Guía para realizar una Auditoría al Sistemas de Gestión de Seguridad de la Información desarrollada bajo la NTC-ISO/IEC 27001:2013

Jorge Mario Guzmán Díaz[1]

Resumen

Un Sistema de Gestión de Seguridad de la Información (SGSI) es fundamental para proteger los activos de información de una organización. Para implementarlo de manera efectiva, se deben identificar y evaluar los riesgos, establecer políticas, procedimientos adecuados, y asignar responsabilidades claras. Para su implementación, se pueden emplear las normas NTC-ISO/IEC 27001 (ICONTEC, 2013), COBIT5 o MAGERIT. La auditoría al SGSI, basada en la norma ISO/IEC 27007 (ISO, 2020), evalúa el cumplimiento y la efectividad mediante la revisión de documentación, entrevistas y pruebas técnicas. El artículo tiene como objetivo proponer una Guía de Auditoría de Sistemas para un Sistema de Gestión de Seguridad de la Información, proporcionando pautas detalladas para realizar auditorías efectivas, evaluar el cumplimiento y verificar la efectividad de los controles de seguridad de la información del SGSI.

Palabras Claves. Sistema de Gestión de Seguridad de la Información, activos de información, controles de seguridad de la información.

Abstract

An Information Security Management System (ISMS) is crucial for protecting an organization's information assets. To effectively implement it, risks must be identified and evaluated, appropriate policies and procedures established, and clear responsibilities assigned. The NTC-ISO/IEC 27001 (ICONTEC, 2013), COBIT5, or MAGERIT standards can be

[1] Jorge Mario Guzmán Díaz, Economista de la Universidad de La Salle, Estudiante de Especialización en Auditoría en Sistemas de la Universidad Antonio Nariño. Jguzman27@uan.edu.co

employed for its implementation. The audit of the ISMS, based on ISO/IEC 27007 (ISO, 2020), assesses compliance and effectiveness through documentation review, interviews, and technical testing. This article aims to propose an Audit Systems Guide for an Information Security Management System, providing detailed guidelines for conducting effective audits, evaluating compliance, and verifying the effectiveness of ISMS information security controls.
Key words. Information Security Management System, information assets, information security controls.

Introducción

La información es un activo vital para las organizaciones, impulsando la toma de decisiones y la competitividad, pero también representa riesgos si no se protege adecuadamente. Por eso, las organizaciones implementan sistemas de gestión de la seguridad de la información (SGSI) que les permita mitigar los riesgos asociados al manejo de esta (Areitio, 2008).

Uno de ellos es el basado en la norma NTC-ISO/IEC 27001 (ICONTEC, 2013) "Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información – Requisitos", que proporciona un modelo para establecer, implementar, operar, seguir, revisar, mantener y mejorar un SGSI (ICONTEC, 2013).

Así mismo, un SGSI basado en la norma NTC-ISO/IEC 27001 (ICONTEC, 2013) requiere una evaluación independiente para verificar su funcionamiento, logro de objetivos y detectar debilidades o vulnerabilidades periódicamente. Esta tarea, es realizada por la auditoría, la cual evalúa la gestión y eficiencia del SGSI e identifica oportunidades de mejora.

Es en este punto, donde la norma ISO/IEC 27007 (ISO, 2020) "Directrices para la Auditoría de los Sistemas de Gestión de la Seguridad de la Información", proporciona

orientación sobre la gestión de un programa de auditoría a un SGSI basado en la NTC-ISO/IEC 27001 (ICONTEC, 2013).

Cabe destacar que la norma NTC-ISO/IEC 27001 (ICONTEC, 2013) no incluye el ciclo PHVA para la ejecución de procesos. Este aspecto solo se aborda en la norma ISO 27001 (ICONTEC, 2005). En el artículo se analizarán ambas normas en relación con el ciclo PHVA y demás aspectos.

La ISO/IEC 27007 (ISO, 2020) exige que el desarrollo de la auditoría debe llevarse a cabo juntamente con las normas[2] ISO 19011: 2018, NTC-ISO/IEC 27000:2017 y ISO/IEC 27004:2016, lo que puede ser inconveniente y derivar en una falta de entendimiento y consistencia en la forma en que se llevan a cabo las auditorías al SGSI.

Otro aspecto para destacar es la diferencia de la norma ISO/IEC 27007 (ISO, 2020) que proporciona orientación en la realización de auditorías del SGSI, y el concepto de guía de auditoría que establece procedimientos, puntos a revisar, técnicas y herramientas específicas para una auditoría efectiva (Muñoz Razo, 2002).

En base a lo anterior se puede establecer que la norma ISO/IEC 27007 (ISO, 2020) aun cuando proporciona orientación para auditar un SGSI, requiere de otras normas complementarias para su interpretación y no contempla en si misma elementos concretos de una Guía de Auditoría.

Dado lo anterior cabe establecer ¿Qué aspectos específicos deben ser cubiertos en una Guía de Auditoría de Sistemas, para realizar eficazmente una auditoría de un Sistema de Gestión de la Seguridad de la Información de una organización bajo la NTC-ISO/IEC 27001:2013?

[2] Norma ISO 19011: 2018 -Directrices para la auditoría de los sistemas de gestión, la NTC-ISO/IEC 27000:2017 - Sistemas de Gestión de Seguridad de la Información - Visión general y vocabulario, ISO/IEC 27004:2016 - Gestión de la seguridad de la información – Medición.

El objetivo del presente artículo es proponer la construcción de una guía integral para la Auditoría de Sistemas, que permita evaluar el Sistema de Gestión de la Seguridad de la Información (SGSI) de una organización desarrollado bajo la norma NTC-ISO/IEC 27001 (ICONTEC, 2013). Esta guía estará contenida en un único documento y se basará en los estándares de auditoría de en la norma ISO/IEC 27007 (ISO, 2020) y complementarias. De esta manera, se busca proporcionar un enfoque integral para realizar la auditoría de un SGSI.

Metodología

El desarrollo del artículo se lleva a cabo utilizando la metodología de investigación cualitativa descriptiva y documental. Para ello se inicia con la descripción de los requisitos, las mejores prácticas y el proceso de implementación, mantenimiento y mejora de un Sistema de Gestión de Seguridad de la Información (SGSI), en concordancia con los estándares establecidos por la norma NTC-ISO/IEC 27001 (ICONTEC, 2013), donde se busca examinar los elementos claves para la implementación, operación, mantenimiento y monitoreo de un SGSI.

A continuación, se procederá a definir el proceso de auditoría al SGSI, tomando como base la norma ISO/IEC 27007 (ISO, 2020) y sus normas relacionadas[3]. Se describirán los pasos necesarios a seguir en la auditoría, incluyendo las técnicas, herramientas y procesos utilizados.

Teniendo claras las normas anteriores, se procederá a diseñar la Guía de Auditoría de Sistemas, al Sistema de Gestión de Seguridad de la Información en base a la NTC-ISO/IEC 27001 (ICONTEC, 2013), abordando las fases del ciclo de auditoría[4] , incluyendo papeles de trabajo, indicadores y ejemplos para una mejor comprensión.

