GUÍA MODELO DE INFORME DE AUDITORÍA

CONTROL DE VERSIONES

VERSIÓN (EDICIÓN)	MOTIVO DEL CAMBIO	PUBLICACIÓN
1	Creación	Julio 2007
2	Actualización general	Mayo 2008
2.1	Revisión General y Actualización de Formato	Agosto 2011
3	Actualización general	Diciembre 2011
3.1	Firma electrónica para garantizar su integridad por las autoridades actuales	Mayo 2017

ÍNDICE

TRÁMITE	
DIRECTORIO	
NOMBRE	**CARGO SUSCERTE**
Carlos Cruz Villarroel	Adjunto a la Superintendente
Carlos A. Acosta	Director de Estandarización y Fiscalización en Certificación Electrónica y Seguridad de la Información.
Daniel Pérez	Director de Servicios de Certificación Electrónica y Criptografía
Olga Sanabria	Asesora Legal
RESPONSABLE (S) DE LA EDICIÓN	

1. OBJETO Y CAMPO DE APLICACIÓN

Esta guía tiene como objeto presentar un modelo del informe de auditoría a seguir por los auditores registrados ante la Superintendencia, y de esta manera dar a conocer los aspectos que SUSCERTE considera como requeridos para la estructuración de dicho documento.

2. REFERENCIAS NORMATIVAS

2.1 Decreto Ley Sobre Mensajes de Datos y Firmas Electrónicas. (LSMDFE).

2.2 Reglamento Parcial de la Ley Sobre Mensajes de Datos y Firmas Electrónicas (RPLSMDFE).

3. DEFINICIONES Y TERMINOLOGÍAS

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

AUDITOR	Persona con la competencia necesaria para llevar a cabo una auditoría.
AUDITORES REGISTRADOS	Personas naturales a quienes se les emite una certificación de inscripción para prestar los servicios como auditor a los Aspirantes a Proveedores de Servicio de Certificación Electrónica (PSC), PSC Acreditados o Casos Especiales.
AUDITORÍA	El proceso sistemático que consiste en obtener y evaluar objetivamente evidencias concernientes a las normas, políticas, planes y procedimientos de seguridad relacionados con Tecnología de Información y Comunicación (TIC), cuyo fin consiste en determinar el grado de correspondencia entre esas afirmaciones y los criterios establecidos, para luego comunicar los resultados a las personas interesadas.
AUDITORÍA DE SEGUIMIENTO	Auditoría que se lleva a cabo para evaluar si el organismo auditado ha realizado los cambios o mejoras relacionadas con los hallazgos y recomendaciones emitidas en la auditoría inicial.
CASO ESPECIAL	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.
HALLAZGO	Resultados de la evaluación de las evidencias obtenidas, recopiladas frente a los criterios de auditoría. Los hallazgos de la auditoría pueden indicar conformidad o no conformidad con los criterios de auditoría, u oportunidades de mejora.
INFORME DE AUDITORÍA	Documento emitido por el auditor como resultado final de su examen y/o evaluación que contiene la exposición analítica de hechos o hallazgos, con la finalidad de transmitir el estado de la información recabada, sus conclusiones y recomendaciones.

CÉDULA DE AUDITORÍA	Instrumento para el Auditor el cual debe contener la identificación de la información recabada.

4. SÍMBOLOS Y ABREVIATURAS

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

DIF	Dirección de Inspección y Fiscalización
LSMDFE	Ley Sobre Mensajes de Datos y Firmas Electrónicas
PSC	Proveedor de Servicios de Certificación
RPLSMDFE	Reglamento Parcial de la Ley Sobre Mensajes de Datos y Firmas Electrónicas
SUSCERTE	Superintendencia de Servicios de Certificación Electrónica.

5. PROCEDIMIENTO

5.1. Principio Básico

El informe de auditoría reviste gran importancia ya que suministra al aspirante a PSC, PSC acreditado o Caso Especial, información sustancial sobre la forma como están operando, a través de las observaciones, conclusiones de hechos significativo así como recomendaciones constructivas para superar las debilidades en cuanto a políticas, procedimiento, cumplimientos de actividades y otros aspectos de interés.

