el análisis de toda la información de los documentos consignados por el Solicitante. 4. DECISIÓN: Decidirá acerca de la solicitud de acreditación, dentro de los veinte (20) días hábiles siguientes a la fecha de admisión de la misma. a)Aprobación: i. Acredita al Solicitante y lo autoriza como PSET para prestar el servicio de Estampado de Tiempo. ii.Ir al paso 6 b)Denegación: i.Declarará la no procedencia de la solicitud de Acreditación como PSET. ii.Ir al paso 6 5. NOTIFICACIÓN: Efectuará la notificación de la decisión tomada. Mediante oficio o mediante correo electrónico firmado por la máxima autoridad, así como también será anunciado de manera oficial a través de su publicación en Gaceta Oficial.
PSET	6. ACEPTACIÓN O RECHAZO DE LA DECISIÓN: a)Si ACEPTA, el contenido de la DECISIÓN: i.Finaliza el Proceso b)Si RECHAZA, el contenido de la DECISIÓN: i.Podrá solicitar la reconsideración de la decisión, sin menoscabo del ejercicio de los demás recursos administrativos y judiciales a

	que hubiera lugar.

5.4. Recaudos

A continuación se muestran los recaudos a presentar conjuntamente con la Solicitud de Acreditación de los aspirantes a Proveedores del Servicio de Estampado de Tiempo y PSC acreditados.

Tabla Nº 2. Recaudos Legales

LEGALES		
No.	**NOMBRE DEL RECAUDO**	**OBSERVACIÓN**
L01	**DOCUMENTOS COMUNES PARA TODOS LOS SOLICITANTES**	
L01.1	Registro de Información Fiscal (RIF) actualizado	Copia fotostática.
L01.2	Contratos de servicios suscritos con terceras personas que guarden relación con alguno de los servicios a ser prestados en virtud de la acreditación	Copia fotostática
L01.3	Modelos de contratos a ser suscritos con los signatarios	En formato electrónico
L01.4	Documento de la Declaración de Prácticas de Certificación y Políticas de Certificados	En formato electrónico
L01.5	Fianza de fiel cumplimiento y cancelación de tasas	En su cualidad de proveedor de servicios, carácter otorgado mediante la Providencia Administrativa N°003-2011, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela N° 39717 de fecha 20 de julio de 2011, actuando de conformidad con la LMDFE, su Reglamento Parcial y lo previsto en el artículo 100° de la Ley de Contrataciones Públicas, los Proveedores de Estampado de Tiempo, deberán presentar Fianza de Fiel Cumplimiento, la cual, debe garantizar el oportuno y cabal cumplimiento de todas y cada unas de las obligaciones que resulten a su cargo y a favor de la República Bolivariana de Venezuela por órgano del Ministerio del Poder Popular para Ciencia y Tecnología a través de la Superintendencia de Servicios de Certificación Electrónica, de conformidad con la Providencia Nº025 de fecha 24 de marzo del año 2.008 publicada en

		la Gaceta Oficial de la República Bolivariana de Venezuela Nº38.916 de fecha 23 de abril del año 2.008, así como, el pago de las tasas correspondientes, de conformidad con el artículo 24 de la LMDFE.
L02	**PARA PERSONA DE DERECHO PRIVADO**	
L02.1	Documento Constitutivo o Estatutos de la empresa Solicitante.	Copia Certificada
L02.2	Actas de Asambleas Ordinarias y/o Extraordinarias, celebradas por el solicitante	Copia Certificada
L02.3	Identificación y datos de ubicación de los Representantes Legales	Incluye: Cédula de Identidad o Pasaporte, domicilio, números telefónicos, fax y correo electrónico
L02.4	Documento donde conste la designación del o los representantes legales y la legitimidad para actuar en nombre del solicitante	Copia Certificada
L02.5	Solvencia Laboral	Copia fotostática
L02.6	Inscripción en el Servicio Nacional de Contratistas (SNC) actualizada	Copia fotostática
L03	**PARA PERSONA DE DERECHO PÚBLICO**	
L03.1	Gaceta Oficial de la publicación del decreto de creación	Copia fotostática, si se trata de un organismo, órgano o ente de la administración pública central, descentralizada o desconcentrada funcionalmente
L03.2	Gaceta Oficial donde conste el acto administrativo que confiera las atribuciones del representante legal del solicitante o documento en el que conste la capacidad para actuar en nombre y representación del solicitante	Copia fotostática
L03.3	Identificación y datos de ubicación de los Representantes Legales.	Incluye: Cédula de identidad o pasaporte, domicilio, números telefónicos, fax y correo electrónico.