[3] Norma ISO 19011:2018 Directrices para la auditoría de los sistemas de gestión.
[4] Planeación, Ejecución, Comunicación y Seguimiento.

Requisitos, Mejores Prácticas y Proceso de Implementación, Mantenimiento y Mejora de un Sistema de Gestión de Seguridad de la Información (SGSI), Acorde con la Norma NTC-ISO/IEC 27001:2013.

El SGSI se define como la combinación de un sistema de gestión organizacional y la gestión de la seguridad de la información para proteger los activos de información de una organización (Areitio, 2008).

Para la implementación y gestión de un SGSI, existen algunos modelos tales como COBIT 5 para la Seguridad de la Información y otros como MAGERIT e ISO/IEC 27001:2005, que de acuerdo con (Colobran, 2008), brindan el marco, metodología y lineamientos necesarios para implementar un SGSI.

ISO/IEC 27001: 2005, 2013

La norma ISO/IEC 27001 (ICONTEC, 2005), es un estándar a nivel internacional diseñado para proporcionar un modelo que permita a las organizaciones "establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Seguridad de la Información" (ICONTEC, 2005).

Para el desarrollo del presente capitulo se describe en la sección "Proceso de implementación del SGSI", lo relacionado con el ciclo PHVA incluido en la norma ISO/IEC 27001 (ICONTEC, 2005). Los aspectos asociados a objetivos, terminología, implementación del SGSI, responsabilidades de la dirección, auditorías internas, revisión de la dirección y mejora del SGSI, se desarrollan en base a la norma NTC-ISO/IEC 27001 (ICONTEC, 2013).

Objetivos de la norma, términos y definiciones NTC-ISO/IEC 27001:2013

La norma NTC-ISO/IEC 27001 (ICONTEC, 2013), es aplicable en organizaciones de cualquier tamaño y tipo, a través de directrices que cubren todas las etapas del SGSI.

También proporciona una lista de términos y definiciones para una comprensión clara de los conceptos clave en la seguridad de la información.

Proceso de implementación del SGSI

La implementación del SGSI requiere del PHVA (ICONTEC, 2005), que es un modelo de procesos que se utiliza para organizar y estructurar todos los procesos del SGSI. El modelo PHVA está compuesto de cuatro fases descritas en la tabla 1:

Tabla 1. *Modelo PHVA*

Planificar	Se definen políticas, objetivos, procesos y procedimientos seguros para gestionar riesgos y mejorar la seguridad información, alineados con políticas y objetivos generales organizacionales.
Hacer	En esta etapa se implementan los controles y se llevan a cabo las acciones necesarias para alcanzar los objetivos y metas del SGSI.
Verificar	En esta fase se monitorea y se evalúa el desempeño del SGSI para asegurarse de que está funcionando adecuadamente y se están logrando los objetivos y metas establecidos.
Actuar	Se llevan a cabo acciones de mejora continua para corregir cualquier problema identificado durante la fase de verificación y para hacer ajustes y mejoras al SGSI en general.

Fuente: Elaboración propia en base a NTC-ISO/IEC 27001 (ICONTEC, 2005)

En la fase de implementación, la organización define, implementa y mejora continuamente el SGSI, alineándolo con los objetivos estratégicos y gestionando los riesgos mediante la selección de objetivos de control adecuados. Esto lo logra aplicando los controles de seguridad que se encuentran relacionados en el anexo A de la norma y descritos en la tabla 2:

Tabla No. 2. *Objetivos de Control y Controles*

Política de seguridad: Debe ser aprobada, comunicada y revisada regularmente para garantizar su efectividad.	**Control de acceso:** Garantizar políticas de acceso, gestión de identidades, controles de acceso físicos y lógicos.
Organización de la SI: La organización establece estructura, roles y responsabilidades, garantizando su cumplimiento.	**Adquisición, desarrollo y mantenimiento de SI**: Incluye la identificación de requisitos, selección de proveedores confiables, gestión de cambios y pruebas de seguridad.
Gestión de activos: La organización protege y gestiona sus activos mediante procedimientos y evaluación de riesgos.	**Gestión de los incidentes de la SI**: Medidas de detección, respuesta y recuperación ante incidentes seguridad información.
Seguridad de los recursos humanos: La organización capacita a empleados y terceros en seguridad de la información.	**Gestión de la continuidad del negocio:** Implementa medidas de continuidad del negocio: identificación de procesos críticos, planes de contingencia y pruebas periódicas.
Seguridad física y del entorno: Implementación de medidas físicas para la protección de activos y asegurar continuidad en desastres.	**Cumplimiento:** De leyes y regulaciones de seguridad de información a través de medidas y revisiones periódicas.

Fuente: Elaboración propia en base a NTC-ISO/IEC 27001 (ICONTEC, 2013)

Responsabilidad de la dirección y compromiso de la dirección.

La alta dirección demuestra su compromiso, estableciendo las políticas de seguridad, asignando roles y proporcionando recursos para el SGSI.

Evaluación de Desempeño y Mejora del SGSI

Por último, en la tabla 3, la norma NTC-ISO/IEC 27001:2013 describe los aspectos a tener en cuenta en la evaluación de desempeño y en la mejora del SGSI:

Tabla 3. *Evaluación de Desempeño y Mejora del SGSI*

Aspecto	Descripción
Auditorías internas del SGSI:	La norma requiere auditorías internas programadas para verificar si el SGSI cumple con los requisitos de la organización y de la norma, y si la está implementado y mantenido de manera efectiva.
Revisión del SGSI por la dirección - generalidades:	La alta dirección revisa regularmente el SGSI alineado con objetivos, identifica oportunidades de mejora, toma decisiones y presenta los informes documentados.
Mejora del SGSI:	La norma NTC-ISO/IEC 27001:2013 enfatiza la mejora continua en el SGSI, corrigiendo no conformidades, tomando medidas preventivas y teniendo un enfoque proactivo en la seguridad de la información.

Fuente. Elaboración propia en base a NTC-ISO/IEC 27001 (ICONTEC, 2013)

COBIT5 para la Seguridad de la Información

COBIT 5 para la Seguridad de la Información (ISACA, 2012), proporciona el marco para el gobierno y gestión organizacional de la seguridad de la información, destacando la importancia de protegerla, mantener su confidencialidad, integridad y disponibilidad. En la tabla 4 se describe los cinco principios COBIT 5 para la gestión de la seguridad de la información:

Tabla 4. *Principios COBIT 5 para la Seguridad de la Información*

Principio	Descripción
Satisfacer las Necesidades de las Partes Interesadas:	Equilibrar beneficios, riesgos y recursos para satisfacer a las partes interesadas, incluyendo la seguridad de la información.
Cubrir la Empresa Extremo-a-Extremo:	El gobierno de las TI debe integrarse con el gobierno de la empresa y cubrir todas las funciones y procesos empresariales.
Aplicar un Marco de Referencia Único Integrado:	COBIT 5 es un marco integrado que se alinea con otros estándares y se puede utilizar como el marco general para el gobierno y gestión de las TI de la empresa.
Hacer Posible un Enfoque Holístico:	COBIT 5 destaca un enfoque integral para gobernar y gestionar las TI con catalizadores para apoyar la implementación del sistema de gobierno y gestión.
Separar el Gobierno de la gestión:	COBIT 5 separa el gobierno de la gestión, al entender que son dos disciplinas diferentes con distintas responsabilidades y objetivos en la empresa.

