Universidad Cenfotec

Maestría en Ciberseguridad

Documento final de Proyecto de Investigación Aplicada 2

Propuesta de una guía de auditoría para el sistema de gestión de la seguridad de la información alineada a estándares y mejores prácticas internacionales

Ureña Agüero Yesenia

Agosto, 2020

Declaratoria de derechos de autor

Yo, Yesenia Ureña Agüero, con cédula de identidad 303690687, autorizo la consulta y uso con fines académicos del documento: “Propuesta de una guía de auditoría para el sistema de gestión de la seguridad de la información alineada a estándares y mejores prácticas internacionales”.

_____

Ureña Agüero Yesenia

Cédula 303690687

Dedicatoria

Dedico este proyecto a mis padres, Rafael Ángel Ureña Rojas y María Isabel Agüero Amado, por su ejemplo de trabajo y fortaleza.

A mi esposo, Alexander Araya Mora y a mi hijo Diego Araya Ureña, por su apoyo incondicional en cada decisión y proyecto que he emprendido.

Agradecimientos

Gracias a Dios, por la oportunidad de estudiar y crecer profesionalmente; además, un agradecimiento especial a todas las personas que contribuyeron a este proceso formativo, entre ellos mis profesores, compañeros y todo el personal administrativo de la Universidad Cenfotec por su atención y buen servicio.

TRIBUNAL EXAMINADOR

Este proyecto fue aprobado por el Tribunal Examinador de la carrera: **Maestría en Ciberseguridad,** requisito para optar por el título de grado de **Maestría,** para el estudiante: **Yesenia de los Ángeles Ureña Agüero.**

MIGUEL PEREZ MONTERO (FIRMA)
Digitally signed by MIGUEL PEREZ MONTERO (FIRMA)
Date: 2020.08.26 09:20:24 -06'00'

M. Sc. Miguel Pérez Montero
Tutor

ARNOLDO LE ROY CORDOBA (FIRMA)
Firmado digitalmente por ARNOLDO LE ROY CORDOBA (FIRMA)
Fecha: 2020.08.26 09:55:50 -06'00'

MBA. Arnoldo Le Roy Córdoba
Lector 1

IGNACIO TREJOS ZELAYA (FIRMA)
Digitally signed by IGNACIO TREJOS ZELAYA (FIRMA)
Date: 2020.08.27 15:30:53 -06'00'

M. Sc. Ignacio Trejos Zelaya
Lector 2

San José, Costa Rica, 25 de agosto de 2020

Tabla de contenido

Índice de figuras

Índice de tablas

Resumen

Actualmente, las organizaciones experimentan una creciente dependencia de las tecnologías de información para el logro de sus objetivos y la mejora de sus procesos. Por este motivo, requieren adherirse a buenas prácticas, estándares, normas y cumplimientos legales o regulatorios, a su vez, deben someterse a procesos de evaluación o auditorías que señalen el nivel de cumplimiento de estos. Así también, la seguridad de la información es una preocupación real en el modelo de negocios de la actualidad, especialmente cuando los ciberataques y las brechas de seguridad son noticia diaria.

Por tanto, es de interés proponer una guía de auditoría para el sistema de gestión de la seguridad de la información, mediante un modelo práctico de hojas de cálculo, el cual sea adaptable a diferentes entornos organizacionales, alineado a estándares y buenas prácticas internacionales.

Se espera que este instrumento operativo favorezca la realización de auditorías parciales o exhaustivas, reduzca el tiempo de las fases de la auditoría y mejore el nivel de aseguramiento de la organización, de forma tal que genere valor y resultados positivos.

Palabras clave: guía de auditoría, seguridad de la información, evaluación, estándares internacionales, cumplimiento, sistema de gestión de la seguridad de la información.

Capítulo 1. Introducción

El presente trabajo final de graduación está centrado en la auditoría al sistema de gestión de la seguridad de la información, mediante el desarrollo de una guía de auditoría, alineada con estándares y buenas prácticas internacionales; los detalles se abordan en las secciones descritas a continuación.

1.1 Generalidades

Esta guía de auditoría pretende ser adaptable, es decir, que puede ser aplicada por el profesional a diversos tipos y tamaños de organizaciones que realizan revisiones de seguridad de la información y verificaciones de cumplimiento, tanto en empresas privadas como públicas, por lo tanto, no se exponen los resultados de la ejecución de esta en una empresa en particular.

1.2 Antecedentes del problema

Cada vez más, las organizaciones deciden incrementar los recursos destinados a proteger sus activos de información, por este motivo, necesitan validar que los controles implementados sean suficientes y minimicen las posibilidades de incidentes, entonces, surgen los profesionales de auditoría en seguridad de la información. Sin embargo, este tipo de auditorías no suelen ser sencillas de llevar a cabo, requiere las habilidades y conocimientos en seguridad de la información, por lo tanto, deben ser cuidadosos, estar actualizados, así como aplicar estándares y normas reconocidas internacionalmente para que la auditoría señale los incumplimientos y se puedan emitir las recomendaciones que generen valor a la organización.

En vista de estas circunstancias, las organizaciones pueden contar con un departamento de auditoría interna o contratar los servicios externamente, puesto que este proceso de revisión debe ser continuo, por ello, si el profesional, ya sea interno o externo, tiene a mano una herramienta para agilizar esta actividad, se espera que los resultados se presenten con más prontitud.

1.3 Definición y descripción del problema

Es responsabilidad de las organizaciones mantener la seguridad de la información dentro de su apetito de riesgo, así como garantizar que los controles se cumplan de acuerdo con las políticas y normativas adoptadas, no obstante, para

garantizar que los planes sean eficientes y efectivos, deben someterse a procesos de revisión o auditorías programadas que señalen las faltas observadas, así como su nivel de cumplimiento.

Tomando en cuenta estas condiciones, surge la necesidad de profesionales en auditoría con conocimientos en la seguridad de la información, así como la necesidad de herramientas que faciliten las fases de la auditoría, especialmente en el momento de la planeación y ejecución. Por lo tanto, se propone una guía de auditoría para el sistema de gestión de la seguridad de la información, de forma tal, que el profesional que ejecuta los procedimientos tenga una base para sustentar su revisión, es decir, no inicie desde cero el planteamiento del estudio, la revisión preliminar y la creación de listas de verificación, por consiguiente, pueda hacer un uso más eficiente del tiempo, los recursos económicos y alineándose a estándares internacionales.

1.4 Justificación

El interés en una guía de auditoría para el sistema de gestión de la seguridad de la información radica en crear un instrumento para operacionalizar y apoyar la aplicación de auditorías a dicho sistema. Con ello, los profesionales en tecnologías de la información, que apliquen la evaluación de cumplimiento a los controles de la seguridad, tendrán una base en apego a normas, estándares y buenas prácticas internacionales, reduciendo el tiempo de las fases de auditoría, así como asegurando pruebas de cumplimento robustas, además de la presentación de resultados de forma clara y oportuna. Por lo tanto, las organizaciones o entidades evaluadas podrán identificar su nivel de cumplimiento de la seguridad de la información y, por consiguiente, tomar acciones para corregir las faltas observadas.

1.5 Viabilidad

Este trabajo se ha llevado a término, debido a los conocimientos obtenidos a través de la Maestría en Ciberseguridad, además, se han investigado las normas y estándares internacionales que existen para los sistemas de gestión de la seguridad de la información.

1.5.1 Punto de vista técnico

Este trabajo ha sido factible puesto que se dispone de los recursos tecnológicos tales como computadora, conexión a Internet, así como los conocimientos básicos en auditoría de la seguridad de la información y los soportes documentales de estándares y mejores prácticas internacionales.

1.5.2 Punto de vista operativo

La realización de este trabajo final de graduación no alteró el funcionamiento normal de ninguna organización en particular**.**

1.5.3 Punto de vista económico

El costo económico de la realización de este trabajo final de graduación fue asumido por la investigadora, incluyó las horas consultor necesarias en la realización del mismo**.** Para el cálculo del costo total, se tomó como base el monto de ₡680,565 por jornada completa de un profesional con Licenciatura universitaria de la lista de salarios mínimos para el sector privado publicados para el 2020 por el Ministerio de Trabajo y Seguridad Social de Costa Rica. La investigadora dedicó medio tiempo de lunes a viernes por 8 meses. La tabla 1 muestra el detalle de costos estimados.

Tabla 1. Costo total horas consultor

Detalle	Costo hora	Horas totales	Costo total
Consultor	4,253.53	640	2,722,260

Origen: elaboración propia

1.6 Objetivos

Para plantear los objetivos de este trabajo final de graduación se ha seleccionado la Taxonomía Revisada de Bloom, debido a su ordenamiento y su estructura ampliamente utilizada.

1.6.1 Objetivo general

Proponer una guía de auditoría para el sistema de gestión de la seguridad de la información alineada a estándares y mejores prácticas internacionales.

1.6.2 Objetivos específicos

- Identificar los estándares y mejores prácticas internacionales que sirven de marco de implementación y operación para el sistema de gestión de la seguridad de la información.
- Comprender el proceso de auditoría para brindar una seguridad razonable de la eficacia y eficiencia del sistema de gestión de la seguridad de la información.
- Comparar los diferentes estándares y mejores prácticas internacionales, para decidir cuáles elementos son aplicables al proceso de auditoría del sistema de gestión de la seguridad de la información.
- Desarrollar la guía de auditoría mediante un modelo práctico de hojas de cálculo adaptable a un amplio espectro de organizaciones.
- Clasificar la guía de auditoría por objetivos de control y controles.

1.7 Alcances y limitaciones

Se espera que esta propuesta sea de interés para auditores o profesionales en tecnologías de la información que presten servicios de auditoría interna o externa a organizaciones; las cuales tengan implementado un sistema de gestión para la seguridad de la información, por tanto, les ayudará a revisar el cumplimiento de los controles y señalar las deficiencias resultantes.

1.7.1 Alcances

Los productos entregables para este trabajo son: documento escrito, una guía de auditoría para la seguridad de la información genérica y adaptable a un amplio espectro de organizaciones, mediante un modelo práctico de hojas de cálculo disponible al público en www.zenodo.org, de la Unión Europea en la dirección http://doi.org/10.5281/zenodo.3977213.

1.7.2 Limitaciones

Para este trabajo no se pretende entregar una guía de auditoría para soluciones tecnológicas específicas entregadas por un proveedor determinado y usadas para cumplir alguna actividad de control.

1.8 Estado de la cuestión

1.8.1 Planificación de la revisión

1.8.1.1 Formulación de la pregunta

La revisión sistemática busca identificar los estándares y mejores prácticas internacionales para la seguridad de la información y la auditoría al sistema de gestión de la seguridad de la información.

1.8.1.2 Amplitud y calidad de la pregunta

- *Definición del problema.* Es responsabilidad de las organizaciones mantener la seguridad de la información dentro de un nivel aceptable de riesgo, también garantizar que los controles se cumplan de acuerdo con las políticas y normativas adoptadas, por lo tanto, deben desarrollar planes de auditoría que señalen las faltas observadas, así como su nivel de cumplimiento. Por ello, surge la necesidad de contar con profesionales en auditoría con conocimientos en la seguridad de la información, así como el desarrollo de herramientas que faciliten las fases de la auditoría para el sistema de gestión de la seguridad de la información.
  - *Pregunta de investigación.* ¿Cómo auditar la seguridad de la información bajo estándares y mejores prácticas internacionales?
  - *Palabras clave.* En la tabla 2 se detallan las palabras clave escogidas para las búsquedas en navegadores web y repositorios digitales, tanto en el idioma español como el inglés.

Tabla 2. Palabras clave

Español	Inglés
Sistema de gestión de la seguridad de la información	Information security management system
Auditoría de seguridad de la información	ISMS
ISO 27001 Seguridad de la información	IT Audit Plan Information Security Standards
COBIT Ciberseguridad	Plan-Do-Check-Act Cybersecurity

Origen: elaboración propia.

1.8.2 Selección de fuentes

1.8.2.1 Definición de criterio para selección de fuentes

Para la selección de fuentes, se optó por la escogencia de fuentes primarias reconocidas por la comunidad académica.

1.8.2.2 Lenguajes de la revisión

Con el fin de obtener un mayor alcance en la revisión del tema, se consultaron documentos en español e inglés.

1.8.2.3 Identificación de fuentes

La comunidad académica tiene identificadas fuentes de confianza para la publicación de artículos, investigaciones y documentos reconocidos, entre estas están: repositorios digitales, revistas científicas y buscadores académicos, por lo tanto, se utilizan estas para fundamentar la revisión.

1.8.2.4 Método de búsqueda de las fuentes.

Las fuentes son escogidas buscando en la web listas de repositorios confiables y consultando con profesionales del área de las tecnologías de la información.

- *Lista de fuentes.* Las fuentes utilizadas en esta revisión son: Google Scholar, Springer Link, IEEE Xplore Digital Library, ACM Digital Library, Semantic Scholar y IOP Science.
- *Cadenas de búsqueda.* Corresponden a las palabras escritas en el buscador web para obtener una lista de artículos que se ajusten a ese criterio, para esta revisión se utilizó una búsqueda sencilla combinando las palabras clave de la tabla 2 mediante los operadores “and” y “or”.

1.8.3 Selección de los estudios

1.8.3.1 Procedimiento para la selección

Para la búsqueda se utilizaron dos pasos, primeramente, escribiendo las palabras clave en Google Scholar con un tamizaje por título y fuente; como segundo paso se seleccionó el documento para redirigirse a la fuente identificada.

1.8.3.2 Definición de criterios de inclusión y exclusión de los estudios

Inicialmente, para la inclusión se revisan los títulos que se ajusten al tema de auditoría al sistema de seguridad de la información y estándares internacionales

para la seguridad de la información; después se revisan las fechas de publicación, también se lee el resumen, con el fin de determinar si se ajusta al objetivo de investigación. Para la exclusión, se descartan los documentos que se encuentren en un rango mayor a 10 años de publicados, con el fin de usar la información más actualizada; también se leen los documentos y se analizan con el fin de verificar que se ajusten a los objetivos de trabajo.

1.8.4 Ejecución de la selección

1.8.4.1 Selección de estudios iniciales

Los estudios seleccionados se resumen mediante una tabla para cada fuente, ordenados de la siguiente manera: número de ficha, título, autor, cita, enlace, cadena de búsqueda y resultados de la revisión. En total se escogieron 17 artículos, los cuales se pueden consultar en el Anexo 01.

1.8.5 Análisis de resultados

Las demandas de mercado y los requisitos de cumplimiento han obligado a las organizaciones a ser más eficientes y efectivas, es decir, necesitan maximizar sus recursos, gestionar el riesgo, garantizar la seguridad, así como ajustarse al modelo de negocios actual. De manera que han surgido estándares, buenas prácticas y normas para ayudar a las organizaciones a alcanzar sus objetivos de negocio, así como mejorar sus procesos.

Comprender y evaluar normas o estándares al mismo tiempo puede ser una actividad compleja, no existe una fórmula que garantice un 100 % de seguridad, aunque su coexistencia o fusión pueden proporcionar pautas para abordar diferentes dimensiones del sistema de gestión de seguridad de la información y gobierno de TI.

En varios de los documentos se señala que el estándar más exitoso para el sistema de gestión de la seguridad de la información es el ISO/IEC 27001, ha sido desarrollado por la comunidad internacional como una familia de normas para uso integral de las empresas, basado en riesgos y dirigido a un proceso de mejora continua, integrando las nuevas tecnologías disruptivas. Este estándar introduce el modelo cíclico de Plan-Do-Check-Act como un proceso de mejora continua.

Los artículos dejan evidencia de marcos y formas de gestión de la seguridad de la información, no obstante, no se ofrecen propuestas prácticas para evaluar la seguridad de la información conforme a una metodología de auditoría TI estandarizada; en otras palabras, es difícil definir un marco universal de auditoría de TI, porque es importante comprender que las auditorías de TI tienen diferentes características, costos, complejidad del riesgo, necesidad de recursos humanos y de tiempo. A pesar de esto, la revisión hace un acercamiento al modelo de auditoría de ciberseguridad CSAM[1], no obstante, es para auditorías únicas en ciberseguridad y la descripción completa de cada dominio no está disponible.

La percepción del auditado es negativa, probablemente la auditoría de TI tradicional no ha sido capaz de dar valor añadido a la organización, pero la transformación digital ha abierto una oportunidad para que la auditoría de TI juegue un papel más importante y brinde percepciones positivas, en especial si aborda retos como el aumento en el volumen de los datos, aparición de nuevas tecnologías tales como IoT, Big Data, BYOD y sin dejar de lado el aumento en los requisitos y las regulaciones en todo el mundo. Para el desarrollo de una auditoría de seguridad de la información que facilite la revisión de los controles implementados y genere valor, es importante destacar los factores críticos de éxito que debe abordar la presente propuesta de guía de auditoría, dentro de los cuales se pueden señalar la alineación a uno o varios estándares, la gestión por parte de la alta dirección, centrada en riesgos, con políticas de seguridad clave ordenadas por área o dominio y la evaluación del conocimiento en seguridad dentro de la empresa. También resulta útil que las guías de auditoría se puedan aplicar de forma parcial en áreas de riesgo específicas o exhaustivas para todo el sistema de gestión.

Lo anterior con el propósito de que las organizaciones puedan ubicar su situación actual y emprender caminos a un incremento de su seguridad de la información a niveles óptimos.

---

[1] CyberSecurity Audit Model

Capítulo 2. Marco conceptual

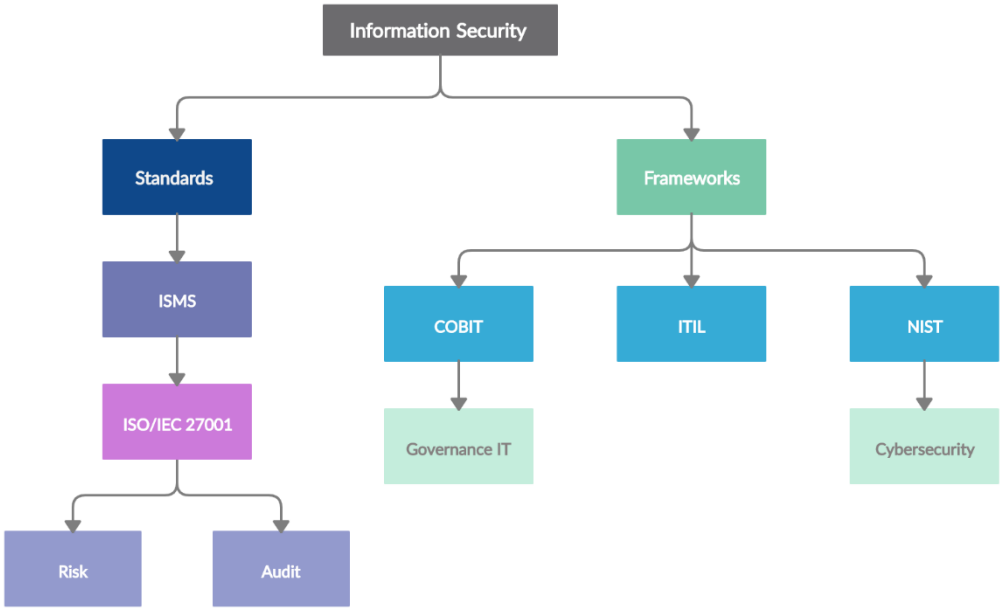
2.1 Elaboración del marco conceptual

El marco conceptual se representa visualmente mediante la nube de palabras, donde aquellas con mayor frecuencia son de mayor tamaño, tal como lo demuestra la figura 1, además, a mayor fuente, mayor relevancia. Para la extracción de estas, se procedió a tomar las palabras clave de cada artículo y para los que no las tenían declaradas, se utilizó un generador de palabras clave. Seguidamente, todas se colocaron en un único documento y se utilizó un generador de nube *online* de palabras.

Figura 1. Nube de palabras (Elaboración propia)

Después de identificar los conceptos más prominentes, es necesario establecer un orden de importancia o dependencia, para ello se utiliza el mapa conceptual jerárquico, en el que se coloca el concepto básico en la parte superior a partir del cual se van sacando las ideas secundarias por ramas. La figura 2 muestra el mapa conceptual para la seguridad de la información y los conceptos asociados a la misma. Esta información ayudará a contextualizar el planteamiento del presente trabajo.

Figura 2. Mapa conceptual jerárquico (Elaboración propia)



2.2 Marco conceptual

La seguridad de la información ha tomado más relevancia desde la última década, a pesar de ser un tema crucial, muchas organizaciones aún muestran dificultades para comprenderla e implementarla, como explican Tagarev y Polimirova (2019): “la seguridad de la información se ocupa de proporcionar confidencialidad, integridad y disponibilidad de información que es ‘sensible’ para la organización, ya sea en formato digital o analógico”.

Para atender la seguridad de la información, se han desarrollado diferentes estándares y marcos de trabajo internacionales que proponen su gestión desde distintos enfoques. Primeramente, dentro de los estándares se reconoce el concepto de Sistema de Gestión de Seguridad de la Información (SGSI) (en inglés: *Information Security Management System,* ISMS), consiste en un conjunto de políticas, procedimientos, y directrices junto a los recursos y actividades asociadas que son administradas por una organización, en la búsqueda de proteger sus activos de información. El término es ampliamente utilizado por el estándar internacional ISO/IEC 27001, el cual proporciona los requisitos para establecer, implementar, operar, mantener, revisar y mejorar un Sistema de Gestión de la Seguridad de la Información en organizaciones y empresas de diferentes tipos y tamaños.

El estándar ISO/IEC 27001 está alineado al Ciclo Deming Plan-Do-Check-Act (PDCA o PHVA que significa Planear-Hacer-Verificar-Actuar) como enfoque de mejora continua, cada fase se detalla como sigue:

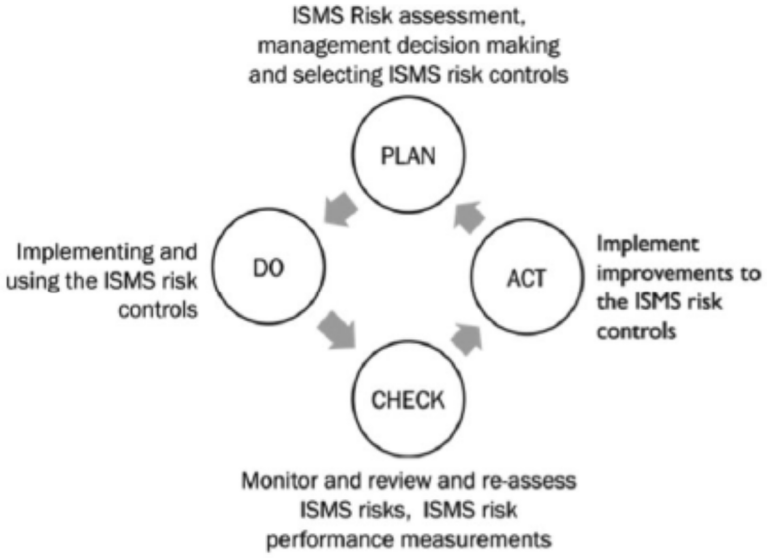
- *Plan*: fase de diseño del SGSI, realizando evaluación de riesgos de seguridad de la información y la selección de los controles adecuados.
- *Do:* fase de implantación y operación de los controles.
- *Check:* fase para revisar y evaluar el desempeño del SGSI.
- *Act:* fase de realización de cambios cuando sea necesario para llevar al SGSI al máximo de su rendimiento.

Toda organización que desee implantar un SGSI debe llevar a cabo una evaluación de riesgos para establecer los controles adecuados de acuerdo con el entorno y el alcance de la organización, como explica Humphreys (2011), el estándar ISO/IEC 27005: “proporciona pautas para la gestión de riesgos de seguridad de la información en una organización, respaldando en particular los requisitos de un SGSI de acuerdo con ISO/IEC 27001”. No obstante, no proporciona una metodología específica para la gestión de riesgos de la información, la misma dependerá del enfoque, el contexto o sector de la organización. Sin embargo, algunas características importantes para la gestión del riesgo en ISO/IEC 27001 y ISO/IEC 27005 se listan a continuación:

- Riesgos identificados y perfiles de riesgo acordados.
- Comprender el impacto de las exposiciones al riesgo.
- Conciencia del usuario sobre el riesgo.
- Plan de gestión de riesgos y prioridades para tomar acciones.
- Riesgos y métricas de la seguridad de la información.
- Revisiones periódicas de riesgos.

La figura 3 muestra cómo la gestión de riesgos encaja en el modelo de mejora continua PDCA.

Figura 3. Proceso de gestión de riesgos (Information Security Management System Standards, Humphreys, 2018)



En vista del uso crucial de TI para el éxito y la continuidad del negocio, la auditoría se ha convertido en un factor inevitable y parte del programa de mejora continua, por tanto, es relevante comprender el concepto y la importancia de realizar evaluaciones periódicas, entonces la auditoría de TI se podría definir como:

> Un proceso de aseguramiento sistemático, independiente y objetivo que se realiza periódicamente y de acuerdo con los estándares, a fin de proporcionar aseguramiento razonable y una mejora continua de una implementación exitosa de TI. (Aditya, Ferdiana y Santosa, 2018)

Para las normas ISO, la auditoría es un proceso sistemático, independiente y documentado para obtener evidencia de auditoría y evaluarla objetivamente, con el fin de determinar en qué medida se cumplen los criterios de auditoría (ISO/IEC 27000:2015).

La auditoría del SGSI se puede atender mediante la familia ISO/IEC 27001, la cual dispone de las siguientes guías:

- El estándar ISO/IEC 27007: establece las directrices para las auditorías internas y externas de un SGSI o para gestionar un programa de auditoría según los requisitos específicos de ISO/IEC 27001.

- El estándar ISO/IEC 27008: orienta para la revisión de los controles de la seguridad de la información, incluida la verificación de cumplimiento técnico de conformidad con los estándares de seguridad de la información establecidos por la organización.

Finalmente, se aborda la rama de los marcos de referencia, el primero de ellos es Cobit, sus siglas significan: Objetivos de Control para la Información y la Tecnología Relacionada. Este marco fue diseñado por ISACA (Asociación de Auditoría y Control de Sistemas de Información) con el objeto de proporcionar un conjunto de buenas prácticas para el gobierno y la gestión de las tecnologías de la información, así como apoyar a los gerentes, auditores y usuarios de TI en la unión de los objetivos comerciales con los objetivos de TI. En la edición de Cobit 5, los objetivos de gobernanza y gestión se agrupan en los siguientes cinco dominios:

1. Evaluar, dirigir, monitorear (EDM)
2. Alinear, planificar, organizar (APO)
3. Construir, adquirir, implementar (BAI)
4. Entrega, servicio, soporte (DSS)
5. Monitorear, evaluar, valorar (MEA)

Los objetivos de gobierno están en el dominio EDM, donde el órgano rector evalúa las estrategias, dirige a la alta gerencia y monitorea el logro de la estrategia. Los objetivos de gestión se abordan en los cuatro dominios restantes, los mismos se describen con más detalle a continuación:

- APO: organización a nivel general, estrategia y actividades de soporte para TI empresarial.
- BAI: definición, adquisición e implementación de soluciones de TI y la integración con procesos comerciales.
- DSS: entrega operativa, soporte de los servicios de TI y la seguridad.
- MEA: monitoreo de desempeño, conformidad de TI con los objetivos internos de desempeño, los objetivos de control interno y los requisitos externos.

Cobit puede adoptarse en un enfoque integral, puesto que está alineado con otros marcos y estándares.