Tabla Nº 3. Recaudos Económico-Financieros

ECONÓMICOS-FINANCIEROS		
No.	**NOMBRE DEL RECAUDO**	**OBSERVACIÓN**
E01	**DOCUMENTOS COMUNES PARA TODOS LOS SOLICITANTES**	
E01.1	Estados Financieros (Balance General, Estado de Ganancias y Pérdidas)	Con sus respectivas notas, debidamente certificado por un contador público colegiado y visado por el colegio de contadores públicos de Venezuela, correspondiente a los dos (02) últimos años
E01.2	Proyecto económico	Para un período mínimo de tres (3) años, presentado en forma anual y en moneda oficial de la República Bolivariana de Venezuela y firmado por un economista colegiado. Debe contener: ● Análisis de Mercado, que incluya localización y sectorización, demanda y oferta ● Explicación detallada de los ingresos ● Fuente de Financiamiento de la inversión ● Cronograma de inversión, indicando la inversión inicial y total ● Costos Fijos desglosados ● Costos variables desglosados ● Gastos de Personal desglosados ● Punto de Equilibrio ● Flujo de Caja Proyectado ● Estado de Ganancias y Pérdidas proyectado ● Amortización de Financiamiento ● Listado de Equipos a adquirir, en moneda oficial de la RBV. ● Estructura de Costos, basada en la tabla definida por SUSCERTE.
E02	**PARA PERSONA DE DERECHO PRIVADO**	
E02.1	Declaración del Impuesto sobre la Renta (ISLR)	De los últimos tres (3) años. Aquellas empresas que tiene tiempo menor a un (01) año, presentar el ISLR de los accionistas.
E02.2	Balance de Apertura	Solo para empresas recién constituidas o sin giro, con sus respectivas notas de los estados financieros, expresado en valores constantes y en bolívares, debidamente certificado por un contador público colegiado y visado por el colegio de contadores públicos de Venezuela.
E02.3	Referencias bancarias A)	Con vigencia de tres (3) meses. Si la empresa es de reciente constitución, serán sus accionistas quienes deberán consignar dichas referencias
E02.4	Carta de intención para financiamiento (cuando se requiera) por parte de una	Destacando: monto del financiamiento, condiciones y términos de respaldo, dirección, teléfonos y dirección del sitio web o e-mail.

	institución financiera reconocida	Si es emitida en el exterior, deberá estar traducida al castellano y legalizada por el Consulado Venezolano
E02.5	Documento autenticado de intención de financiamiento, si el financiamiento es a través de terceros (persona natural o jurídica) B)	Acompañado de los estados financieros debidamente firmados por un contador público colegiado y visado por el colegio de contadores públicos de Venezuela. Destacando: monto del financiamiento, condiciones y términos de respaldo, dirección, teléfonos y dirección del sitio web o e-mail.
E02.6	**SI EL O LOS ACCIONISTAS SON PERSONAS JURÍDICAS DEBE PRESENTAR ADICIONALMENTE**	
E02.6.1	Balance General Estado de ganancias y pérdidas, flujo de efectivo y movimiento de patrimonio	Con sus notas explicativas de las partidas que integran dicho balance con una vigencia no mayor de seis (6) meses y en moneda oficial de la República Bolivariana de Venezuela, firmada por un contador público colegiado y visado por el colegio de contadores públicos de Venezuela
E02.7	**SI EL O LOS ACCIONISTAS SON PERSONAS NATURALES DEBE PRESENTAR ADICIONALMENTE**	
E02.7.1	Balance personal actualizado	Con sus notas explicativas de las partidas que integran dicho balance con una vigencia no mayor de seis (6) meses y en moneda oficial de la República Bolivariana de Venezuela, firmada por un contador público colegiado y visado por el colegio de contadores públicos de Venezuela.
E03	**PARA PERSONA DE DERECHO PÚBLICO**	
E03.1	Apartado presupuestario	Presupuesto de ingreso Presupuesto de gasto

Tabla Nº 4. Recaudos Técnicos

TÉCNICOS		
No.	**NOMBRE DEL RECAUDO**	**OBSERVACIÓN**
T01	**DOCUMENTOS COMUNES PARA TODOS LOS SOLICITANTES**	
T01.1 C)	Estructura de los Token de Tiempo a generar bajo lo referido en el estándar RFC 3161.	En el Anexo Nº 8 de éste documento se hace mención a los aspecto fundamentales de la estructura de Protocolo de Estampado de Tiempo detallado explícitamente en la RFC 3161.
T01.2 D)	Registro de acceso público para la Prestación del Servicio de Estampado de Tiempo.	Documento descriptivo que contenga al menos: detalle del sitio web donde se publicará la información para interactuar con los usuarios, descripción de la tecnología, disponibilidad, accesibilidad, conexión, esquemas, medidas de seguridad y diagramas de funcionamiento.
T02	**SEGURIDAD**	

