



Norma de Auditoría del SGSI

Versión: 2.1

Confeccionó	Revisó	Aprobó
BDO Consultoría Externa	 Carla Leiva - CISO	 Francisco Canale - Director

NORMA DE AUDITORÍA DEL SGSI	intiza
	Clasificación: Restringida
Tipo: Norma	Fecha vigencia: 27/11/2024
Código: NO-SI-16- Auditoría del SGSI	Versión: 2.1

Contenido

1. Objetivo	3
2. Alcance	3
3. Responsabilidades	3
4. Desarrollo	4
4.1. Definición del Alcance de la Auditoría	4
4.2. Planificación	4
4.3. Elaboración y aprobación de la planificación	4
4.4. Contratación de un estudio de auditoría externo para realizar trabajos de auditoría interna	5
4.5. Equipo Auditor	5
4.5.1. Conocimientos y habilidades generales requeridas en el equipo auditor	6
4.5.2. Características personales del auditor	7
5. Referencias	8
5.1. Normativa Relacionada	8
5.2. Definiciones	8
6. Historial de Versiones	8

NORMA DE AUDITORÍA DEL SGSI	intiza
	Clasificación: Restringida
Tipo: Norma	Fecha vigencia: 27/11/2024
Código: NO-SI-16- Auditoría del SGSI	Versión: 2.1

1. Objetivo

Definir las pautas que permitan medir la eficacia y eficiencia del Sistema de Gestión de Seguridad de la Información (SGSI) a través de un proceso de auditoría que permita la adecuada identificación y seguimiento de dicha gestión.

2. Alcance

La presente norma comprende desde la necesidad de efectuar una Auditoría hasta los lineamientos para su ejecución, evaluación de resultados obtenidos, generación, distribución del informe y posterior seguimiento.

3. Responsabilidades

Seguridad de la información será quien defina los objetivos de la auditoría y la aprobación del equipo auditor, adicionalmente será responsable de la revisión y aprobación del plan, selección de equipo de auditores, notificaciones, coordinación y comunicación de recursos necesarios para la auditoría de acuerdo al plan, distribución de informes, aseguramiento de la planificación y seguimiento de los planes de acción asociados a los hallazgos de la auditoría.

El **equipo auditor** será responsable de:

- Elaborar el plan
- Ejecutar
- Comunicar los resultados de la auditoría.

Este equipo auditor puede ser personal interno de INTIZA idóneo o bien personal externo contratado para tal fin.

El **Sector auditado** debe:

NORMA DE AUDITORÍA DEL SGSI	intiza
	Clasificación: Restringida
Tipo: Norma	Fecha vigencia: 27/11/2024
Código: NO-SI-16- Auditoría del SGSI	Versión: 2.1

- Elaborar planes de acción para resolver las no conformidades y observaciones detectadas en la auditoría.
- Cumplir con los planes de acción presentados.

4. Desarrollo

4.1. Definición del Alcance de la Auditoría

El alcance de las auditorías puede ser parcial o integral y será determinado en función de la importancia de los procesos o áreas a auditar, los cambios que afecten a los procesos, y los resultados de auditorías previas.

4.2. Planificación

Se debe realizar un plan de auditoría por lo menos una vez al año. El mismo se planificará con 30 días de anticipación la fecha de la auditoría propiamente dicha y determinando como mínimo:

- Alcance y Objetivo
- Periodo de la auditoría
- Responsables
- Equipo auditor
- Detalle de las actividades / tareas a auditar
- Fecha y hora por cada actividad / tarea

4.3. Elaboración y aprobación de la planificación

El equipo auditor deberá elaborar el plan de auditoría de acuerdo con lo dispuesto por el Comité de Seguridad de la Información. El programa de auditoría será desarrollado en función

NORMA DE AUDITORÍA DEL SGSI	intiza
	Clasificación: Restringida
Tipo: Norma	Fecha vigencia: 27/11/2024
Código: NO-SI-16- Auditoría del SGSI	Versión: 2.1

de los procesos alcanzados por el SGSI, la estimación de esfuerzos necesarios y los recursos disponibles.

Se deberá mantener actualizado el Plan efectuando los ajustes que se consideren necesarios debido a cambios en el negocio o el contexto en general.

La Dirección podrá proponer las modificaciones que considere pertinentes en el Plan de Auditoría.

El plan de auditoría deberá estar aprobado por el Comité de Seguridad de la Información.

4.4. Contratación de un estudio de auditoría externo para realizar trabajos de auditoría interna

A efectos de dar ayuda técnica en los relevamientos, documentación, interpretación, etc., pueden ser utilizados los servicios de un estudio de auditoría externo. Los trabajos encomendados a un consultor externo serán supervisados por Seguridad de la Información de INTIZA.

4.5. Equipo Auditor

El equipo auditor deberá disponer de los atributos profesionales, así como las aptitudes y competencias idóneas, para defender los principios de la revisión.

El Equipo Auditor que se designe para efectuar una Auditoría deberá considerar:

- Contactar al área a auditar.
- Elaborar y enviar el “Plan de Auditoría”.
- Ejecutar el plan de auditoría.
- Liderar la reunión de apertura y de cierre comunicando los hallazgos detectados.
- Elaborar el Informe de Auditoría, firmarlo y distribuirlo.

Estará compuesto pero no se limita a los siguientes miembros:

Este documento es propiedad exclusiva de INTIZA y su reproducción total o parcial está totalmente prohibida. El uso, copia, reproducción o venta de esta publicación, sólo podrá realizarse con autorización expresa y por escrito del propietario de la publicación. La versión impresa de este documento pierde automáticamente su vigencia.