El segundo marco es ITIL, cuyas siglas significan Informatión Tecnology Infrastructure Library (en español, Biblioteca de Infraestructura de Tecnología de la información), según explican Aditya y Menzelthe (2019): “ITIL es un conjunto de conceptos y prácticas para la Gestión de los Servicios de Tecnología de la Información, el desarrollo de la tecnología de la información y las operaciones de TI, que se centra en la seguridad”.

Este marco facilita el gobierno de TI, para la medición y el mejoramiento continuo de la calidad de los servicios entregados basado en el ciclo Deming. Contiene los siguientes componentes principales:

- Soporte de servicio
- Entrega de servicio
- Gestión de la infraestructura de TI
- Gestión de la seguridad
- Gestión de aplicaciones
- Gestión de activos de software
- Planificación para implementar la gestión de servicios
- Implementación a pequeña escala

ITIL contribuye a definir un nivel de seguridad del servicio, para el manejo de incidentes.

Para finalizar el marco de referencia para la ciberseguridad, se encuentra NIST, sus siglas significan National Institute of Standards and Tecnology (en español Instituto Nacional de Estándares y Tecnología), pertenece a la agencia federal de tecnología que trabaja con la industria para desarrollar y aplicar tecnología y medidas estándares. Seguidamente, se hace referencia al concepto de ciberseguridad de forma ampliada, puesto que la información traspasa las fronteras de la organización y vincula nuevos riesgos.

La ciberseguridad se ocupa de la protección de la información y el acceso a través del ciberespacio, que interactúa y puede ser de gran importancia para la prestación de los servicios esenciales, el funcionamiento de infraestructuras críticas y sitios estratégicos o la manipulación de los cuales pueden usarse para influir en el

comportamiento individual o colectivo y, por lo tanto, puedan ser blanco de las llamadas amenazas híbridas (Tagarev y Polimirova, 2019).

La ciberseguridad se engloba dentro del concepto de seguridad de la información.

Capítulo 3. Marco metodológico

3.1 Tipo de investigación

El tipo de metodología de investigación por utilizar es el aplicado, por ende, busca la utilización de conocimientos existentes, con el fin de implementarlos de forma práctica para satisfacer necesidades de un contexto determinado, mientras proporciona una solución para problemas de un sector social o productivo.

El presente trabajo propone la elaboración de una guía práctica para la auditoría del sistema de gestión de la seguridad de la información, para ello se utilizan los conocimientos base existentes, pero, a su vez, se espera pueda aplicarse a diversos tipos de organizaciones, es decir, no está enfocada en una organización en específico.

3.2 Alcance investigativo

Este trabajo utiliza el alcance descriptivo, de manera que se observan las características, procesos y objetivos de estándares y buenas prácticas internacionales en la gestión de la seguridad de la información, tal y como están especificados; entonces, a partir de ahí se define el contexto y la situación actual de las organizaciones, con el fin de extraer una guía general que contribuya al proceso de monitoreo y evaluación.

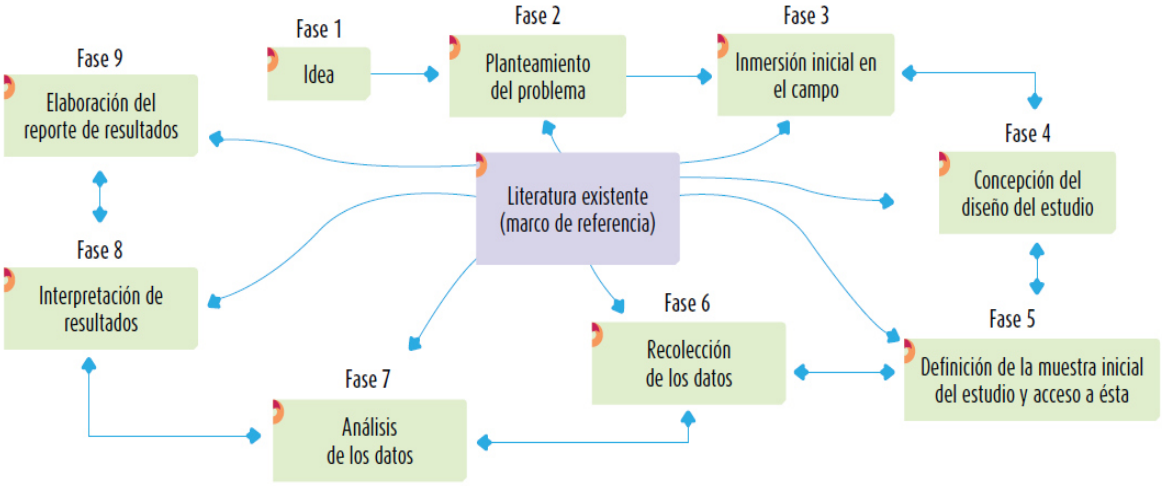
Los estudios descriptivos buscan especificar las propiedades, las características y los perfiles importantes de personas, grupos, comunidades o cualquier otro fenómeno que se someta a un análisis. Describen situaciones, eventos o hechos, recolectando datos sobre una serie de cuestiones y se efectúan mediciones sobre ellas; buscan especificar propiedades, características y rasgos importantes de cualquier fenómeno que se analice (Cortés, 2005).

3.3 Enfoque

El enfoque utilizado para el desarrollo de este trabajo es el cualitativo, puesto que los resultados corresponden, primeramente, a una idea con un planteamiento del problema, a partir del cual se da un proceso de investigación para después realizar un análisis e interpretar la documentación revisada, así también el investigador está involucrado en la generación de las propuestas. La figura 3 muestra el proceso cualitativo representado de forma circular, este varía

dependiendo de cada estudio en particular y contempla regresiones en cualquier fase del proceso.

Figura 4. El proceso cualitativo (Metodología de la Investigación, Hernández, Collado y Baptista, 2006)



La revisión literaria puede realizarse en cualquier etapa del estudio y apoyar desde el planteamiento del problema hasta la elaboración del reporte de resultados.

> Las etapas pueden seguir una secuencia más bien lineal si todo resulta como se esperaba: planteamiento del problema, inmersión inicial en el campo, concepción del diseño, muestra, recolección y análisis de datos, interpretación de resultados y elaboración del reporte (Hernández, Fernández y Baptista, 2006).

3.4 Diseño

Para el diseño de la investigación cualitativa, se toman los conceptos propuestos por Hernández et al. (2006), quienes plantean estos cinco marcos interpretativos: “diseños de teoría fundamentada, diseños etnográficos, diseños narrativos, diseños de investigación-acción y diseños fenomenológicos”. El diseño que mejor se adapta a este trabajo es el diseño de investigación-acción, cuya finalidad es resolver problemas cotidianos e inmediatos, y mejorar prácticas concretas. Su propósito fundamental se centra en aportar información que guíe la toma de decisiones para programas, procesos y reformas estructurales (Salgado, 2007).

3.5 Población y muestreo

La población para este trabajo corresponde a las normas, estándares y buenas prácticas internacionales para la gestión del sistema de la seguridad de la información. Para la selección de la muestra, se eligió el muestreo intencional en el cual, según Cortés (2005): "el investigador selecciona los elementos que a su juicio son representativos, lo cual exige del investigador un conocimiento previo de la población". Entonces, se toman como punto de partida el marco de gestión COBIT y los estándares internacionales ISO/IEC 27001 e ISO/27002.

3.6 Instrumentos de recolección de datos

El principal instrumento de recolección de datos para el estudio y proceso de interpretación es el análisis documental, el cual constituye el punto de entrada de la investigación (Quintana, 2006).

Esta técnica es válida para este trabajo, puesto que permite conseguir un modelo estructurado de la información para ser analizada y sometida a un proceso de interpretación. La figura 5 resume los pasos de este instrumento.

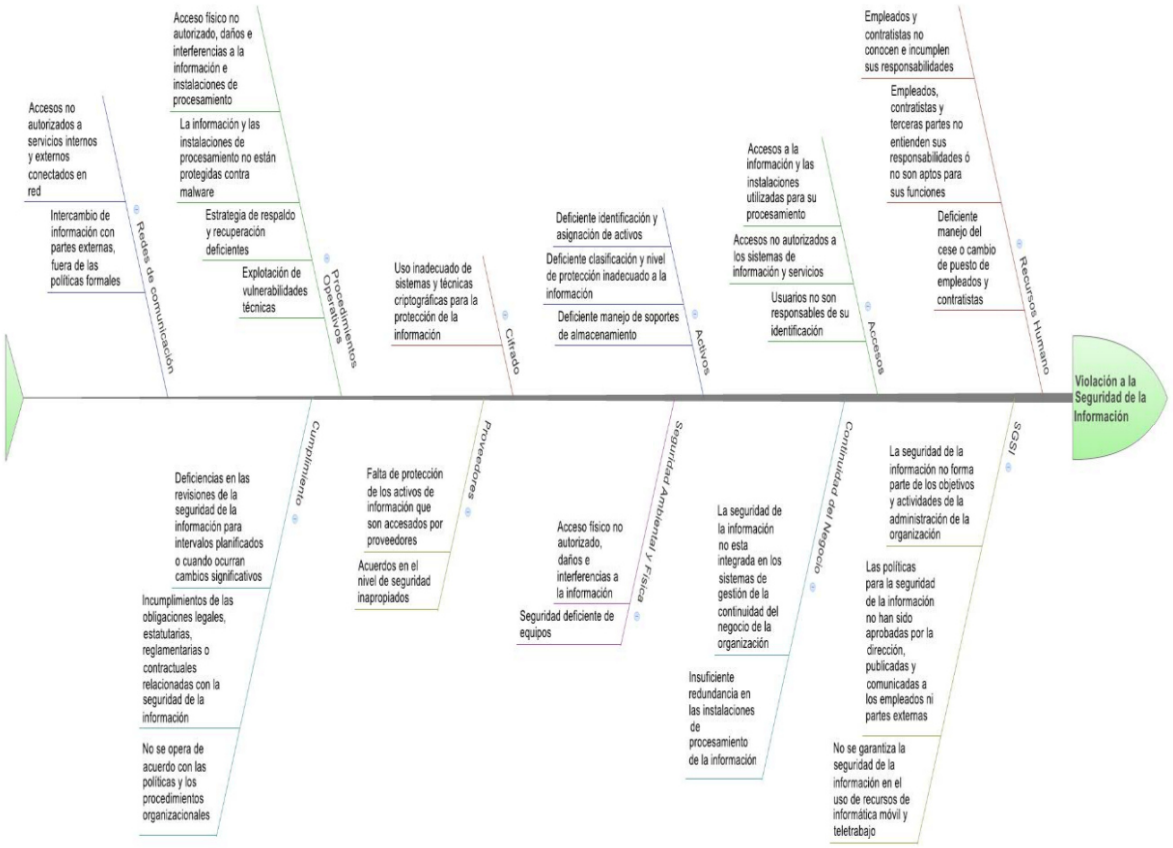
Figura 5. Las cinco acciones del análisis documental (Elaboración propia a partir de las Técnicas para la generación y recolección de información de Quintana, 2006)

3.7 Técnicas de análisis de información

La primera técnica de análisis de información utilizada es el diagrama de Ishikawa, también conocido como diagrama de espina de pez, en el cual se representan gráficamente diferentes causas colocadas en las espinas y que dan origen a un efecto o problema principal colocado a la derecha.

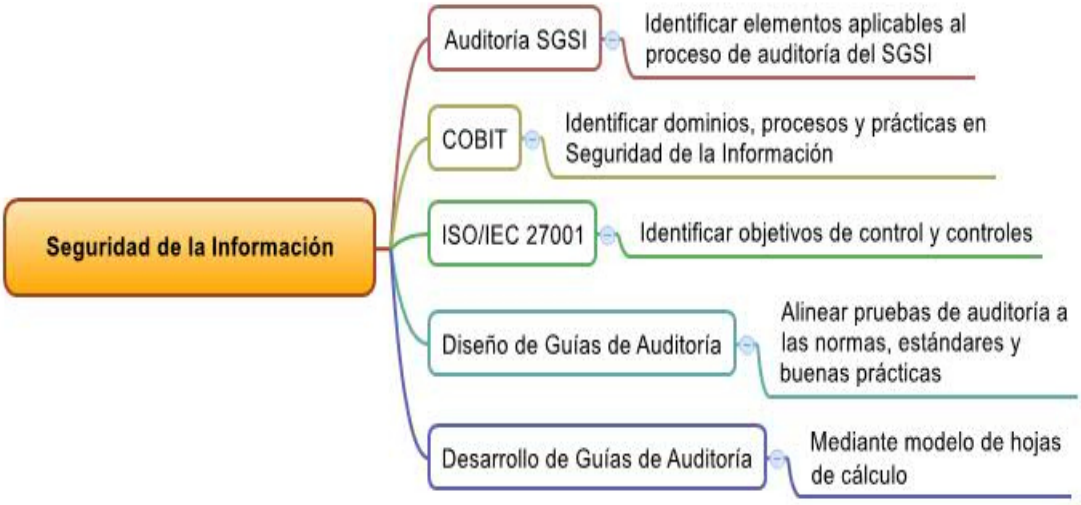
La figura 6 muestra las posibles causas que dan como resultado una violación a la seguridad de la información, obtenidas a través del análisis documental.

Figura 6. Diagrama de Ishikawa (Elaboración propia a partir del estándar ISO/IEC 27002, ISO/IEC 27002:2015)



La segunda técnica de análisis de información seleccionada es el mapa conceptual utilizado para demostrar las relaciones existentes entre distintos conceptos. La figura 7 muestra la forma en que este proyecto está conceptualizado y el orden lógico para el desarrollo de este, es decir, representa de forma lineal la manera en que se aborda la información para que tenga sentido.

Figura 7. Mapa conceptual (Elaboración propia)



Capítulo 4. Análisis del diagnóstico

4.1 Planificación de la auditoría

El enfoque de auditoría utilizado se basa en la Guía de Cobit 5 para el Aseguramiento, como parte de los estándares de auditoría generalmente aceptados e incluido dentro de los marcos de trabajo estudiados en el presente documento.

Como punto de partida, es indispensable determinar el alcance de la iniciativa de aseguramiento, por eso se desarrollaron plantillas genéricas para identificar las partes interesadas, así como realizar el estudio preliminar de la organización por auditar, debido a que las actividades de auditoría variarán dependiendo del tamaño, funcionalidad, complejidad y nivel de madurez del SGSI. Entonces, se hace necesario comprender el contexto organizacional, así como los riesgos relevantes asociados al negocio. Por otra parte, en esta etapa también es importante recabar la información y documentación generada al establecer el sistema de gestión, tales como políticas, manuales de procedimientos, personas responsables, entre otros, para luego plantear el programa de auditoría que visualiza los procedimientos con los cuales asociar las guías de auditoría.

El segundo punto consistió en entender los catalizadores para establecer los criterios de evaluación adecuados, de forma tal que el profesional que ejecuta la auditoría comprenda las estructuras organizativas, procesos, cultura, ética, comportamiento y elementos de información mientras realiza la evaluación.

Para finalizar, el proceso completo de las fases de auditoría incluye comunicar los resultados del aseguramiento, sin embargo, para efectos de este trabajo, no se incluyó, puesto que no se hace la aplicación de las guías generadas a ninguna organización en específico.

4.2 Selección de marcos, estándares y buenas prácticas para la seguridad de la información

Cada organización es un universo diferente, por esta razón, tiene validez el hecho de que existan marcos de referencias, estándares y buenas prácticas que permitan alinear criterios para la evaluación de la seguridad de la información, de ahí que el presente texto tomó como referencia el marco de trabajo Cobit 5 Procesos Catalizadores; en concreto se seleccionaron los procesos para gestión de TI,

Alinear, Planificar, Organizar conocido por las siglas APO y el proceso Entregar, Dar Servicio y Soporte, reconocido con las siglas DSS, los cuales proporcionan lineamientos básicos para la seguridad de la información. También se escogió como estándar ISO/IEC 27001 para los lineamientos generales de implementación de un SGSI y la ISO/IEC 27002 para las buenas prácticas de elección de los objetivos de control y controles.

4.2.1 Procesos catalizadores de Cobit 5

A razón de incluir los dominios y prácticas de gestión aplicables que atañen a la seguridad de la información, la tabla 8 contiene los elementos principales del modelo de referencia de procesos de Cobit 5, dentro de los cuales se encuentran los catalizadores APO01 Gestionar el marco de gestión de TI, APO13 Gestionar la Seguridad, DSS04 Gestionar la continuidad y DSS05 Gestionar Servicios de Seguridad.

Tabla 8. Mapeo de dominios, procesos y prácticas de seguridad de Cobit

COBIT 5 Catalizadores			
Proceso	Descripción	Propósito	Práctica de gestión
Dominio APO01			
Gestionar el marco de gestión de TI	Aclarar y mantener el gobierno de la misión y la visión corporativa de TI.	Proporcionar un enfoque de gestión consistente que permita cumplir los requisitos de gobierno corporativo e incluya procesos de gestión, estructuras, roles y responsabilidades, organizativos, actividades fiables y reproducibles, así como habilidades y competencias.	APO01.02 Establecer roles y responsabilidades. APO01.04 Comunicar los objetivos y la dirección de gestión. APO01.06 Definir la propiedad de la información (datos) y del sistema. APO01.07 Gestionar la mejora continua de los procesos. APO01.08 Mantener el cumplimiento con las políticas y procedimientos.
Dominio APO13			
Gestionar la seguridad	Definir, operar y supervisar un sistema	Mantener el impacto y ocurrencia de los	APO13.01 Establecer y mantener un SGSI.

	para la gestión de la seguridad de la información.	incidentes de la seguridad de la información dentro de los apetitos de riesgo de la empresa.	APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la SI. APO13.03 Supervisar y revisar un SGSI.
Dominio DSS04			
Gestionar la continuidad	Establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos del negocio y los servicios TI requeridos, así como mantener la disponibilidad de la información a un nivel aceptable para la empresa.	Continuar las operaciones críticas para el negocio y mantener la disponibilidad de la información a un nivel aceptable para la empresa ante el evento de una interrupción significativa.	DSS04.03 Desarrollar e implementar una respuesta a la continuidad del negocio DSS04.04 Ejercitar, probar y revisar el BCP. DSS04.07 Gestionar acuerdos de respaldo.
Dominio DSS05			
Gestionar servicios de seguridad	Proteger la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información, así como realizar la	Minimizar el impacto en el negocio de las vulnerabilidades e incidentes operativos de seguridad de la información.	DSS05.01 Proteger contra *software* malicioso. DSS05.02 Gestionar la seguridad de la red y las conexiones. DSS05.03 Gestionar la seguridad de los puestos de usuario final. DSS05.04 Gestionar la identidad del usuario y el acceso lógico. DSS05.05 Gestionar el acceso físico a los activos de TI.

	supervisión de la seguridad.		DSS05.06 Gestionar documentos sensibles y dispositivos de salida. DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.

Origen: elaboración propia a partir de Cobit 5, Procesos Catalizadores.

4.2.2 Selección de los objetivos de control y controles

Para la escogencia de los objetivos de control, se recurrió al estándar ISO/IEC 27001 Sistema de gestión de la seguridad de la información, el cual señala los requisitos que deben seguir las organizaciones para establecer, implementar y mantener un sistema de gestión, en el anexo 02 se muestra la tabla 9 con los dominios y objetivos de control considerados.

Para los controles se tomó como referencia el estándar internacional ISO/IEC 27002, debido a que proporciona las pautas y las prácticas de gestión para los controles en un entorno de seguridad de la información.

4.2.3 Mapeo de la seguridad de la información del SGSI

Las guías de auditoría planteadas requieren la integración y ordenamiento de dominios, objetivos de control y prácticas de gestión, con el fin de abarcar diferentes escenarios y posibles riesgos asociados a la información en el ámbito normal de las operaciones de un amplio espectro de organizaciones, por ende, se ejecutó un mapeo que se puede consultar en el anexo 3, el cual provee una correlación que facilita el seguimiento de las actividades para evaluar el SGSI; de manera que el marco de trabajo de Cobit 5 y los estándares internacionales ISO/IEC 27001 e ISO/IEC 27002 coexisten y se complementan con el fin de apoyar las prácticas para proteger la información.

4.3 Diseño de las guías de auditoría

Las guías de auditoría propuestas integran los elementos descritos anteriormente, a razón de ser los instrumentos principales de orden genérico que permitan llevar a cabo encargos de aseguramiento en acatamiento a estándares referentes de la industria. Entonces, a partir de ahí, se generó el formato de la tabla 11, el cual contiene un número de consecutivo con las siglas AUD-SGSI-#-Año,

nombre de la organización por ser evaluada, área específica donde se realizó la evaluación, fecha de aplicación, nombre de la persona responsable de aplicar la guía, objetivo del control, dominio ISO/IEC 27001, número de referencia de ISO/IEC 27002 y práctica de gestión de Cobit 5; para luego detallar los criterios que serán objeto de evaluación, el estado de cumplimiento se mide marcando las casillas Sí, No, parcial o No aplica. Por último, se deja un espacio para anotar las observaciones que se consideren relevantes. Este formato se construyó sobre una hoja de cálculo para tabular el estado de cumplimiento.

Tabla 11. Formato de guía de auditoría de la seguridad de la información

AUD-SGSI- #-año	**Guía de Auditoría** **Evaluación del Sistema de Gestión de la Seguridad de la Información**					
Nombre de la ogranización evaluada:						
Area evaluada:				**Fecha:**		
Responsable de la evaluación:						
Objetivo:						
Dominio ISO/IEC 27001:						
Guía de referencia ISO/IEC 27002:		**Práctica de gestión:**				
No.	**Criterio a evaluar**	**Cumplimiento**			**No aplica**	**Observaciones**
		Si	**No**	**Parcial**		
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						

Origen: elaboración propia.

Capítulo 5. Propuesta de solución

5.1 Escenarios de aplicación

Una organización podrá utilizar la familia ISO/IEC 27000 o Cobit 5 para el manejo de la seguridad de la información, es decir, se puede usar uno o ambos marcos de trabajo según las disposiciones de la alta dirección; entonces, los tres escenarios listados seguidamente describen algunas áreas de aplicación.

5.1.1 Escenario 1

Suponga que una entidad usa el marco de gobierno de TI basado en Cobit 5, además, tiene implementado un SGSI basado en el estándar internacional ISO/IEC 27001 y desea cumplir con la práctica de gestión APO13.03 Supervisar y revisar el SGSI.

5.1.2 Escenario 2

Suponga que una entidad tiene implementado un sistema de gestión de la seguridad de la información bajo el estándar ISO/IEC 27001 y desea acatar el dominio de cumplimiento en el cual se encuentran las revisiones independientes de seguridad de la información, cumplimiento con las políticas y normas de seguridad y revisiones de cumplimiento técnico.

5.1.3 Escenario 3

Suponga que una organización tiene implementado un SGSI completo o parcialmente, pero desea realizar una auditoría dirigida, es decir, solo pretende hacer una evaluación a ciertos controles que son de interés para el Departamento de seguridad de la información y la Junta directiva.

5.2 Determinar el alcance de la auditoría

Esta etapa comienza con un estudio preliminar de la organización, con la finalidad de obtener un mayor entendimiento de la naturaleza, necesidades y contexto donde se realizan las actividades sustantivas, así como identificar el alcance de la auditoría y a quienes va dirigida.

5.2.1 Plan de revisión preliminar

Tabla 12. Plan de revisión preliminar

Plan de revisión preliminar			
Elaborado por: Yesenia Ureña Agüero			
Organización evaluada:			
Período evaluado:		**Período de revisión:**	
Revisado por:		**Fecha revisión:**	
Objetivo: Determinar el alcance de la auditoría mediante la comprensión del contexto de la organización, las partes interesadas y su interés.			
Alcance: Se recopilará y analizará información sobre las actividades sustantivas de la organización y otros aspectos que se consideran relevantes.			
No.	**Procedimientos**	**Responsable**	**Ref. P/T**
Determinar el alcance de la iniciativa de aseguramiento			
1.	Identificar los usuarios a los que se destina el informe de auditoría y su interés en el encargo de aseguramiento.		
2.	Identificar las partes interesadas responsables del área sobre la que se debe proporcionar el aseguramiento.		
Determinar los objetivos de la auditoría sobre la base de la evaluación del contexto interno y externo, así como de los riesgos relevantes			
1.	Conocer la estrategia y las prioridades de la organización.		
2.	Conocer el contexto interno de la organización.		
3.	Conocer el contexto externo de la organización.		
4.	Definir los límites organizativos de la iniciativa de aseguramiento.		
Determinar los catalizadores en el alcance y la instancia de los catalizadores			
1.	Conocer los principios, las políticas y los marcos del SGSI.		
2.	Definir qué procesos están en el alcance de la revisión.		
3.	Definir qué estructuras organizativas están en el alcance de la revisión.		

4.	Conocer la cultura, la ética y los aspectos de comportamiento de la organización.		
5.	Conocer los elementos de información (dentro de las etapas del ciclo de vida) que son relevantes para el alcance de la revisión.		
6.	Conocer los servicios, la infraestructura y las aplicaciones de la organización.		
7.	Conocer las habilidades y competencias del personal, relacionadas con los niveles de educación, capacitación y conocimiento técnico para llevar a cabo las funciones de la organización.		

Origen: elaboración propia a partir de la Guía de Cobit 5 para el aseguramiento.

5.3 Entender los catalizadores y establecer los criterios de evaluación

Para esta segunda etapa, se desarrolló un programa de auditoría genérico que puede adaptarse a cualquiera de los tres escenarios propuestos anteriormente. Mediante la tabla 13, se definen los procedimientos que requieren ser aplicados para cumplir con el objetivo de evaluar el sistema de gestión de la seguridad de la información, alineado a estándares reconocidos internacionalmente.

5.3.1 Programa de auditoría

Tabla 13. Programa general de auditoría

Programa general de auditoría		
Organización evaluada:		
Elaborado por:		
Período evaluado:		
Revisado por:	**Firma**	**Fecha revisión:**
Objetivo: Evaluar el sistema de gestión de la seguridad de la información alineado a estándares y buenas prácticas internacionales.		
Alcance: El estudio se realiza a las actividades propias del SGSI durante el período evaluado. Contempla el alcance de auditoría establecido por la organización.		