T02.1	Evaluación de riesgos	Debe incluir el reporte de la valoración de riesgos y la estructura del proceso de valoración de riesgos
T02.2	Política de seguridad de la información	Debe estar basada en las recomendaciones del estándar ISO 27002 y en los anexos No. 2 y 4, presentados en el Capitulo 8.
T02.3	Plan de continuidad del negocio y recuperación ante desastres	● Debe estar basada en las recomendaciones del estándar ISO/IEC 27002:2007 sección 14 y en los anexos No. 2 y 5 del Capitulo 8 de éste documento. ● En caso de mantenimiento o mejoras del sistema,, el PSET dispondrán de 72 horas anuales sin que se vea afectado el servicio hacia el usuario. ● En caso de fallas técnicas y/o incidentes telemáticos el PSET debe garantizar la disponibilidad del servicio.
T02.4	Plan de Seguridad de la información	Debe basarse en las recomendaciones del estándar ISO 27002 y en el anexo 6 y 9 del Capitulo 8.
T02.5	Plan de Administración de Claves Criptográficas	Debe estar basada en las recomendaciones del estándar ETSI TS 102 042 y FIPS 140-2.
T02.6	Documento de la Implementación de seguridad física y ambiental	Debe seguirse las recomendaciones del apartado de Seguridad física y ambiental de la Norma ISO 27002 contemplado en la sección 9 del anexo 2 en el Capitulo 8.
T02.7	La estructura de datos y protocolos empleados	Debe basarse en la recomendaciones de la norma ISO/IEC 18014,
T03	**PLATAFORMA TECNOLÓGICA**	
T03.1	Evaluación de la plataforma Tecnológica	● Debe especificarse los elementos relacionados a la estructura de la plataforma tecnológica para los servicios del PSET, ● Entre ellos se tiene: ● Garantía y tipo de Servicio redundante (espejo) en caso de falla operativa. ● Tiempos previstos de recuperación y de paradas programadas. ● Garantía de que los Token de Estampado de Tiempo sean generados de acuerdo al RFC 3161. (contemplado en el Anexo 8.7) ● TSS, servidores NTP, auditables bajo esquemas log. ● Características de los aplicativos relacionados con la prestación del Servicio de Estampado de Tiempo, en lo que respecta a: Base de Datos y

		Servicio Web. ● Mecanismos de respaldo para la información sensible en el proceso de Prestación del Servicio de Estampado de tiempo. ● Mecanismos para ofrecer la integridad de los componentes del sistema TSA y la información referente a la protección contra virus, software maliciosos y no autorizados.
T04	**ADMINISTRACIÓN DE LOS SERVICIOS DE ESTAMPADO DE TIEMPO**	
T04.1	Manual de Operación del Servicio de Generación de Estampado de tiempo del PSET	Debe reflejarse el paso a paso de todos los procesos, necesarios y utilizados para la operatividad, administración y mantenimiento en la generación de Estampado de Tiempo.
T05	**MODELO ORGANIZACIONAL**	
T05.1	Evaluación del personal	Se deben presentar: - Perfiles de los cargos que manejan información y/o los sistemas - Currículo de las personas que ocupan los cargos y/o funciones - Procedimientos de seguridad aplicados en la contratación - Identificación del personal calificado como crítico.

6. PROCESO DE AUDITORIA DE CONFORMIDAD PARA EL SERVICIO ESTAMPADO DE TIEMPO

6.1. Principio Básico

En este apartado de la norma se presenta el proceso de Auditoría de Conformidad del Servicio de Estampado de Tiempo de los equipos y entes que intervienen en ella, así como para las DPC y Listas de Certificados Revocados de los PSET.

6.2. Consideraciones

Las auditorías, realizadas por auditores registrados ante SUSCERTE, a los PSET se realizarán para verificar si sus procesos, procedimientos y actividades se ajustan con sus DPC, PC y las demás normas y procedimientos establecidos por SUSCERTE, relacionadas con la materia. El auditor podrá solicitar información relacionada a:

6.2.1 Registros Log del Sistema TSS donde se refleje la ultima actualización o sincronización con los TMC ó SNTP de SUSCERTE, Archivos de Autenticación con la TSA (SUSCERTE) cuando aplique, Cantidad de Token de Estampado de Tiempo generados y almacenados en la Base de Datos de los TSS, entre otros. Las auditorías se llevaran a cabo por los Auditores autorizados e inscritos en el Registro de Auditores de SUSCERTE, previa selección del aspirante a PSET o PSET acreditado. El auditor debe presentar a SUSCERTE el Plan de Auditoría ya aprobado y acordado con el aspirante a PSET o PSET acreditado.

6.2.2 El proceso de auditoría se realizará en presencia de los Representantes del PSET y el auditor seleccionado, tanto para el proceso de Acreditación y posteriormente en cada proceso de Renovación de la Acreditación. Igualmente se llevarán a cabo Inspecciones al menos una vez al año, bien sea por oficio o denuncias de terceros.

6.2.3 El proceso de auditoría, se llevará a cabo en las instalaciones que enmarquen la operaciones técnicas y administrativas del PSET, el cual deberá permitir recorrer dichas instalaciones en su totalidad y proporcionar la documentación e información técnica y de acreditación que solicite el personal.

