Commented [AES1]: Para saber cómo completar este documento, y ver ejemplos reales de lo que necesita escribir, vea este tutorial en vídeo: "How to Write ISO 27001/ISO 22301 Internal Audit Procedure and Audit Program".

Para acceder al tutorial: en su bandeja de entrada, busque el correo electrónico que recibió en el momento de la compra. Allí, verá un enlace y una contraseña que le permitirán acceder al tutorial en vídeo.

[logo de la organización]

Commented [AES2]: Se deben completar todos los campos de este documento que estén marcados con corchetes [ ].

[nombre de la organización]

PROCEDIMIENTO PARA AUDITORÍA INTERNA

Commented [AES3]: Para conocer más sobre este tema, lea estos artículos:

- Dilemmas with ISO 27001 internal auditors https://advisera.com/27001academy/blog/2010/03/22/dilemmas-with-iso-27001-bs-25999-2-internal-auditors/
- How to prepare for an ISO 27001 internal audit https://advisera.com/27001academy/blog/2016/07/11/how-to-prepare-for-an-iso-27001-internal-audit/

Considere realizar esta formación gratuita en línea:
ISO 27001 Internal Auditor Course
https://training.advisera.com/course/iso-27001-internal-auditor-course/

Además, eche un vistazo a este libro:
Auditoría interna ISO: Una guía en un lenguaje sencillo
https://advisera.com/books/auditoria-interna-iso-una-guia-en-un-lenguaje-sencillo/

Código:	
Versión:	
Fecha de la versión:	
Creado por:	
Aprobado por:	
Nivel de confidencialidad:	

Commented [AES4]: Si necesita ayuda para realizar la auditoría interna de ISO 27001 y/o ISO 22301 en su organización, consulte este ISO Consultant Directory para encontrar al experto adecuado.

Commented [AES5]: El sistema de codificación del documento debe coincidir con el sistema actual de codificación de documentos de la organización. En el caso que no exista ese sistema, se puede eliminar esta línea.

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
	0.1	Advisera	Descripción básica del documento

Tabla de contenido

1. OBJETIVO, ALCANCE Y USUARIOS 3
2. DOCUMENTOS DE REFERENCIA 3
3. AUDITORÍA INTERNA 3
   - 3.1. OBJETIVO DE LA AUDITORÍA INTERNA 3
   - 3.2. PLANIFICACIÓN DE LA AUDITORÍA INTERNA 3
   - 3.3. DESIGNACIÓN DE AUDITORES INTERNOS 4
   - 3.4. REALIZACIÓN DE AUDITORÍAS INTERNAS INDIVIDUALES 4
4. GESTIÓN DE REGISTROS GUARDADOS EN BASE A ESTE DOCUMENTO 5
5. VALIDEZ Y GESTIÓN DE DOCUMENTOS 5
6. APÉNDICES 6

1. Objetivo, alcance y usuarios

El objetivo de este Procedimiento es describir todas las actividades relacionadas con la auditoría: redacción del programa de auditoría, selección del auditor, realización de auditorías individuales e informes.

Este procedimiento se aplica a todas las actividades realizadas dentro del Sistema de Gestión de Seguridad de la Información (SGSI) [Sistema de Gestión de Continuidad de Negocio (SGCN)].

Los usuarios de este documento son [miembros de la alta dirección] de [nombre de la organización] y los auditores internos.

Commented [AES6]: Se debe insertar esta leyenda en lugar de SGSI en caso que el procedimiento se refiera exclusivamente a la gestión de continuidad de negocio.

Commented [AES7]: El organismo directivo supremo dentro del alcance del SGSI/SGCN.

Commented [AES8]: Incluya el nombre de su organización.

2. Documentos de referencia

- Norma ISO/IEC 27001, cláusulas 9.2, A.5.30, A.5.35 y A.8.34
- Norma ISO 22301, cláusula 9.2
- Política de seguridad de la información
- Política de continuidad de negocio
- Procedimiento para la acción correctiva

Commented [AES9]: Borrar este ítem si el Procedimiento se refiere sólo a gestión de continuidad de negocio.

Commented [AES10]: Borrar este ítem si el Procedimiento se refiere sólo a la seguridad de la información.

Commented [AES11]: Borrar este ítem si el Procedimiento se refiere sólo a gestión de continuidad de negocio.

Commented [AES12]: Puede encontrar una plantilla para este documento en la carpeta del Paquete Premium de documentos sobre ISO 27001 e ISO 22301 "05_Politicas_generales".

Commented [AES13]: Puede encontrar una plantilla para este documento en la carpeta del Paquete Premium de documentos sobre ISO 27001 e ISO 22301 "10_Documentos_basicos_de_continuidad_del_negocio_ISO_22301".

Commented [AES14]: Puede encontrar una plantilla para este documento en la carpeta del Paquete Premium de documentos sobre ISO 27001 e ISO 22301 "14_Acciones_correctivas".

3. Auditoría interna

3.1. Objetivo de la auditoría interna

El objetivo de la auditoría interna es determinar si los procedimientos, controles, procesos, acuerdos y demás actividades dentro del SGSI [SGCN] concuerdan con las normas ISO 27001 e ISO 22301, con las regulaciones correspondientes y con la documentación interna de la organización; como también verificar si son implementados y sostenidos y si cumplen requisitos de políticas y establecen objetivos.

La auditoría interna también es útil para la evaluación periódica de las capacidades de continuidad del negocio de las cosas o procedimientos más críticos.