No.	Procedimiento	Ref. AUD-SGSI-#	Hecho por	Fecha		Total días
				Inicio	Fin	
Políticas de seguridad de la información						
1.	Analizar si la dirección ha proporcionado la gestión y soporte para la seguridad de la información, de acuerdo con los requisitos del negocio y con las regulaciones y leyes pertinentes.	AUD-SGSI-01-2020				
Organización de la seguridad de la información						
2.	**Organización interna** Indagar la existencia y cumplimiento de un marco de gestión para iniciar y controlar la implementación y operación de seguridad de la información dentro de la entidad.	AUD-SGSI-02-2020				
3.	**Dispositivos móviles y teletrabajo** Determinar la existencia y cumplimiento de la seguridad del teletrabajo y el uso de dispositivos móviles.	AUD-SGSI-03-2020				
Seguridad ligada a los recursos humanos						
4.	**Previo al empleo** Indagar si existe un proceso de selección de los empleados y contratistas, que incluya sus responsabilidades, y que sean aptos para los roles en los cuales están siendo considerados.	AUD-SGSI-04-2020				
5.	**Durante el empleo** Indagar si existen las gestiones para que los empleados y contratistas tomen conciencia de sus responsabilidades en seguridad de la información y las cumplan.	AUDI-SGSI-05-2020				
6.	**Finalización o cambio de empleo** Indagar si se protegen los intereses de la organización como parte del proceso de finalización o cambio de empleo.	AUDI-SGSI-06-2020				

Gestión de activos						
7.	**Responsabilidad por los activos** Constatar si se han identificado los activos de la organización y se han definido las responsabilidades para la apropiada protección.	AUDI-SGSI-07-2020				
8.	**Clasificación de la información** Constatar que la información recibe un nivel de protección apropiado, de acuerdo con su importancia para la organización.	AUDI-SGSI-08-2020				
9.	**Manejo de medios** Constatar si existen procedimientos para prevenir la divulgación, modificación, remoción o destrucción no autorizada de la información almacenada en los medios.	AUDI-SGSI-09-2020				
Control de acceso						
10.	**Requisitos del negocio para el control de acceso** Verificar la existencia y cumplimiento de acciones para controlar el acceso a la información y a los recursos de procesamiento de esta.	AUDI-SGSI-10-2020				
11.	**Gestión del acceso de usuarios** Determinar la existencia de gestiones para asegurar el acceso autorizado de los usuarios y evitar el acceso no autorizado a los sistemas y servicios.	AUDI-SGSI-11-2020				
12.	**Responsabilidades de los usuarios** Verificar si los usuarios son responsables de salvaguardar su información de autenticación.	AUDI-SGSI-12-2020				
13.	**Control de acceso a sistemas y aplicaciones** Determinar la existencia y cumplimiento de acciones para evitar el acceso no autorizado a los sistemas y aplicaciones.	AUDI-SGSI-13-2020				
Criptografía						
14.	**Controles de criptografía** Indagar sobre el uso apropiado y efectivo de la	AUDI-SGSI-14-2020				

	criptografía para proteger la confidencialidad, autenticidad e integridad de la información.					
Seguridad física y ambiental						
15.	**Áreas seguras** Determinar la existencia y cumplimiento de gestiones para prevenir el acceso físico no autorizado, daño e interferencia a la información y a las instalaciones de procesamiento de la organización.	AUDI-SGSI-15-2020				
16.	**Equipo** Determinar la existencia y cumplimiento de acciones para prevenir la pérdida, daño, robo o compromiso de los activos y la interrupción de las operaciones de la organización.	AUDI-SGSI-16-2020				
Seguridad de las operaciones						
17.	**Procedimientos y responsabilidades operacionales** Indagar sobre las gestiones y procedimientos para asegurar las operaciones correctas y seguras de los recursos de procesamiento de la información.	AUDI-SGSI-17-2020				
18.	**Protección contra código malicioso** Verificar que las instalaciones de procesamiento de información y la información están protegidas contra el código malicioso.	AUDI-SGSI-18-2020				
19.	**Respaldo** Verificar y revisar la existencia de gestiones para proteger contra la pérdida de datos mediante copias de respaldo.	AUDI-SGSI-19-2020				
20.	**Registro y seguimiento** Determinar la existencia del registro de eventos y generación de evidencia.	AUDI-SGSI-20-2020				
21.	**Control del software operativo** Determinar la existencia de procedimientos para asegurar la integridad de los sistemas operativos.	AUDI-SGSI-21-2020				

22.	**Gestión de vulnerabilidades técnicas** Indagar sobre las gestiones para prevenir la explotación de vulnerabilidades técnicas.	AUDI-SGSI-22-2020				
Seguridad de las comunicaciones						
23.	**Gestión de seguridad de la red** Indagar sobre la existencia de controles para asegurar la protección de la información en las redes y sus recursos de soporte de procesamiento de información.	AUDI-SGSI-23-2020				
24.	**Transferencia de información** Determinar la existencia de políticas, procedimientos y controles para mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.	AUDI-SGSI-24-2020				
Adquisición, desarrollo y mantenimiento de los sistemas de información						
25.	**Requisitos de seguridad de sistemas de información** Indagar la existencia de requisitos para asegurar que la seguridad de la información sea parte integral de los sistemas de información a través de todo el ciclo de vida. Así como los requisitos para los sistemas de información que proporcionan los servicios a través de redes públicas.	AUDI-SGSI-25-2020				
26.	**Seguridad en los procesos de desarrollo y soporte** Determinar la existencia de gestiones para asegurar que la seguridad de la información sea diseñada e implementada dentro del ciclo de vida del desarrollo de sistemas de información.	AUDI-SGSI-26-2020				
27.	**Pruebas de datos** Verificar la protección de los datos utilizados para pruebas de los sistemas de información.	AUDI-SGSI-27-2020				
Relaciones con los proveedores						

28.	**Seguridad de la información en la relación con proveedores** Constatar la existencia de gestiones para asegurar la protección de los activos que son accesibles a los proveedores en la prestación de los servicios contratados.	AUDI-SGSI-28-2020				
29	**Gestión de la entrega de servicios del proveedor** Indagar si se mantiene un nivel de seguridad de la información y la entrega de servicios alineado con los acuerdos con proveedores.	AUDI-SGSI-29-2020				
Gestión de incidentes de seguridad de la información						
30.	**Gestión de incidentes y mejoras en la seguridad de la información** Determinar la existencia y cumplimiento de un enfoque coherente y efectivo para la gestión de los incidentes de seguridad de la información, incluyendo la comunicación de los eventos y debilidades.	AUDI-SGSI-30-2020				
Aspectos de seguridad de la información en la gestión de la continuidad del negocio						
31.	**Continuidad de la seguridad de la información** Constatar si la continuidad de la seguridad de la información está integrada en los sistemas de gestión de la continuidad de negocio de la organización.	AUDI-SGSI-31-2020				
32.	**Redundancias** Constatar la implementación de los recursos de procesamiento de información con redundancia suficiente para asegurar la disponibilidad.	AUDI-SGSI-32-2020				
Cumplimiento						
33.	**Cumplimiento de los requisitos legales y contractuales** Identificar y verificar la legislación aplicable para evitar brechas entre las obligaciones legales, estatutarias, reglamentarias o contractuales	AUDI-SGSI-33-2020				

	relacionadas con seguridad de la información y cualquier requisito de seguridad.					
34.	**Revisión de seguridad de la información** Verificar que la seguridad de la información fue implementada y opere de acuerdo con las políticas y procedimientos de la organización.	AUDI-SGSI-34-2020				
Tiempo estimado del estudio						
Fecha de asignación:		Tiempo estimado:		Tiempo real	Diferencia	
Justificación de la diferencia en cumplimiento del tiempo:						
Observaciones:						
Fecha inicio:		Fecha finalización:				

Origen: elaboración propia.

5.3.2 Alfabetización de la seguridad de la información

La organización debe dar capacitación, concienciación y educación apropiada en seguridad de la información a todos los empleados, además, donde sea relevante, a contratistas y proveedores. Este entrenamiento incluye el conocimiento de las políticas y procedimientos organizacionales, de modo similar, la entidad debe realizar revisiones periódicas de la comprensión de la seguridad de la información, por ende, el anexo 04 incluye una guía de auditoría para evaluar el nivel de alfabetización de la seguridad de la información de todos los usuarios.

5.3.3 Guías de auditoría para la gestión de la seguridad de la información

Las guías de auditoría propuestas fueron desarrolladas en hojas de cálculo, divididas por dominio y objetivos de control, además, tienen disponibles varios estados de cumplimiento como ejemplo demostrativo; las mismas pueden ser accedidas a través del programa general de auditoría mediante vínculos, el total corresponde a 34 guías de auditoría para la evaluación del sistema de gestión de la seguridad de la información, disponibles para revisión en el anexo 05 o en la dirección http://doi.org/10.5281/zenodo.3977213.

Capítulo 6. Conclusiones y recomendaciones

Seguidamente, se plantean las conclusiones del presente documento, en concordancia con el objetivo general y los correspondientes objetivos específicos planteados para el desarrollo de este. Por su parte, las recomendaciones corresponden a un conjunto de sugerencias para contribuir a las actividades de ejecución del trabajo llevado a cabo.

6.1 Conclusiones

Sobre la identificación de los estándares y mejores prácticas internacionales que sirven de marco de implementación y operación para el sistema de gestión de la seguridad de la información, se concluye:

- Existe una gran variedad de artículos que hacen referencia al estándar internacional ISO/IEC 27000 como el principal en la implementación y operación del sistema de gestión de la seguridad de la información, porque ofrece toda una familia de normas que facilitan su uso en diferentes entornos organizacionales, por ejemplo, la ISO/IEC 27001 ofrece los requisitos para la seguridad de la información y ISO/IEC 27002 ofrece el código de prácticas para la gestión de la seguridad de la información.
- Dentro de las mejores prácticas internacionales, se puede concluir que Cobit 5 para la seguridad de la información es una guía que ofrece las pautas para el gobierno y la gestión de las tecnologías de la información de la empresa, además, tiene como práctica de gobierno gestionar y mantener un SGSI.

Sobre la comprensión del proceso de auditoría para brindar una seguridad razonable de la eficacia y eficiencia del sistema de gestión de la seguridad de la información, se concluye:

- El proceso de auditoría, de manera general, conlleva tres fases: la planificación, ejecución y presentación de resultados; cada fase exige la preparación de instrumentos que direccionen las actividades de aseguramiento, así como seguir una metodología como la de Cobit 5 para el Aseguramiento, la cual contribuyó a comprender la estructura de una auditoría tomando en cuenta los objetivos, alcance y los criterios de la evaluación.

- Este documento toma en cuenta los requisitos de información que se deben obtener de la organización para la fase de planificación y diseña los instrumentos de verificación de manera genérica para el SGSI, requeridos para la fase de ejecución. La última fase de presentación de resultados no está incluida en esta propuesta.
- La auditoría es una actividad independiente que agrega valor mediante el hallazgo de oportunidades de mejora a los procesos y actividades de control, por ende, contribuye a la eficiencia y eficacia del sistema de gestión de la seguridad de la información, sin embargo, la organización no debe esperar que los resultados de la auditoría le digan qué hacer y cómo hacerlo.

Luego de comparar los diferentes estándares y mejores prácticas internacionales, para decidir cuáles elementos son aplicables al proceso de auditoría del sistema de gestión de la seguridad de la información, se concluye que:

- La comparación se realizó mediante un mapeo de estándares. Primeramente, se compararon los estándares ISO/IEC 27001 y 27002 de forma muy armoniosa, puesto que son complementarios y señalan muy claramente las líneas de acción, además, todos sus dominios son aplicables al proceso de auditoría, no obstante, el nivel de profundidad de un estudio dependería del objetivo y alcance de la auditoría.
- La comparación de ISO/IEC 27001 y 27002 con Cobit 5 Procesos Catalizadores permitió relacionar ambos marcos de trabajo parcialmente, puesto que los lineamientos en Cobit 5 son más generales y no existe una concordancia exacta, así que en algunas ocasiones se puede usar más de un proceso de Cobit 5 para cumplir con un dominio ISO/IEC 27001, pero no todas las actividades de Cobit 5 se aplican e inclusive algunos dominios no tienen prácticas de gestión con las cuales se pueda correlacionar.

Al desarrollar la guía de auditoría mediante un modelo práctico de hojas de cálculo adaptable a un amplio espectro de organizaciones, se concluye que:

- Las guías de auditoría desarrolladas se pueden aplicar mediante una hoja de cálculo para cada guía, donde se puede escoger entre varias opciones para el estado de cumplimiento. Este instrumento permite agregar o eliminar preguntas, así como ajustar el contenido a algún parámetro específico de la organización, además, contempla la generación de gráficos de cumplimiento para la representación de resultados obtenidos.
- Desde el programa general de auditoría, se puede seleccionar cada guía de auditoría según sea un estudio dirigido o completo.

Al clasificar la guía de auditoría por objetivos de control y controles, se concluye que:

- Las guías de auditoría están diseñadas en función de los objetivos de control y controles de ISO/IEC 27002, de modo que los criterios de evaluación de cada guía están ajustados a los procedimientos de implementación de cada dominio.

Luego de la propuesta de una guía de auditoría para el sistema de gestión de la seguridad de la información alineada a estándares y mejores prácticas internacionales, se concluye:

- Cada organización, que desee evaluar el nivel de cumplimiento de la seguridad de la información con base en el estándar ISO/IEC 27001 y las prácticas de gestión de la seguridad de la información de Cobit 5, puede aplicar las guías de auditoría propuestas y revisar si están siguiendo las mejores prácticas internacionales para proteger la información.
- Cada organización debe señalar el alcance de la auditoría, también debe proporcionar toda la información del estudio preliminar, para identificar los requisitos del negocio, políticas, procedimientos, las leyes y regulaciones pertinentes.
- Estas guías de auditoría contemplan las principales actividades de revisión de forma clara, sin ser exhaustivas.
- La auditoría de la seguridad de la información es de utilidad para respaldar las decisiones presupuestarias, inversiones y acciones correctivas referentes a la seguridad de la información de la organización.

6.2 Recomendaciones

Es importante que las organizaciones que deseen aplicar la guía de auditoría propuesta para el SGSI cuenten con la implementación del estándar ISO/IEC 27001, ya sea de forma parcial o completa. Por otra parte, deben seguir las buenas prácticas para la seguridad de la información de Cobit 5, de forma que los procedimientos de revisión de cada guía puedan ser atendidos.

Para mostrar los resultados de la ejecución de las guías de auditoría, es conveniente utilizar los gráficos incluidos dentro del modelo de hojas de cálculo, si se considera conveniente observar el comportamiento por objetivo o por dominio.

La guía de auditoría está dirigida a auditores en seguridad de la información o profesionales de las tecnologías de la información, por tanto, es recomendable estar familiarizado con las buenas prácticas esperadas de la implementación de la seguridad de la información dentro de la organización, para que la pericia del auditor facilite encontrar las deficiencias y aportar recomendaciones viables.

Es vital reconocer que la comprobación de cumplimiento pasa por la solicitud de evidencia al auditado y recomendar que este tipo de evaluaciones se realicen con los más altos grados de ética del profesional que ejecuta el aseguramiento.

Capítulo 7. Reflexiones finales

Para este proceso de aprendizaje, fue relevante el estudio de estándares internacionales de la familia ISO/IEC 27000 y los marcos de trabajo de Cobit 5, puesto que señalan las mejores prácticas para la seguridad de la información, independientemente del tamaño o tipo de entidad, además, marcan las directrices generales que deben implementar y seguir las organizaciones. Desde el punto de vista de la auditoría, contribuyeron a crear un instrumento que evalúa el cumplimiento de la seguridad de la información de manera operativa, pero que, al mismo tiempo, podría ser adaptado a las condiciones particulares de cada organización, dado que las normas sirven como modelo de referencia y reúnen las características esperadas para un sistema de gestión de la seguridad de la información.

A propósito de la importancia de las tecnologías de la información y la comunicación en la dinámica de los negocios, hace pensar que la protección de los datos impacta directamente en el logro de los objetivos y la continuidad del negocio, sin embargo, trae consigo otros riesgos, tales como el compromiso de la información, fallos técnicos, acciones no autorizadas, compromiso de las funciones laborales, entre otros. Entonces, se puede señalar que auditar es relevante para la gestión de las tecnologías de la información y la comunicación, con el fin de asegurar que no se introduzcan riesgos a niveles inaceptables en la implementación y operación de dichas tecnologías.

Además, con el aumento de nuevas tecnologías, vienen nuevas amenazas que hacen también necesario el aumento de profesionales en auditoría con conocimientos más calificados y especializados, por ejemplo, en la rama de la seguridad de la información o la ciberseguridad, se espera que este documento brinde un apoyo a esos profesionales.

Capítulo 8. Trabajos a futuro

Con el fin de dar continuidad a la idea de generar herramientas para el proceso de auditoría de la seguridad de la información, resultaría favorable conocer y desarrollar procedimientos para diferentes métodos y técnicas para la revisión de controles, sistemas, datos, transacciones, registros, prácticas de gestión, entre otros.

También se podrían desarrollar guías de auditoría para la seguridad de la información basadas totalmente en el marco de referencia Cobit 5 para la seguridad de la información y atender escenarios en los que solamente se tenga implementada esta práctica.

Todo estudio de auditoría forma parte de una actividad mayor de planeación, así que diseñar un plan anual de auditoría para la seguridad de la información de índole genérico, que sea aplicable a diferentes tipos y tamaños de organizaciones, resultaría favorable para entornos donde se cuente con poco personal o estén iniciando con este proceso.

Otro aspecto importante es revisar periódicamente las guías, con el fin de realizar los ajustes necesarios que puedan surgir del uso de estas y así mantenerlas lo más cercanas a la realidad cotidiana de los auditores.

En esta propuesta, se optó por usar hojas de cálculo para el diseño y aplicación de las guías de auditoría, no obstante, a futuro se podría desarrollar una solución de *software* para este fin, que incluya una generación automática de planes, resultados, papeles de trabajo e informes.

Por último, también se podría desarrollar una metodología para llevar a cabo estudios de auditoría en condiciones donde la presencia física del auditor resulte difícil por situaciones excepcionales o de emergencia, mientras que no se afecte la observancia de las fallas adaptando las prácticas actuales a plataformas como las virtuales o el trabajo remoto.

Referencias

Cortés, M. E. C., & León, M. I. (2005). *Generalidades sobre Metodología de la Investigación*. Universidad Autónoma del Carmen. Recuperado el 22 de marzo de 2020 de http://www.ucipfg.com/Repositorio/MIA/MIA-12/Doc/metodologia_investigacion.pdf

Christopher Anoruo, C. I. S. M., & CGEIT, C. (2019). COBIT FOCUS Employing COBIT 2019 for Enterprise Governance Strategy. Recuperado en 16 de marzo de 2020, de https://www.isaca.org/resources/news-and-trends/newsletters/cobit-focus/2019/employing-cobit-2019-for-enterprise-governance-strategy

Guirao Goris, Silamani J. Adolf. (2015). Utilidad y tipos de revisión literatura. *Ene*, *9*(2)https://dx.doi.org/10.4321/S1988-348X2015000200002, Recuperado el 16 de marzo de 2020, de http://scielo.isciii.es/scielo.php?script=sci_abstract&pid=S1988-348X2015000200002

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2006). Metodología de la investigación. Recuperado el 23 de marzo de 2020 de https://investigar1.files.wordpress.com/2010/05/1033525612-mtis_sampieri_unidad_1-1.pdf

ISO/IEC 27000:2018, Information technology – Security Techniques – Information Security Management Systems – Overview and vocabulary

Quintana Peña, A. (2006). Metodología de investigación científica cualitativa. Recuperado el 23 de marzo de http://biblioteca.udgvirtual.udg.mx:8080/jspui/handle/123456789/2724

Salgado Lévano, Ana Cecilia. (2007). Quality investigation: designs, evaluation of the methodological strictness and challenges. Liberabit, 13(13), 71-78. Recuperado en 24 de marzo de 2020, de http://www.scielo.org.pe/scielo.php?script=sci_arttext&pid=S1729-48272007000100009&lng=es&tlng=en

Vidal Ledo, María, Febles Rodríguez, Pedro, & Estrada Sentí, Vivian. (2007). Conceptual maps. *Educación Médica Superior*, *21*(3) Recuperado en 14 de

marzo de 2020, de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S0864-21412007000300011&lng=es&tlng=en

Bibliografía

Encalada Loja, C., & Cordero Guzmán, D. (2016). Guía de auditoría para la evaluación del control interno de seguridad de la información con enfoque COBIT 5: caso Universidad Católica de Cuenca (UCACUE). Revista Científica Y Tecnológica UPSE, 3(3), 113-121. https://doi.org/10.26423/rctu.v3i3.204. Recuperado el 08 de abril de 2020, de https://incyt.upse.edu.ec/ciencia/revistas/index.php/rctu/article/view/204

INTE/ ISO/IEC 27001:2014 Tecnología de la información —Técnicas de seguridad Sistemas de gestión de la seguridad de la información — Requisitos

ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls

ISACA. (2012). COBIT, Cobit 5 Procesos Catalizadores

ISACA. (2012). COBIT, Cobit 5 Para el Aseguramiento

Ruíz Hernández Rosibel. (2013). Propuesta de una guía de auditoría para evaluar el cumplimiento de la gestión de la seguridad de la información en el Ministerio de Educación Pública, de conformidad con las normas técnicas para la gestión y el control de las tecnologías de información (N-2-2007-CO-DFOE). Universidad de Costa Rica. Posgrado en Administración y Dirección de Empresas. Maestría Profesional en Auditoría de Tecnologías de Información, 2013. Recuperado el 05 de mayo de 2020 de http://www.kerwa.ucr.ac.cr/handle/10669/27693

Sheikhpour, R. y Modiri, N. (2012). Un enfoque para mapear los procesos COBIT a los controles de gestión de seguridad de la información ISO / IEC 27001. Revista Internacional de Seguridad y sus Aplicaciones, 6 (2), 13-28

Anexo 01

Tabla 3. Artículos relevantes de IEEE Xplore Digital Library

Ficha: 01	
Título:	A Model for Assessing COBIT 5 and ISO 27001 Simultaneously
Autor:	Rafael Almedia; Renato Lounrinho; Miguel Mira da Silva; Rubén Pereira
Cita:	R. Almeida, R. Lourinho, M. Mira da Silva and R. Pereira, "A Model for Assessing COBIT 5 and ISO 27001 Simultaneously," 2018 IEEE 20th Conference on Business Informatics (CBI), Vienna, 2018, pp. 60-69.
Enlace:	https://ieeexplore-ieee-org.ezproxy.sibdi.ucr.ac.cr/document/8452659
Cadena búsqueda	https://scholar.google.com/scholar?hl=en&as_sdt=1%2C5&as_ylo=2010&as_yhi=2020&as_vis=1&q=%22COBIT%22+and+%22ISO+27001%22&btnG=
Resultados de la revisión:	La revisión señala que los estándares son adoptados por las organizaciones con el fin de mejorar su competitividad o porque requieren cumplir con regulaciones obligatorias. Coindicen en que COBIT e ISO 27001 se encuentran entre las prácticas más adoptadas para proteger los activos de información. COBIT está diseñado para ser un marco único de gobernanza, así como para gestión y es la mejor opción para ser mapeado con ISO 27001 que tiene requisitos más detallados para hacer cumplir la seguridad de la información. Sin embargo, asumirlos simultáneamente implica un esfuerzo razonable.
Ficha: 02	
Título:	Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations
Autor:	Shamsul Sahibudin; Mohammad Sharifi; Masarat Ayat
Cita:	S. Sahibudin, M. Sharifi and M. Ayat, "Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations," 2008 Second Asia International Conference on Modelling & Simulation (AMS), Kuala Lumpur, 2008, pp. 749-753
Enlace:	https://ieeexplore-ieee-org.ezproxy.sibdi.ucr.ac.cr/document/4530569
Cadena de búsqueda:	https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=%22COBIT%22+and+%22ISO+27002%22&btnG=
Resultados de la revisión:	Este artículo señala que los marcos y estándares por sí solos no son suficientes, por lo tanto, propone un marco para integrarlos; primero analiza ITIL, COBIT e ISO 27002 individualmente. En COBIT hace referencia a los dominios de alto nivel, específicamente para este trabajo, resulta de valor señalar el dominio de Monitoreo y Evaluación, porque se enfoca en evaluar las necesidades de la

	organización y determinar si el sistema de gestión cumple o no con los objetivos para los que fue creado y si los controles cumplen los requisitos reglamentarios.
Ficha: 03	
Título:	ISO/IEC 27001 implementation in public organizations: A case study
Autores:	Bayona Sussy; Chauca Wilber; López Milagros; Maldonado Carlos
Cita:	B. Sussy, C. Wilber, L. Milagros and M. Carlos, "ISO/IEC 27001 implementation in public organizations: A case study," 2015 10th Iberian Conference on Information Systems and Technologies (CISTI), Aveiro, 2015, pp. 1-6
Enlace:	https://ieeexplore-ieee-org.ezproxy.sibdi.ucr.ac.cr/document/7170355
Cadena de búsqueda:	https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=%22ISO%2FIEC+27001+IMPLEMENTATION%22+&btnG=
Resultados de la revisión:	Señala la creciente dependencia de las tecnologías de la información para el éxito de las empresas y cómo se han convertido en un foco de ciberataques. Siendo la información el activo más importante de la organización, entonces, la implementación de un Sistema de Gestión de la Seguridad de la Información es una buena práctica para proteger la confidencialidad, integridad y disponibilidad de esta. Para este trabajo resultan relevantes los pasos del Ciclo Deming: Planear, Hacer, Verificar y Actuar, en especial los dos últimos pasos, porque la auditoría entra en la fase de verificar para que los hallazgos permitan tomar las acciones pertinentes. Además, propone seis factores críticos de éxito para SGSI, los cuales son relevantes durante un proceso de evaluación.
Ficha:04	
Título:	A Framework for Information Security Governance and Management
Autores:	Marian Carcary; Karen Renaud; Stephen McLaughlin; Conor O'Brien
Cita:	M. Carcary, K. Renaud, S. McLaughlin and C. O'Brien, "A Framework for Information Security Governance and Management," in IT Professional, vol. 18, no. 2, pp. 22-30, Mar.-Apr. 2016.
Enlace:	https://ieeexplore-ieee-org.ezproxy.sibdi.ucr.ac.cr/document/7436688
Cadena de búsqueda:	https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&as_ylo=2010&as_yhi=2020&q=%22framework+for+information+security%22&btnG=
Resultados de la revisión:	Del artículo se puede extraer la importancia de establecer un marco de medición para la madurez de la gobernanza y gestión de la seguridad de la información, con el fin de comprender el nivel de madurez de la organización para ir reduciendo brechas de cumplimiento. El marco propone los siguientes cinco niveles: inicial, básico, intermedio, avanzado y optimizado.

Ficha:05	
Título:	Governance Practices and Critical Success Factors Suitable for Business Information Security
Autores:	Yuri Bobbert; Hans Mulder
Cita:	Y. Bobbert and H. Mulder, "Governance Practices and Critical Success Factors Suitable for Business Information Security," 2015 International Conference on Computational Intelligence and Communication Networks (CICN), Jabalpur, 2015, pp. 1097-1104.
Enlace	https://ieeexplore-ieee-org.ezproxy.sibdi.ucr.ac.cr/document/7546267
Cadena de búsqueda:	https://scholar.google.com/scholar?start=40&q=%22governance%22+and+%22information+security%22&hl=en&as_sdt=0,5&as_ylo=2010&as_yhi=2020
Resultados de la revisión:	Este documento comprende un estudio del 2013 donde se muestra que la seguridad de la información se ha centrado en la seguridad operativa y menos en la gobernanza, políticas y continuidad del negocio. Por tanto, proponen una lista de las 20 mejores prácticas de gobierno críticas para el éxito de la seguridad de la información, dentro de las cuales resultan de interés para este trabajo: el control interno, determinar el apetito de riesgo, reportes regulares, evaluación periódica del conocimiento y seguridad como una parte integral.
Ficha:06	
Título:	Requirement and Potential for Modernizing IT Risk Universe in IT Audit Plan
Autores:	Bayu Rima Aditya; Ridi Ferdiana; Sri Suning Kusumawardani
Cita:	B. R. Aditya, R. Ferdiana and S. S. Kusumawardani, "Requirement and Potential for Modernizing IT Risk Universe in IT Audit Plan," 2018 2nd International Conference on Informatics and Computational Sciences (ICICoS), Semarang, Indonesia, 2018, pp. 1-5.
Enlace:	https://ieeexplore-ieee-org.ezproxy.sibdi.ucr.ac.cr/document/8621808
Cadena de búsqueda:	https://scholar.google.com/scholar?q=%22IT+AUDIT+PLAN%22&hl=en&as_sdt=0%2C5&as_ylo=2010&as_yhi=2020
Resultados de la revisión:	El enfoque actual de la auditoría de TI requiere construir un plan de auditoría basado en riesgos y diseñado para abordar los riesgos consistentes con los objetivos de la organización. Propone cuatro categorías de riesgo basadas de TI para la transformación digital, entre las cuales están: riesgos sociales, riesgos de movilidad, riesgos analíticos y riesgos en la nube, así que el programa de auditoría debe llevar incluido este tipo de riesgos.
Ficha:07	
Título	Toward Modern IT Audit- Current Issues and Literature Review
Autores:	Bayu Rima Aditya; Ridi Ferdiana; Paulus Insap Santosa

Cita:	B. R. Aditya, R. Ferdiana and P. I. Santosa, "Toward Modern IT Audit- Current Issues and Literature Review," 2018 4th International Conference on Science and Technology (ICST), Yogyakarta, 2018, pp. 1-6
Enlace:	https://ieeexplore-ieee-org.ezproxy.sibdi.ucr.ac.cr/document/8528627
Cadena de búsqueda:	https://scholar.google.com/scholar?start=20&q=allintitle:+%22IT+AUDIT%22&hl=en&as_sdt=0,5&as_ylo=2015&as_yhi=2020
Resultados de la revisión:	En esta investigación del 2018, se muestran varias razones del porqué la auditoría de TI ha recibido poca atención en la literatura académica y una de ellas es el complejo entorno de las organizaciones que conlleva a auditorías más complejas. Además, existe la percepción de que la auditoría de TI no ha proporcionado resultados tangibles o de valor y con frecuencia conducen a incorporar más proyectos de TI, así también las guías de auditoría tradicionales son difíciles de administrar y no se corresponden con una codificación estándar.