6.2.4 El experto que realice la auditoría se regirá por los manuales y guías existentes emanadas por SUSCERTE. Para aquellos casos que así lo requieran, los criterios generales expuestos en los manuales y guías conocidos podrán ser completados o precisados en las respectivas normas aprobadas por SUSCERTE. Los procedimientos de auditoría estarán basados, en estándares internacionales para garantizar su interoperabilidad y neutralidad tecnológica.

6.2.5 Toda auditoría al finalizar, generará un informe como parte de los recaudos que debe entregar el PSET a SUSCERTE, donde el auditor deberá pronunciarse sobre la conformidad o no de la auditoría y deberá referirse según lo establecido a la Norma SUSCERTE Nº 45 “GUÍA MODELO DE INFORME DE AUDITORIA”.

6.2.6 SUSCERTE elabora un informe de acreditación o de renovación de acreditación donde se incluirán las observaciones producto de la supervisión que lleva sobre el PSET, exponiendo las acciones a llevar a cabo con respecto a la situación del PSET planteada en el informe.

6.2.7 La relación entre el auditor y la autoridad auditada se debe limitar estrictamente a los procesos e información requerida para la auditoría. Por lo tanto, la parte auditada no deberá tener ninguna relación, actual o planificada, financiera, legal o de cualquier otra clase que pueda derivar en un conflicto de intereses con el auditor. Por lo tanto deberán aplicar los mismos principios y desarrollo profesional expresados en la Norma ° 47 referente a Código de ética para Auditores.

6.2.8 El Proceso de Auditoría, en ambos niveles estará regido según las normas SUSCERTE Nº 43 correspondiente al PROCEDIMIENTO PARA LA REALIZACIÓN DE LA AUDITORIA A LOS ASPIRANTES A PROVEEDORES DE SERVICIO DE CERTIFICACION ELECTRONICA, PROVEEDORES DE ESTAMPADO DE TIEMPO (PSET) en cuanto sea aplicable a los PSET.

Tabla Nº 5. Recaudos de Auditoria

AUDITORÍA		
No.	**NOMBRE DEL RECAUDO**	**OBSERVACIÓN**
A01	**DOCUMENTOS COMUNES PARA TODOS LOS SOLICITANTES**	
A01	Informe de Auditoría Técnica A)	Elaborado por un Auditor inscrito en el Registro de auditores de SUSCERTE y deberá tomar como objeto de estudio: ● Proceso de Estampado de Tiempo. ● Sistema y elementos asociados a la plataforma tecnológica. ● Centro de Datos. ● Documentación de los servicios y procesos. ● Los detalles de como se llevará a cabo la auditoría se refleja en el anexo N° 8.

7. PLANILLA DE SOLICITUD DEL SERVICIO DE ESTAMPADO DE TIEMPO

A continuación se presenta anexa la planilla que deberá ser impresa y completada por los aspirantes a PSET, para ser entregada a SUSCERTE, en el marco del proceso de Acreditación.

7.1 Anexo N°1

SOLICITUD PARA LA PRESTACIÓN DEL SERVICIO DE ESTAMPADO DE TIEMPO

- PREVIO AL LLENADO DE ESTA PLANILLA, CONSULTE Y VERIFIQUE LOS DOCUMENTOS QUE ESTABLECEN LOS REQUISITOS DE ACUERDO A SU SOLICITUD (DECRETO-LEY 1.204, REGLAMENTO, PROCEDIMIENTO DE ACREDITACIÓN Y LEY ORGÁNICA DE PROCEDIMIENTOS ADMINISTRATIVOS)
- LA INFORMACIÓN PUEDE SER RECABADA A TRAVÉS DE LA PÁGINA WEB DE SUSCERTE www.suscerte.gob.ve

DATOS DEL SOLICITANTE

Nombre o Razón Social:_____

Número de identificación: _____

POR FAVOR RESPONDA LAS SIGUIENTES PREGUNTAS:

¿Para qué requiere el Servicio de Estampado de Tiempo?:_____

_____

Cuantos token de tiempo estima emitir anualmente?:_____

_____

Por favor indique nombre y teléfono de la persona contacto o responsable por parte del PSET: _____

_____

Enlace que direccione al sitio web del PSET:_____

_____

Solicito a la Superintendencia de Servicios de Certificación Electrónica sírvase proceder al análisis de la documentación anexa, la cual expreso como verdadera y ajustada a los requisitos exigidos. Asimismo, manifiesto conocer las obligaciones que conllevan la autorización de dicha solicitud.
En tal sentido, me comprometo a cumplir con los procedimientos establecidos por SUSCERTE y estoy en disposición de dar facilidades al personal designado para llevar a cabo el proceso de evaluación de la documentación consignada.

Nombre del Representante Legal del PSET acreditado:	
Firma:	
Fecha:	

8. ANEXOS NORMATIVOS.

GUÍA DE ESTÁNDARES TECNOLÓGICOS Y LINEAMIENTOS DE SEGURIDAD PARA LA ACREDITACIÓN COMO PROVEEDOR DE SERVICIOS DE ESTAMPADO DE TIEMPO

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, tales como seguridad, buenas prácticas en el modelo de estampado de tiempo 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 Estampado de Tiempo.

