PROCEDIMIENTO PARA LA REALIZACIÓN DE AUDITORÍA A LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

CONTROL DE VERSIONES

VERSIÓN (EDICIÓN)	MOTIVO DEL CAMBIO	PUBLICACIÓN
1	Creación	Julio 2008
1.1	Actualización de Formato	Agosto 2011
2.1	Revisión General y Actualización del Formato	Agosto 2011
3	Actualización General	Diciembre 2011
3.1	Firma electrónica para garantizar su integridad por autoridades actuales	Mayo 2017
4	Actualización General	Agosto 2024

Versión del Documento: Agosto 20, 2024 4:57 p.m.

ÍNDICE

CONTROL DE VERSIONES..... 2
1. OBJETO Y CAMPO DE APLICACIÓN..... 5
2. REFERENCIAS NORMATIVAS..... 5
3. DEFINICIONES Y TERMINOLOGÍAS..... 5
4. SÍMBOLOS Y ABREVIATURAS..... 6
5. PROCEDIMIENTO..... 7
5.1 Principio Básico..... 7
5.2 Consideraciones Generales..... 7
5.3 Consideraciones Específicas..... 7
5.4. Procedimiento General..... 9

ELABORACIÓN	
DIRECTORIO	
NOMBRE	**CARGO**
Gerardo Gómez	Superintendente
Juan Carlos Monsalve	Gerente de Acreditación, Estandarización y Fiscalización
Mónica Lugo	Consultora Jurídica
EDICIÓN Y REVISIÓN	
Marcial Quevedo	

Versión del Documento: Agosto 20, 2024 18:03 p.m.

1. OBJETO Y CAMPO DE APLICACIÓN

Esta norma tiene por finalidad establecer los lineamientos y pasos a seguir para la planificación, realización y documentación de la auditoría a personas jurídicas de derecho público y privado por parte del auditor, a objeto de verificar el cumplimiento de los requisitos establecidos en la Ley Sobre Mensajes de Datos y Firmas Electrónicas, su Reglamento y las normas SUSCERTE.

2. REFERENCIAS NORMATIVAS

2.1. Decreto N.º 1.204 con Fuerza de Ley Sobre Mensajes de Datos y Firmas Electrónicas.

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

2.3. Norma SUSCERTE Nº 045 “Guía modelo de informe de auditoría en el ámbito de las Tecnología de la Información y Comunicación”

3. DEFINICIONES Y TERMINOLOGÍAS

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

AUDITOR	Experto técnico capacitado para realizar auditorías en materia de las TIC, con conocimientos en sistemas y procesos de certificación electrónica, inscritos en el Registro de Auditores de SUSCERTE.
AUDITORÍA	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.
CASO ESPECIAL	Son entidades de certificación excepcionales para Proyectos de Interés Nacional que son acreditados por SUSCERTE
CONFIDENCIALIDAD	Preservación y resguardo de la información y de los datos de la organización sobre la cual se ha fundamentado la Auditoría.
CRITERIOS DE LA AUDITORÍA	Conjunto de políticas, procedimientos o requisitos utilizados como referencia.

HALLAZGOS	Resultados de la evaluación de la evidencias de la Auditoría 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 mejoras.
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.
REGISTRO DE AUDITORES	Base de datos donde se detalla la información correspondiente a los Auditores inscritos en el registro de Auditores de SUSCERTE para efectuar la Auditoría, de conformidad con el RPLSMDFE.
SOLICITANTE	Es la persona jurídica de derecho público o privado que requiera una auditoría en el ámbito de las TIC.

4. SÍMBOLOS Y ABREVIATURAS

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

GEAF	Gerencia de Estandarización, Acreditación 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.
TIC	Tecnología de Información y Comunicaciones

5. PROCEDIMIENTO

5.1 Principio Básico

El propósito de este procedimiento es definir la secuencia de acciones y responsabilidades involucradas en el proceso de Auditoría a ser realizada al Solicitante, a los fines de verificar que se cumplan con lo establecido en la LSMDFE, normas SUSCERTE, procedimientos, Declaración de Prácticas de Certificación y Políticas de Certificados, para ofrecer un servicio eficaz.

5.2 Consideraciones Generales

5.2.1 A los efectos de lo establecido en el artículo 26 de la LSMDFE, la Auditoría a la que se refiere debe ser realizada por Auditores debidamente inscritos en el Registro de Auditores de SUSCERTE. conforme los artículos 26 y siguientes del Reglamento Parcial del Decreto Ley sobre Mensajes de Datos y Firmas Electrónicas.

5.2.2 El Solicitante seleccionará un Auditor inscrito en el Registro de Auditores de SUSCERTE, para la realización de la Auditoría.

5.2.3 En el caso que el Solicitante no esté de acuerdo con el Informe de Auditoría presentado por el Auditor podrá solicitar los servicios de un nuevo Auditor.

5.2.4 El personal de SUSCERTE con acceso autorizado a la información, y los Auditores, deberán mantener la confidencialidad de la información y documentos entregados por los solicitantes, cuando dicha información revista tal carácter en virtud de algún acuerdo, convenio, declaración o norma legal.

5.3 Consideraciones Específicas

5.3.1 Una vez que el interesado contacte al Auditor seleccionado, éste deberá cursar comunicación por escrito al Solicitante, que incluya el Plan de Auditoría donde indique el objetivo, alcance preliminar, las áreas a revisar, los requerimientos de información para realizar las revisiones, la fecha prevista para el inicio, el tiempo estimado para culminar y entregar el Informe de Auditoría.

5.3.2 Inmediatamente después de aprobado el Plan de Auditoría por el Solicitante, el Auditor debe notificar por correo electrónico a SUSCERTE de la contratación de la Auditoría, acompañado de dicho Plan. El tiempo para notificar a SUSCERTE de dicha solicitud no podrá exceder de cinco (5) días hábiles contados a partir de la contratación de la auditoría.