Origen: elaboración propia.

Tabla 4. Artículos relevantes de Springer Link

Ficha:01	
Título:	Information security management system standards
Autor:	Edward Humphreys
Cita:	Humphreys, E. DuD (2011) 35: 7. https://doi-org.ezproxy.sibdi.ucr.ac.cr/10.1007/s11623-011-0004-3
Enlace:	https://link-springer-com.ezproxy.sibdi.ucr.ac.cr/article/10.1007/s11623-011-0004-3
Cadena de búsqueda:	https://scholar.google.com/scholar?hl=en&as_sdt=1%2C5&as_ylo=2010&as_yhi=2020&as_vis=1&q=%22ISMS%22+or+%22Information+security+management+system%22&btnG=
Resultados de la revisión:	ISMS se origina a finales de los 80 y principios de los 90 en Reino Unido, con BS 7799-1 y BS 7799-2 se fue extendiendo y adoptando por varios países. En el 2000 fue enviado a ISO/IEC y fue publicado con el nombre ISO/IEC 17799; en el 2006 fue renombrado ISO/IEC 27002, después el BS 7799-2 se introdujo en ISO y fue renombrado ISO/IEC 27001.
Ficha:02	
Título:	The Future Landscape of ISMS Standards
Autor:	Edward Humphreys

Cita:	Humphreys, E. Datenschutz Datensich (2018) 42: 421. https://doi-org.ezproxy.sibdi.ucr.ac.cr/10.1007/s11623-018-0971-8
Enlace:	https://link-springer-com.ezproxy.sibdi.ucr.ac.cr/article/10.1007/s11623-018-0971-8
Cadena de búsqueda:	https://scholar.google.com/scholar?start=10&q=%22ISMS%22+source:Springer&hl=en&as_sdt=1,5&as_ylo=2010&as_yhi=2020&as_vis=1
Resultados de la revisión:	El ISMS sobre el cual se han desarrollado una familia de estándares es el ISO/IEC 27001, cuyo diseño ha sido aplicable a organizaciones de todo tipo, tamaño y complejidad. Las organizaciones se enfrentan a cambios de mercado, nuevas amenazas y riesgos, así como retos para adaptarse a los tecnologías disruptivas, cambios tecnológicos e innovaciones, así que el ISMS puede actualizarse para cumplir estas demandas mediante un proceso de mejora continuo y monitoreo de seguridad. En la actualidad, este estándar continúa en expansión, sin embargo, a medida que surjan nuevos riesgos, será necesario realizar una revisión y actualizarlo para cumplir con los nuevos desarrollos tecnológicos o sectores específicos de aplicación.
Ficha:03	
Título:	Standardization in information security management
Autor:	A. M. Fal’
Cita:	Fal’, A.M. Standardization in information security management. Cybern Syst *Anal* 46**,** 512–515 (2010). https://doi-org.ezproxy.sibdi.ucr.ac.cr/10.1007/s10559-010-9227-9
Enlace:	https://link-springer-com.ezproxy.sibdi.ucr.ac.cr/article/10.1007/s10559-010-9227-9
Cadena de búsqueda:	https://scholar.google.com/scholar?as_q=Information+security+management+system&as_epq=&as_oq=&as_eq=&as_occt=any&as_sauthors=&as_publication=Springer&as_ylo=2010&as_yhi=2020&hl=en&as_sdt=1%2C5&as_vis=1

Resultados de la revisión:	Este artículo describe los estándares de la gestión de la seguridad de la información desarrollados por el subcomité SC27 Security Techniques de ISO/IEC JTC 1 Tecnología de la Información, en los cuales la protección de la información es para la información en todas sus formas (escrita o impresa en papel o en medios electrónicos, transmitida por correo ordinario, email, video o voz). Se muestra que los modelos más adoptados son el Plan-Do-Check-Act y el modelo de procesos. Además, se hace una revisión de la familia de estándares ISO/IEC 27000 desde el ISO/IEC 27001 hasta el ISO/IEC 27037; es de interés para este trabajo considerar el ISO/IEC 27002 que describe los códigos de práctica para la seguridad de la información que se deben revisar durante un proceso de verificación, cumplimiento y el ISO/IEC 27007 que establece las directrices para la auditoría del SGSI.

Origen: elaboración propia.

Tabla 5. Artículos relevantes de Semantic Scholar

Ficha:01	
Título:	A Practical Model to Perform Comprehensive Cybersecurity Audits
Autor:	Regner Sabillon
Cita:	Sabillon, R. (2018). A Practical Model to Perform Comprehensive Cybersecurity Audits
Enlace:	https://www.semanticscholar.org/paper/A-Practical-Model-to-Perform-Comprehensive-Audits-Sabillon/0e198c8105005bc3c62241fb6545cfc702c42b64
Cadena de búsqueda:	https://scholar.google.com/scholar?start=10&q=%22cybersecurity+audit%22&hl=en&as_sdt=0,5
Resultados de la revisión:	Este artículo presenta el Modelo de Auditoría de Ciberseguridad CSAM, contiene 18 dominios, 26 subdominios, 87 listas de chequeo, 80 pautas de evaluación y un cuadro de evaluación, sin embargo, en el documento solo se hace mención a los mismos. La evaluación propone un rango de cumplimiento de 0 a 100, asignando puntuación según el nivel de madurez, los cuales son inmaduro (0-30), en desarrollo (31-70), maduro (71-90) y avanzado (91-100). Este modelo se puede usar en auditorías únicas de ciberseguridad o puede ser parte de un programa de auditoría para controles de ciberseguridad.
Ficha:02	
Título:	Information Security Management System Standards: A Comparative Study of the Big Five
Autores:	Heru Susanto; Mohammad Nabil Almunawar; Chee Tuan

Cita:	Susanto, H., Almunawar, M.N., & Tuan, Y.C. (2011). Information Security Management System Standards: A Comparative Study of the Big Five.
Enlace:	https://www.semanticscholar.org/paper/Information-Security-Management-System-Standards-%3A-Susanto-Almunawar/1b583de114c74c7480e25eac6fee348af980d627
Cadena de búsqueda:	https://www.semanticscholar.org/search?year%5B0%5D=2010&year%5B1%5D=2020&q=Information%20Security%20Management%20System%20Standard&sort=relevance
Resultados de la revisión	Este artículo hace una comparación de cinco estándares para la seguridad de la información, los cuales resuelven problemas desde diferentes vértices, estos son ISO 27001, BS7799, PCIDSS, ITIL y COBIT; se proponen 11 ítems de comparación donde en su mayoría cumple con las especificaciones, además, se muestra un gráfico donde ISO 27001 es el estándar más utilizado globalmente para la seguridad de la información, seguido de COBIT para la gobernanza.

Origen: elaboración propia.

Tabla 6. Artículos relevantes de ACM DIGITAL LIBRARY

Ficha:01	
Título:	Main Considerations in Elaborating Organizational Information Security Policies
Autores:	Todor Tagarev; Dimitrina Polimirova
Cita:	Todor Tagarev and Dimitrina Polimirova. 2019. Main Considerations in Elaborating Organizational Information Security Policies. In Proceedings of the 20th International Conference on Computer Systems and Technologies (CompSysTech '19). Association for Computing Machinery, New York, NY, USA, 68–73. DOI:https://doi.org/10.1145/3345252.3345302
Enlace:	https://dl-acm-Org.ezproxy.sibdi.ucr.ac.cr/doi/abs/10.1145/3345252.3345302
Cadena de búsqueda:	https://dl.acm.org/action/doSearch?AllField=information+security+policies
Resultados de la revisión:	Este artículo revela los conceptos de seguridad de la información y ciberseguridad, así como cuáles consideraciones deben tomar en cuenta organizaciones pequeñas como centros educativos y organizaciones públicas a la hora de diseñar una política de seguridad. Primeramente, hace una revisión de estándares como COBIT y ISO 27001. Para después proponer una lista de políticas distribuidas en las siguientes áreas: políticas generales, personas, *hardware, software, e-services* y manejo de incidentes, siempre y cuando

	consideren un monitoreo continuo de panorama de amenazas y vulnerabilidades.
Ficha:02	
Título:	A new comprehensive solution to handle information security Governance in organizations
Autores:	Zaydi Mounia; Nassereddine Bouchaib
Cita:	Zaydi Mounia and Nassereddine Bouchaib. 2019. A new comprehensive solution to handle information security Governance in organizations. In Proceedings of the 2nd International Conference on Networking, Information Systems & Security (NISS19). Association for Computing Machinery, New York, NY, USA, Article 50, 1–5. DOI:https://doi.org/10.1145/3320326.3320382
Enlace:	https://dl-acm-org.ezproxy.sibdi.ucr.ac.cr/doi/abs/10.1145/3320326.3320382
Cadena de búsqueda:	https://dl.acm.org/action/doSearch?AllField=Information+System+Security+Management%2C+ITIL%2C+ISO+%2C+ISO+27001
Resultados de la revisión	Este documento propone la unión de ITIL, ISO 38500 procesos y ISO 27001 controles, donde ITIL e ISO señalan la necesidad de fortalecer la seguridad para los aspectos de servicio y gestionar riesgos de infraestructura, mientras que ISO 38500 señala la necesidad de un marco de gobernanza de TI. El modelo consiste en cuatro ejes de integración, primeramente, gobernanza (integra estrategia de servicio, diseño de servicio, contexto de la organización, liderazgo, planeamiento, soporte); monitoreo (integra transición de servicio, operación de servicio, operaciones); evaluación (integra servicio de mejora continua y evaluación de desempeño), por último, supervisar e informar (integra servicios de mejora continua y mejora).

Origen: elaboración propia.

Tabla 7. Artículos relevantes de IOP SCIENCE

Ficha:01	
Título:	The Use of ISO and COBIT for IT Governance Audit
Autores:	Y Aprilinda; A K Puspa; F N Affandy
Cita:	Y Aprilinda et al 2019 J. Phys.: Conf. Ser. 1381 012028
Enlace:	https://iopscience.iop.org/article/10.1088/1742-6596/1381/1/012028/meta
Cadena de búsqueda:	https://scholar.google.com/scholar?start=30&q=%22COBIT%22+and+%22ISO+27001%22&hl=en&as_sdt=1,5&as_ylo=2010&as_yhi=2020&as_vis=1
Resultados de la revisión:	Este artículo discute la fusión de COBIT e ISO en el gobierno corporativo, señala que COBIT es el más popular para ser usado en auditorías, sin embargo, su complejidad limita la frecuencia de las mismas. COBIT evalúa qué tan buena es

	la gestión de TI en una organización, por lo general, es un marco para ser usado a nivel estratégico y de toma de decisiones. COBIT necesita incluir estándares adicionales como ISO, el cual es un marco más específico y detallado para ser usado a nivel operativo. En la práctica se pueden usar juntos y complementarse entre sí.
Ficha:02	
Título:	The Role of IT Audit in the Era of Digital Transformation
Autores:	BR Aditya: R Hartanto; LE Nugroho
Cita:	B R Aditya et al 2018 IOP Conf. Ser: Mater. Sci. Eng. 407 012164
Enlace:	https://iopscience.iop.org/article/10.1088/1757-899X/407/1/012164
Cadena de búsqueda:	https://scholar.google.com/scholar?start=10&q=%22IT+AUDIT%22&hl=en&as_sdt=0,5&as_ylo=2015&as_yhi=2020
Resultados de la revisión:	La transformación digital ha cambiado la forma en la que se ve la auditoría de TI, en otras palabras, la auditoría de TI actual debe contribuir al mejoramiento de las funciones de la organización, integrando las nuevas tecnologías, con prácticas de auditoría global, atendiendo el creciente aumento en los requisitos y regulaciones. Por lo tanto, la alta dirección debe entender el papel de la auditoría de TI, definiendo un universo de esta con referencia a un marco existente o creando su propio universo de auditoría de TI adaptado a sus necesidades. No se puede dar un carácter universal a la auditoría de TI, porque cada universo de esta tiene diferentes características, ya que las necesidades de personal, costo, complejidad del riesgo y metodología de auditoría de TI diferirán entre sí.
Ficha:03	
Título	IT Audit Guidance: Side by Side Comparison
Autores:	B R Aditya1 and Y Menzelthe
Cita:	B R Aditya and Y Menzelthe 2019 IOP Conf. Ser.: Mater. Sci. Eng. 662 022055
Enlace:	https://iopscience.iop.org/article/10.1088/1757-899X/662/2/022055/meta
Cadena de búsqueda:	https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&as_ylo=2010&as_yhi=2020&q=ISO+27007+and+ISO+27008+and+Audit&btnG=
Resultados de la revisión:	Este artículo hace una comparación de las ocho principales guías de auditoría que se pueden usar para dar dirección al proceso de auditoría sistemático de las tecnologías de la información; propone una evaluación cualitativa para otorgar el nivel de relevancia, en la clasificación muy alto están ITAF, GTAF y Programas de auditoría; en alto se destacan Guía de aseguramiento de TI usando COBIT, ISO 27007 e ISO 27008, Trust Service Criteria; para la

	calificación baja está ISO 20000 y ITIL. Es importante para el auditor comprender la dirección de auditoría de TI necesaria y su adecuación a los objetivos de la auditoría que se lleve a cabo. No obstante, todavía hay dificultades a la hora de elegir la guía de auditoría que se utilizará para definir el universo de auditoría de TI.

Origen: elaboración propia.

Anexo 02

Tabla 9. Mapeo de objetivos de control de ISO/IEC 27001

ISO/IEC 27001		
Dominios		Objetivos
A.5 Políticas de seguridad de la información	A.5.1 Dirección de la gestión para la seguridad de la información	Proporcionar dirección de la gestión y soporte para la seguridad de la información, de acuerdo con los requisitos del negocio y con las regulaciones y leyes pertinentes.
A.6 Organización de la seguridad de la información	A.6.1 Organización interna	Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de seguridad de la información dentro de la organización.
	A.6.2 Dispositivos móviles y teletrabajo	Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.
A.7 Seguridad ligada a los recursos humanos	A.7.1 Previo al empleo	Asegurar que los empleados y contratistas entiendan sus responsabilidades, y que sean aptos para los roles para los cuales están siendo considerados.
	A.7.2 Durante el empleo	Asegurar que los empleados y contratistas sean conscientes y cumplan con sus responsabilidades de seguridad de la información.
	A.7.3 Finalización o cambio de empleo	Proteger los intereses de la organización como parte del proceso de finalización o cambio de empleo.
A.8 Gestión de activos	A.8.1 Responsabilidad por los activos	Identificar los activos de la organización y definir las responsabilidades para la apropiada protección.
	A.8.2 Clasificación de la información	Asegurar que la información recibe un nivel de protección apropiado, de acuerdo con su importancia para la organización.

	A.8.3 Manejo de los medios	Prevenir la divulgación, modificación, remoción o destrucción no autorizada de la información almacenada en los medios.
A.9 Control de acceso	A.9.1 Requisitos del negocio para el control de acceso	Limitar el acceso a la información y a los recursos de procesamiento de la información.
	A.9.2 Gestión del acceso de usuarios	Asegurar el acceso autorizado de los usuarios y evitar el acceso no autorizado a los sistemas y servicios.
	A.9.3 Responsabilidades de los usuarios	Hacer responsables a los usuarios de salvaguardar su información de autenticación.
	A.9.4 Control de acceso a sistemas y aplicaciones	Prevenir el acceso no autorizado a los sistemas y aplicaciones.
A.10 Criptografía	A.10.1 Controles de criptografía	Asegurar del uso apropiado y efectivo de la criptografía para proteger la confidencialidad, autenticidad o la integridad de la información.
A.11 Seguridad física y ambiental	A.11.1 Áreas seguras	Prevenir el acceso físico no autorizado, daños e interferencia a la información y a los recursos de procesamiento de la información de la organización.
	A.11.2 Equipo	Prevenir la pérdida, daño, robo o compromiso de los activos y la interrupción de las operaciones de la organización.
A.12 Seguridad de las operaciones	A.12.1 Procedimientos y responsabilidades operacionales	Asegurarse de las operaciones correctas y seguras de los recursos de procesamiento de la información.
	A.12.2 Protección contra código malicioso (*malware*)	Asegurar que las instalaciones de procesamiento de información y la información están protegidas contra el código malicioso.
	A.12.3 Respaldo	Proteger contra la pérdida de datos.

	A.12.4 Registro y seguimiento	Registrar los eventos y generar evidencia.
	A.12.5 Control de *software* operativo	Asegurar la integridad de los sistemas operativos.
	A.12.6 Gestión de vulnerabilidades técnicas	Prevenir la explotación de vulnerabilidades técnicas.
	A.12.7 Consideraciones de auditoría de sistemas de información	Minimizar el impacto de las actividades de auditoría en los sistemas en operación.
A.13 Seguridad de las comunicaciones	A.13.1 Gestión de seguridad de la red	Asegurar la protección de la información en las redes y sus recursos de soporte de procesamiento de información.
	A.13.2 Transferencia de información	Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.
A.14 Adquisición, desarrollo y mantenimiento de sistemas	A.14.1 Requisitos de seguridad de sistemas de información	Asegurar que la seguridad de la información sea parte integral de los sistemas de información a través de todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcionan los servicios a través de redes públicas.
	A.14.2 Seguridad en los procesos de desarrollo y soporte	Asegurar que la seguridad de la información sea diseñada e implementada dentro del ciclo de vida del desarrollo de sistemas de información.
	A.14.3 Pruebas de datos	Asegurar la protección de los datos utilizados para la prueba.
A.15 Relaciones con los proveedores	A.15.1 Seguridad de la información en la relación con los proveedores	Asegurar la protección de los activos de la organización que son accesibles por los proveedores.
	A.15.2 Gestión de la entrega de servicios del proveedor	Mantener un nivel acordado de seguridad de la información y la

		entrega de servicios alineada con los acuerdos con proveedores.
A.16 Gestión de incidentes de seguridad de la información	A.16.1 Gestión de incidentes y mejoras en la seguridad de la información	Asegurar que se aplique un enfoque coherente y efectivo para la gestión de los incidentes de seguridad de la información, incluyendo la comunicación de los eventos y debilidades de seguridad.
A.17 Aspectos de seguridad de la información en la gestión de la continuidad del negocio	A.17.1 Continuidad de la seguridad de la Información	La continuidad de la seguridad de la información debe ser integrada en los sistemas de gestión de la continuidad de negocio de la organización.
	A.17.2 Redundancias	Asegurar la disponibilidad de los recursos de procesamiento de información.
A.18 Cumplimiento	A.18.1 Cumplimiento de los requisitos legales y contractuales	Evitar brechas entre las obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con seguridad de la información y cualquier requisito de seguridad.
	A.18.2 Revisión de seguridad de la información	Asegurar que la seguridad de la información sea implementada y opere de acuerdo con las políticas y procedimientos de la organización.

Origen: elaboración propia a partir del Anexo “A” del estándar ISO/IEC 27001.

Anexo 03

Tabla 10. Mapeo ISO/IEC 27001, ISO/IEC 27002 y Cobit 5

Mapeo ISO/IEC 27001, ISO/IEC 27002 y COBIT 5			
	ISO/IEC 27001 Dominios	ISO/IEC 27002 Controles	Cobit 5 Práctica gestión
Políticas de seguridad	A.5.1.1 Políticas para la seguridad de la información. A.5.1.2 Revisión de las políticas para la seguridad de la información.	5.1.1 Políticas para la seguridad de la información. 5.1.2 Revisión de las políticas de seguridad de la información.	APO01.04 Comunicar los objetivos y la dirección de gestión. APO01.08 Mantener el cumplimiento con las políticas y procedimientos. APO13.01 Establecer y mantener un SGSI. APO13.03 Supervisar y revisar el SGSI.
Organización de la seguridad de la información	A.6.1.1 Roles y responsabilidades de seguridad de la información. A.6.1.2 Segregación de funciones. A.6.1.3 Contacto con autoridades. A.6.1.4 Contacto con grupos de interés especial. A.6.1.5 Seguridad de la información en gestión de proyectos. A.6.2.1 Política de dispositivo móvil. A.6.2.2 Teletrabajo.	6.1.1 Asignación de responsabilidades sobre seguridad de la información. 6.1.2 Segregación de tareas. 6.1.3 Contacto con autoridades. 6.1.4 Contacto con grupos de interés especial. 6.2.5 Seguridad de la información en gestión de proyectos. 6.2.1 Política de dispositivo móvil. 6.2.2 Teletrabajo.	APO01.06 Definir la propiedad de la información (datos) y del sistema. APO01.04 Comunicar los objetivos y la dirección de gestión. APO13.01 Establecer y mantener un SGSI DSS05.02 Gestionar la seguridad de la red y las conexiones. DSS05.03 Gestionar la seguridad de los puestos de usuario final. DSS05.04 Gestionar la identidad del usuario y el acceso lógico.

Seguridad ligada a los recursos humanos	Previo al empleo A.7.1.1 Investigación. A.7.1.2 Términos y condiciones del empleo durante la contratación. A.7.2.1 Responsabilidades de la dirección. A.7.2.2 Toma de conciencia educación y formación en seguridad de la información. A.7.2.3 Proceso disciplinario finalización o cambio de empleo. A.7.3.1 Finalización o cambio de empleo.	A.7.1.1 Investigación de antecedentes. A.7.1.2 Términos y condiciones de contratación. 7.2.1. Responsabilidades de gestión. 7.2.2 Concientización, educación y capacitación en seguridad de la información. A.7.2.3 Proceso disciplinario. 7.3.1 Cese o cambio de puesto de trabajo.	APO01.02 Establecer roles y responsabilidades. DSS05.05 Gestionar el acceso físico a los activos de TI.
Gestión de activos	A.8.1 Responsabilidad por los activos. A.8.1.2 Propiedad de los activos. A.8.1.3 Uso aceptable de los activos. A.8.1.4 Devolución de activos. A.8.2.1 Clasificación de la información. A.8.2.2 Etiquetado de la información. A.8.2.3 Manejo de los activos. A.8.3.1 Gestión de medios removibles.	8.1.1 Inventario de activos. 8.1.2 Propiedad de los activos. 8.1.3 Uso aceptable de los activos. 8.1.4 Devolución de activos. 8.2.1 Directrices de clasificación. 8.2.2 Etiquetado y manejo de la información. 8.2.3 Manipulación de activos. 8.3.1 Gestión de soportes extraíbles.	APO01.06 Definir la propiedad de la información (datos) y del sistema. DSS05.03 Gestionar la seguridad de los puestos de usuario final. DSS05.06 Gestionar documentos sensibles y dispositivos de salida.

	A.8.3.2 Eliminación de medios. A.8.3.3 Traslado de medios físicos.	8.3.2 Eliminación de soportes. 8.3.3 Soportes físicos en tránsito.	
Control de acceso	A.9.1.1 Política de control de acceso. A.9.1.2 Acceso a redes y servicios de red. A.9.2.1 Registro y cancelación de registro de usuarios. A.9.2.2 Aprovisionamiento de acceso a usuarios. A.9.2.3 Gestión de derechos de acceso privilegiados. A.9.2.4 Gestión de la información secreta de autenticación de usuarios. A.9.2.5 Revisión de los derechos de acceso de los usuarios. A.9.2.6 Eliminación o ajuste de los derechos de acceso. A.9.3.1. Uso de la información secreta de autenticación. A.9.4.1 Restricción de acceso a la información. A.9.4.2 Procedimientos de accesos (logon) seguros. A.9.4.3 Sistema de gestión de contraseñas.	9.1.1 Política de control de accesos. 9.1.2. Control de acceso a las redes y servicios asociados. 9.2.1 Gestión de altas/bajas en el registro de usuarios. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.2.4 Gestión de información confidencial de autenticación de usuarios. 9.2.5 Revisión de los derechos de acceso de los usuarios. 9.2.6 Retirada o adaptación de los derechos de acceso. 9.3.1 Uso de información confidencial para la autenticación. 9.4.1 Restricción del acceso a la información. 9.4.2 Procedimientos seguros de inicio de sesión. 9.4.3 Gestión de contraseñas de usuario.	APO01.04 Comunicar los objetivos y la dirección de gestión. DSS05.02 Gestionar la seguridad de la red y las conexiones. DSS05.04 Gestionar la identidad del usuario y el acceso lógico. DSS05.05 Gestionar el acceso físico a los activos de TI.

	A.9.4.4 Uso de programas utilitarios privilegiados. A.9.4.5 Control de acceso al código fuente de programas.	9.4.4 Uso de herramientas de administración de sistemas. 9.4.5 Control de acceso al código fuente de programas.	
Criptografía	A.10.1.1 Política sobre el uso de controles criptográficos. A.10.1.2 Gestión de llaves.	10.1.1 Política de uso de controles criptográficos. 10.1.2. Gestión de claves.	
Seguridad física y ambiental	A.11.1.1 Perímetro de seguridad física. A.11.1.2 Controles de entrada física. A.11.1.3 Aseguramiento de oficinas, salas e instalaciones. A.11.1.4 Protección contra amenazas externas y ambientales. A.11.1.5 Trabajando en áreas seguras. A.11.1.6 Áreas de entrega y carga. A.11.2.1 Colocación y protección del equipo. A.11.2.2 Servicios de soporte. A.11.2.3 Seguridad del cableado. A.11.2.4 Mantenimiento del equipo. A.11.2.5 Remoción de activos.	11.1.1 Perímetro de seguridad física. 11.1.2 Controles de entrada física. 11.1.3 Seguridad de oficinas, despachos y recursos. 11.1.4 Protección contra las amenazas externas y del ambiente. 11.1.5 El trabajo en áreas seguras. 11.1.6 Áreas de acceso público, carga y descarga. 11.2.1 Emplazamiento y protección de equipos. 11.2.2 Instalaciones de suministro. 11.2.3 Seguridad del cableado. 11.2.4 Mantenimiento de los equipos. 11.2.5 Salida de activos fuera de las dependencias de la empresa.	DSS05.03 Gestionar la seguridad de los puestos de usuario final. DSS05.05 Gestionar el acceso físico a los activos de TI.