Fuente: Elaboración propia en base a COBIT 5 (ISACA, 2012)

Además de los principios mencionados, COBIT 5 (ISACA, 2012) describe elementos importantes para la gestión de la seguridad de la información denominados, "catalizadores" que se refieren a los factores que ayudan a habilitar y ejecutar la gestión efectiva de la empresa. En la tabla 5 se describen los catalizadores que tiene implementada la metodología:

Tabla 5. *Catalizadores de COBIT 5 para Implantar la Seguridad de la Información*

Catalizador	Descripción
Principios, Políticas y Marcos de Referencia:	Define los principios y políticas de seguridad de la información para la organización y proporciona marcos de referencia para su implementación.
Procesos:	Este describe un enfoque estructurado y procesos necesarios para la gestión efectiva de la seguridad de la información
Estructuras Organizativas:	Establece la estructura organizativa necesaria para la gestión efectiva de la seguridad de la información, incluyendo roles y responsabilidades claras y definidas.
Cultura, Ética y Comportamiento:	Fomenta cultura y comportamiento ético en toda la organización para asegurar la seguridad de la información en todas las actividades.
Información:	Define los requisitos para la gestión efectiva de la información, incluyendo la identificación, clasificación y protección adecuada de la información crítica.
Servicios, Infraestructuras y Aplicaciones:	Asegura que los servicios, infraestructuras y aplicaciones de la organización sean seguros, proporcionando un entorno seguro para la información de la organización.
Personas, Habilidades y Competencias	Define requisitos de habilidades y competencias para la gestión de seguridad de la información, incluyendo formación y educación del personal.

Fuente: Elaboración propia COBIT 5 (ISACA, 2012)

MAGERIT Metodología de Análisis y Gestión de Riesgos de las Administraciones Públicas

El modelo MAGERIT (CSAE, 2012) es un enfoque de gestión de riesgos de seguridad de la información en cinco fases: identificación de activos relevantes, evaluación de amenazas, evaluación de salvaguardas, estimación de impacto y cálculo de riesgos. Permite comprender el valor de los activos, evaluar las amenazas, verificar las salvaguardas existentes y calcular el riesgo basado en la tasa de ocurrencia y el impacto potencial.

Los marcos, modelos y metodologías mencionadas para implementar y gestionar un SGSI, tienen cada uno enfoque diferente. COBIT 5 se centra en la gobernanza y gestión de TI, MAGERIT se enfoca en la evaluación de riesgos y la planificación de la continuidad del negocio, mientras que la norma NTC-ISO/IEC 27001:2013 se enfoca en la implementación del SGSI.

Auditoría de Sistemas al Sistema de Gestión de la Seguridad de la Información (SGSI) con base en las ISO/IEC 27007:2020.

Para auditar la implementación de un SGSI en base a la norma NTC-ISO/IEC 27001:2013 y poder evaluar la gestión de riesgos y oportunidades de mejora, la norma ISO/IEC 27007:2020[5], proporciona orientación sobre cómo gestionar un programa de auditoría de sistemas al SGSI de una organización, la cual se describirá a continuación de manera general.

Referencias Normativas

La norma ISO/IEC 27007 (ISO, 2020) tiene como base los lineamientos de la ISO 19011 (ISO, 2018) y en ISO/IEC 27000 (ISO, 2018), enfocándose en los términos y definiciones, principios de la auditoría, gestión del programa de auditoría y competencia de los auditores.

Principios de la Auditoría, Gestión del Programa y Competencia de los Auditores.

En la tabla 6 se describen las etapas para el desarrollo de la auditoría a un SGSI en base a la ISO ISO/IEC 27007 (ISO, 2020):

Tabla 6. *Principios de la auditoría, gestión del programa y competencia de los auditores.*

Principios de la Auditoría	**Establecimiento del programa de auditoría**
La auditoría se basa en siete principios clave para ser una herramienta eficaz y confiable en apoyo de las políticas y controles de gestión **ISO 19011:2018** Integridad, Enfoque Basado en Riesgos y evidencia, Presentación Imparcial, Independencia, Confidencialidad.	Se establecen las funciones, responsabilidades y competencias de la persona responsable de la gestión del programa de auditoría, **ISO 19011:2018** • Responsable auditoría: establece, evalúa, implementa, monitorea programa, reporta alta gerencia. • Auditor: competente, habilidades actualizadas. • Riesgos: afectan objetivos auditoría (planeación, recursos, equipo, implementación). • Gestor programa auditoría: planifica, ejecuta, mejora auditorías, asegura competencia auditores, reporta a la alta dirección. • Establecer funciones, responsabilidades, competencias responsable gestión programa auditoría
Establecimiento de los objetivos del programa de auditoría El cliente de la auditoría debe asegurarse de que los objetivos del programa de auditoría estén alineados con su estrategia y apoyen su política y objetivos de gestión. **ISO 19011:2018** Durante auditoría: identificar necesidades y expectativas partes interesadas, requisitos, riesgos, oportunidades. Evaluar desempeño y madurez SG con indicadores, revisar resultados anteriores.	
ISO/IEC 27007:2020 Se evalúan los requisitos de seguridad, desempeño y tamaño del SGSI, incluyendo riesgos e incidencias. También se identifican los riesgos de seguridad de la información para las partes relevantes.	**ISO/IEC 27007:2020** • Priorización auditoría: basada en tamaño, complejidad, riesgos, importancia comercial del SGSI para gestión seguridad información.

[5] ISO/IEC 27007 (ISO, 2020) -Tecnología de la información. Técnicas de seguridad. Directrices para la auditoría de los sistemas de gestión de la seguridad de la información.