8.1 Anexo N° 2. Controles del Estándar ISO/IEC 27002, Secciones 5 a 14, Aplicables

SECCIÓN 5 Política de Seguridad

5.1 Política de Seguridad de la información

Objetivo: Proporcionar a la gerencia la dirección y soporte para la seguridad de la información en concordancia con los requerimientos comerciales y las leyes y regulaciones relevantes.

- 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: Manejar la seguridad de la información dentro de la Organización.

- Compromiso de la gerencia con la seguridad de la información (6.1.1).
- Asignación de las responsabilidades de la seguridad de la información (6.1.3).
- Autorización de proceso para facilidades procesadoras de 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 medios de procesamiento de información de la organización que son ingresados, procesados, comunicados a, o manejados por, grupos externos.

- Identificación de los riesgos relacionados con los grupos externos (6.2.1).
- Tratamiento de la seguridad cuando se lidia con clientes (6.2.2).
- Tratamiento de la seguridad en acuerdos con terceros (6.2.3).

SECCIÓN 7 Gestión de activos

7.1 Responsabilidad por los Activos

Objetivo: Lograr y mantener una apropiada protección de los activos organizacionales.

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

7.1Clasificación de la Información

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

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

SECCIÓN 8 Seguridad del recurso humano

8.1Antes del empleo

Objetivo: Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean idóneos para los roles para los cuales son considerados; y reducir el riesgo de robo, fraude y mal uso de los medios.

- Roles y responsabilidades (8.1.1).
- Investigación de antecedentes (8.1.2).
- Términos y condiciones del empleo (8.1.3).

8.2Durante el empleo

Objetivo: Asegurar que los usuarios empleados, contratistas y terceras personas estén al tanto de las amenazas e inquietudes de la seguridad de la información, sus responsabilidades y obligaciones, y estén equipadas para apoyar la política de seguridad organizacional en el curso de su trabajo normal, y reducir el riesgo de error humano.

- Responsabilidad de la gerencia (8.2.1).
- Conocimiento, educación y capacitación en seguridad de la información (8.2.2).
- Proceso disciplinario (8.2.3).

8.3Terminación o cambio de empleo

Objetivo: Asegurar que los usuarios empleados, contratistas y terceras personas salgan de la organización o cambien de empleo de una manera ordenada.

- Responsabilidad 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

9.1Áreas Seguras

Objetivo: Evitar el acceso físico no autorizado, daño e interferencia con la información y los locales de la organización.

- Perímetro de la seguridad física (9.1.1).
- Controles de ingreso físico (9.1.2).
- Asegurar las oficinas, habitaciones y medios (9.1.3).
- Protección contra amenazas externas e internas (9.1.4).
- Trabajo en áreas aseguradas (9.1.5).
- Áreas de acceso público, entrega y carga (9.1.6).

9.2Equipo de seguridad

Objetivo: Evitar pérdidas, daños, robo o compromiso de los activos y la interrupción de las actividades de la organización.

- Ubicación y protección del equipo (9.2.1).
- Servicios públicos de soporte (9.2.2).
- Seguridad del cableado (9.2.3).
- Mantenimiento de equipos (9.2.4).
- Seguridad de los equipos fuera del local (9.2.5).
- Seguridad de la eliminación o reuso del equipo (9.2.6).
- Retiro de la propiedad (9.2.7).

SECCIÓN 10 Gestión de las Comunicaciones y operaciones

10.1 Procedimientos y Responsabilidades Operacionales

Objetivo: Asegurar la operación correcta y segura de los medios de procesamiento de la información.

- Procedimientos de operación documentados (10.1.1).
- Gestión de cambios (10.1.2).
- Segregación de los deberes (10.1.3).
- Separación de los medios de desarrollo, pruebas y operación (10.1.4).

10.2 Gestión de la entrega de servicios de terceros

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

- Entrega del servicio (10.2.1).
- Monitoreo y revisión de los servicios de terceros (10.2.2).
- Manejo de cambios en los servicios de terceros (10.2.3).

10.3 Planeación y aceptación del sistema

Objetivo: Minimizar el riesgo de fallas en el sistema

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

10.4 Protección contra Software Malicioso y móvil

Objetivo: Proteger la integridad del software y la integración.

- Controles contra códigos maliciosos (10.4.1).
- Controles contra códigos móviles (10.4.2).

10.5 Respaldo o backup

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

10.6 Gestión de la seguridad de Redes

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

- Controles de redes (10.6.1).
- Seguridad de los servicios de la red (10.6.2).

10.7 Gestión de Medios

Objetivo: Evitar la divulgación no autorizada, modificación, eliminación o destrucción de activos; y la interrupción de las actividades comerciales.

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

10.8 Intercambio de Información

Objetivo: Mantener la seguridad en el intercambio de información y software dentro de la organización y con cualquier otra entidad externa.