	A.11.2.6 Seguridad del equipo y los activos fuera de las instalaciones. A.11.2.7 Seguridad en la eliminación o reutilización del equipo. A.11.2.8 Equipo desatendido por el usuario. A.11.2.9 Política de pantalla y escritorio limpios.	11.2.6 Seguridad del equipo y los activos fuera de las instalaciones. 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento. 11.2.8 Equipo informático de usuario desatendido. 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.	
Seguridad de las operaciones	A.12.1.1 Procedimientos de operación documentados. A.12.1.2 Gestión de cambios. A.12.1.3 Gestión de la capacidad. A.12.1.4 Separación de ambientes de desarrollo, pruebas y operación. A.12.2.1 Controles contra el código malicioso. A.12.3.1 Respaldo de la información. A.12.4.1 Registro de eventos. A.12.4.2 Protección del registro de información. A.12.4.3 Registros del administrador y el operador. A.12.4.4 Sincronización de reloj.	12.1.1 Documentación de procedimientos de operación. 12.1.2 Gestión de cambios. 12.1.3 Gestión de capacidades. 12.1.4 Separación de entornos de desarrollo, prueba y producción. 12.2.1 Controles contra el código malicioso. 12.3.1 Copias de seguridad de la información. 12.4.1 Registro y gestión de eventos de actividad. 12.4.2 Protección de los registros de información. 12.4.3 Registros del administrador y el operador del sistema. 12.4.4 Sincronización de relojes.	APO01.04 Comunicar los objetivos y la dirección de gestión. DSS05.01 Proteger contra *software* malicioso (*malware*). DSS05.04 Gestionar la identidad del usuario y el acceso lógico. DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.

	A.12.5.1 Instalación de *software* en los sistemas en operación. A.12.6.1 Gestión de vulnerabilidades técnicas. A.12.6.2 Restricciones en la instalación de *software.* A.12.7.1 Controles de auditoría de sistemas de información.	12.5.1 Instalación del *software* en sistemas en producción. 12.6.1 Gestión de vulnerabilidades técnicas. 12.6.2 Restricciones en la instalación de *software*. 12.7.1 Controles de auditoría de sistemas de información.	
Seguridad de las comunicaciones	A.13.1.1 Controles de red. A.13.1.2 Seguridad de los servicios de red. A.13.1.3 Segregación en las redes. A.13.2.1 Políticas y procedimientos de transferencia de información. A.13.2.2 Acuerdos de transferencia de información. A.13.2.3 Mensajería electrónica. A.13.2.4 Acuerdos de confidencialidad o no divulgación.	13.1.1 Controles de red. 13.1.2 Mecanismo de seguridad asociados a servicios en red. 13.1.3 Segregación de redes. 13.2.1 Políticas y procedimientos de intercambio de información. 13.2.2 Acuerdos de intercambio. 13.2.3 Mensajería electrónica. 13.2.4 Acuerdos de confidencialidad y secreto.	APO01.04 Comunicar los objetivos y la dirección de gestión. DSS05.02 Gestionar la seguridad de la red y las conexiones.
Adquisición, desarrollo y mantenimiento de sistemas	A.14.1.1 Análisis y especificación de los requisitos de seguridad de la información. A.14.1.2 Asegurar los servicios de aplicaciones en las redes públicas.	14.1.1 Análisis y especificación de los requisitos de seguridad. 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.	APO01.04 Comunicar los objetivos y la dirección de gestión.

	A.14.1.3 Protección de las transacciones de servicios de aplicación.	14.1.3 Protección de las transacciones por redes telemáticas.	
	A.14.2.1 Política de desarrollo seguro.	14.2.1 Política de desarrollo seguro de *software.*	
	A.14.2.2 Procedimientos de control de cambios del sistema.	14.2.2 Procedimientos de control de cambios en los sistemas.	
	A.14.2.3 Revisión técnica de las aplicaciones después de realizar cambios de plataforma de operación.	14.2.3 Revisión técnica de las aplicaciones tras efectuar en el sistema operativo.	
	A.14.2.4 Restricciones en los cambios a los paquetes de *software.*	14.2.4 Restricciones a los cambios en los paquetes de *software.*	
	A.14.2.5 Principios de ingeniería de sistemas seguros.	14.2.5 Uso de principios de ingeniería en protección de sistemas.	
	A.14.2.6 Ambiente de desarrollo seguro.	14.2.6 Seguridad en entornos de desarrollo.	
	A.14.2.7 Desarrollo contratado externamente.	14.2.7 Externalización del desarrollo de *software.*	
	A.14.2.8 Pruebas de seguridad de sistemas.	14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.	
	A.14.2.9 Pruebas de aceptación del sistema.	14.2.9 Pruebas de aceptación.	
	A.14.3.1 Protección de los datos de prueba.	14.3.1 Protección de los datos utilizados en pruebas.	

Relaciones con los proveedores	A.15.1.1 Política de seguridad de la información para las relaciones con los proveedores. A.15.1.2 Abordar la seguridad dentro de los acuerdos de proveedores. A.15.1.3 Cadena de suministro de tecnologías de información y comunicaciones. A.15.2.1 Seguimiento y revisión de los servicios de proveedores. A.15.2.2 Gestión de cambios en los servicios de proveedores.	15.1.1 Política de seguridad de la información para suministradores. 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores. 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones. 15.2.1 Supervisión y revisión de los servicios prestados por terceros. 15.2.2 Gestión de cambios en los servicios prestados por terceros.	APO01.04 Comunicar los objetivos y la dirección de gestión. DSS05.05 Gestionar el acceso físico a los activos de TI.
Gestión de incidentes de seguridad de la información	A.16.1.1 Responsabilidades y procedimientos. A.16.1.2 Reporte de eventos de seguridad de la información. A.16.1.3 Reporte de debilidades de seguridad de la información. A.16.1.4 Evaluación y decisión sobre los eventos de seguridad de la información. A.16.1.5 Respuesta a incidentes de seguridad de la información. A.16.1.6 Aprendiendo de los incidentes de seguridad información.	16.1.1 Responsabilidades y procedimientos 16.1.2 Notificación de los eventos de seguridad de la información. 16.1.3 Notificación de puntos débiles de la seguridad. 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones. 16.1.5 Respuesta a los incidentes de seguridad. 16.1.6 Aprendizaje de los incidentes de seguridad de la información.	APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información. APO13.03 Supervisar y revisar el SGSI. DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.

	A.16.1.7 Recolección de evidencia.	16.1.7 Recopilación de evidencias.	
Seguridad de la información en la gestión de la continuidad del negocio	A.17.1.1 Planificación de la continuidad de seguridad de la información. A.17.1.2 Implementación de la continuidad de seguridad de la información. A.17.1.3 Verificar, revisar y evaluar la continuidad de seguridad de la información. A.17.2.1 Disponibilidad de recursos de procesamiento de información.	17.1.1 Planificación de la continuidad de la seguridad de la información. 17.1.2 Implantación de la continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de la continuidad de seguridad de la información. 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.	DSS04.03 Desarrollar e implementar una respuesta la continuidad del negocio. DSS04.04 Ejercitar, probar y revisar el plan de continuidad. DSS04.07 Gestionar acuerdos de respaldo.
Cumplimiento	A.18.1.1 Identificación de la legislación aplicable y los requisitos contractuales. A.18.1.2 Derechos de propiedad intelectual. A.18.1.3 Protección de registros. A.18.1.4 Privacidad y protección de datos personales. A.18.1.5 Regulación de los controles criptográficos. A.18.2.1 Revisiones independientes de	18.1.1 Identificación de la legislación aplicable. 18.1.2 Derechos de propiedad intelectual. 18.1.3 Protección de los registros de la organización. 18.1.4 Protección de los datos y privacidad de la información personal. 18.1.5 Regulación de los controles criptográficos. 18.2.1 Revisión independiente de la seguridad de la información.	APO01.08 Mantener el cumplimiento con las políticas y procedimientos. APO13.03 Supervisar y revisar el SGSI.

	seguridad de la información. A.18.2.2 Cumplimiento con las políticas y normas de seguridad. A.18.2.3 Revisiones de cumplimiento técnico.	18.2.2 Cumplimiento de las políticas y normas de seguridad. 18.2.3 Comprobación de cumplimiento.	

Origen: elaboración propia a partir de las normas ISO/IEC 27001 e ISO/IEC 27002 y Cobit 5.

Anexo 04

Alfabetización de la seguridad de la información dentro de la organización

AUD-SGSI-35-2020	**Guía de Auditoría** **Evaluación del Sistema de Gestión de la Seguridad de la Información**		
Nombre de la organización evaluada:			
Área evaluada:		**Fecha:**	
Responsable de la evaluación:			
Objetivo:	Indagar sobre el nivel de alfabetización de la seguridad de la información en los usuarios de la organización.		
Dominio ISO/IEC 27001: A.7 Seguridad ligada a los recursos humanos			
Guía de referencia ISO/IEC 27002: 7.2.2		**Práctica de gestión:**	No aplica
No.	**Criterio a evaluar**	**Cumplimiento**	**Observaciones**
1	¿La organización le ha comunicado sobre las políticas de seguridad de la información?	**SÍ**	
2	¿Las políticas de la seguridad de la información están disponibles para consultar en cualquier momento?	**SÍ**	
3	¿Conoce sus responsabilidades para la protección de los activos de información?	**SÍ**	
4	¿Conoce cuál es su rol y sus responsabilidades asociadas a la seguridad de la información?	**SÍ**	
5	¿Ha recibido capacitación periódica en seguridad de la información?	**SÍ**	
6	¿La organización le ha informado sobre buenas prácticas de seguridad de la información?	**SÍ**	
7	¿Conoce la política para el uso de dispositivos móviles dentro de la organización?	**SÍ**	
8	¿La organización le provee de dispositivos móviles para realizar sus funciones? Por ejemplo, portátil, tabletas, celulares.	**SÍ**	
9	¿La organización le ha provisto de una red independiente para conectar sus dispositivos móviles personales?	**SÍ**	

10	¿Mantiene SIEMPRE protegido su equipo mientras realiza teletrabajo?	**SÍ**	
11	¿Tiene firmado un acuerdo de confidencialidad y no divulgación de información con la organización?	**SÍ**	
12	¿Conoce las implicaciones disciplinarias o penales por robo, fraude y uso indebido de la información?	**SÍ**	
13	¿Conoce los procedimientos para realizar denuncias por incumplimientos a las políticas de la seguridad de la información?	**SÍ**	
14	¿Ha recibido formación en seguridad de la información por diferentes medios, por ejemplo, web, presencial, virtual?	**SÍ**	
15	¿Conoce el esquema de clasificación de los activos de información adoptado por la organización?	**SÍ**	
16	¿Acostumbra almacenar la información sensible SOLO en los medios autorizados, por tanto, EVITA utilizar llaves USB, memorias extraíbles o CD sin autorización?	**SÍ**	
17	¿Sus derechos de acceso SOLO le permiten tener acceso a las áreas o sistemas necesarios para realizar las funciones propias de su puesto de trabajo?	**SÍ**	
18	¿Conoce sus derechos y responsabilidades asociadas a las credenciales de acceso? Por ejemplo, claves, tarjetas de acceso e ID usuario.	**SÍ**	
19	¿Ha firmado alguna declaración de confidencialidad sobre la necesidad de mantener sus credenciales de autenticación secretas?	**SÍ**	
20	¿Cambia sus claves de acceso a los sistemas mínimo cada 3 meses?	**SÍ**	
21	¿Acostumbra utilizar claves ÚNICAS para acceder a los sistemas de información de la organización?	**SÍ**	
22	¿Dispone de un medio seguro para guardar sus contraseñas organizacionales? Por ejemplo, gestor de contraseñas.	**SÍ**	
23	¿Tiene deshabilitada la opción de recordar contraseña para los equipos que utiliza en las funciones de su puesto de trabajo?	**SÍ**	

24	¿Cierra las sesiones de trabajo cuando deja su equipo desatendido?	SÍ	
25	¿Verifica que sus contraseñas de acceso NO sean visibles para otras personas mientras las ingresa?	SÍ	
26	¿Se ha NEGADO a prestar o ceder sus credenciales de acceso a otros usuarios, visitantes o cuando cambia de puesto?	SÍ	
27	¿Ha reportado la existencia de usuarios genéricos o compartidos por más de una persona?	SÍ	
28	¿EVITA comer y tomar líquidos cerca de su computadora?	SÍ	
29	¿Reporta o custodia cualquier equipo que encuentre desatendido?	SÍ	
30	¿Acostumbra mantener su escritorio libre de documentos cuando deja su puesto de trabajo?	SÍ	
31	¿Acostumbra mantener la pantalla de su computadora limpia de accesos directos?	SÍ	
32	¿Acostumbra cerrar con llave los cajones de su escritorio cuando deja su puesto de trabajo?	SÍ	
33	¿Sabe que son los virus o *malware*?	SÍ	
34	¿Conoce los riesgos de visitar sitios web no autorizados?	SÍ	
35	¿Cuenta con autorización para instalar en su equipo de trabajo archivos, aplicaciones y *software* obtenido a través de internet o medios de almacenamiento?	SÍ	
36	¿La organización ha dispuesto reglas y directrices para el uso del correo electrónico?	SÍ	
37	¿Conoce el uso adecuado del correo electrónico y mensajería instantánea?	SÍ	
38	¿Conoce a que se refiere el concepto de ingeniería social y *fishing*?	SÍ	
39	¿NO abre correos, adjuntos o enlaces de correos en los cuales no conoce o desconfía del remitente?	SÍ	
40	¿Evita dar información de la organización a personas externas a esta? Por ejemplo, familiares, medios de comunicación, desconocidos, redes sociales.	SÍ	

41	¿Conoce cómo identificar un evento de seguridad y cómo reportarlo?	SÍ	
42	¿Conoce las disposiciones sobre el uso de redes sociales?	SÍ	
43	¿Ha recibido comunicaciones sobre ética, cultura organizativa y normas de comportamiento?	SÍ	
44	¿Conoce cómo construir contraseñas fuertes o de reglas de complejidad de contraseñas?	SÍ	
45	¿Considera que la información sensible de la organización es tratada según su nivel de protección?	SÍ	
46	¿Los sistemas de información de la organización le exigen el uso de contraseñas fuertes?	SÍ	
47	¿Los sistemas de información de la organización le permiten reutilizar contraseñas antiguas?	SÍ	
48	¿Se le ha formado en buenas prácticas para la formulación de contraseñas seguras y el almacenamiento de las mismas?	SÍ	
49	¿Utiliza controles de autenticación biométrica o multi-factor para el acceso a sistemas de información o servicios de la organización?	SÍ	
50	¿Usted considera que se le han proporcionado herramientas adecuadas, técnicas y directrices para garantizar la seguridad y el control efectivo sobre la información?	SÍ	

Anexo 05

Guía de auditoría para el sistema de gestión de la seguridad de la información

AUD-SGSI-01-2020	Guía de Auditoría Evaluación del Sistema de Gestión de la Seguridad de la Información

Nombre de la organización evaluada:

Área evaluada: | **Fecha:**

Responsable de la evaluación:

Objetivo: Analizar si la dirección ha proporcionado gestión y soporte para la seguridad de la información, de acuerdo con los requisitos del negocio y con las regulaciones y leyes pertinentes.

Dominio ISO/IEC 27001: A.5 Políticas de seguridad de la información

Guía de referencia ISO/IEC 27002: 5.1.1, 5.1.2 | **Práctica de gestión:** APO01.04, APO01.08, APO13.01, APO13.03

No.	Criterio a evaluar	Cumplimiento	Observaciones
1	¿Se tiene un conjunto de políticas para la seguridad de la información aprobadas, publicadas y comunicadas?	**SI**	
2	¿La políticas de seguridad de la información contienen una definición de la seguridad de la información, sus objetivos, alcance general y declaración de la importancia de la seguridad de la información?	**NO**	
3	¿La políticas de seguridad de la información contienen una declaración de la intención de la dirección, apoyando los objetivos y principios de la seguridad de la información alineada con las estrategias y objetivos del negocio?	**PARCIAL**	
4	¿La políticas de seguridad de la información contienen un marco para fijar objetivos de control y controles, incluyendo la estructura de la evaluación del riesgo y gestión del riesgo?	**SI**	
5	¿La políticas de seguridad de la información contienen una breve explicación de principios, estándares y requisitos de cumplimiento importantes para la organización?	**SI**	
6	¿La políticas de seguridad de la información contienen una definición de los responsables generales y específicos para la gestión de la seguridad de la información?	**SI**	
7	¿La políticas de seguridad de la información contienen referencias a documentación y procedimientos más detallados para sistemas de información específicos o las reglas de	**PARCIAL**	

	seguridad que los usuarios deberían cumplir?		
8	¿La políticas de seguridad de la información fueron comunicadas a todos los empleados, así como a las partes externas relevantes de manera pertinente, accesible y comprensible?	**SI**	
9	¿La políticas de seguridad de la información tienen un propietario con responsabilidad de gestión aprobada para el desarrollo, revisión y evaluación de la política de seguridad?	**PARCIAL**	
10	¿La políticas de seguridad de la información están formalmente escritas, son legibles, razonables y viables?	**SI**	
11	¿Las políticas de seguridad de la información están razonablemente completas y cubren los riesgos de información y controles más relevantes?	**PARCIAL**	
12	¿Las políticas de seguridad de la información cumplen un formato y estilo consistente?	**NO**	
13	¿La revisión de las políticas de seguridad de la información cumplen el plan de revisión planificado?	**NO**	
14	¿Han ocurrido incidentes de seguridad reportados, acciones preventivas y correctivas implementadas por la empresa, cambio en el ambiente laboral, disponibilidad de los recursos, condiciones contractuales, regulaciones internas y legales o cambio en entorno técnico y otros cambios significativos, que ameriten la actualización de la políticas de seguridad?	**PARCIAL**	
15	¿Las revisiones de las políticas de seguridad han incluido retroalimentación de terceras partes, revisiones independientes, cumplimiento de políticas y procedimientos, tendencias de amenazas y vulnerabilidades?	**NO**	
16	¿El control de cambios y versiones tiene la aprobación de la dirección?	**SI**	
17	¿Las políticas de seguridad después de la última revisión aprobada se han vuelto a publicar y comunicar?	**SI**	
18	¿Se mantiene un registro de evidencia para la difusión y revisión de las políticas de seguridad de la información?	**NO**	
19	¿Las políticas se encuentran disponibles para todos los empleados y las partes externas relevantes?	**SI**	
20	¿Las políticas indican las áreas a las que se aplican y excepciones?	**PARCIAL**	

AUD-SGSI-02-2020	**Guía de Auditoría Evaluación del Sistema de Gestión de la Seguridad de la Información**

Nombre de la organización evaluada:

Área evaluada: **Fecha:**

Responsable de la evaluación:

Objetivo: Indagar la existencia y cumplimiento de un marco de gestión para iniciar y controlar la implementación y operación de seguridad de la información dentro de la organización.

Dominio ISO/IEC 27001: A.6 Organización de la seguridad de la información

Guía de referencia ISO/IEC 27002: 6.1.1, 6.1.2, 6.1.3, 6.1.4, 6.1.5

Práctica de gestión: APO01.06, APO13.01, DSS05.02, DSS05.03, DSS05.04

No.	Criterio a evaluar	Cumplimiento	Observaciones
1	¿Se designado un responsable total para el desarrollo e implementación de la seguridad de la información?	**SI**	
2	¿Se han identificado y defino los activos y procesos de seguridad de la información?	**SI**	
3	¿Se han asignado las responsabilidades para la protección de los activos individuales de información?	**PARCIAL**	
4	¿Se han asignado las responsabilidades de los procesos de seguridad de la información específicos?	**SI**	
5	¿Se han definido las responsabilidades para las actividades de gestión del riesgo de la seguridad de la información?	**SI**	
6	¿Se han definido y documentado los niveles de autorización de cada rol para la seguridad de la información?	**SI**	
7	¿Las personas responsables de los activos y procesos de seguridad de la información están adecuadamente capacitados?	**PARCIAL**	
8	¿Las tareas o áreas de responsabilidad asignadas a la seguridad de la información mantienen una adecuada segregación de deberes para reducir las oportunidades de modificación no autorizada o el mal uso de activos de la organización?	**SI**	
9	¿Se mantiene actualizada una lista de contacto con autoridades pertinentes, por ejemplo policía, bomberos, proveedor de servicios de internet?	**SI**	

10	¿Están asignadas las personas responsables de realizar contacto con cada autoridad en caso de ser necesario?	**PARCIAL**	
11	¿Se tiene un registro de la pertenencia a grupos de interés especiales, como foros de seguridad y asociaciones de profesionales?	**NO**	
12	¿La pertenencia a grupos de interés especial ha contribuido en la resolución y atención de problemas?	**NO**	
13	¿Están definidas las personas que tienen acceso a grupos, foros, listas de correo, entre otras?	**NO**	
14	¿La seguridad de la información se contempla en la gestión de proyectos e independientemente del tipo de proyecto a desarrollar por la organización?	**PARCIAL**	
15	¿Personal del área de seguridad de la información forma parte de la gestión proyectos?	**SI**	
16	¿Los proyectos incluyen requerimientos para la seguridad de la información, independientemente del tipo de proyecto?	**PARCIAL**	
17	¿Objetivos de seguridad de la información están incluidos en los objetivos de proyectos? (Tomar una muestra)	**NO**	
18	¿La seguridad de la información está incluida en todas las etapas de la gestión de proyectos?	**NO**	

AUD-SGSI-03-2020	**Guía de Auditoría** **Evaluación del Sistema de Gestión de la Seguridad de la Información**

Nombre de la organización evaluada:

Área evaluada: **Fecha:**

Responsable de la evaluación:

Objetivo: Determinar la existencia y cumplimiento de la seguridad del teletrabajo y el uso de dispositivos móviles.

Dominio ISO/IEC 27001: A.6 Organización de la seguridad de la información

Guía de referencia ISO/IEC 27002: 6.2.1 y 6.2.2

Práctica de gestión: APO01.04, DSS05.02 y DSS05.03

No.	Criterio a evaluar	Cumplimiento	Observaciones
1	¿Se tiene una política formal para el uso de dispositivos móviles, aprobada, publicada y comunicada?	SI	
2	¿La política de dispositivos móviles tiene identificado los riesgos asociados al uso de dispositivos móviles?	SI	
3	¿La política de dispositivos móviles autoriza el uso de dispositivos móviles personales dentro de la red de la organización?	SI	
4	¿Se provee de dispositivos móviles a los empleados para la realización de las funciones del puesto de trabajo?	NO	
5	¿Se lleva un registro de todos los dispositivos móviles de la organización?	SI	
6	¿Se facilitan contraseñas o puertos de acceso de red a dispositivos móviles externos sin solicitar autorización?	NO	
7	¿Se han implementado mecanismos de bloqueo para dispositivos móviles?	NO	
8	¿Las computadoras portátiles cuentan con mecanismos de protección física?	NO	
9	¿Los dispositivos móviles cuentan con monitoreo de actividad?	SI	
10	¿Los dispositivos móviles cuentan con protección de malware?	NO	
11	¿La organización usa el modelo de teletrabajo?	SI	

12	¿La organización tiene una política formal para el teletrabajo, aprobada, publicada y comunicada?	**SI**	
13	¿Se da soporte y mantenimiento de software y hardware a los dispositivos en teletrabajo?	**SI**	
14	¿Los empleados en teletrabajo tienen mecanismo de acceso seguro a la información y a la red de la organización?	**SI**	
15	¿Se han implementado mecanismos de protección a la información accedida, procesada o almacenada en ubicaciones destinadas al teletrabajo? (antivirus, firewall)	**SI**	
16	¿Se han reportado eventos de seguridad relacionados a puestos en teletrabajo?	**NO**	
17	¿Se usa una conexión exclusiva a internet en el puesto trabajo remoto?	**SI**	

AUD-SGSI-04-2020	**Guía de Auditoría** **Evaluación del Sistema de Gestión de la Seguridad de la Información**

Nombre de la organización evaluada:

Área evaluada: **Fecha:**

Responsable de la evaluación:

Objetivo: Indagar la existencia de un proceso de selección para los empleados y contratistas, que incluya sus responsabilidades, y que sean aptos para los roles en los cuales están siendo considerados.

Dominio ISO/IEC 27001: A.7 Seguridad ligada a los recursos humanos

Guía de referencia ISO/IEC 27002: 7.1.1 y 7.1.2 **Práctica de gestión:** No aplica

No.	Criterio a evaluar	Cumplimiento	Observaciones
1	¿El proceso de contratación lo hace la organización o un tercero?	SI	
2	¿Si el proceso es subcontratado, se han revisado y aceptado los procedimientos?	NO	
3	¿Se hace verificación de antecedes a los candidatos del empleo en concordancia con las regulaciones, ética, leyes y proporcionales al perfil del puesto y/o los requerimientos del negocio?	PARCIAL	
4	¿Se hace una comprobación completa del curriculum vitae de los candidatos al empleo?	PARCIAL	
5	¿Existe un método de comprobación para validar que la revisión fue realizada?	SIN OBSERVAR	
6	¿Los futuros empleados, contratistas y terceras partes firman y aceptan un contrato de empleo con los términos y condiciones de la contratación?	SIN OBSERVAR	
7	¿Se hace distinción entre perfiles de puestos críticos o relacionados con la seguridad de la información y los empleados en general?	SIN OBSERVAR	
8	¿Todos los empleados, contratistas y terceras partes a los cuales se les dé acceso a información sensible firman un acuerdo de confidencialidad o de no divulgación?	SIN OBSERVAR	
9	¿Los términos y condiciones de contratación incluyen las obligaciones de la organización en cuanto al manejo de la información personal?	SIN OBSERVAR	

10	¿Los términos y condiciones de contratación señalan las acciones a ser tomadas si el empleado, contratista o usuario de terceras partes desatiende los requisitos de seguridad de la organización?	**SIN OBSERVAR**	
11	¿Los términos y condiciones de contratación señalan las responsabilidades y derechos legales relativos a derechos de autor o legislación de protección de datos, en concordancia con las necesidades del negocio?	**SIN OBSERVAR**	
12	¿Los términos y condiciones de contratación señalan las responsabilidades para la clasificación de información, la gestión de activos de la organización y servicios de información manejados por el empleado, el contratista o el usuario de terceras partes?	**SIN OBSERVAR**	

AUD-SGSI-05-2020	**Guía de Auditoría Evaluación del Sistema de Gestión de la Seguridad de la Información**

Nombre de la organización evaluada:

Área evaluada: **Fecha:**

Responsable de la evaluación:

Objetivo: Indagar si existen las gestiones para que los empleados y contratistas tomen conciencia de sus responsabilidades en seguridad de la información y las cumplan.