Commented [AES15]: Borrar este ítem si el Procedimiento se

Commented [AES16]: Borrar si el Procedimiento se refiere sólo

Commented [AES17]: Borrar si no implementa continuidad de negocio.

Commented [AES18]: Elimine este párrafo si el auditor interno

3.2. Planificación de la auditoría interna

El [cargo] aprueba un programa anual de auditorías internas, redactado como se detalla en el formulario del Apéndice 1 Programa anual de auditoría interna.

Commented [AES19]: Ej.: gerente de continuidad del negocio,

Se deben realizar una o más auditorías internas en el transcurso de un año, asegurando una cobertura acumulativa de todo el alcance del SGSI [SGCN]. Las auditorías internas son planificadas en base a la evaluación de riesgos, como también por los resultados de auditorías anteriores. Generalmente son realizadas antes de la revisión por parte de la dirección.

El Programa anual de auditoría interna debe incluir la siguiente información sobre cada auditoría interna individual:

- Momento de la auditoría (especificando fechas o el mes en el que está planificada la auditoría).
- Alcance de la auditoría (departamentos, procesos, puntos de la norma, etc.).
- [illegible]
- [illegible]
- [illegible]

Los auditores internos designados deben registrar el registro de las auditorías realizadas en el Programa anual de auditoría interna.

3.3. Designación de auditores internos

El [cargo] debe designar a los auditores internos.

Un auditor interno puede ser alguien de la organización o una persona externa a la misma. Los criterios para la designación de los auditores son:

- Que conozca las normas ISO/IEC 27001 e ISO 22301.
- [illegible]
- [illegible]

[illegible]

Se recomienda que los auditores internos realicen un curso para auditores internos según la norma ISO/IEC 27001.

3.4. Realización de auditorías internas individuales

Las personas responsables de las auditorías internas individuales están identificadas en el Programa anual de auditoría interna. Si una auditoría es realizada por un equipo de varios auditores, la persona responsable de la auditoría es aquella que está indicada como Líder de equipo de auditoría.

Durante la realización de una auditoría interna se deben tener en cuenta los siguientes puntos:

- El criterio establecido en el Programa anual de auditoría interna.
- [illegible]
- [illegible]
- [illegible]

Commented [AES20]: Estos son todos obligatorios; no elimine [illegible]

Commented [AES21]: Por ejemplo: gerente de continuidad de [illegible]

Commented [AES22]: Borrar si el Procedimiento se refiere sólo [illegible]

Commented [AES23]: Borrar si no implementa continuidad de negocio.

Commented [AES24]: Por ejemplo: gerente de continuidad de [illegible]

Commented [AES25]: O ISO 22301.

Commented [AES26]: Para obtener consejos sobre cómo realizar auditorías efectivas, lea este artículo:

[illegible]

Se deben documentar los siguientes elementos como resultado de la auditoría interna:

- Informa de auditoría interna, debe ser enviado al [cargo]
- Las posibles acciones correctivas deben ser documentadas en el Formulario de acción correctiva, de acuerdo a lo establecido en el Procedimiento para la acción correctiva.

Commented [AES27]: Por ejemplo: gerente de continuidad de negocio, gerente de seguridad de la información, oficial de cumplimiento, responsable de la unidad de negocio, etc.

Commented [AES28]: Puede encontrar una plantilla para este documento en la sección de Plantilla Premium de documentos sobre ISO 27001 en línea. Es gratuita, completa

4. Gestión de registros guardados en base a este documento

Nombre del registro	Ubicación de archivo	Persona responsable del archivo	Controles para la protección del registro	Tiempo de retención
Programa anual de auditoría interna (en formato electrónico)	Ordenador del [cargo]	[cargo]	Solamente el [cargo] y el auditor interno pueden ingresar datos y modificaciones al Programa anual de auditoría interna.	Los programas son almacenados por el plazo de 3 años.
Informe de auditoría interna (en formato electrónico)	Ordenadores del auditor interno y del [cargo]	Auditor interno	Los informes son almacenados en versiones de solo lectura.	Los informes son guardados por un período de 3 años.
Lista de verificación de auditoría interna (completada durante la auditoría interna)	Ordenador del auditor interno	Auditor interno	La lista de verificación se guarda como solo lectura.	La lista de verificación es almacenada por el plazo de 3 años.

Commented [AES29]: Adapte el período en esta columna a sus necesidades específicas.

Commented [AES30]: Generalmente, es la persona que aprobó el programa anual.

Commented [AES31]: Generalmente, en formato PDF.

Commented [AES32]: Generalmente, en formato PDF.

Solamente el [cargo] puede otorgar a otros empleados el derecho de acceso al Programa anual de auditoría interna, al Informe de auditoría interna y a la Lista de verificación de auditoría interna.

5. Validez y gestión de documentos

Este documento es válido hasta el [fecha].

El propietario de este documento es el [cargo], que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

Commented [AES33]: Por ejemplo: gerente de continuidad de negocio, gerente de seguridad de la información, oficial de cumplimiento, etc.

Commented [AES34]: Esto es sólo una recomendación; ajustar a la realidad de su empresa.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Cantidad de acciones correctivas identificadas durante la auditoría.

- Cantidad de acciones correctivas identificadas durante la auditoría de certificación realizada luego de la auditoría interna.
- [illegible]

6. Apéndices

- Apéndice 1 – Programa anual de auditoría interna
- [illegible]
- [illegible]

[cargo]
[nombre]

[firma]

Commented [AES35]: Sólo es necesario si el Procedimiento para el control de documentos y registros establece que los documentos en papel deben ser firmados.