- Políticas y procedimientos de intercambio de información (10.8.1).
- Acuerdo de intercambio (10.8.2).
- Medios físicos en tránsito (10.8.3).
- Mensajes electrónicos (10.8.4).
- Sistema de información comercial (10.8.5).

10.9 Servicios de comercio electrónico

Objetivo: Asegurar la seguridad de los servicios de comercio electrónico y su uso seguro.

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

10.10 Monitoreo

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

- Registro de auditoría (10.10.1).
- Uso del sistema de monitoreo (10.10.2).
- Protección del registro de información (10.10.3).
- Registros del administrador y operador (10.10.4).
- Registro de fallas (10.10.5).
- Sincronización de relojes (10.10.6).

SECCIÓN 11 Control de Acceso

11.1 Requerimiento del Negocio para el Control del Acceso

Objetivo: Controlar el acceso a la información.

- Política de control del acceso (11.1.1).

11.2 Gestión de Acceso del usuario

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

- Registro del usuario (11.2.1).
- Gestión de privilegios (11.2.2).
- Gestión de las claves secretas de los usuarios (11.2.3).
- Revisión de los derechos de acceso del usuario (11.2.4).

11.3 Responsabilidades del usuario

Objetivo: Evitar el acceso de usuarios no-autorizados, evitar poner en peligro la información y evitar el robo de información y los medios de procesamiento de la información.

- Uso de claves secretas (11.3.1).
- Equipo del usuario desatendido (11.3.2).
- Política de escritorio y pantalla limpios (11.3.3).

11.4 Control de Acceso a la Red

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

- Política sobre el uso de los servicios de la red (11.4.1).
- Autenticación del usuario para las conexiones externas (11.4.2).
- Identificación del equipo en las redes (11.4.3).
- Protección del puerto de diagnóstico y configuración remoto (11.4.4).
- Segregación en redes (11.4.5).
- Control de conexión a la red (11.4.6).
- Control de routing de la red (11.4.7)

11.5 Control de Acceso al Sistema Operativo

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

- Procedimientos para un registro seguro (11.5.1).
- Identificación y autenticación del usuario (11.5.2).
- Sistema de gestión de claves secretas (11.5.3).
- Uso de las utilidades del sistema (11.5.4).
- Cierre de una sesión por inactividad (11.5.5).
- Limitación del tiempo de conexión (11.5.6).

11.6 Control de acceso a la aplicación y la información

Objetivo: Evitar el acceso no autorizado a la información mantenida en los sistemas de aplicación.

- Restricción del acceso a la información (11.6.1).
- Aislar el sistema confidencial (11.6.2).

11.7 Computación y tele-trabajo móvil

Objetivo: Asegurar la seguridad de la información cuando se utiliza medios de computación y tele-trabajo móviles.

- Computación y comunicaciones móviles (11.7.1).
- Teletrabajo (11.7.2).

SECCIÓN 12 Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información.

12.1 Requerimientos de Seguridad de los Sistemas de Información.

Objetivo: Garantizar que la seguridad sea una parte integral de los sistemas de información.

- Análisis y especificación de los requerimientos de seguridad (12.1.1).

12.2 Procesamiento correcto en las aplicaciones

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

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

12.3 Controles Criptográficos

Objetivo: Proteger la confidencialidad, autenticidad o integridad a través de medios criptográficos

- Política sobre el uso de controles criptográficos (12.3.1)
- Gestión de claves (12.3.2)

12.4 Seguridad de los Archivos de Sistema

Objetivo: Garantizar la seguridad de los archivos del sistema.

- Control del software operacional (12.4.1)
- Protección de la data 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 del control del cambio (12.5.1)
- Revisión técnica de la aplicación después de cambios en el sistema (12.5.2)
- Restricciones sobre los cambios en los paquetes de software (12.5.3)
- Filtración de información (12.5.4)
- Desarrollo de software abastecido externamente (12.5.5)

12.6 Gestión de la vulnerabilidad técnica

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

- Control de las vulnerabilidades técnicas (12.6.1)

SECCIÓN 13 Gestión de un incidente en la seguridad de la información

13.1 Reporte de los eventos y debilidades de la seguridad de la información

Objetivo: Asegurar que los eventos y debilidades de la seguridad de la información asociados con los sistemas de información sean comunicados de una manera que permita que se realice una acción correctiva oportuna.

- Reporte de eventos en la seguridad de la información (13.1.1)
- Reporte de las debilidades en la seguridad (13.1.2)

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

Objetivo: Asegurar que se aplique un enfoque consistente y efectivo a la gestión de los incidentes en la seguridad de la información.

- Responsabilidades y procedimientos (13.2.1)
- Aprender de los incidentes en la seguridad de la información (13.2.2)
- Recolección de evidencia (13.2.3)

SECCIÓN 14 Gestión de la Continuidad del Negocio

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

Objetivo: Contraatacar las interrupciones a las actividades comerciales y proteger los procesos comerciales críticos de los efectos de fallas importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.