Dominio ISO/IEC 27001: A.7 Seguridad ligada a los recursos humanos

Guía de referencia ISO/IEC 27002: 7.2.1, 7.2.2 y 7.2.3

Práctica de gestión: APO01.02 y DSS05.05

No.	Criterio a evaluar	Cumplimiento	Observaciones
1	¿Los empleados y contratistas son informados sobre sus roles y responsabilidades de seguridad antes de otorgar acceso a la información sensible o sistemas de información?	**SI**	
2	¿Se motiva a los empleados y contratistas a mantener el cumplimiento de las políticas de seguridad?	**NO**	
3	¿Se les dan directrices a los empleados y contratistas que establezcan las expectativas de seguridad de la información de sus roles dentro de la organización?	**PARCIAL**	
4	¿Se dispone de un canal para realizar denuncias anónimas de incumplimientos a la política y procedimientos de seguridad de la información?	**SI**	
5	¿Los responsables de la seguridad de la información reciben capacitación adicional para atender actividades propias de función y mantenerse actualizados?	**SI**	
6	¿La organización dispone de un programa de concientización, educación y capacitación en seguridad de la información para todos los empleados?	**SIN OBSERVAR**	
7	¿El programa de concientización incluye varias actividades de toma de conciencia, tales como, campañas, folletos, infografías, conferencias, entre otros?	**SIN OBSERVAR**	
8	¿El programa de concientización, educación y capacitación se actualiza con forme la aparición de nuevas amenazas, vulnerabilidades, incidentes o cambios en las políticas de seguridad?	**SIN OBSERVAR**	

9	¿El programa de toma de conciencia utiliza diferentes medios de aprendizaje, tales como clases en aula, aprendizaje en web o aprendizaje a distancia?	**SIN OBSERVAR**	
10	¿La educación y formación en seguridad de la información comprende la necesidad de familiarizarse con las reglas y obligaciones de seguridad de la información aplicables y cumplir con ellas?	**SIN OBSERVAR**	
11	¿La educación y formación en seguridad de la información comprende la rendición personal de cuentas por las acciones y omisiones propias?	**SIN OBSERVAR**	
12	¿La educación y formación en seguridad de la información incluye la enseñanza de los procedimientos básicos de seguridad de la información y los controles básicos?	**SIN OBSERVAR**	
13	¿La educación y entrenamiento iniciales se lleva a cabo para nuevos contratos o cuando se hace un cambio en el puesto de trabajo con requisitos de seguridad de la información?	**SIN OBSERVAR**	
14	¿Al finalizar el curso de concientización, educación y formación en seguridad de la información se realizan valoraciones de la comprensión de los empleados capacitados?	**SIN OBSERVAR**	
15	¿Las valoraciones de la comprensión en seguridad de la información por parte de los empleados son aceptables?	**SIN OBSERVAR**	
16	¿Se da seguimiento a las empleados que presentan valoraciones de comprensión deficientes en seguridad de la información?	**SIN OBSERVAR**	
17	¿La gerencia de la organización participa del programa de concientización, educación y capacitación de la seguridad de la información?	**SIN OBSERVAR**	
18	¿El programa de concientización, educación y capacitación está al día, es decir tiene cumplidas las actividades según lo planeado?	**SIN OBSERVAR**	
19	¿Existe un proceso disciplinario formal para los empleados que comentan una violación a la seguridad de la información?	**SIN OBSERVAR**	
20	¿Las acciones disciplinarias en caso de violación a la seguridad de la información son comunicadas a todos los empleados?	**SIN OBSERVAR**	
21	¿Se hace una verificación de la posible violación a la seguridad de la información antes de iniciar el proceso disciplinario?	**SIN OBSERVAR**	
22	¿El proceso disciplinario provee una respuesta acorde a la naturaleza, gravedad e impacto al negocio de la falta cometida?	**SIN OBSERVAR**	

AUD-SGSI-06-2020	**Guía de Auditoría Evaluación del Sistema de Gestión de la Seguridad de la Información**

Nombre de la organización evaluada:

Área evaluada: **Fecha:**

Responsable de la evaluación:

Objetivo: Indagar si se protegen los intereses de la organización como parte del proceso de finalización o cambio de empleo.

Dominio ISO/IEC 27001: A.7 Seguridad ligada a los recursos humanos

Guía de referencia ISO/IEC 27002: 7.3.1 **Práctica de gestión:** No aplica

No.	Criterio a evaluar	Cumplimiento	Observaciones
1	¿Están definidas las personas responsables de ejecutar la finalización o cambio de un puesto de trabajo?	**SI**	
2	¿Están definidos los procedimientos para llevar a cabo la finalización del empleo?	**SI**	
3	¿Existe un documento de terminación de la relación laboral el cual debe ser firmado por el personal que es desvinculado?	**SI**	
4	¿Durante la desvinculación se retoman las responsabilidades y obligaciones de confidencialidad asumidas durante la contratación?	**NO**	
5	¿Durante la desvinculación se levanta un documento formal para la devolución de todos los activos asignados?	**PARCIAL**	
6	¿El expediente del exempleado tiene constancia de la devolución de activos?	**SI**	
7	¿Se cuentan con procedimientos para la transferencia o eliminación de información relevante, contenida en dispositivos personales utilizados para la realización de las funciones del puesto de trabajo?	**SIN OBSERVAR**	
8	¿El inventario refleja el ingreso de activos o cambio de propietario cuando se da un cese o cambio de puesto?	**SIN OBSERVAR**	
9	¿Se revocan los derechos de accesos como consecuencia de la desvinculación del empleo, con su correspondiente validación de revocación?	**SIN OBSERVAR**	

10	¿Se ajustan los derechos de acceso como consecuencia de un cambio en el puesto de trabajo?	**SIN OBSERVAR**	
11	¿Los derechos de acceso a activos de información o instalaciones son removidos antes que la relación laboral termine o cambie?	**SIN OBSERVAR**	
12	¿Se hace un seguimiento del uso del correo electrónico de las personas desvinculadas antes de salir definitivamente de la empresa?	**SIN OBSERVAR**	

AUD-SGSI-07-2020	**Guía de Auditoría Evaluación del Sistema de Gestión de la Seguridad de la Información**

Nombre de la organización evaluada:

Área evaluada: **Fecha:**

Responsable de la evaluación:

Objetivo: Constatar si se han identificado los activos de la organización y se han defino las responsabilidades para la apropiada protección.

Dominio ISO/IEC 27001: A.8 Gestión de activos

Guía de referencia ISO/IEC 27002: 8.1.1, 8.1.2, 8.1.3, 8.1.4

Práctica de gestión: APO01.06, DSS05.03 y DSS05.06

No.	Criterio a evaluar	Cumplimiento	Observaciones
1	¿Se cuenta con un inventario de los activos pertinentes en el ciclo de vida de la información?	**SI**	
2	¿El inventario de activos incluye activos de información digital o manual, activos de software, activos físicos, activos de servicios, activos intangibles?	**NO**	
3	¿El inventario de activos tiene una persona responsable asignada?	**NO**	
4	¿El inventario es suficientemente detallado y completo?	**SI**	
5	¿Los activos físicos están claramente etiquetados conforme los requerimientos de la organización? por ejemplo, con número de serie, modelo, ubicación.	**SI**	
6	¿El inventario concuerda contra la existencia en bodega?	**SIN OBSERVAR**	
7	¿El inventario concuerda con los activos de un área específica? Tomar muestra.	**SIN OBSERVAR**	
8	¿El inventario de los activos de información tiene asignado un propietario para cada activo?	**SIN OBSERVAR**	
9	¿Los activos asociados a los recursos de procesamiento de información tienen asignado un propietario?	**SIN OBSERVAR**	
10	¿Los propietarios de los activos de información conocen sus responsabilidades?	**SIN OBSERVAR**	
11	¿El propietario de los activos revisa que los activos estén clasificados y protegidos adecuadamente?	**SIN OBSERVAR**	

12	¿El propietario de los activos participa en el proceso de eliminado o destrucción de los activos?	**SIN OBSERVAR**	
13	¿Se ha dispuesto de un reglamento para el uso aceptable de los activos de información y los activos asociados a el procesamiento de la información?	**SIN OBSERVAR**	
14	¿Los empleados y usuarios de terceras partes reciben concienciación sobre los requisitos de seguridad de la información de los activos de la organización?	**SIN OBSERVAR**	
15	¿Se tienen definido medios para denunciar un mal uso de los activos de información?	**SIN OBSERVAR**	
16	¿Los empleados y usuarios de terceras partes devuelven los activos de la organización que estén bajo su responsabilidad una vez finalizado el contrato o acuerdo?	**SIN OBSERVAR**	
17	¿La organización dispone de procedimientos para la recuperación de activos después de finalizado el empleo o contrato?	**SIN OBSERVAR**	
18	¿El inventario de activos se actualiza inmediatamente después del finalizado el empleo o contrato?	**SIN OBSERVAR**	
19	¿En casos que el empleado o usuario de terceras partes compre dispositivos de la organización después de terminada la relación laboral o contrato, se hace una transferencia o borrado de la información contenida en dichos equipos?	**SIN OBSERVAR**	
20	¿En casos que el empleado o usuario de terceras partes posea conocimientos importantes para las operaciones de la organización esta información se documenta o transfiere a la organización?	**SIN OBSERVAR**	
21	¿Se hace monitoreo de las actividades del empleado o usuario de terceras partes que deja la organización, con el fin de evitar copiado o destrucción no autorizada de la información?	**SIN OBSERVAR**	

AUD-SGSI-08-2020	**Guía de Auditoría Evaluación del Sistema de Gestión de la Seguridad de la Información**

Nombre de la organización evaluada:

Área evaluada: **Fecha:**

Responsable de la evaluación:

Objetivo: Constatar que la información recibe un nivel de protección apropiado, de acuerdo con su importancia para la organización.

Dominio ISO/IEC 27001: A.8 Gestión de activos

Guía de referencia ISO/IEC 27002: 8.2.1, 8.2.3, 8.2.3 **Práctica de gestión:** No aplica

No.	Criterio a evaluar	Cumplimiento	Observaciones
1	¿Se han establecido las directrices de clasificación de la información en relación a su valor, requisitos legales, sensibilidad y criticidad para la organización?	SI	
2	¿La información se reclasifica a largo de tiempo?	NO	
3	¿El propietario del activo de información es quién clasifica, revisa y asegura que este actualizado?	SI	
4	¿El esquema de clasificación es beneficioso y fácil de utilizar?	SIN OBSERVAR	
5	¿La clasificación garantiza la confidencialidad, integridad y disponibilidad del activo de información?	SIN OBSERVAR	
6	¿La información se protege según su nivel de clasificación?	SIN OBSERVAR	
7	¿Se han desarrollado e implantado procedimientos para el etiquetado de la información?	SIN OBSERVAR	
8	¿Los procedimientos para el etiquetado y tratamiento de la información, están de acuerdo con el esquema de clasificación adoptado por la organización?	SIN OBSERVAR	
9	¿Los procedimientos de etiquetado cubren los activos de información en formato físico y digital?	SIN OBSERVAR	
10	¿Los activos de información están correctamente etiquetados conforme el esquema de clasificación? Tomar una muestra	SIN OBSERVAR	

11	¿Se han desarrollado e implantado procedimientos para el manejo, almacenamiento y comunicación de información de acuerdo con el esquema de clasificación?	**SIN OBSERVAR**	
12	¿Se tienen restricciones de acceso de acuerdo con los requisitos de protección para cada nivel de clasificación?	**SIN OBSERVAR**	
13	¿Los copias de información temporal o permanente tienen protección al mismo nivel de protección de la información original?	**SIN OBSERVAR**	

AUD-SGSI-09-2020	**Guía de Auditoría Evaluación del Sistema de Gestión de la Seguridad de la Información**

Nombre de la organización evaluada:

Área evaluada: **Fecha:**

Responsable de la evaluación:

Objetivo: Constatar si existen procedimientos para prevenir la divulgación, modificación, remoción o destrucción no autorizada de la información almacenada en los medios.

Dominio ISO/IEC 27001: A.8 Gestión de activos

Guía de referencia ISO/IEC 27002: 8.3.1, 8.3.2, 8.3.3 **Práctica de gestión:** APO01.06 y DSS05.06

No.	Criterio a evaluar	Cumplimiento	Observaciones
1	¿Se han establecido procedimientos para la gestión de medios informáticos removibles acorde con el esquema de clasificación?	SI	
2	¿Existe un inventario de los medios removibles tales como CD, almacenamiento USB y otros soportes removibles?	NO	
3	¿Los medios removibles están clasificados y etiquetados?	SI	
4	¿Los medios removibles se encuentran almacenados en un lugar seguro?	SI	
5	¿Todos los equipos tienen habilitado unidades de medios removibles?	SIN OBSERVAR	
6	¿Los medios removibles mantienen un nivel de protección conforme su nivel de clasificación? Tomar muestra,	SIN OBSERVAR	
7	¿Se acostumbra utilizar medios removibles para almacenar información clasificada como confidencial o sensible?	SIN OBSERVAR	
8	¿Se usan técnicas criptográficas para proteger los datos almacenados en medios removibles con el fin de proveer confidencialidad e integridad?	SIN OBSERVAR	
9	¿Los medios removibles tienen asignado un responsable o propietario?	SIN OBSERVAR	
10	¿Se utilizan medios removibles para realizar respaldos de información?	SIN OBSERVAR	
11	¿Se guardan copias de datos valiosos en diferentes medios para reducir el riesgo de daño o pérdida del medio?	SIN OBSERVAR	

12	¿Se han establecido procedimientos para la eliminación de medios removibles de forma segura y sin riesgo?	SIN OBSERVAR	
13	¿Se lleva un registro de los medios removibles dados de baja?	SIN OBSERVAR	
14	¿Antes de eliminar medios removibles se respalda la información contenida en ellos?	SIN OBSERVAR	
15	¿Antes de eliminar medios removibles se borran todos los datos contenidos en ellos?	SIN OBSERVAR	
16	¿Los medios removibles son destruidos y desechados con la basura común?	SIN OBSERVAR	
17	¿Se utilizan soportes físicos para transportar información fuera de la organización?	SIN OBSERVAR	
18	¿El servicio de transporte o mensajería es confiable?	SIN OBSERVAR	
19	¿Se verifica la identificación del servicio de mensajería al utilizar el servicio?	SIN OBSERVAR	
20	¿Se hace embalaje suficiente para proteger los medios durante el transporte?	SIN OBSERVAR	
21	¿Los medios removibles son cifrados cuando se transportan fuera de la organización?	SIN OBSERVAR	
22	¿Se verifica la recepción de los medios removibles al llegar a su lugar de destino?	SIN OBSERVAR	
23	¿Se puede evitar él envió de información mediante medios de almacenamiento?	SIN OBSERVAR	

AUD-SGSI-10-2020	**Guía de Auditoría** **Evaluación del Sistema de Gestión de la Seguridad de la Información**

Nombre de la organización evaluada:

Área evaluada: **Fecha:**

Responsable de la evaluación:

Objetivo: Verificar la existencia y cumplimiento de acciones para controlar el acceso a la información y a los recursos de procesamiento de la información.

Dominio ISO/IEC 27001: A.9 Control de acceso

Guía de referencia ISO/IEC 27002: 9.1.1, 9.1.2

Práctica de gestión: APO01.04, DSS05.02 y DSS05.04

No.	Criterio a evaluar	Cumplimiento	Observaciones
1	¿Se tiene una política de control de accesos conforme las necesidades de seguridad y negocio de la organización aprobada, publicada y comunicada?	SI	
2	¿La política de control de accesos tiene una segregación de deberes apropiada?	NO APLICA	
3	¿La política de control de accesos es consistente con los requisitos de seguridad de la aplicaciones?	PARCIAL	
4	¿La política de control de accesos cubre todo el ciclo de vida del acceso de los usuarios?	SI	
5	¿La política de control de accesos incluye a los usuarios, proveedores y terceras partes?	SI	
6	¿La política de control de acceso fue revisada y autorizada en el último año?	SIN OBSERVAR	
7	¿La política de control de acceso tiene coherencia entre los derechos de acceso y las políticas de clasificación de la información de los sistemas o redes?	SIN OBSERVAR	
8	¿La política de control de acceso favorece el registro de los eventos significativos de las actividades del proceso de control de acceso?	SIN OBSERVAR	
9	¿La política de control de acceso considera los roles de acceso privilegiados?	SIN OBSERVAR	
10	¿La política de control de acceso considera los controles físicos así como lógicos?	SIN OBSERVAR	

11	¿La política de control de acceso es consistente con los principios de necesidad de conocer y necesidad de usar?	**SIN OBSERVAR**	
12	¿Se ha formulado una política para el uso de redes y servicios de red?	**SIN OBSERVAR**	
13	¿Están definidas las redes y servicios de red a los cuales se puede acceder según el perfil de control de acceso?	**SIN OBSERVAR**	
14	¿Se han definido los procedimientos formales para permitir acceso a la red y servicios de red?	**SIN OBSERVAR**	
15	¿Se han definido los medios seguros y autorizados para acceder a la red y servicios de red?	**SIN OBSERVAR**	
16	¿Se hace autenticación multifactor para acceso a redes, sistemas y aplicaciones críticas?	**SIN OBSERVAR**	
17	¿Se han definido los medios para dar seguimiento y monitoreo al uso de redes y servicios de red?	**SIN OBSERVAR**	
18	¿El cumplimiento de las políticas de control de acceso a la información, redes y servicios de red es revisado regularmente?	**SIN OBSERVAR**	

AUD-SGSI-11-2020	**Guía de Auditoría Evaluación del Sistema de Gestión de la Seguridad de la Información**

Nombre de la organización evaluada:

Área evaluada: **Fecha:**

Responsable de la evaluación:

Objetivo: Determinar la existencia de gestiones para asegurar el acceso autorizado de los usuarios y evitar el acceso no autorizado a los sistemas de información y servicios.

Dominio ISO/IEC 27001: A.9 Control de acceso

Guía de referencia ISO/IEC 27002: 9.2.1, 9.2.2, 9.2.3, 9.2.4, 9.2.5, 9.2.6

Práctica de gestión: DSS05.04, DSS05.05

No.	Criterio a evaluar	Cumplimiento	Observaciones
1	¿Existe un procedimiento formal para otorgar y revocar usuarios?	SI	
2	¿Se utiliza un identificador único (ID) para cada usuario?	PARCIAL	
3	¿Se deshabilitan o retiran las identificaciones únicas de los usuarios que han dejado la organización?	SI	
4	¿Los ID de usuarios redundantes se reasignan a otros usuarios?	NO APLICA	
5	¿Existe un procedimiento formal para el cambio de derechos de acceso (creación, modificación, eliminación) que incluya todos los tipos de usuarios y todos los sistemas y servicios?	SIN OBSERVAR	
6	¿Los propietarios de los sistemas de información o servicios autorizan su uso para cada solicitud de acceso?	SIN OBSERVAR	
7	¿Los derechos de acceso están en concordancia con los roles y responsabilidades definidos para cada ID usuario? Tomar muestra.	SIN OBSERVAR	
8	¿Se mantiene un registro de los derechos de acceso suministrados a cada ID de usuario para acceder a los sistemas y servicios?	SIN OBSERVAR	
9	¿Se otorga acceso a todos los usuarios hasta que el proceso de autorización este completado?	SIN OBSERVAR	
10	¿Se hace una revisión periódica de los derechos de acceso con los propietarios de los sistemas de información y servicios? Solicitar evidencia de esto.	SIN OBSERVAR	
11	¿Se le entrega a los usuarios una declaración de sus derechos y responsabilidades de acceso?	SIN OBSERVAR	

12	¿Existe un procedimiento de autorización formal para controlar la asignación de derechos de acceso privilegiados?	SIN OBSERVAR	
13	¿Se tienen identificados los derechos de acceso privilegiados asociados a cada sistema o proceso?	SIN OBSERVAR	
14	¿Los derechos de acceso privilegiados se dan con base en la necesidad de uso?	SIN OBSERVAR	
15	¿Se mantiene un registro de todos los privilegios asignados a cada usuario?	SIN OBSERVAR	
16	¿Los derechos de acceso privilegiados se otorgan por un periodo de tiempo definido?	SIN OBSERVAR	
17	¿Los derechos de acceso privilegiados tienen una ID diferente a la usada para las actividades regulares?	SIN OBSERVAR	
18	¿Se revisan y controlan frecuentemente las actividades de los usuarios con derechos de acceso privilegiados?	SIN OBSERVAR	
19	¿Los usuarios firman una declaración de confidencialidad para mantener su información de autenticación secreta?	SIN OBSERVAR	
20	¿Se provee de una contraseña inicial segura que debe ser cambiada una vez ingresado a los sistemas o servicios?	SIN OBSERVAR	
21	¿Es requisito confirmar la identidad del usuario antes de cualquier cambio de contraseña?	SIN OBSERVAR	
22	¿Se modifican las contraseñas por defecto del fabricante después de la instalación de los sistemas o software?	SIN OBSERVAR	
23	¿Los propietarios de los activos hacen una revisión de los derechos de acceso de los usuarios de sistemas de información y servicios a intervalos regulares y después de cualquier cambio en el empleo?	SIN OBSERVAR	
24	¿Los derechos de acceso son revisados y reasignados cuando ocurre un cambio en el puesto de trabajo dentro de la misma organización?	SIN OBSERVAR	
25	¿Se revocan todos los derechos de acceso de empleados, contratistas y terceras partes antes de finalizado el empleo, contrato o acuerdo?	SIN OBSERVAR	
26	¿Se mantienen pistas de auditoría de los accesos a los sistemas de información y servicios?	SIN OBSERVAR	

AUD-SGSI-12-2020	**Guía de Auditoría Evaluación del Sistema de Gestión de la Seguridad de la Información**

Nombre de la organización evaluada:

Área evaluada: **Fecha:**

Responsable de la evaluación:

Objetivo: Verificar si los usuarios son responsables de salvaguardar su información de autenticación.

Dominio ISO/IEC 27001: A.9 Control de acceso

Guía de referencia ISO/IEC 27002: 9.3.1 **Práctica de gestión:** DSS05.05

No.	Criterio a evaluar	Cumplimiento	Observaciones
1	¿Ha recibido capacitación o educación en seguridad de la información?	SI	
2	¿Conoce buenas prácticas para la selección, uso y almacenamiento de información de autenticación?	NO	
3	¿La organización le ha provisto de dispositivos para la autenticación? por ejemplo, firma digital, tarjetas de acceso	PARCIAL	
4	¿Guarda sus contraseñas en la computadora o navegador?	NO APLICA	
5	¿Mantiene activada la función de recordar contraseña para los accesos a los sistemas y servicios?	SIN OBSERVAR	
6	¿Lleva un registro físico o digital con su información de autenticación?	SIN OBSERVAR	
7	¿Utiliza un gestor de contraseñas para los sistemas de información o servicios de la organización?	SIN OBSERVAR	
8	¿Usa contraseñas fuertes concordantes con los requerimientos de complejidad de la organización?	SIN OBSERVAR	
9	¿Usa contraseñas fáciles de recordar, con menos de 8 caracteres y con datos personales?	SIN OBSERVAR	
10	¿Cambia las contraseñas regularmente, por ejemplo cada 3 meses?	SIN OBSERVAR	
11	¿Ha cambiado las contraseñas iniciales en la primer conexión de nuevos accesos a sistemas y servicios?	SIN OBSERVAR	

12	¿Comparte su información de autenticación con compañeros de trabajo o cuando hace un cambio en su puesto de trabajo?	**SIN OBSERVAR**	
13	¿Acostumbra reutilizar contraseñas personales para los accesos a los sistemas de la organización?	**SIN OBSERVAR**	
14	¿Utiliza contraseñas diferentes para cada sistema de información y servicio?	**SIN OBSERVAR**	
15	¿Pierde u olvida su información de autenticación con frecuencia?	**SIN OBSERVAR**	
16	¿Ha firmado algún documento que le obligue a mantener suscontraseñas o información de autenticación confidenciales?	**SIN OBSERVAR**	

AUD-SGSI-13-2020	**Guía de Auditoría Evaluación del Sistema de Gestión de la Seguridad de la Información**

Nombre de la organización evaluada:

Área evaluada: **Fecha:**

Responsable de la evaluación:

Objetivo: Determinar la existencia y cumplimiento de acciones para evitar el acceso no autorizado a los sistemas y aplicaciones.

Dominio ISO/IEC 27001: A.9 Control de acceso

Guía de referencia ISO/IEC 27002: 9.4.1,9.4.2, 9.4.3, 9.4.4 y 9.4.5 **Práctica de gestión:** DSS05.05

No.	Criterio a evaluar	Cumplimiento	Observaciones
1	¿Están definidas las restricciones de acceso según los requisitos de los sistemas y aplicaciones?	SI	
2	¿Se controlan los accesos a las funciones del sistema de aplicaciones mediante menús?	NO	
3	¿Los derechos de acceso de los usuarios permiten controlar la lectura, gravado, borrado o ejecución?	PARCIAL	
4	¿Las salidas de los sistemas y aplicaciones que procesan información sensible sólo contienen información importante para el uso de la salida? Tomar muestra	NO APLICA	
5	¿Se utiliza autenticación multifator para acceder a sistemas y aplicaciones críticas?	NO	
6	¿Existen mensajes de ayuda durante el procedimiento de ingreso a sistemas?	SIN OBSERVAR	
7	¿Se válida toda la información de credenciales hasta que esté completa y se muestra que parte es incorrecta?	SIN OBSERVAR	
8	¿Se registran los inicios de sesión exitosos y fallidos?	SIN OBSERVAR	
9	¿Se declara un evento de seguridad después de un intento o violación exitosa de credenciales?	SIN OBSERVAR	
10	¿Se esconde la contraseña durante el ingreso de credenciales?	SIN OBSERVAR	
11	¿Los intentos de ingreso inválidos generan bloqueos de los sistemas y aplicaciones?	SIN OBSERVAR	

12	¿Se cierran las sesiones después de un tiempo definidode inactividad?	SIN OBSERVAR	
13	¿Las credenciales de inicio de sesión se validan cada vez que el sistema se bloquee por inactividad?	SIN OBSERVAR	
14	¿Las contraseñas se transmiten y almacenan de forma cifrada?	SIN OBSERVAR	
15	¿Se ha dispuesto de un sistema de gestión de contraseñas para los usuarios?	SIN OBSERVAR	
16	¿Los sistemas de gestión de contraseñas validan la longitud y requisitos de complejidad de las credenciales de autenticación?	SIN OBSERVAR	
17	¿Se tienen programas utilitarios con capacidad de anular el sistema y los controles de las aplicaciones?	SIN OBSERVAR	
18	¿Se dispone de procedimientos de identificación, autenticación y autorización para programas utilitarios?	SIN OBSERVAR	
19	¿Se tiene limitado el uso de programas utilitarios al mínimo práctico de usuarios autorizados?	SIN OBSERVAR	
20	¿Se otorga acceso a los programas utilitarios en base a los roles y responsabilidades?	SIN OBSERVAR	
21	¿Se limita el uso de programas utilitarios en tiempo o para uso exclusivo de un cambio autorizado?	SIN OBSERVAR	
22	¿Se registran todas las actividades derivadas del uso de programas utilitarios?	SIN OBSERVAR	
23	¿Se mantiene una adecuada segregación de tareas en el uso de programas utilitarios?	SIN OBSERVAR	
24	¿Los códigos fuente de los programas se mantienen en un almacenamiento central controlado por medio de librerías de fuente?	SIN OBSERVAR	
25	¿El código fuente se guarda en un entorno seguro? Por ejemplo, control de versiones, lugar, acceso adecuado.	SIN OBSERVAR	
26	¿Se mantiene acceso restringido a las librerías de código fuente?	SIN OBSERVAR	
27	¿Se mantiene un registro de todos los accesos a las librerías de código fuente?	SIN OBSERVAR	

AUD-SGSI-14-2020	**Guía de Auditoría Evaluación del Sistema de Gestión de la Seguridad de la Información**		
Nombre de la organización evaluada:			
Área evaluada:			**Fecha:**
Responsable de la evaluación:			
Objetivo: Indagar sobre el uso apropiado y efectivo de la criptografía para proteger la confidencialidad, autenticidad e integridad de la información.			
Dominio ISO/IEC 27001: A.10 Criptografía			
Guía de referencia ISO/IEC 27002: 10.1.1, 10.1.2		**Práctica de gestión:** No aplica	
No.	**Criterio a evaluar**	**Cumplimiento**	**Observaciones**
1	¿Se ha desarrollado e implementado una política sobre el uso de controles criptográficos para la protección de la información?	**SI**	
2	¿La política de controles criptográficos tiene el nivel de protección criptográfica ajustado a la valoración estipulada en el análisis de riesgos? Tomando en cuenta: Tipo, fortaleza y calidad del algoritmo de encriptación.	**SI**	
3	¿La política de controles criptográficos, incluye la protección de la información transportada en dispositivos móviles o líneas de comunicación?	**NO**	
4	¿La política de controles criptográficos tiene declarados los métodos para la gestión de llaves, protección de llaves y recuperación de información encriptada en caso de pérdida o llaves comprometidas?	**SIN OBSERVAR**	
5	¿La política de controles criptográficos tiene señalados los roles y responsabilidades para la implementación de la política y la gestión de llaves?	**SIN OBSERVAR**	
6	¿Están señalados los casos en que la información debe ser protegida a través de criptografía?	**SIN OBSERVAR**	
7	¿Se ha desarrollado e implementado una política sobre el uso, la protección y el ciclo de vida de las llaves criptográficas?	**SIN OBSERVAR**	
8	¿La política toma en cuenta, procesos seguros de generación, almacenamiento, archivo, recuperación, distribución, retiro y distribución de las llaves?	**SIN OBSERVAR**	

9	¿Se ha definido los medios para proteger todas las llaves criptográficas contra modificación y pérdida?	SIN OBSERVAR	
10	¿Se protege el equipo utilizado para generar, almacenar y archivar llaves criptográficas?	SIN OBSERVAR	
11	¿Se ha definido un sistema de gestión de llaves?	SIN OBSERVAR	
12	¿El sistema de gestión de llaves tiene métodos seguros de generación de llaves para diferentes sistemas criptográficos y diferentes aplicaciones?	SIN OBSERVAR	
13	¿El sistema de gestión de llaves tiene métodos seguros para generar y obtener certificados de llaves públicas?	SIN OBSERVAR	
14	¿Se han establecido los procedimientos para distribuir, recibir y activar las llaves a las entidades previstas?	SIN OBSERVAR	
15	¿Se han establecido los procedimientos para el almacenamiento de llaves y como acceden a ellas los usuarios autorizados?	SIN OBSERVAR	
16	¿Se han establecido reglas para cambiar o actualizar llaves y cómo y cuándo hacerlo?	SIN OBSERVAR	
17	¿El sistema de gestión de llaves señala como dar tratamiento a llaves cuya seguridad ha sido comprometida?	SIN OBSERVAR	
18	¿Se han establecido procedimientos para recuperar llaves pérdidas o dañadas?	SIN OBSERVAR	
19	¿Se han establecido los procedimientos para hacer copias de respaldo de las llaves o como archivarlas?	SIN OBSERVAR	
20	¿Se han declarado los procedimientos para destruir llaves criptográficas?	SIN OBSERVAR	
21	¿Se definen fechas de activación y desactivación de llaves criptográficas?	SIN OBSERVAR	
22	¿Se registran todas las actividades de la gestión de llaves criptográficas?	SIN OBSERVAR	

AUD-SGSI-15-2020	**Guía de Auditoría Evaluación del Sistema de Gestión de la Seguridad de la Información**

Nombre de la organización evaluada:

Área evaluada: **Fecha:**

Responsable de la evaluación:

Objetivo: Determinar la existencia y cumplimiento de gestiones para prevenir el acceso físico no autorizado, daño e interferencia a la información y a las instalaciones de procesamiento de la organización.