Gestión de un programa de auditoría	**Establecimiento del programa de auditoría**
Establecer un programa de auditoría que se adapte al tamaño y complejidad de la organización auditada. **ISO 19011:2018** **Contexto del Auditado:** Objetivos Organizacionales, Necesidades de Seguridad **Información y recursos:** Confidencialidad de la información, para ser eficiente en el tiempo especificado	• Riesgos programa auditoría: afectan confidencialidad requisitos. • Seguridad información: cumplir requisitos legales, contractuales y partes relevantes, incluyendo auditados. • Auditores: tiempo adecuado para revisar riesgos y oportunidades SGSI.
Gestión de un programa de auditoría	
Implementación del programa de auditoría: De ser monitoreado y medido, Para alcanzar los objetivos	**ISO/IEC 27007:2020** **Establecer la auditoría en base a:** Riesgos y oportunidades al planificar el SGSI
Implementación del programa de auditoría	
La gestión del programa de auditoría incluye objetivos, coordinación y selección de equipos competentes, recursos y plazos adecuados.	
ISO 19011:2018	**ISO/IEC 27007:2020**
La auditoría define objetivos, alcance y criterios coherentes con programas relevantes, alineando métodos de auditoría. Selección del equipo auditor considera competencia, complejidad e independencia, incluyendo expertos técnicos si necesario.	La auditoría del SGSI evalúa procesos, controles, riesgos y oportunidades según criterios establecidos, incluyendo auditorías conjuntas. Se requiere un equipo auditor competente en gestión de riesgos de seguridad de la información.

Fuente: Elaboración propia en base a ISO/IEC 27007 (ISO, 2020)

Finalmente, como se describe en la tabla 7, la norma ISO/IEC 27007 (ISO, 2020) dedica sus dos últimos capítulos a las directrices que deben seguirse para llevar a cabo la auditoría y para evaluar las competencias de los auditores que forman parte del equipo de trabajo.

Tabla 7. *Implementación del programa de auditoría*

Realización de la auditoría	**Realización de las actividades de auditoría**
Al respecto se describe de manera general el proceso que se debe seguir para llevar a cabo una auditoría de sistemas de gestión de seguridad de la información (SGSI) de acuerdo con la norma ISO 27007: 2020 • Contacto inicial con Auditado • Factibilidad de la auditoría • Actividades de auditoría • Revisión de documentos • Preparación plan de auditoría • Asignación trabajo al equipo • Preparación PTs.	Incluye actividades como reunión de apertura, revisión de documentos, comunicación durante la auditoría, asignación de roles, recolección información, generación de hallazgos, preparación de conclusiones y reunión de cierre. • Realización reunión apertura • Rev. docs. • Comunicación en la auditoría • Roles observadores • Recopilación-verificación Inf. • Generación hallazgos • Preparación de conclusiones
Preparación y distribución del informe de auditoría	**Evaluación Competencias Auditores**
Este capítulo describe cómo se debe preparar el informe de auditoría y cómo se debe distribuir. • Preparación informe auditoría • Completando la auditoría • Realización seguimiento • Distribución informe auditoría	Se centra en la evaluación de la competencia de los auditores y cómo se deben evaluar sus habilidades y conocimientos.

Fuente. Elaboración propia en base a ISO/IEC 27007 (ISO, 2020)

En general la ISO/IEC 27007 (ISO, 2020) proporciona orientación sobre cómo llevar a cabo auditorías de SGSI. Esta norma se basa en gran medida en la norma ISO 19011 (ISO, 2018), que establece los principios y requisitos para la auditoría a sistemas de gestión en general.

Al basarse en la norma ISO 19011 (ISO, 2018), la ISO/IEC 27007 (ISO, 2020), aprovecha los beneficios de un enfoque sistemático, siendo coherente con los requisitos generales de la auditoría de sistemas al SGSI.

Guía de Auditoría de Sistemas Propuesta para Evaluar un Sistema de Gestión de Seguridad de la Información de una Organización, Desarrollado Bajo la Norma ISO/IEC 27007:2020

Teniendo en cuenta lo desarrollado en el punto uno de este documento, en relación con la implementación de un SGSI y las directrices para realizar la auditoría al SGSI vistas en el punto dos, se propone la siguiente guía[6] que busca integrar los dos temas vistos de manera práctica y con ejemplos que permitirán al auditor, tener un mejor entendimiento al realizar la auditoría.

La guía propuesta está estructurada acorde a los tres componentes básicos del ciclo de auditoría y ajustados para la evaluación del SGSI descritos en la figura 1:

Figura 1. *Guía de Auditoría a un SGSI*

Fuente: Elaboración propia.

Planeación

Gestión del Programa de Auditoría

Para el diseño y gestión del programa de auditoría se recomienda seguir las directrices de la norma ISO 27007 (ICONTEC, 2013), descritas en la tabla 8:

[6] La guía de auditoría es fundamental en la auditoría de sistemas informáticos, proporcionando un procedimiento detallado, puntos de evaluación, áreas a revisar y herramientas necesarias, incluyendo técnicas de evaluación y ponderación específica. (Muñoz Razo, 2002)

Tabla 8. *Gestión Programa de Auditoría*

Etapa	Descripción
Establecimiento de los objetivos:	Definir propósitos y metas de la auditoría.
Determinación y evaluación de riesgos:	Identificar posibles riesgos y oportunidades asociados a la auditoría.
Establecimiento del programa de auditoría:	Crear un plan detallado con alcance, procedimientos, recursos y cronograma.
Implementación del programa de auditoría:	Realizar actividades planificadas de recopilación, análisis y evaluación.
Seguimiento del programa de auditoría:	Monitorear el progreso, cumplimiento de plazos y ajustes necesarios.
Revisión y mejora del programa:	Evaluar efectividad, identificar mejoras y actualizar enfoques futuros de la auditoría.

Fuente. Elaboración propia. ISO 27007 (ICONTEC, 2013)

Establecer Contacto con el Auditado

En la reunión de apertura se recopilan datos, se establecen objetivos, el alcance y responsables. Para esta etapa se sugiere desarrollar el papel de trabajo de la tabla 9.

Tabla 9. *Papel de Trabajo para Establecer Contacto con el Auditado*

Nombre de la empresa, Identificación. No. De Referencia PT, Tipo de PT, Fecha, Auditor Responsable.	
Objetivos: Establecer contacto con el auditado para obtener acceso a la información necesaria, programar reuniones, recopilar los datos relevantes y expectativas del auditado, para llevar a cabo una auditoría exhaustiva.	
Alcance: -Identificar los responsables del SGSI - Establecer ubicación de las políticas, procedimientos, manuales del SGI - Establecer cronograma para la realización de reuniones para entendimiento del SGSI - Conocer la matriz de riesgos asociada al SGSI si existe.	
Procedimiento	**Ejemplo**
Informar al auditado sobre los objetivos y alcance de la auditoría a realizar sobre el SGSI.	El objetivo de la presente auditoría es evaluar la implementación, mantenimiento y mejora del (SGSI) que ha sido implementado bajo la norma NTC-ISO/IEC 27001:2013.En cuanto al alcance, se evaluara el cumplimiento de los lineamientos definidos en la NTC-ISO/IEC 27001:2013.
Solicitar ubicación y tipo de documentos asociados al SGSI (Matriz de Riesgo, Invetarios, políticas, manuales, procedimientos, etc.). Registrar ubicación electrónica y tipo de documento.	**Documento:** Política de Ciberseguridad **Ubicación**: https://empresa.politica.ciberseguridad **Documento:** Flujo de proceso Ubicación: Aplicativo Visio Microsoft 365
Consulte al usuario si existe áreas específicas responsables del SGSI, quienes son los responsables y que parte del SGSI gestionan	**Responsable**: CEO, presidentes, directores ejecutivos Responsabilidades:Establecer la visión, los objetivos y las políticas de seguridad de la información.