5.2. Consideraciones Generales

5.2.1 Estructura del Informe de Auditoría

El Informe de Auditoría debe contener los siguientes aspectos:

- Comunicación de presentación del auditor
- Ficha de identificación del auditor
- Contenido
  - ✓ Resumen ejecutivo
  - ✓ Informe
    - ➢ Introducción
      - ◆ Antecedentes (si es auditoría de seguimiento y/o quedan pendientes por resolver hallazgos de auditorias anteriores)
      - ◆ Objetivo
      - ◆ Alcance
    - ➢ Criterios de revisión
    - ➢ Análisis situacional.
      - ◆ Observaciones
      - ◆ Conclusiones y recomendaciones

- Observaciones finales
- Anexos

5.3. Consideraciones Obligatorias

5.3.1 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.

5.3.2 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.

C) Declaración de conformidad de cada una de las condiciones previstas en el Artículo Nº 31 de la LSMDFE, las demás previstas en su Reglamento Parcial (RPLSMDFE) y normativa de carácter sub legal que en materia de certificación electrónica emite y aprueba SUSCERTE.

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

E) Firma del auditor.

5.3.3 El contenido

Incluye las características y condiciones de la auditoría efectuada:

A) **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.

B) **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:

b.1) Introducción: describe en forma narrativa los aspectos relativos al aspirante a

PSC, PSC acreditado o Caso Especial. La información introductoria que se presenta, debe exponer la naturaleza del aspirante a PSC, PSC acreditado o Caso Especial y mostrar los antecedentes, objetivo y alcance, descritos a continuación :

- **Antecedentes:** 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 aspirante a PSC, PSC acreditado o Caso Especial.

- **Objetivo:** describir la finalidad de la Auditoría a ser realizada al aspirante a PSC, PSC acreditado o Caso Especial, 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 PSC, PSC acreditado o Caso Especial.

  iii. Comprobar que existan y se cumplan razonablemente las condiciones básicas de control sobre los criterios correspondientes a políticas, normas, procesos y procedimientos de Certificación, Certificados y Claves Electrónicas que conforman el ambiente organizacional del aspirante a PSC, PSC acreditado o Caso Especial.

- **Alcance:** en caso de auditorías de seguimiento se refiere a las delimitaciones particulares del caso y las áreas a examinar o reevaluar en el proceso de auditoría. Para el caso de auditorias de renovación de acreditación o acreditación se exponen las áreas a ser evaluadas.

b.2) Criterios de Revisión:

A) El auditor debe pronunciarse sobre la conformidad o no del resultado de la auditoria, de acuerdo a lo establecido en el marco legal y sub legal vigente en materia de certificación electrónica, y la evaluación debe ir consona a la siguiente escala:

Calificación	Descripción
Conforme	El Aspirante a PSC, PSC Acreditado o Caso Especial, cumple a cabalidad con todos los requisitos exigidos en el marco legal y sub legal vigente.
Conforme con Observaciones	• El Aspirante a PSC, PSC Acreditado o Caso Especial, incurrió en el incumplimiento de algunos de los requisitos, exigidos en el marco legal y sub legal vigente, pero se determina que el incumplimiento es subsanable a corto

	plazo (hasta tres (3) meses) y no afecta el correcto funcionamiento del sistema ni los fines previstos en la LSMDFE y el RPLSMDFE. • El Aspirante a PSC, PSC Acreditado o Caso Especial debe consignar un plan para la remediación de las observaciones el cual debe formar parte integrante del informe de auditor.
No conforme	• El Aspirante a PSC, PSC Acreditado o Caso Especial no cumple algunos de los requisitos, exigidos en el marco legal y sub legal vigente y se determina que no son subsanables a corto plazo o afecta el correcto funcionamiento del sistema o los fines previstos en LSMDFE y el RPLSMDFE. • El Aspirante a PSC, PSC Acreditado o Caso Especial, reincide en el incumplimiento de algunos de los requisitos exigidos en el marco legal y sub legal vigente de acuerdo a informes de auditorias anteriores.

b.3) 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.

  Sobre cada observación el auditor debe declarar su conformidad, conformidad con observaciones o no conformidad de acuerdo al caso. 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 aspirantes a PSC, PSC acreditados o Casos Especiales 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.

  El auditor debe concluir con un dictamen el cual debe ir expresado y justificado en los términos anteriormente descritos: conforme, conforme con observaciones o no conforme.

5.4. Observaciones finales

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

5.5. Anexos

El auditor debe anexar los papeles de trabajo e información recabada para aquellos casos en que se deban presentar evidencias o pruebas.