5.3.3 La duración de la Auditoría y la entrega del respectivo Informe, no podrá exceder de treinta (30) días

hábiles contados a partir del día del inicio de la misma. En caso de necesitar una prórroga, el Auditor lo solicitará por escrito al Solicitante y acordado el lapso de la prórroga, el Auditor deberá notificarlo a SUSCERTE.

5.3.4 El Auditor debe revisar y discutir todas las observaciones conjuntamente con el personal designado por parte del Solicitante, para determinar que las evidencias encontradas estén debidamente documentadas, soportadas y sean suficientes para la elaboración del Informe de Auditoría.

5.3.5 Una vez subsanadas las evidencias encontradas ambas partes deben firmar el Informe Final y sus anexos. Así mismo el informe de auditoría debe tener el aval de la máxima autoridad de SUSCERTE.

5.3.6 El Informe de Auditoría debe ir acompañado con los soportes suficientes para sustentar el resultado de la evaluación realizada por el Auditor.

5.3.7 Los resultados y conclusiones de la Auditoría deben estar apoyados por un apropiado análisis e interpretación sobre los elementos susceptibles de revisión, de acuerdo a las normas y estándares aplicables de SUSCERTE.

5.3.8 En caso de incumplimiento de lo establecido en el Artículo 35 de LSMDFE, el Auditor podrá declarar irrealizable el proceso de Auditoría, por no llenar los requerimientos mínimos para efectuarla y deberá notificarlo así a SUSCERTE.

5.3.9 El Auditor debe pronunciarse sobre la conformidad o no del resultado de la auditoría y la evaluación debe ir cónsona a la siguiente escala:

Calificación	Descripción
Conforme	Solicitante cumple a cabalidad con todos los requisitos exigidos en el marco legal y sublegal vigente.

Conforme con Observaciones	• El Solicitante no cumple algunos de los requisitos, exigidos en el marco legal y sub legal, pero se determina que el incumplimiento es subsanable a corto plazo de hasta dos (2) meses, y no afecte el correcto funcionamiento del sistema ni los fines previstos en la LSMDFE y el RPLSMDFE. • El Solicitante debe consignar un plan para la remediación de las observaciones el cual debe formar parte integrante del informe del auditor.
No conforme	• El Solicitante no cumple algunos de los requisitos, exigidos en el marco legal y sub legal 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 Solicitante que reincide en el incumplimiento de algunos de los requisitos exigidos en el marco legal y sublegal vigente, de acuerdo a informes de auditorías anteriores.

5.4. Procedimiento General

A continuación se describe el procedimiento general.

Responsable	Acción
SOLICITANTE	1. Solicita el listado del Registro de Auditores en la GEAF. 2. Revisa el Registro de Auditores y contacta al Auditor seleccionado. 3. Envía Solicitud al Auditor para la realización de la Auditoría.
AUDITOR	4. Recibe solicitud de parte del Solicitante. 5. Notifica a SUSCERTE la solicitud para la realización de la Auditoría. 6. Elabora el plan de Auditoría. 7. Realiza reunión con el Solicitante a fin de explicar los métodos y procedimientos a emplear durante la auditoría. 8. Envía al solicitante el plan de Auditoría definitivo para su aprobación.

SOLICITANTE	9. Recibe el plan de auditoría. 10. Una vez revisado y aprobado, se lo notifica al Auditor.
AUDITOR	11. Recibe el Plan de Auditoría aprobado y lo envía a SUSCERTE. 12. Inicia la Auditoría basándose en procesos sistemáticos e independientes, que le permitan verificar: la existencia, eficacia y cumplimiento de las normas, planes y procedimientos de seguridad relacionados con Tecnología de Información y Comunicación (TIC), para minimizar los riesgos y determinar el cumplimiento de las garantías de calidad y sus niveles de servicios asociados, siguiendo lo establecido en la LSMDFE, RPLSMDFE, y las Normas SUSCERTE. 13. Determina las observaciones que tengan lugar durante el proceso de auditoría. 14. Llena el registro de detección de evidencias y/o hallazgos. 15. Realiza reunión con el responsable del Solicitante informando las evidencias y/o hallazgos encontrados en la Auditoría. A) Si hay evidencias que pueden ser corregidas: ● Establece un lapso de tiempo para que el Solicitante realice las correcciones pertinentes. ● Una vez transcurrido el lapso establecido, si es el caso, procede a cambiar el estatus de las evidencias en el registro de detección de evidencias y/o hallazgos. B) Si las evidencias no pueden ser corregidas: ● Ir al paso 16 16. Realiza reunión de cierre de auditoría, presentando las observaciones, manifestando el comportamiento del desarrollo de la misma e informando a los responsables de las áreas auditadas, las evidencias y/o hallazgos encontrados. 17. Culminado el proceso de Auditoría, emite Informe preliminar de Auditoría al Solicitante, con los lineamientos establecidos en la Norma SUSCERTE Nº 045

	"Guía modelo de informe de auditoría en el ámbito de las Tecnologías de la Información y Comunicación"
SOLICITANTE	18. Recibe el informe preliminar de auditoría. A) Si hay evidencias y/o hallazgos: ● Elabora plan de acciones correctivas para realizar las correcciones pertinentes. ● Envía dicho plan al auditor. B) Si no hay evidencias: ● Ir al paso 19.
AUDITOR	19. Recibe plan de acciones correctivas. 20. Elabora Informe de Auditoría. 21. Ambas partes deben firmar el Informe Final y sus anexos. Así mismo el informe de auditoría debe tener el aval de la máxima autoridad de SUSCERTE.