Fuente. Elaboración propia.

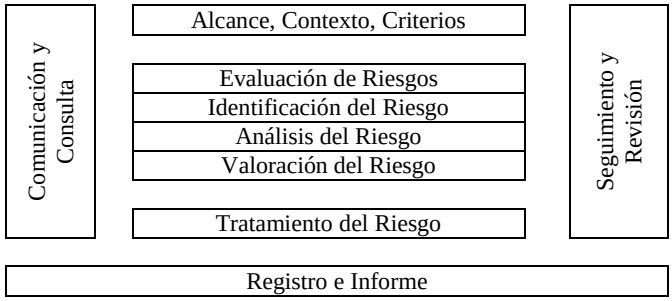
El cronograma de la evaluación debe incluir: área evaluada, número de papel de trabajo, fecha de elaboración, responsable, objetivos del cronograma, alcance, fechas y nombres de las etapas, actividades a realizar y objetivo de las actividades. El cronograma de la auditoría no se define necesariamente en la reunión de apertura, sino que puede ser acordado posteriormente.

Ejecución

Evaluación de la Gestión Riesgos

Durante esta etapa, el auditor recopila la información necesaria para evaluar la efectividad de la gestión de riesgos del SGSI realizada por la organización, conforme al proceso de administración de riesgos de la norma ISO 31000 (ISO, 2018)[7], descrito en la figura 2:

Figura 2. *Gestión de Riesgos ISO 31000:2018*



Fuente: Norma ISO 31000 (ISO, 2018) Sección 6 Procesos

Adicionalmente, evalúa el resultado de la valoración de riesgos asociados al SGSI, contenidos en la matriz de riesgos de la compañía, particularmente los calificados por la administración como altos o relevantes. La matriz debería contener al menos la información descrita en la tabla 10:

Tabla 10. *Modelo Matriz de Riesgos*

Aspecto	**Descripción**
Escenario:	Mantenimiento de las Bases de Datos en el Servidor 1
Amenaza:	Malware
Descripción:	Virus, gusanos o los troyanos, que puede infectar sistemas y redes, comprometiendo la confidencialidad, la integridad o la disponibilidad de la información.
Evento:	Descarga de archivos desde sitios web no seguros.
Efecto:	Perdida de información, corrupción de datos, interceptación de información.
Activo afectado:	Bases de Datos Cliente - Bases de Datos Contables - Redes y Comunicaciones
Propiedad de la Información:	Disponibilidad, Integridad, Confidencialidad
Probabilidad:	Esta dada en número de eventos posibles en un periodo determinado. Ej. No. De veces que los usuarios accedes y descargan información en sitios no autorizados.
Calificación:	Acorde a lo definido en la matriz de probabilidad definida por la organización se puede obtener la calificación dada a la misma. (Alto, Medio, Bajo).
Impacto:	Esta dada en el valor posible de pérdidas ocasionadas por la materialización del riesgo. Ej. Multas por perdida de datos confidenciales.
Riesgo Inherente	Alto

[7] ISO 31000:2018 Administración/Gestión de riesgos — Lineamientos guía

Fuente. Elaboración propia.

La calificación otorgada al riesgo inherente permitirá al auditor establecer los activos críticos a evaluar dados los riesgos identificados por la organización.

Evaluar los Activos de Información

El auditor determina los activos prioritarios para la organización tras las conversaciones y el entendimiento de los procesos. En la tabla 11 se describen las pruebas a realizar sobre el inventario de activos críticos:

Tabla 11. *Papel de Trabajo para Evaluación Activos de información*

Nombre de la empresa, Identificación. No. De Referencia PT, Tipo de PT, Fecha, Auditor Responsable.		
Objetivos: Identificar los Activos de información.		
Alcance: - Identificar si existe inventario de Activos de información - Verificar los responsables - Verificar las características del inventario (Uso de la información, Frecuencia de Generación, Acción principal de la información, Uso, etc)		
Procedimiento	**Ejemplo**	
Verificar si existe el inventario de activos y ruta donde se encuentra almacenada, y responsable de la administración del inventario.	**Nombre Documento:** Inventario de Activos **Ubicación:** https://empresa.politica.ciberseguridad **Responsable:** Gerente TI **Área:** Dpto de Tecnología	
	Características – Activos de información	
Validar si el inventario de activos comprende las siguientes características. Validar la existencia del activo.	• Propósito de la información • Tipo de Dato (publico, semiprivado, Privado) • Medio de intercambio de la información • Frecuencia de generación • Calificación de Criticidad	• Información propia o de terceros • Forma de almacenamiento • Acción principal sobre la información (actualizar, crear, consultar etc) • Uso de la información
Indicadores: Porcentaje de criterios que cumplen con los criterios definidos en el la prueba.		

Fuente: Elaboración propia.

Evaluación de los Controles

El auditor evalúa los controles con base a la criticidad definida para cada riesgo por los dueños de los activos. En la tabla 12, se describe el modelo de un posible control a evaluar.

Tabla 12. *Modelo Diseño de Control*

No. de Control CTR1	**Descripción del Control:** Implementar soluciones antivirus y antimalware actualizadas en todos los dispositivos. Realizar análisis de malware periódicos en los sistemas.
Amenaza: Malware	
Nombre del Control: Control de Malware	
Objetivo del Control: Prevenir y detectar la presencia de malware en el sistema.	
Frecuencia de Ejecución: Diaria	**Evidencias de Ejecución:** Reportes de análisis de malware. Registro de actualización de soluciones antivirus. Registro de detección y acciones tomadas ante amenazas de malware.
Responsable: Equipo de Seguridad de la Información	
Tipo de Ejecución: Automático	

Fuente. Elaboración propia.

Pruebas a los controles SGSI. En la tabla 13 se relacionan las pruebas sugeridas para la evaluación de la efectividad de los controles establecidos por la organización:

Tabla 13. *Papel de Trabajo Evaluación de Controles sobre Activos SGSI*

Nombre de la empresa, Identificación. No. De Referencia PT, Tipo de PT, Fecha, Auditor Responsable.	
Objetivos: Evaluar el diseño y efectividad de los controles asociados a garantizar la Seguridad de la información de (controles de acceso, controles criptográficos, de comunicación de datos.).	
Alcance: Evaluación de Diseño, Evaluación de operatividad del control.	**Técnicas:** Revisión documental y de flujos de proceso, pruebas de recorrido con los ejecutores del proceso
Herramientas: Entrevistas presenciales o mediante plataformas colaborativas (Teams, Meet) con los responsables de cada uno de los controles seleccionados. / Acceso a las plataformas de publicación de proceso y flujos los cuales pueden estar en Ms Visio, y otras plataformas de diseño de flujos y repositorios de información. / Herramientas de análisis Estadístico, Excel o IDEA / Acceso a aplicativos utilizados por la organización./ Pruebas de observación para verificación de estado de activos físicos, comprobación de funcionamiento de controles como cámaras, tarjetas de acceso, puertas de bloqueo.	
Instrucciones 1) Leer manuales y procesos relacionados al control antes de la prueba de recorrido. 2) Coordinar fechas con el auditado para la evaluación. 3) Verificar la realización del control según lo definido en el proceso y las preguntas de la guía. 4) Seleccionar muestra de evidencias para corroborar eficacia del control según la guía.	
Pruebas a realizar sobre Validaciones de Diseño (SI ____ NO____ N/A____) 1. Control ejecutado según matriz de riesgos/controles o flujo de proceso. 2. Responsable del control definido en procesos o políticas. 3. Naturaleza del control correspondiente al proceso (preventivo, correctivo, detectivo). 4. Tipo de control conforme a lo definido en el proceso (automático, manual, semiautomático). 5. Idoneidad del ejecutor/responsable del control (capacitación, experiencia, nivel académico). 6. Adecuación del responsable del control en autoridad y responsabilidades definidas. 7. Segregación de funciones en el control. 8. Conservación de evidencias del control en repositorio designado (servidor, nube, registros).	
Pruebas a realizar sobre Validación de Operatividad (0% al 100%) Seleccione una muestra aleatoria acorde a la frecuencia de ejecución teniendo en cuenta un nivel de confianza del 95% y margen de error del 5%, la tasa esperada de error es del 1% de la muestra evaluada de 1) Evidencias que se encuentran conservadas en el lugar destinado para tal fin. 2) Desviaciones que son gestionadas. 3) Ejecución frente a lo definido en el proceso. 4) Casos de la muestra que coinciden con otras fuentes información oficiales (Ej. Monitoreo diario de accesos Vs Bases de Datos de Accesos, Historial de Mantenimiento de Equipos físicos Vs Estado actual de los Equipos)	
Indicadores: Para cada punto en la validación del diseño se establece una calificación de SI / NO. Se otorgará un porcentaje de cumplimiento sobre el total de pruebas evaluadas para cada lineamiento así:1) % SI Alto Superior al 80% 2) % SI Medio - entre el 80% y 60% 3) % SI Bajo - menor al 60%.Para las pruebas de operatividad se sacará un promedio porcentual de cumplimiento el cual debe ser superior al 99%.	

Fuente. Elaboración propia.

La plantilla descrita es un modelo que puede variar según el tipo de control y empresa. Se sugiere ajustarla de manera general de acuerdo con los controles de seguridad de la tabla 14:

Tabla 14. *Controles Sugeridos a Evaluar en un SGSI*

Tipo	Descripción
Identidad y Accesos	**Autenticación multifactor:** Controles de autenticación multifactor para verificación de identidad de usuarios.
	Control contraseñas: Controles gestión segura de contraseñas: complejidad, caducidad y prohibición de reutilización
	Monitoreo acceso: Controles de monitoreo, registro de actividad de acceso, inicio de sesión, intentos no autorizados.
	Capacitación y concientización: Realizar capacitación y concientización sobre seguridad de la información.
Criptografía	**Almacenamiento seguro de claves:** Controles almacenamiento seguro de claves criptográficas con HSM, KMS, etc.
	Certificados digitales: Gestión segura los certificados digitales, incluyendo emisión, renovación y revocación.
	Uso de cifrado fuerte: Controles sobre algoritmos de cifrado AES y RSA para proteger la confidencialidad de la información en reposo, en tránsito y en procesamiento.

Tipo	Descripción
	Auditoría y cumplimiento: Auditorías para supervisar la implementación y uso de la criptografía, así como para verificar el cumplimiento de políticas y regulaciones.
Física	**Acceso físico controlado**: Implementar controles de acceso físico, como cerraduras electrónicas, tarjetas de acceso y sistemas de biometría, para evitar accesos no autorizados a instalaciones.
	Vigilancia y monitoreo: Control cámaras de seguridad y Sist. de monitoreo áreas críticas, detectar actividad sospechosa.
	Protección contra incendios Controles para garantizar funcionamiento de los Sist. de detección - extinción de incendios.
	Respaldo de energía: Control sobre sistemas de alimentación ininterrumpida (UPS) y generadores de respaldo para mantener la energía eléctrica y evitar interrupciones en las operaciones del SGSI.
	Respaldo y almacenamiento seguro: Controles sobre copias de respaldo regulares y almacenar los datos de manera segura en ubicaciones protegidas, como gabinetes ignífugos o salas de servidores con acceso restringido.
Aplicaciones	**Autenticación y autorización:** Control de autenticación robusta, permisos adecuados y gestión de usuarios para acceder a funcionalidades y datos relevantes.
	Gestión de vulnerabilidades: Evaluaciones regulares de vulnerabilidades, aplicar parches de seguridad y mantener sistemas y frameworks actualizados.
	Monitoreo y registro de actividades: Registrar y monitorear las actividades en las aplicaciones para detectar y responder rápidamente a eventos sospechosos o no autorizados.
	Protección de datos sensibles: Control de cifrado y enmascaramiento de datos en las aplicaciones para proteger la confidencialidad de la información sensible.
	Control de cambios: Establecer procesos y controles para gestionar cambios en las aplicaciones, incluyendo pruebas rigurosas y documentación adecuada.
	Seguridad en el desarrollo de aplicaciones: Implementar procesos y controles para garantizar la seguridad durante el desarrollo de aplicaciones, incluyendo pruebas y documentación adecuada.
Comunicaciones	**Cifrado de datos:** Controles cifrado (HTTPS, VPN, cifrado correo electrónico) protección confidencialidad comunicaciones.
	Autenticación y autorización de usuarios: Contraseñas robustas, autenticación de dos factores, gestión de usuarios y monitoreo de acceso para seguridad de sistemas.
	Protección ataques de red: Firewall, IDS/IPS y filtros de contenido detección y bloqueo ataques en comunicaciones.
	Control calidad de servicio: Priorización y asignación de ancho de banda para rendimiento óptimo y respuesta rápida en comunicaciones.
	Respaldo y recuperación de comunicaciones: Duplicación de enlaces, conmutación por error y respaldo de configuraciones para continuidad en caso de fallas.
	Auditoría y registro de comunicaciones: Sistemas de registro y auditoría para monitoreo, detección de anomalías y apoyo forense en seguridad.

Fuente. Elaboración propia NTC-ISO/IEC 27001 (ICONTEC, 2013)

Evaluación al Proceso de Implementación del SGSI

Prueba sobre definición de políticas, alcance y diseño del SGSI. La tabla 15 contiene las pruebas sugeridas para evaluar las políticas de seguridad, alcance y diseño del SGSI.