NORMA DE AUDITORÍA DEL SGSI	intiza
	Clasificación: Restringida
Tipo: Norma	Fecha vigencia: 27/11/2024
Código: NO-SI-16- Auditoría del SGSI	Versión: 2.1

- **Auditor Líder:** contacta al área a auditar, elabora y envía el Plan de Auditoría, lidera el equipo evaluador, asigna las tareas dentro del equipo auditor, lidera la reunión de apertura y de cierre comunicando los hallazgos detectados, elabora el Informe de auditoría, lo firma y distribuye.
- **Auditor Acompañante:** participa, opcionalmente, como auditor calificado en la auditoría, siguiendo los lineamientos definidos y acordados con el Auditor Líder. Puede liderar algunas entrevistas, solicitar evidencias y relevar información, y participación en la confección del Informe de Auditoría.
- **Auditor Observador:** en caso de ser necesario, acompaña a los otros auditores a modo de entrenamiento.

4.5.1. Conocimientos y habilidades generales requeridas en el equipo auditor

El auditor debe ser capaz de:

- Aplicar principios, procedimientos y técnicas de auditoría;
- Planificar y organizar el trabajo con eficacia;
- Conducir la revisión dentro del calendario acordado;
- Priorizar y enfocarse en asuntos de importancia;
- Recolectar información a través de entrevistas, escuchas, observaciones y revisiones efectivas de documentos, registros y datos;
- Comprender la idoneidad y las consecuencias del uso de técnicas de muestreo para la revisión;
- Planificar la revisión y hacer un uso eficaz de los recursos durante la revisión;
- Prevenir o resolver conflictos;
- Preparar y completar el informe de revisión.
- Verificar la exactitud de la información recopilada;

NORMA DE AUDITORÍA DEL SGSI	intiza
	Clasificación: Restringida
Tipo: Norma	Fecha vigencia: 27/11/2024
Código: NO-SI-16- Auditoría del SGSI	Versión: 2.1

- Verificar la adecuación de las evidencias de revisión para apoyar los resultados y conclusiones de la revisión;
- Evaluar los factores que pueden afectar a la fiabilidad de los resultados y conclusiones de la revisión;
- Preparar informes de revisión de calidad y profesionalidad adecuadas;
- Mantener la confidencialidad y seguridad de la información;
- Comunicar eficazmente.

4.5.2. Características personales del auditor

Un auditor debe ser:

- Ético, justo, veraz, sincero, honesto y discreto;
- De mente abierta y dispuesto a considerar ideas alternativas o puntos de vista;
- Diplomático, con tacto en el trato con las personas, en particular aquellos que son mayores o están sobre comprometidos;
- Observador, consciente activamente del entorno;
- Perceptivo, es decir intuitivamente consciente y capaz de entender situaciones;
- Versátil, capaz de ajustarse a diferentes situaciones;
- Persistente, centrado en la consecución de objetivos;
- Independiente, actúa y funciona de forma autónoma mientras interactúa eficazmente con los demás.

5. Referencias

5.1. Normativa Relacionada

Categoría	Título	Código
Política	Seguridad de la Información	PO-SI-01

Este documento es propiedad exclusiva de INTIZA y su reproducción total o parcial está totalmente prohibida. El uso, copia, reproducción o venta de esta publicación, sólo podrá realizarse con autorización expresa y por escrito del propietario de la publicación. La versión impresa de este documento pierde automáticamente su vigencia.

NORMA DE AUDITORÍA DEL SGSI	
	Clasificación: Restringida
Tipo: Norma	Fecha vigencia: 27/11/2024
Código: NO-SI-16- Auditoría del SGSI	Versión: 2.1

5.2. Definiciones

Término	Descripción
Auditor	El auditor es el profesional encargado de revisar si los documentos de la empresa reflejan la realidad.
Terceros	Se entiende por terceros a contratistas, proveedores, clientes, consultores, pasantes y todo el personal que no forma parte de la nómina de empleados de INTIZA pero que interactúen con ella.

6. Historial de Versiones

Versión	Fecha	Resumen de Cambios
1.0	01/12/2021	Creación de la Norma de Auditoría de Sistemas y Seguridad de la Información.
1.0	27/01/2022	Aprobado por Comité de Dirección: MI-DI-02 Minuta de Comité de Dirección N° 2.
2.0	24/08/2022	Se modificó el nombre del documento y se realizaron modificaciones en el objetivo, alcance y responsabilidades y se realizaron cambios en el contenido.
2.0	11/10/2022	Aprobado por Comité de Dirección: MI-DI-06- Minuta de Comité de Dirección N° 6.
2.1	27/11/2024	Se realizó una revisión general del documento y se ajustaron

Este documento es propiedad exclusiva de INTIZA y su reproducción total o parcial está totalmente prohibida. El uso, copia, reproducción o venta de esta publicación, sólo podrá realizarse con autorización expresa y por escrito del propietario de la publicación. La versión impresa de este documento pierde automáticamente su vigencia.

NORMA DE AUDITORÍA DEL SGSI	intiza
	Clasificación: Restringida
Tipo: Norma	Fecha vigencia: 27/11/2024
Código: NO-SI-16- Auditoría del SGSI	Versión: 2.1

		algunos detalles sin cambios significativos en el contenido.
2.1	27/11/2024	Aprobado por Comité.