Dominio ISO/IEC 27001: A.11 Seguridad física y ambiental

Guía de referencia ISO/IEC 27002: 11.1.1, 11.1.2, 11.1.3, 11.1.4, 11.1.4, 11.1.6

Práctica de gestión: DSS05.05

No.	Criterio a evaluar	Cumplimiento	Observaciones
1	¿Se han definido perímetros de seguridad para proteger áreas que contengan información sensible o crítica e instalaciones de manejo de información?	SI	
2	¿El recorrido por las instalaciones internas y externas confirma la existencia de perímetros de seguridad física?	SI	
3	¿Los perímetros de seguridad concuerdan con los requisitos de seguridad de los activos ubicados dentro del área?	SI	
4	¿Los perímetros de seguridad se ajustan a una valoración de riesgos?	NO	
5	¿Las áreas de procesamiento de información permanecen cerradas cuando no hay supervisión?	PARCIAL	
6	¿Se dispone de una recepción para controlar el acceso físico autorizado al edificios o áreas?	SI	
7	¿Existen puertas contra incendio dentro del perímetro de seguridad?	SIN OBSERVAR	
8	¿Las puertas contra incendio tienen alarmas, están monitoreadas y probadas?	SIN OBSERVAR	
9	¿Las puertas contra incendio funcionan correctamente?	SIN OBSERVAR	
10	¿Se tiene sistemas de detección de intrusos tales como, alarmas, CCTV con monitoreo?	SIN OBSERVAR	
11	¿Existen instalaciones de procesamiento de información dentro de la organización gestionadas externamente?	SIN OBSERVAR	
12	¿Se lleva un registro con el nombre, fecha, hora de entrada y salida de los visitantes?	SIN OBSERVAR	

13	¿La revisión del registro de visitantes confirma el cumplimiento del registro de los movimientos de visitantes?	SIN OBSERVAR	
14	¿Todos los visitantes son supervisados durante su visita?	SIN OBSERVAR	
15	¿Se utiliza autenticación multifactor para las áreas donde se procesa o almacena información?	SIN OBSERVAR	
16	¿Se lleva un registro de los accesos a las áreas donde se procesa o almacena información?	SIN OBSERVAR	
17	¿Todos los empleados, contratista y partes externas utilizan una identificación visible?	SIN OBSERVAR	
18	¿Los empleados deben reportar al personal de seguridad si se encuentran partes externas no acompañados y sin identificación?	SIN OBSERVAR	
19	¿Se supervisa todas las actividades realizadas por personal de soporte de partes externas?	SIN OBSERVAR	
20	¿Se otorga acceso a áreas seguras o instalaciones de procesamiento basado en un plan de mantenimiento o solicitudes de mesa de ayuda autorizadas?	SIN OBSERVAR	
21	¿Los derechos de acceso a áreas seguras o instalaciones de procesamiento de información se revisan, actualizan o revocan regularmente?	SIN OBSERVAR	
22	¿Las instalaciones de procesamiento o almacenamiento de información están ubicadas de forma que son accesibles al público?	SIN OBSERVAR	
23	¿Las instalaciones de procesamiento de datos, presentan identificaciones o señales externas o internas que alerten sobre actividades de procesamiento de información?	SIN OBSERVAR	
24	¿Las instalaciones con información o actividades confidenciales son visibles y audibles desde el exterior?	SIN OBSERVAR	
25	¿Las guías telefónicas internas de uso general identifican los lugares de las instalaciones de procesamiento de información?	SIN OBSERVAR	
26	¿Se tiene protección física contra daños causados por incendios, inundaciones, terremotos, disturbios civiles, desastres naturales o causados por el hombre?	SIN OBSERVAR	
27	¿Existen personal trabajando permanentemente en áreas seguras destinadas al procesamiento y almacenamiento de información?	SIN OBSERVAR	
28	¿Las actividades dentro de áreas seguras siempre se realiza bajo supervisión?	SIN OBSERVAR	
29	¿En la revisión de instalaciones se confirma que todas las áreas seguras vacías están cerradas	SIN OBSERVAR	

	con llave?		
30	¿Está prohibido para los empleados y partes externas el uso de equipo fotográfico, de video, audio o cualquier otro dispositivo de grabación en áreas restringidas?	**SIN OBSERVAR**	
31	¿El acceso al área de despacho y carga desde el exterior de las instalaciones solo se restringe a personal identificado y autorizado?	**SIN OBSERVAR**	
32	¿El área de despacho y carga facilita el acceso del personal de despacho a otras partes de las instalaciones de la organización?	**SIN OBSERVAR**	
33	¿En el recorrido se confirmó que las puertas externas permanecen cerradas cuando las puertas internas están abiertas?	**SIN OBSERVAR**	
34	¿El material que ingresa se examina para determinar la presencia de explosivos, químicos u otros materiales peligrosos?	**SIN OBSERVAR**	
35	¿Los materiales que ingresan siguen los procedimientos de gestión de activos?	**SIN OBSERVAR**	
36	¿El material que ingresa se inspecciona para determinar evidencia de manipulación durante el viaje?	**SIN OBSERVAR**	

AUD-SGSI-16-2020	**Guía de Auditoría Evaluación del Sistema de Gestión de la Seguridad de la Información**

Nombre de la organización evaluada:

Área evaluada: **Fecha:**

Responsable de la evaluación:

Objetivo: Determinar la existencia y cumplimiento de acciones para prevenir la pérdida, daño, robo o compromiso de los activos y la interrupción de las operaciones de la organización.

Dominio ISO/IEC 27001: A.11 Seguridad física y ambiental

Guía de referencia ISO/IEC 27002: 11.2.1, 11.2.2, 11.2.3, 11.2.4, 11.2.5, 11.2.6, 11.2.7, 11.2.8, 11.2.9

Práctica de gestión: DSS05.03

No.	Criterio a evaluar	Cumplimiento	Observaciones
1	¿Los equipos están ubicados de forma que se minimice el acceso a las áreas de trabajo?	SI	
2	¿Las instalaciones de procesamiento de información que manejan datos sensibles están ubicadas para reducir la visibilidad de la información a personas no autorizadas?	NO	
3	¿Las instalaciones de almacenamiento están aseguradas para evitar el acceso no autorizado?	NO	
4	¿Los equipos están protegidos contra robo, incendio, agua, polvo, interferencia eléctrica, interferencia de las comunicaciones y vandalismo?	NO APLICA	
5	¿Está permitido comer, tomar líquidos y fumar cerca de las instalaciones de procesamiento de información?	SI	
6	¿Se monitorea la temperatura y humedad de las instalaciones de procesamiento de información?	NO	
7	¿La edificación(es) está protegida contra descargas eléctricas atmosféricas?	NO	
8	¿Se dispone de electricidad, iluminación, agua y aire acondicionado de emergencia para los equipos?	SIN OBSERVAR	
9	¿El sistema UPS proporciona una potencia adecuada y confiable?	SIN OBSERVAR	
10	¿Se han dispuesto servicios de telecomunicaciones y comunicaciones alternos ante interrupciones del servicio?	SIN OBSERVAR	

11	¿Las válvulas para interrumpir energía, agua u otros servicios están cerca de las salidas de emergencia o recintos?	SIN OBSERVAR	
12	¿Los cables de potencia están separados de los cables de comunicaciones?	SIN OBSERVAR	
13	¿El acceso a paneles de conexión y recintos de cables se da mediante procedimientos de autorización?	SIN OBSERVAR	
14	¿Hay protección física adecuada para cables externos y cajas de conexiones?	SIN OBSERVAR	
15	¿Los equipos están incluidos dentro de un plan de mantenimiento?	SIN OBSERVAR	
16	¿Se ha definido el personal de mantenimiento autorizado para el mantenimiento y servicio de los equipos?	SIN OBSERVAR	
17	¿Se lleva un registro con las fallas reales o sospechosas de los equipos?	SIN OBSERVAR	
18	¿Se lleva un registro de los mantenimientos preventivos y correctivos de los equipos?	SIN OBSERVAR	
19	¿Los equipos con información confidencial son protegidos antes de las actividades de mantenimiento? Por ejemplo, borrado de información.	SIN OBSERVAR	
20	¿Se inspecciona el equipo después de las actividades de mantenimiento para asegurar su funcionamiento y garantizar que no haya sido alterado?	SIN OBSERVAR	
21	¿Se tienen identificados los empleados y usuarios de partes externas autorizados para retirar activos de la organización?	SIN OBSERVAR	
22	¿Existen horarios para el retiro de activos de la organización?	SIN OBSERVAR	
23	¿Se lleva un monitoreo del cumplimiento en las fechas de devolución de activos?	SIN OBSERVAR	
24	¿Se utilizan documentos de autorización para la salida e ingreso de activos?	SIN OBSERVAR	
25	¿Se han dictado directrices sobre el uso de equipos fuera de las instalaciones de la organización? Por ejemplo, uso en lugares públicos o transferencia de equipos a otras personas.	SIN OBSERVAR	
26	¿Los medios de almacenamiento son extraídos de los equipos antes de su destrucción o reusó en otras ubicaciones?	SIN OBSERVAR	
27	¿Los medios de almacenamiento con información confidencial son destruidos	SIN OBSERVAR	

	físicamente al cumplir su vida útil?		
28	¿Los medios de almacenamiento con información confidencial son borrados usando técnicas seguras de sobre escritura cuando son reusados?	**SIN OBSRVAR**	
29	¿Se han hecho actividades de toma de conciencia a los usuarios para atender los procedimientos de seguridad para proteger los equipos desatendidos?	**SIN OBSERVAR**	
30	¿Se define un tiempo de inactividad adecuado para el cierre de sesiones en los equipos inactivos?	**SIN OBSERVAR**	
31	¿Se cierran o finalizan automáticamente las sesiones inactivas en los equipos	**SIN OBSERVAR**	
32	¿Se protegen los bloqueos de pantalla con contraseña?	**SIN OBSERVAR**	
33	¿Se ha definido, aprobado, implementado y comunicado una política de escritorio limpio y pantalla limpia?	**SIN OBSERVAR**	
34	¿La información sensible para el negocio ya sea en papel o medios removibles se guarda o se mantiene bajo llave cuando no se esté utilizando?	**SIN OBSERVAR**	
35	¿Están definidas las condiciones de autorización para la reproducción de información dentro de la organización, con impresoras, escáneres, fotocopiadoras u otros medios?	**SIN OBSERVAR**	
36	¿Se mantienen las fotocopiadoras, impresoras y escáneres despejados de documentación?	**SIN OBSERVAR**	
37	¿Los escritorios se muestran visiblemente limpios cuando están desatendidos?	**SIN OBSERVAR**	

AUD-SGSI-17-2020	**Guía de Auditoría Evaluación del Sistema de Gestión de la Seguridad de la Información**

Nombre de la organización evaluada:

Área evaluada: **Fecha:**

Responsable de la evaluación:

Objetivo: Indagar sobre las gestiones y procedimientos para asegurar las operaciones correctas y seguras de los recursos de procesamiento de la información.

Dominio ISO/IEC 27001: A.12 Seguridad de las operaciones

Guía de referencia ISO/IEC 27002: 12.1.1, 12.1.2, 12.1.3,12.1.4 **Práctica de gestión:** No aplica

No.	Criterio a evaluar	Cumplimiento	Observaciones
1	¿Se han documentado formalmente los procedimientos operacionales de las TICs y están en disposición de los usuarios que los necesiten?	SI	
2	¿Existen instrucciones documentadas para la instalación y configuración de sistemas?	SI	
3	¿Existen instrucciones documentadas para las copias de respaldo?	SIN OBSERVAR	
4	¿Existen contactos de apoyo en caso de dificultades operacionales o técnicas inesperadas?	SIN OBSERVAR	
5	¿Existen instrucciones para el manejo de medios removibles?	SIN OBSERVAR	
6	¿Existen procedimientos de reinicio y recuperación del sistema para uso en caso de falla?	SIN OBSERVAR	
7	¿Existen instrucciones para el manejo de rastros de auditoría y logs de los sistemas?	SIN OBSERVAR	
8	¿Existen procedimientos de seguridad de la información?	SIN OBSERVAR	
9	¿Todos los procedimientos están actualizados?	SIN OBSERVAR	
10	¿El personal está capacitado para seguir los procedimientos documentados en función de su rol y responsabilidades?	SIN OBSERVAR	
11	¿Los procedimientos accesibles y usados regularmente?	SIN OBSERVAR	
12	¿Existen procedimientos formales de gestión de cambios que afecten a la seguridad de la información?	SIN OBSERVAR	

13	¿Los cambios en los procesos de negocio y los sistemas de procesamiento de la información se planifican y ponen a prueba?	SIN OBSERVAR	
14	¿Se registran los cambios significativos en los sistemas y procesos de negocio relacionados con la seguridad de la información?	SIN OBSERVAR	
15	¿Se verifican los requisitos de seguridad antes de la aprobación formal de un cambio?	SIN OBSERVAR	
16	¿Se comunican los cambios a todas las partes relacionadas?	SIN OBSERVAR	
17	¿Existen procedimientos para abortar cambios no exitosos, eventos no previstos y recuperarse de ellos?	SIN OBSERVAR	
18	¿Existen procedimientos rápidos de cambio para resolver incidentes de emergencia?	SIN OBSERVAR	
19	¿Existen un plan de gestión de la capacidad de sistemas críticos?	SIN OBSERVAR	
20	¿Existen requisitos de capacidad documentados para el óptimo funcionamientos de los sistemas?	SIN OBSERVAR	
21	¿Se aplica monitoreo de la capacidad con indicadores que disparen alertas preventivas en base a niveles preestablecidos?	SIN OBSERVAR	
22	¿Se realizan actividades de optimización de los sistemas, aplicaciones y bases de datos?	SIN OBSERVAR	
23	¿Se separan los ambientes de desarrollo, prueba y producción?	SIN OBSERVAR	
24	¿Se tienen controles de accesos diferenciados para cada ambiente?	SIN OBSERVAR	
25	¿Se utilizan datos de prueba con información sensible?	SIN OBSERVAR	
26	¿Después de completadas las pruebas, se borra toda información sensible del ambiente de pruebas?	SIN OBSERVAR	

AUD-SGSI-18-2020	**Guía de Auditoría Evaluación del Sistema de Gestión de la Seguridad de la Información**

Nombre de la organización evaluada:

Área evaluada: **Fecha:**

Responsable de la evaluación:

Objetivo: Verificar que las instalaciones de procesamiento de información y la información están protegidas contra el código malicioso.

Dominio ISO/IEC 27001: A.12 Seguridad de las operaciones

Guía de referencia ISO/IEC 27002: 12.2.1 **Práctica de gestión:** APO01.04, DSS05.01

No.	Criterio a evaluar	Cumplimiento	Observaciones
1	Se tiene una política de prevención de software malicioso aprobada, publicada y comunicada?	SI	
2	¿Se ha prohibido el uso de software no autorizado a todos los empleados?	SI	
3	¿Se utilizan listas blancas y negras para controlar el uso de software autorizado y no autorizado?	SIN OBSERVAR	
4	¿Hay prohibición de abrir o instalar, archivos, aplicaciones y software obtenido mediante redes externas, internet o medios de almacenamiento?	SIN OBSERVAR	
5	¿Se dispone de software anti-malware en todos los equipos de usuario final e instalaciones de procesamiento de información?	SIN OBSERVAR	
6	¿Se han implementado mecanismos de filtrado para evitar y detectar el uso de sitios web maliciosos?	SIN OBSERVAR	
7	¿Se realizan regularmente escaneos de vulnerabilidades técnicas en todos los equipos?	SIN OBSERVAR	
8	¿El software anti-malware se actualiza automáticamente?	SIN OBSERVAR	
9	¿Se generan alertas cuando ocurre una detección de malware?	SIN OBSERVAR	
10	¿Se analiza diariamente archivos recibidos por red o por cualquier otro medio de almacenamiento?	SIN OBSERVAR	
11	¿Existe filtrado de tráfico entrante para analizar todos los adjuntos y descargas de correos electrónicos antes de su?	SIN OBSERVAR	
12	¿Se han definido los procedimientos y las responsabilidades de protección contra el código malicioso?	SIN OBSERVAR	

13	¿El plan de continuidad incluye la recuperación en caso de ataque por software malicioso con copias de respaldo del software y disposiciones para recuperación?	**SIN OBSERVAR**	
14	¿Se recibe información oficial de nuevas amenazas de software malicioso y su forma de operación?	**SIN OBSERVAR**	
15	¿Se revisa y evalúa regularmente la información sobre nuevas amenazas de software malicioso?	**SIN OBSERVAR**	
16	¿Se toman acciones rápidas para minimizar los efectos de software malicioso?	**SIN OBSERVAR**	
17	¿Todo el personal ha recibido capacitación y concientización sobre los peligros del software malicioso?	**SIN OBSERVAR**	
18	¿Todo el personal conoce sobre técnicas de ingeniería social y fishing?	**SIN OBSERVAR**	
19	¿Se han comunicado las responsabilidades de prevención de los usuarios ante el software malicioso?	**SIN OBSERVAR**	

AUD-SGSI-19-2020	**Guía de Auditoría Evaluación del Sistema de Gestión de la Seguridad de la Información**

Nombre de la organización evaluada:

Área evaluada: **Fecha:**

Responsable de la evaluación:

Objetivo: Verificar y revisar la existencia de gestiones para proteger contra la pérdida de datos mediante copias de respaldo.

Dominio ISO/IEC 27001: A.12 Seguridad de las operaciones

Guía de referencia ISO/IEC 27002: 12.3.1 **Práctica de gestión:** APO01.04

No.	Criterio a evaluar	Cumplimiento	Observaciones
1	¿Se tiene una política de copias de respaldo aprobada, publicada y comunicada?	SI	
2	¿Se lleva un inventario de las copias de respaldo con su ubicación?	SI	
3	¿Las copias de respaldo se almacenan en ubicaciones adecuados y protegidas contra desastres y acceso indebidos?	SIN OBSERVAR	
4	¿Existen copias de respaldo almacenadas en un lugar remoto que permita escapar de un daño en el sitio principal?	SIN OBSERVAR	
5	¿Se han definido requisitos de retención y protección en concordancia con las necesidades de la organización?	SIN OBSERVAR	
6	¿Las copias de respaldo cubren todos los sistemas, aplicaciones, servidores, datos y todo software o información acorde a las necesidades de la organización?	SIN OBSERVAR	
7	¿Se ha definido la cobertura (completa, diferencial o incremental) y la frecuencia de las copias de respaldo?	SIN OBSERVAR	
8	¿La cobertura y frecuencia de las copias de respaldo se ajustan a los requisitos del negocio y la criticidad de la información para la continuidad del negocio?	SIN OBSERVAR	
9	¿Las copias de respaldo tienen el mismo nivel de protección física y del entorno que las del sitio principal?	SIN OBSERVAR	
10	¿Existen procedimientos formales de restauración de copias de respaldo?	SIN OBSERVAR	

11	¿Los medios de respaldo se ponen a prueba regularmente para asegurar que se puedan utilizar en caso de emergencia?	**SIN OBSERVAR**	
12	¿Las pruebas de restauración de copias de respaldo se realizan en un ambiente de pruebas?	**SIN OBSERVAR**	
13	¿Se lleva un registro de los resultados de las pruebas de restauración de copias de respaldo?	**SIN OBSERVAR**	
14	¿Se tienen tiempos estimados de recuperación de la información, software y sistemas?	**SIN OBSERVAR**	
15	¿Las copias de respaldo están protegidas con técnicas de encriptación según su nivel de clasificación?	**SIN OBSERVAR**	
16	¿Para los sistemas y servicios críticos las copias de respaldo abarcan toda la información necesaria para recuperar el sistema completo en caso de desastre?	**SIN OBSERVAR**	
17	¿Se tienen definidos los requisitos de capacidad y equipos necesarios para realizar una restauración en caso de desastre?	**SIN OBSERVAR**	
18	¿Se tiene un plan anual de pruebas de restauración de respaldos?	**SIN OBSERVAR**	
19	¿Se han realizado todas las pruebas de restauración planteadas a la fecha?	**SIN OBSERVAR**	

AUD-SGSI-20-2020	**Guía de Auditoría Evaluación del Sistema de Gestión de la Seguridad de la Información**

Nombre de la organización evaluada:

Área evaluada: **Fecha:**

Responsable de la evaluación:

Objetivo: Determinar la existencia del registro de eventos y generación de evidencia.

Dominio ISO/IEC 27001:A.12 Seguridad de las operaciones

Guía de referencia ISO/IEC 27002: 12.4.1, 12.4.2, 12.4.3, 12.4.4

Práctica de gestión: DSS05.07

No.	Criterio a evaluar	Cumplimiento	Observaciones
1	¿Se dispone de un sistema centralizado de gestión de eventos?	**SI**	
2	¿Se ha asignado un responsable para revisar y hacer seguimiento al registro de eventos de seguridad de la información?	**SI**	
3	¿Se registran, mantienen y revisan periódicamente las actividades de los usuarios, excepciones, fallas y eventos de seguridad de la información?	**SI**	
4	¿El registro de eventos incluye un nivel de detalle suficiente que permita identificar todos los actores incluidos en evento?	**SIN OBSERVAR**	
5	¿Los registros son protegidos contra alteración y acceso no autorizado?	**PARCIAL**	
6	¿Se han implementado alertas para analizar registros relacionados a la seguridad de la información?	**SIN OBSERVAR**	
7	¿Se han definido procedimientos para atender alertas de seguridad relacionadas al registro de eventos?	**SIN OBSERVAR**	
8	¿Se han activado alertas cuando la capacidad de almacenamiento de registros este por alcanzar su nivel máximo?	**SIN OBSERVAR**	
9	¿Los registros se almacenan en un formato no editable?	**SIN OBSERVAR**	
10	¿Existen copias de seguridad de los registros?	**SIN OBSERVAR**	
11	¿El sistema de registro tiene la capacidad de almacenar las actividades de los administradores y operadores del sistema de registro?	**SIN OBSERVAR**	
12	¿Los administradores de sistemas puedan borrar o desactivar registros de sus propias actividades?	**SIN OBSERVAR**	

13	¿Existen procedimientos relacionados a la sincronización de relojes?	**SIN OBSERVAR**	
14	¿Existen requisitos legales, reglamentarios, contractuales o de cumplimiento para la sincronización y exactitud del tiempo?	**SIN OBSERVAR**	
15	¿Hay un tiempo de referencia único definido? Por ejemplo, reloj atómico, GPS, NTP.	**SIN OBSERVAR**	
16	¿Se utiliza un método de sincronización de relojes para todo el entorno de la organización? Por ejemplo, equipos, CCTV, control de accesos, registros de eventos.	**SIN OBSERVAR**	
17	¿La exactitud del tiempo es vital para las actividades críticas del negocio?	**SIN OBSERVAR**	
18	¿Existe forma de identificar relojes desincronizados en los sistemas de información de la organización?	**SIN OBSERVAR**	

AUD-SGSI-21-2020	**Guía de Auditoría Evaluación del Sistema de Gestión de la Seguridad de la Información**

Nombre de la organización evaluada:

Área evaluada: **Fecha:**

Responsable de la evaluación:

Objetivo: Determinar la existencia de procedimientos para asegurar la integridad de los sistemas operativos.