Tabla 15. *Papel de Trabajo para Evaluación Políticas de Seguridad de la Información*

Nombre de la empresa, Identificación. No. De Referencia PT, Tipo de PT, Fecha, Auditor Responsable.	
Objetivos: Objetivo de la evaluación de políticas del Sistema de Gestión de Seguridad de la Información (SGSI) es asegurar que las políticas establecidas cumplan con los requisitos de seguridad, sean efectivas y estén alineadas con los objetivos y las necesidades de la organización	
Alcance: Definición Políticas, alcance y límites del SGSI.	**Tipo de propiedad de la información:** Confiabilidad
Técnicas: Revisión documental (incluye políticas internas, procesos y normas asociadas a la actividad de la compañía.), entrevistas, consultas en los repositorios de información. Revisión documental. Consultas en los repositorios de información.	
Herramientas: 1) Entrevistas presenciales o mediante plataformas colaborativas (Teams, Meet) con los responsables del diseño y administración SGSI. 2) Acceso a la Intranet de la compañía, para identificar si se encuentra documentado el proceso de diseño del SGSI. 3) Acceso a servicios de mensajería Outlook u otros para consulta de correspondencia asociada al diseño e implementación del SGSI, como comunicaciones, agendamiento, resultados o actas. 4) Acceso a la Intranet de la compañía, para establecer si se encuentra documentado los procedimientos, políticas, manuales para cada aspecto evaluado del SGSI.	
Pruebas a realizar sobre Diseño del SGSI (Cumple ____ No Cumple ____)	

Nombre de la empresa, Identificación. No. De Referencia PT, Tipo de PT, Fecha, Auditor Responsable.
1. Verificar identificación de partes interesadas en diseño del SGSI. 2. Establecer análisis necesidades, expectativas partes interesadas, metodología priorización (ej. Análisis DOFA, y riesgos). 3. Identificar grado de influencia y poder en relación al SGSI y metodología utilizada (ej. análisis de stakeholders). 4. Evaluar estrategia de comunicación y participación en la implementación del SGSI (ej. publicaciones internas, reuniones)
Pruebas a realizar sobre Definiciones del SGSI en las políticas (Cumple ____ No Cumple ____) 1. Identificar declaración de alcances y limitaciones del SGSI. 2. Verificar modelo de gobierno y comunicación en documentos obtenidos. 3. Identificar norma base y su inclusión en declaraciones, políticas, manuales o procedimientos. 4. Identificar dominios aplicables al SGSI (ejemplo: ciberseguridad, gestión de riesgos, seguridad física, etc.). 5. Verificar disponibilidad de información para partes interesadas en intranet u otros medios de comunicación.
Pruebas a realizar sobre Definiciones del SGSI en las políticas (Cumple ____ No Cumple ____) 1. Verificar consistencia de objetivos de seguridad de la información con los de la organización, protegiendo activos relevantes y alineados con riesgos pertinentes. 2. Verificar actualización periódica de la política, con evidencia de versionamiento y responsables de actualización. 3. Verificar existencia de políticas asociadas a gestión de activos de información, servicios en la nube, sistemas de información, telecomunicaciones, infraestructura física, continuidad y gestión de incidentes de seguridad.
Indicadores: Para cada punto de los tres lineamientos se aplicará una calificación de CUMPLE/NO CUMPLE. Se otorgará un porcentaje de cumplimiento sobre el total de pruebas evaluadas para cada lineamiento así: 1) % de cumplimiento Alto Superior al 80%. 2) % de cumplimiento Medio entre el 80%- 60%. 3) % de cumplimiento Bajo menor al 60%

Fuente. Elaboración propia

Evaluación Responsabilidad y Compromiso de la Dirección

En la tabla 16 se observa el papel de trabajo sugerido para evaluar el compromiso de la dirección sobre la política, roles, responsabilidades y recursos necesarios para SGSI eficaz.

Tabla 16. *Papel de trabajo Evaluar Responsabilidad y compromiso de la dirección*

Nombre de la empresa, Identificación. No. De Referencia PT, Tipo de PT, Fecha, Auditor Responsable.	
Objetivos: Evaluar el compromiso y liderazgo de la gerencia en el SGSI para garantizar la dirección estratégica, la asignación de recursos adecuados y la promoción de una cultura de seguridad en toda la organización.	
Alcance: Evaluación de las políticas y directrices establecidas, la asignación de responsabilidades y recursos, la comunicación efectiva de la importancia de la seguridad de la información,	**Tipo de propiedad de la información:** Confiabilidad
Técnicas: - Revisión documental (incluye políticas internas, procesos y normas asociadas a la actividad de la compañía.), entrevistas, consultas en los repositorios de información. - Revisión documental. Consultas en los repositorios de información.	
Herramientas: 1. Entrevistas con responsables del diseño y administración del SGSI (presenciales o virtuales). **2.** Acceso a la Intranet para verificar documentación del proceso de diseño del SGSI. **3.** Consulta de correspondencia en servicios de mensajería para información relacionada al SGSI. **4.** Acceso a la Intranet para revisar procedimientos, políticas del SGSI.	
Pruebas a realizar sobre Liderazgo y Compromiso (Cumple __ No Cumple __) 1. Identificar sin en las políticas, manuales o procedimientos, se encuentra definida la declaración de compromiso de la Alta Dirección con el SGSI. 2. ¿Los niveles que aprueban dicha declaración están dentro de los niveles jerárquicos de la Alta Administración? **Verifique que mecanismo se establece para confirmar el compromiso y liderazgo de la Alta Dirección.** 1. ¿Está definido un comité para el SGSI? 2. ¿El comité se reúne regularmente acorde a lo definido en las políticas de SGSI? 3. ¿Se comunica me manera clara y oportuna el estado actual, brechas y cambios del SGSI, a todos los actores interesados?	
Pruebas a realizar sobre Gestión de Recursos (Cumple __ No Cumple __) 1. ¿Modelos o metodologías para cuantificar recursos económicos y humanos del SGSI? 2. ¿Asignación de recursos económicos al SGSI valorada por área financiera y contable? 3. ¿Coherencia de recursos asignados con apetito de riesgo y riesgos inherentes? 4. ¿Monitoreo frecuente de eficiencia y coherencia de recursos del SGSI? 5. ¿Destinación de recursos para cubrir fallas asociadas al SGSI?	
Indicadores: Para cada punto en la validación del diseño se establece una calificación de Cumple / No cumple. Se otorgará un porcentaje de cumplimiento sobre el total de pruebas evaluadas para cada lineamiento así: 1) % Cumplimiento Alto Superior al 80% 2) % Cumplimiento Medio - entre el 80% y 60% 3)% Cumplimiento Bajo - menor al 60%	

Fuente. Elaboración propia

Evaluación del Desempeño y Mejora del SGSI

El auditor identifica las métricas de desempeño del SGSI, considerando modelos de madurez como COBIT, para evaluar su efectividad. Adicionalmente tiene en cuenta auditorías previas descritas en la tabla 17.