- Incluir la seguridad de la información en el proceso de gestión de continuidad del negocio (14.1.1)
- Continuidad del negocio y evaluación del riesgo (14.1.2)
- Desarrollar e implementar los planes de continuidad incluyendo la seguridad de la información (14.1.3)
- Marco Referencial de la planeación de la continuidad del negocio (14.1.4)
- Prueba, mantenimiento y re-evaluación de los planes de continuidad del negocio (14.1.5)

8.2 Anexo N° 3. Documento Estándar de una Política de Seguridad

Según la ISO 27002: 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 de referencia 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 .

• Monitorizar 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.

• 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.

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.

8.3 Anexo N° 4. Estándar ETSI TS 102 042 Sección 7.4.8: Administración de la Continuidad.

El PSET 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 PSET, incluyendo hardware y software. En particular:

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

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

8.4 Anexo N° 5. 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?

¿Está la infraestructura computacional y de red instalada y operando de acuerdo a lo descrito en: el Plan de Seguridad, el Manual de Operación 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 PSET.

6.Plan de administración de claves criptográficas.

7.Control de media removible.

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

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

Administración del FW Internet .

10. Procedimientos y mecanismos que tengan un rol relevante en reducir las amenazas a las operaciones del Proveedor de Servicio de Estampado de Tiempo.

8.5 Anexo N° 6. Controles físicos del centro de datos del Proveedor de Servicios de Estampado de Tiempo.

Ubicación de las instalaciones

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

Los Proveedores de Servicios de Estampado de Tiempo (PSET) deben detallar los aspectos de construcción de sus instalaciones, referidos a los controles de seguridad física.

Acceso físico a las instalaciones

Todas los PSET 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 sus equipos.

Zona 1

Debe estar ubicada detrás de la primera barrera de control de las instalaciones en donde se encuentren alojados los equipos del PSET. Para accesar 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 visible. En esta zona no podrán realizarse operaciones ni procesos administrativos del PSET. 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 del PSET. 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 PSET, en donde se podrán realizar actividades relacionadas al servicio de Estampado de Tiempo a partir de ésta zona.

Las personas que no estén relacionadas con estas actividades no deben tener permiso de acceso a esta zona, lo que significa que si no posee autorización, no podrán permanecer en esta zona sin estar acompañadas por el 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 del PSET 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 del PSET, tales como: Administración de los equipos de generación de Token de Tiempo, administración de Base de Datos, aplicativos Web y Sistemas relacionados a la prestación del Servicio de Estampado de Tiempo.

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 PSET.

Zona 5

Esta zona es interior a la Zona 4, y lo constituye una caja de seguridad o gabinete reforzado con cerradura antirobo. 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.

En esta zona, los equipos del PSET, alojados en el Rack, deberán estar diferenciados de los demás y deberá ser uso exclusivo para el PSET.

En caso de que el PSET, sea un PSC acreditado, los equipos que prestan el Servicio de Estampado de Tiempo podrán estar incorporados en el mismo Rack donde se encuentra instalada la plataforma del Servicio de Certificación Electrónica.

8.6 Anexo N° 7. Estructura del Informe de Auditoría

El Informe de Auditoría debe contener los siguientes aspectos:

- Comunicación de presentación del auditor

Es un requisito para la entrega formal del Informe de Auditoría y debe contener:

A) Fecha de entrega de la comunicación.

B) Identificación del Auditor remitente.

C) Referencia al documento de Informe de Auditoría que se consigna.

D) Extracto del contenido del Informe con la información más relevante del resultado de la auditoría y del dictamen efectuado.

E) Firma del Auditor remitente.

- Ficha de identificación del auditor

De conformidad con lo establecido en el Artículo No 5 del RPLSMDFE la Ficha de Identificación debe contener:

A) Nombre e identificación del auditor.

B) Fecha de inicio y terminación de la auditoría.

D) Manifestación del cumplimiento de lo indicado en la LSMDFE y su Reglamento Parcial (RPLSMDFE).

E) Firma del auditor.

- Contenido

Incluye las características y condiciones de la auditoría efectuada:

- Resumen ejecutivo

Es un segmento del informe de tres (03) páginas, donde se expresa de manera resumida los resultados de la auditoría, indicando las observaciones más significativas del Informe. Este resumen, está dirigido a un nivel gerencial, con la finalidad de que en un contexto corto, conozcan los resultados visualizados en forma global, para la toma de decisiones.

- Informe

Tiene como finalidad presentar de manera explícita los resultados de la auditoría, presentando en detalle la información recabada, las observaciones, hallazgos y evidencias relacionados a cada información que ha sido revisada, así como su grado de criticidad en función a la valoración de las deficiencias encontradas y su nivel de severidad.

El informe está comprendido por:

Introducción: describe en forma narrativa los aspectos relativos al solicitante a PSET. La información introductoria que se presenta, debe exponer la naturaleza del solicitante a PSET y mostrar los antecedentes, objetivo y alcance, descritos a continuación :

Objetivo

Antecedentes (si es auditoría de seguimiento) : aplica para las auditorías de seguimiento y se establecen con la finalidad de verificar la gestión relacionada con la ejecución del plan de mejoras, propuesto por el PSET.

Alcance (si es auditoría de seguimiento) : describir la finalidad de la Auditoría a ser realizada al solicitante a PSET, en función de los lineamientos establecidos por el Marco Jurídico vigente y las Normas y procedimientos específicos a ser cumplidos en la materia.

Se deben considerar para la construcción de los objetivos del informe de auditoría los siguientes aspectos:

i. Evaluar el cumplimiento y mejoramiento continuo de los estándares de seguridad, de conformidad con los artículos N° 34 y N° 35 del RPLSMDF.

ii. Comprobar que existan y se cumplan razonablemente las condiciones básicas de control sobre los criterios correspondientes a políticas, normas y procedimientos que conforman el ambiente organizacional del aspirante a PSET.

iii. Comprobar que existan y se cumplan razonablemente las condiciones básicas de control sobre los criterios correspondientes a políticas, normas, procesos y Criterios de revisión .

Análisis situacional: Se encuentra conformado por los siguientes aspectos:

Observaciones: para cada criterio/atributo/dimensión en el cual se haya detectado un hallazgo, el auditor debe plasmar la información recabada con su respectivo análisis, reflejando “qué” se está revisando, “cómo” se comporta el elemento revisado y expresar las “causas o factores” que inciden en él.

Respecto a los hallazgos que indiquen no conformidades, el auditor debe dirigirlas con responsabilidad, reportarlas de acuerdo a los procedimientos y áreas examinadas, orientarlas con un enfoque positivo y explicar a los solicitantes a PSET acreditados las ventajas de descubrirlas, como una oportunidad para mejorar el sistema por medio de acciones correctivas.

Conclusiones y recomendaciones: describir los resultados obtenidos en la auditoría, hallazgos encontrados, recomendaciones generales y oportunidades de mejora.
Las recomendaciones pueden hacer referencia a observaciones, al igual que a las no conformidades.

Observaciones finales: Cualquier aspecto significativo que el auditor considere importante resaltar como valor agregado al informe de auditoría.

8.7 Anexo N° 8. RFC 3161 Protocolo para el Estampado de Tiempo.

SECCIÓN 2. 1. Requerimientos del Proveedor de Servicios de Estampado de Tiempo

El PSET podrá:

1.Utilizar una fuente de tiempo de confianza.

2.Incluir un valor de tiempo de confianza para cada estampado de tiempo.

3.Incluir un número entero único para cada Token de tiempo.

4.Producir un estampado de tiempo después de recibir una solicitud válida del solicitante, cuando sea posible.

5.Incluir dentro de un token de tiempo un identificador único para indicar la política de seguridad en virtud de la cual la se ha creado.

6.Asignar al token de estampado de tiempo un hash de representación de los datos. La Función hash esta identificada exclusivamente por un OID.

7.Examinar la OID hash, verificando si la longitud del valor del hash es coherente con el algoritmo de control.

8.No deberá de ninguna manera, examinar la huella que un estampado cronológico (a menos que, para comprobar su longitud, tal como se especifica en el punto anterior).

9.No deberá incluir ninguna identificación de la entidad solicitante.

10. Firmar cada Estampado de tiempo utilizando una clave generada exclusivamente para este fin, indicando esta propiedad en su correspondiente certificado.

11. Incluir información adicional en estampado de tiempo, preguntando por el solicitante mediante las extensiones de campo, con que cuenta el PSET.

SECCIÓN 2.2. Transacciones del PSET

Como el primer mensaje de este mecanismo, la entidad que requiere del servicio, solicita un estampado de tiempo con el envío de una solicitud (que incluye un TimeStampReq), a la PSET. Como segundo mensaje, el PSET envía una respuesta, al solicitante. Al recibir la respuesta (que incluye un TimeStampToken), la entidad solicitante deberá verificar el estado de error devuelto en el respuesta y si no hay error deberá verificar los campos que figuran en el TimeStampToken y la validez de la firma digital de la TimeStampToken. El solicitante deberá verificar que la TimeStampToken contiene el certificado de identificación correcta de la PSET**,** así como también que todos los datos mostrados estén correcto, el algoritmo has OID sean el correcto. También el solicitante deberá verificar la puntualidad de la respuesta de verificación, ya sea el tiempo incluido en la respuesta contra un tiempo de referencia local, si está disponible. Si alguna de las verificaciones anterior falla, la TimeStampToken deberá ser rechazada.

SECCIÓN 2.3. Identificación del PSET

El PSET deberá firmar cada mensaje de estampado de tiempo con una clave reservada específicamente para tal fin. Su correspondiente certificado deberá contener sólo una instancia del campo de extensión con la clave de uso extendido, tal como se define en la sección [RFC2459].