Tabla 17. *Aspectos de Auditorías Previas*

Revisar informes anteriores: Analizar los informes de auditorías previas del SGSI para comprender las deficiencias y hallazgos identificados, así como las acciones correctivas y preventivas implementadas.
Evaluar el seguimiento: Verificar si se ha realizado un seguimiento adecuado de las recomendaciones y acciones derivadas de las auditorías previas, y evaluar la efectividad de las medidas tomadas.
Identificar áreas de mejora: Identificar áreas en las que se han observado problemas recurrentes o deficiencias persistentes, para enfocar la auditoría actual en dichas áreas y asegurar que se hayan abordado adecuadamente
Evaluar la evolución del SGSI: Comparar la situación actual del SGSI con los resultados y hallazgos de las auditorías previas para evaluar la evolución y mejora del sistema, así como la implementación de medidas correctivas.
Realizar pruebas de seguimiento: Realizar pruebas de seguimiento para verificar si las recomendaciones y acciones tomadas en auditorías previas han sido efectivas y se han mantenido en el tiempo.

Fuente. Elaboración propia. ISO 27007 (ICONTEC, 2013)

Comunicación

Proceso de Comunicación de la Auditoría

En la fase de comunicación descrita en la tabla 18, se elabora un informe detallado de la auditoría y seguimiento para garantizar la implementación de acciones para la mejora del SGSI.

Tabla 18. *Proceso de Comunicación de la Auditoría*

Realizar pruebas de seguimiento: Realizar pruebas de seguimiento para verificar si las recomendaciones y acciones tomadas en auditorías previas han sido efectivas.	**Revisión y Aprobación:** Revisión y validación del informe por parte de los responsables de la auditoría y de la dirección.
Recopilación de Datos: Obtención de información relevante y precisa sobre los hallazgos de la auditoría.	**Distribución** Entrega del informe a los destinatarios pertinentes y comunicación efectiva de los resultados de la auditoría.
Análisis y Evaluación Interpretación de los datos recopilados, evaluación de los resultados y conclusiones	**Seguimiento:** Monitoreo de las acciones tomadas en respuesta al informe de auditoría y seguimiento de su implementación.
Elaboración del Informe: Presentación clara y estructurada de los hallazgos, conclusiones y recomendaciones de la auditoría.	

Fuente. Elaboración propia. ISO 19011 (ISO, 2018)

Informe de Auditoría

El informe de auditoría se utiliza para comunicar de manera clara y precisa los hallazgos, conclusiones y recomendaciones obtenidos durante la auditoría, para lo cual se sugiere seguir el modelo relacionado en la tabla 19:

Tabla 19. *Papel de trabajo Informe de Auditoría*

Nombre de la empresa, Código del Trabajo. Nombre de la Evaluación, Fecha de Elaboración
Objetivos: Ej. Evaluar la implementación del SGSI acorde con los requisitos establecidos estándares, como ISO 27001
Alcance: Ej. La auditoría del SGSI cubrirá: políticas y procedimientos, evaluación de riesgos, controles de seguridad técnica y física, gestión de incidentes y cambios en TI, y gestión de accesos y privilegios.
Hallazgos Relevantes: Se sugiere relacionar de manera resumida los hallazgos principales con el fin de dar un contexto rápido de los resultados obtenidos en la Evaluación. Ej. 50% de cumplimiento en la efectividad de controles de Identidad y Accesos.
Conclusión: En este punto se redacta el resultado general de la auditoría. Ej. El resultado de la evaluación es **Insatisfactorio** en lo relacionado con los controles de Identidad y Accesos.
Resultados: En este capítulo se redactan los resultados de manera detallada obtenidos de la evaluación con la siguiente estructura: **Criterio**: La organización debe garantizar la correcta ejecución de controles asociados a la identidad y accesos de todos los funcionarios. **Hallazgo**: Se identifico no existen controles de autenticación multifactor. **Causa**: Fallas en el desarrollo de seguridad de autenticación. **Efecto**: Acceso no autorizado a equipos y aplicativos, por fallas en la autenticación ocasionando perdida de información.

Fuente. Elaboración propia

Conclusiones

La auditoría de sistemas a un Sistema de Gestión de Seguridad de la Información (SGSI) implementado bajo la norma ISO 27001:2013 permite evaluar la eficacia del SGSI en la protección de la información, identifica posibles vulnerabilidades del sistema, deficiencias en los controles existentes, verifica el cumplimiento de los requisitos legales, identifica posibles ineficiencias o redundancias en los procesos y comunica a la administración los hallazgos relevantes para que esta tome realice las mejoras al SGSI.

La guía propuesta puede ser empleada de manera complementaria a la norma ISO 27007:2020, al proporcionar modelos de papeles de trabajo, que facilitan la evaluación de los controles del SGSI, el compromiso y responsabilidad de la dirección, el cumplimiento de políticas de seguridad de la información y la elaboración de informes.

Además, la guía propuesta establece el ciclo a seguir en la evaluación y la estructura general de los elementos a considerar en la auditoría, como matrices de riesgo, diseños de control y características de los activos de información. Así mismo, brinda algunos indicadores de

cumplimiento y ejemplos para ayudar al auditor a comprender mejor los escenarios que puede enfrentar durante la evaluación del SGSI.

Referencias

Areitio, J. (2008). Seguridad de la Información. Madrid: Paraninfo.

Colobran Huguet, M., Arques Soldevila, J. M., & Galindo, E. M. (2008). Administración de Sistemas Operativos. Barcelona: UOC.

CSAE. (2012). MAGERIT – versión 3.0 - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Ministerio de Hacienda y Administraciones Públicas.

ICONTEC. (2005). Norma Técnica Colombiana NTC-ISO/IEC 27001. Recuperado de https://img1.wsimg.com/blobby/go/b653c9ee-535c-4528-a9c5-bb00166ad0dc/downloads/1cd65ml0r_919353.pdf

ICONTEC. (2013). Norma Técnica Colombiana NTC-ISO/IEC 27001. Recuperado de ICONTEC: https://ebooks.icontec.org/product/seguridad-de-la-informacin-ciberseguridad-y-proteccin-privacidad-sistemas-gestin-requisitos

ISACA. (2012). COBIT 5 - para Seguridad de la Información. ISACA.

ISO. (2018). Norma Internacional - ISO 31000: 2018. Recuperado de http://simudatsalud-risaralda.co/normatividad_inv9/normas_tecnicas/NTC-ISO31000_Gestion_del_riesgo.pdf

ISO. (2018). Norma - ISO 19011 - Directrices para la auditoría de los sistemas de gestión. Recuperado de https://www.cecep.edu.co/documentos/calidad/norma-iso-19011-2018.pdf

ISO. (2020). ISO/IEC 27007 - Tecnología de la información. Técnicas de seguridad. Directrices para la auditoría de los sistemas de gestión de la seguridad de la información.

https://cdn.standards.iteh.ai/samples/77802/5bb0caa59ce4411aa0508cf83f9a62d9/ISO-IEC-27007-2020.pdf

Muñoz Razo, C. (2002). Auditoría en Sistemas Computacionales. México: Prentice Hall.