Dominio ISO/IEC 27001: A.12 Seguridad de las operaciones

Guía de referencia ISO/IEC 27002: 12.5.1 **Práctica de gestión:** No aplica

No.	Criterio a evaluar	Cumplimiento	Observaciones
1	¿Existen procedimientos para controlar la instalación de software en sistemas operativos?	PARCIAL	
2	¿La actualización de software operativo, aplicaciones y bibliotecas la realiza personal capacitado con su correspondiente autorización?	NO APLICA	
3	¿Se instalan aplicaciones y software operacional solamente después de pruebas extensas y exitosas?	NO	
4	¿Se mantiene un sistema de control de la configuración del software implementado?	SIN OBSERVAR	
5	¿Se tiene una estrategia de retroceso (roll back) antes de implementar cambios?	SIN OBSERVAR	
6	¿El registro de eventos incluye todas las actualizaciones de programas operacionales?	SIN OBSERVAR	
7	¿Se guardas las versiones anteriores de software junto con los procedimientos de configuración, como medida de contingencia?	SIN OBSERVAR	
8	¿Se verifica que no se utilice software sin soporte del fabricante o proveedor?	SIN OBSERVAR	
9	¿Se aplican parches de software para eliminar o reducir debilidades de los sistemas?	SIN OBSERVAR	
10	¿Se da acceso a los proveedores para realizar actividades de apoyo solo después de cumplir el proceso de autorización?	SIN OBSERVAR	
11	¿Existe monitoreo y alertas para informar de instalaciones de software no autorizadas?	SIN OBSERVAR	
12	¿Se hace revisión de equipos, portátiles, servidores para asegurar que no haya instalado software no autorizado?	SIN OBSERVAR	
13	¿Se realizan instalaciones de software como parte de proceso formal de control de cambios?	SIN OBSERVAR	

AUD-SGSI-22-2020	**Guía de Auditoría Evaluación del Sistema de Gestión de la Seguridad de la Información**

Nombre de la organización evaluada:

Área evaluada: **Fecha:**

Responsable de la evaluación:

Objetivo: Indagar sobre las gestiones para prevenir la explotación de vulnerabilidades técnicas.

Dominio ISO/IEC 27001: A.12 Seguridad de las operaciones

Guía de referencia ISO/IEC 27002: 12.6.1 y 12.6.2 **Práctica de gestión:** No aplica

No.	Criterio a evaluar	Cumplimiento	Observaciones
1	¿Se tiene actualizado el inventario de activos sobre los cuales se realiza el escaneo de vulnerabilidades técnicas?	SI	
2	¿Se establecido los roles y responsabilidades para la gestión de vulnerabilidades técnicas?	NO APLICA	
3	¿Se dispone del software y los recursos de información para la gestión de vulnerabilidades técnicas?	PARCIAL	
4	¿Se toman las previsiones de tiempo para atender las vulnerabilidades técnicas en consecuencia con su nivel de daño potencial?	SI	
5	¿La aplicación de parches se aplica conforme el control formal de cambios?	SI	
6	¿Se valoran los riesgos de la vulnerabilidad en relación al riesgo de aplicación de parches?	SIN OBSERVAR	
7	¿Se prueban y evalúan los parches antes de su instalación?	SIN OBSERVAR	
8	¿Existen vulnerabilidades técnicas que no se han podido remediar con parches de actualización?	SIN OBSERVAR	
9	¿Se registran y mantienen registros de eventos para el escaneo de vulnerabilidades?	SIN OBSERVAR	
10	¿Se comunican los resultados de la evaluación de vulnerabilidades a los responsables de la gestión de incidentes?	SIN OBSERVAR	
11	¿Los usuarios están autorizados a instalar software en los equipos?	SIN OBSERVAR	

12	¿Se han definido qué tipo de instalaciones de software están permitidas?	**SIN OBSERVAR**	
13	¿Se han definido qué tipo de instalaciones de software están prohibidas?	**SIN OBSERVAR**	
14	¿Se han establecido un proceso de autorización para la instalación de software por parte de para los usuarios?	**SIN OBSERVAR**	
15	¿Se han definido los orígenes autorizados de software para la instalación por parte de los usuarios?	**SIN OBSERVAR**	

AUD-SGSI-23-2020	**Guía de Auditoría Evaluación del Sistema de Gestión de la Seguridad de la Información**

Nombre de la organización evaluada:

Área evaluada: **Fecha:**

Responsable de la evaluación:

Objetivo: Indagar sobre la existencia de controles para asegurar la protección de la información en las redes y sus recursos de soporte de procesamiento de información.

Dominio ISO/IEC 27001: A.13 Seguridad en las comunicaciones

Guía de referencia ISO/IEC 27002: 13.1.1, 13.1.2 , 13.1.3

Práctica de gestión: DSS05.02

No.	Criterio a evaluar	Cumplimiento	Observaciones
1	¿Se tienen definidos los roles y responsabilidades para la gestión de equipos de red?	**SI**	
2	¿Están separadas las actividades de la infraestructura de red de la administración de los sistemas operacionales?	**SI**	
3	¿Existe monitorización de la red y los dispositivos que se conectan a ella?	**SI**	
4	¿Hay un sistema de autenticación para todos los accesos a la red de la organización?	**NO**	
5	¿Existe segmentación adecuada de la red?	**PARCIAL**	
6	¿La organización gestiona el cumplimiento de los acuerdos en la contratación de los servicios de red?	**SIN OBSERVAR**	
7	¿La organización contrata externamente servicios de red para la seguridad de la información? Por ejemplo, firewall, IPS, IDS, WAF, VPN, entre otros.	**SIN OBSERVAR**	
8	¿Los servicios de red cuentan con tecnologías de seguridad, tales como, autenticación, encriptación, controles de conexión?	**SIN OBSERVAR**	
9	¿Existe un monitoreo de los servicios de red?	**SIN OBSERVAR**	
10	¿Se revisan regularmente las configuraciones de los servicios de red para la seguridad de la información?	**SIN OBSERVAR**	
11	¿La organización tiene defina una estructura para la segmentación de red?	**SIN OBSERVAR**	
12	¿La segmentación de la red está clasificada en dominios de confianza? Por ejemplo, público, equipos de escritorio, servidores.	**SIN OBSERVAR**	

13	¿Existen segmentación en la red inalámbrica? Por ejemplo, público en general y dominios.	**SIN OBSERVAR**	
14	¿La servicios a través de la red inalámbrica están reducidos?	**SIN OBSERVAR**	
15	¿La autenticación de acceso para la red inalámbrica se realiza a través de un portal de acceso?	**SIN OBSERVAR**	

AUD-SGSI-24-2020	Guía de Auditoría Evaluación del Sistema de Gestión de la Seguridad de la Información

Nombre de la organización evaluada:

Área evaluada: **Fecha:**

Responsable de la evaluación:

Objetivo: Determinar la existencia de políticas, procedimientos y controles para mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.

Dominio ISO/IEC 27001: A.13 Seguridad en las comunicaciones

Guía de referencia ISO/IEC 27002: 13.2.1, 13.2.2, 13.2.3, 13.2.4

Práctica de gestión: APO01.04 y DSS05.02

No.	Criterio a evaluar	Cumplimiento	Observaciones
1	¿Se tiene una política para la transferencia de información aprobada, publicada y comunicada?	SI	
2	¿Se dispone de procedimientos y controles formales para la transferencia de información?	PARCIAL	
3	¿Los procedimientos adoptados protegen la información transferida contra interceptación, copiado, modificación, enrutado y destrucción?	PARCIAL	
4	¿Los procedimientos adoptados incluyen la detección y protección contra software malicioso?	NO APLICA	
5	¿Los procedimientos señalan como proteger la información sensible comunicada como adjunto?	SIN OBSERVAR	
6	¿Se usan técnicas criptográficas en la transferencia de información?	SIN OBSERVAR	
7	¿Existen directrices para la retención y disposición de toda correspondencia del negocio?	SIN OBSERVAR	
8	¿Existen controles y restricciones asociadas con el correo electrónico y otros medios de comunicación? Por ejemplo envío automático a correos externos.	SIN OBSERVAR	
9	¿Todos los empleados reciben concientización para no revelar información del negocio por ningún medio?	SIN OBSERVAR	
10	¿Existen directrices para no dejar información confidencial en contestadoras o mensajes de voz?	SIN OBSERVAR	
11	¿Los empleados tienen señalados los medios	SIN OBSERVAR	

	oficiales para la transferencia y comunicación de información?		
12	¿Se tienen contemplados todos los tipos diferentes de transferencia de información dentro de los controles? Por ejemplo, email, FTP, servicios de nube, grupos, wifi, USB.	SIN OBSERVAR	
13	¿Se motiva a los empleados a no mantener conversaciones confidenciales de la empresa en lugares públicos?	SIN OBSERVAR	
14	¿Se mantienen acuerdos de transferencia segura de información entre la organización y partes externas?	SIN OBSERVAR	
15	¿Los acuerdos de transferencia señalan las responsabilidades para controlar, notificar, despacho y recibo de la información?	SIN OBSERVAR	
16	¿Los acuerdos de transferencia señalan el uso de soluciones de transferencia de información seguros y confiables?	SIN OBSERVAR	
17	¿Los acuerdos de transferencia tienen niveles aceptables de control de acceso, para ambas partes?	SIN OBSERVAR	
18	¿Se ha dispuesto de plataformas oficiales para el uso de mensajería electrónica por parte de todos los empleados? Por ejemplo, email, chats, foros.	SIN OBSERVAR	
19	¿Se usa mensajería electrónica para interactuar con clientes? Por ejemplo, redes sociales o chats propios	SIN OBSERVAR	
20	¿Existe autorización y directrices formales para el intercambio de información a través de redes sociales y mensajería instantánea?	SIN OBSERVAR	
21	¿La organización tiene firmados acuerdos de confidencialidad con los empleados y las terceras partes?	SIN OBSERVAR	
22	¿Los acuerdos de confidencialidad y no divulgación son revisados por el departamento legal?	SIN OBSERVAR	
23	¿Los acuerdos de confidencialidad declaran la información que se debe proteger?	SIN OBSERVAR	
24	¿Los acuerdos de confidencialidad declaran la duración y acciones requeridas para cuando termina el acuerdo?	SIN OBSERVAR	
25	¿Los acuerdos de confidencialidad tienen señaladas las responsabilidades y acciones de los firmantes para evitar la divulgación no autorizada de información?	SIN OBSERVAR	

26	¿Los acuerdos de confidencialidad tienen señalado el uso permitido de información confidencial y los derechos del firmante para usar la información?	**SIN OBSERVAR**	
27	¿Los acuerdos de confidencialidad señalan las acciones a tomar en caso de violación del acuerdo?	**SIN OBSERVAR**	
28	¿Los acuerdos de confidencialidad son revisados periódicamente y cuando ocurren cambios que influyan en las necesidades de protección de la información?	**SIN OBSERVAR**	

AUD-SGSI-25-2020	**Guía de Auditoría Evaluación del Sistema de Gestión de la Seguridad de la Información**

Nombre de la organización evaluada:

Área evaluada: **Fecha:**

Responsable de la evaluación:

Objetivo: Indagar la existencia de requisitos para asegurar que la seguridad de la información sea parte integral de los sistemas de información a través de todo el ciclo de vida. Así como los requisitos para los sistemas de información que proporcionan los servicios a través de redes públicas.

Dominio ISO/IEC 27001: A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información

Guía de referencia ISO/IEC 27002: 14.1.1, 14.1.2, y 14.1.3 **Práctica de gestión:** No aplica

No.	Criterio a evaluar	Cumplimiento	Observaciones
1	¿La organización ha desarrollado o hecho mejoras en los sistemas de información comprendidas dentro del periodo de evaluación?	SI	
2	¿Los proyectos han incluido requisitos de seguridad de la información para la adquisición, desarrollo y mantenimiento de sistemas de información?	SI	
3	¿Los proyectos incluyeron en las primeras etapas la identificación y gestión de requisitos de seguridad de la información?	SI	
4	¿Los requisitos de seguridad son obligatorios para todos los nuevos sistemas o cambios en los sistemas existentes?	NO	
5	¿Los requisitos de seguridad consideran el nivel de confianza declarada de los usuarios para obtener los requisitos de autenticación de usuario?	SI	
6	¿Los requisitos de seguridad consideran las necesidades de protección de los activos involucrados en cuanto a confidencialidad, disponibilidad e integridad?	SIN OBSERVAR	
7	¿Los requisitos de seguridad consideran los requisitos de otros controles de seguridad?	SIN OBSERVAR	
8	¿Los requisitos de seguridad consideran los requisitos obtenidos de los procesos de negocio?	SIN OBSERVAR	
9	¿Se ha dispuesto de guías de configuración de la seguridad de la información en el software implementado?	SIN OBSERVAR	

10	¿Se ha contratado la adquisición de soluciones o productos a proveedores externos dentro del periodo de evaluación?	**SIN OBSERVAR**	
11	¿Las soluciones o productos son evaluados y probados contra los requisitos de seguridad estipulados antes de la adquisición?	**SIN OBSERVAR**	
12	¿Las soluciones o productos adquiridos externamente cumplen un proceso de análisis de cumplimientos de requisitos para la seguridad de la información?	**SIN OBSERVAR**	
13	¿Existe un proceso formal de aceptación de las soluciones o productos, para desarrollos internos como para adquisiciones externas?	**SIN OBSERVAR**	
14	¿La organización usa o proporciona aplicaciones web para el comercio electrónico?	**SIN OBSERVAR**	
15	¿Los servicios de aplicaciones sobre redes públicas consideran aspectos de seguridad como control de acceso y autenticación de usuarios, integridad de datos y disponibilidad del servicio?	**SIN OBSERVAR**	
16	¿Los servicios de aplicaciones contienen validaciones de datos de entrada y salida, encriptación, autenticación de mensajes e irrenunciabilidad?	**SIN OBSERVAR**	
17	¿Los servicios de aplicaciones web usan conexiones seguras como HTTPS?	**SIN OBSERVAR**	
18	¿Los servicios de aplicaciones web señalan la responsabilidad civil asociada a cualquier transacción fraudulenta?	**SIN OBSERVAR**	
19	¿Los servicios de aplicaciones usan medios de pagos seguros y confiables?	**SIN OBSERVAR**	
20	¿Los servicios de aplicaciones informan los acuerdos de protección de información confidencial?	**SIN OBSERVAR**	
21	¿La seguridad de la información se incluye en los términos y condiciones del contrato de servicios de aplicaciones?	**SIN OBSERVAR**	
22	¿La organización provee transacciones en los servicios de aplicaciones y estos se protegen contra transmisión incompleta, alteración, divulgación, duplicación o reproducción no autorizada?	**SIN OBSERVAR**	
23	¿La organización contrata la protecciónde las transacciones para los servicios de aplicaciones?	**SIN OBSERVAR**	
24	¿La protección de las transacciones cumple con los requisitos legales y regulatorios de la jurisdicción en que se genera, se procesa y almacena la transacción?	**SIN OBSERVAR**	

AUD-SGSI-26-2020	**Guía de Auditoría Evaluación del Sistema de Gestión de la Seguridad de la Información**

Nombre de la organización evaluada:

Área evaluada: **Fecha:**

Responsable de la evaluación:

Objetivo: Determinar la existencia de gestiones para asegurar que la seguridad de la información sea diseñada e implementada dentro del ciclo de vida del desarrollo de sistemas de información.

Dominio ISO/IEC 27001: A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información

Guía de referencia ISO/IEC 27002: 14.2.1, 14.2.2, 14.2.3,14.2.4, 14.2.5, 14.2.6, 14.2.7, 14.2.8, 14.2.9

Práctica de gestión: APO01.04

No.	Criterio a evaluar	Cumplimiento	Observaciones
1	¿Se tiene una política de desarrollo seguro aprobada, publicada y comunicada?	SI	
2	¿El desarrollo seguro es un requisito para crear un sistema, arquitectura o software?	SI	
3	¿La política de desarrollo seguro considera la seguridad en ambientes de desarrollo?	PARCIAL	
4	¿Los ambientes de desarrollo usan repositorios seguros con control de acceso y control de cambios?	NO	
5	¿La política de desarrollo seguro considera la seguridad en el control de versiones?	SI	
6	¿La política de desarrollo seguro considera la seguridad en todas las fases del desarrollo de software?	SI	
7	¿La política de desarrollo seguro considera directrices de codificación seguras para los lenguajes de programación usados?	SIN OBSERVAR	
8	¿Los nuevos sistemas y cambios importantes a los sistemas actuales, cumplen un proceso formal de especificación, pruebas, control de calidad y gestión de implementación?	SIN OBSERVAR	
9	¿Existe un procedimiento formal de control de cambios dentro del ciclo de vida del desarrollo de software?	SIN OBSERVAR	
10	¿Los procedimientos de control de cambios incluyen niveles de autorización?	SIN OBSERVAR	
11	¿Los procedimientos de control de cambios identifican el software, la información, bases de datos y hardware que requieran	SIN OBSERVAR	

	corrección?		
12	¿Los procedimientos de control de cambios incluyen una aprobación formal antes de iniciar cualquier cambio?	SIN OBSERVAR	
13	¿Los procedimientos de control de cambios incluyen la necesidad de actualización de la documentación del sistema?	SIN OBSERVAR	
14	¿Los procedimientos de control de cambios incluyen el control de versiones para las actualizaciones de software?	SIN OBSERVAR	
15	¿Los procedimientos de control de cambios aseguran que se actualicen los procedimientos operacionales y que los usuarios puedan seguir realizando sus funciones?	SIN OBSERVAR	
16	¿Los procedimientos de control de cambios señalan el momento correcto para la implementación de cambios y que no afecte los procesos de negocios?	SIN OBSERVAR	
17	¿Se hace una valoración del riesgo y del impacto de los cambios para la seguridad existente antes de su aprobación?	SIN OBSERVAR	
18	¿Se han cambiado las plataformas de operación dentro el periodo de evaluación? Por ejemplo, sistema operativo, bases de datos.	SIN OBSERVAR	
19	¿Se revisan y ponen a prueba las aplicaciones críticas del negocio cuando se cambian las plataformas operacionales?	SIN OBSERVAR	
20	¿Existe un registro de los resultados de las pruebas y control de integridad de la información cuando se cambian las plataformas?	SIN OBSERVAR	
21	¿Se actualizan los planes de continuidad del negocio tras cambios en las plataformas operacionales?	SIN OBSERVAR	
22	¿Se hacen modificaciones a los paquetes de software adquiridos?	SIN OBSERVAR	
23	¿El proveedor puede realizar las modificaciones que la organización considere necesarias?	SIN OBSERVAR	
24	¿Se obtiene el consentimiento y participación del proveedor en modificaciones a paquetes de software?	SIN OBSERVAR	
25	¿El proveedor puede continuar dando soporte después de una modificación por parte de la organización?	SIN OBSERVAR	
26	¿El contrato con el proveedor posibilita la realización de modificaciones por parte de la organización?	SIN OBSERVAR	

27	¿Se realizan copias de respaldo de los paquetes de software originales antes de hacer modificaciones?	SIN OBSERVAR	
28	¿La organización sería la responsable de las actualizaciones futuras como resultado de una modificación en los paquetes de software?	SIN OBSERVAR	
29	¿Se ha explorado la pasividad de adquirir paquetes de software que cubran las necesidades del negocio, antes de incurrir en modificaciones internas?	SIN OBSERVAR	
30	¿Se tienen establecidos y documentados principios de construcción de sistemas de información seguros?	SIN OBSERVAR	
31	¿El personal involucrado en el desarrollo de sistemas recibe capacitación para aplicar principios de seguridad en la ingeniería de sistemas?	SIN OBSERVAR	
32	¿Se aplican procedimientos de construcción segura a las actividades de implementación de sistemas internos?	SIN OBSERVAR	
33	¿Se han establecido ambientes seguros para las tareas de desarrollo e integración de sistemas? Con las personas, procesos y tecnología	SIN OBSERVAR	
34	¿Se hace una clasificación del nivel de protección para cada ambiente de desarrollo específico?	SIN OBSERVAR	
35	¿Se analizan y establecen los requisitos internos y externos, controles y carácter sensible de los datos para cada ambiente de desarrollo específico?	SIN OBSERVAR	
36	¿La organización ha contratado el desarrollo de software externamente dentro del periodo de tiempo evaluado?	SIN OBSERVAR	
37	¿Los contratos consideran los acuerdos de licenciamiento, propiedad de los códigos y derechos de propiedad intelectual?	SIN OBSERVAR	
38	¿Los contratos incluyen los requisitos de desarrollo seguro dentro del ciclo de desarrollo?	SIN OBSERVAR	
39	¿Los contratos incluyen como requisito el suministro de evidencia de pruebas de vulnerabilidades, calidad, exactitud, seguridad y privacidad?	SIN OBSERVAR	
40	¿Los contratos incluyen el derecho a controles de auditoría?	SIN OBSERVAR	
41	¿Los contratos exigen la entrega de la documentación del ambiente de desarrollo usado?	SIN OBSERVAR	
42	¿Los contratos exigen el acceso al código fuente si el código ejecutable necesita ser	SIN OBSERVAR	

	modificado?		
43	¿Durante el desarrollo se llevan a cabo pruebas de funcionalidad de la seguridad?	**SIN OBSERVAR**	
44	¿Se realizan pruebas de aceptación para sistemas de información nuevo, actualizaciones o nuevas versiones?	**SIN OBSERVAR**	
45	¿Las pruebas de aceptación incluyen los requisitos de seguridad de la información planteados por la organización?	**SIN OBSERVAR**	
46	¿Las pruebas de aceptación replican entornos ysituaciones operativas reales de la organización?	**SIN OBSERVAR**	
47	¿Se realizan pruebas de aceptación con herramientas para el análisis de código y escaneo devulnerabilidades?	**SIN OBSERVAR**	
48	¿Se realizan pruebas de aceptación para los usuarios antes de la aprobación final?	**SIN OBSERVAR**	
49	¿Los defectos relacionados con la seguridad surgidos de la aplicación de pruebas aceptación de sistemas de información son corregidos antes de la aceptación?	**SIN OBSERVAR**	

AUD-SGSI-27-2020	**Guía de Auditoría Evaluación del Sistema de Gestión de la Seguridad de la Información**

Nombre de la organización evaluada:

Área evaluada: **Fecha:**

Responsable de la evaluación:

Objetivo: Verificar la protección de los datos utilizados para pruebas de los sistemas de información.

Dominio ISO/IEC 27001: A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información

Guía de referencia ISO/IEC 27002: 14.3.1 **Práctica de gestión:** No aplica

No.	Criterio a evaluar	Cumplimiento	Observaciones
1	¿Se usan datos operacionales con datos personales o información sensible para propósitos de pruebas?	**SI**	
2	¿Se utilizan mecanismos de protección para los datos de prueba, como la seudoniminazación, enmascaramiento, datos falsos?	**NO APLICA**	
3	¿Los detalles y contenido de la información sensible se modifica para proteger los datos?	**SI**	
4	¿Cada copia de información operacional usada en ambientes de prueba es aprobada por el dueño del activo?	**SI**	
5	¿Existen un proceso para crear, preparar y utilizar adecuadamente datos de prueba según las características del sistema de información a probar?	**SIN OBSERVAR**	
6	¿Los sistemas de aplicación de pruebas siguen los mismos procedimientos de control de acceso que se aplican a los sistemas operacionales?	**SIN OBSERVAR**	
7	¿La información operacional es borrada inmediatamente del ambiente de pruebas después de finalizada la prueba?	**SIN OBSERVAR**	
8	¿Existen registros de las actividades de copiado y uso de información para pruebas?	**SIN OBSERVAR**	
9	¿Los volúmenes de información usados para pruebas se acercan a los entornos reales de operación?	**SIN OBSERVAR**	
10	¿Se ha explorado la posibilidad de usar generadores de datos de pruebas?	**SIN OBSERVAR**	

AUD-SGSI-28-2020	**Guía de Auditoría Evaluación del Sistema de Gestión de la Seguridad de la Información**

Nombre de la organización evaluada:

Área evaluada: **Fecha:**

Responsable de la evaluación:

Objetivo: Constatar la existencia de gestiones para asegurar la protección de los activos que son accesibles a los proveedores en la prestación de los servicios contratados.

Dominio ISO/IEC 27001: A.15 Relaciones con los proveedores

Guía de referencia ISO/IEC 27002: 15.1.1, 15.1.2 , 15.1.3 **Práctica de gestión:** APO01.04 y DSS05.05

No.	Criterio a evaluar	Cumplimiento	Observaciones
1	¿Se tiene una política de seguridad de la información para proveedores aprobada, publicada y comunicada?	SI	
2	¿Se tienen identificados y documentados los tipos de proveedores de TI?	SI	
3	¿Se han definido los controles de acceso según el tipo de información y tipo de proveedor?	NO	
4	¿Los proveedores son monitoreados rutinariamente para asegurar el cumplimiento de los procedimientos y requisitos de seguridad?	PARCIAL	
5	¿Se realizan controles de exactitud y totalidad a la información o procesamiento de información realizada por proveedores?	NO APLICA	
6	¿Se han definido las obligaciones de los proveedores para proteger la información de la organización?	SI	
7	¿Se dispone de un plan de manejo de incidentes y contingencias para actividades realizadas por proveedores?	SIN OBSERVAR	
8	¿El personal que se relaciona con proveedores ha recibido formación con respecto a las reglas apropiadas de interacción y comportamiento con base en el tipo de proveedor y tipo de acceso?	SIN OBSERVAR	
9	¿Se han definido procedimientos para asegurar la seguridad de la información durante transacciones necesarias de información o sobre gestiones en las instalaciones de procesamiento de información llevadas a cabo por	SIN OBSERVAR	

	proveedores?		
10	¿Se han firmado acuerdos de confidencialidad o no divulgación con proveedores que accedan información sensible o crítica para la organización?	**SIN OBSERVAR**	
11	¿La organización realiza una evaluación de riesgos para cada activo, aplicación, servicio, tarea o proceso que contrata con un proveedor?	**SIN OBSERVAR**	
12	¿Los contratos con proveedores incluyen los requisitos y controles de seguridad de la información bajo los cuales ambas partes firman un acuerdo?	**SIN OBSERVAR**	
13	¿Los términos del contrato con proveedores contiene una descripción de la información que se va a suministrar o a la que se va a tener acceso y los métodos para suministrar o acceder a ella?	**SIN OBSERVAR**	
14	¿Los términos del contrato con proveedores señalan el esquema de clasificación de la información que utiliza la organización?	**SIN OBSERVAR**	
15	¿Los términos del contrato con proveedores consideran los requisitos legales, reglamentarios, derechos de propiedad intelectual y como la organización se asegurará que se cumplan?	**SIN OBSERVAR**	
16	¿Los términos del contrato con proveedores señalan la obligación de ambas partes de acordar controles para el acceso, desempeño, seguimiento, reporte y auditoría?	**SIN OBSERVAR**	
17	¿Los términos de contrato con proveedores incluyen las reglas de uso aceptable e inaceptable de la información?	**SIN OBSERVAR**	
18	¿Los términos del contrato con proveedores incluyen una lista del personal del proveedor que prestará servicios y tendrá acceso a la información?	**SIN OBSERVAR**	
19	¿Los términos del contrato con proveedores incluyen la obligación de informar cualquier cambio de personal dedicado a la prestación de servicios dentro del acuerdo firmado?	**SIN OBSERVAR**	
20	¿Los términos del contrato con proveedores incluyen los requisitos y procedimientos de gestión de incidentes?	**SIN OBSERVAR**	
21	¿Los términos del contrato con proveedores señalan la necesidad de formación y toma de conciencia para procedimientos que la organización considere relevantes?	**SIN OBSERVAR**	

22	¿Los términos del contrato con proveedores incluyen una persona de contacto para asuntos de seguridad?	**SIN OBSERVAR**	
23	¿Los términos del contrato con proveedores incluyen el derecho a auditar los procesos y controles de seguridad de la información de los proveedores relacionados con el acuerdo?	**SIN OBSERVAR**	
24	¿Los términos del contrato con proveedores señalan los procesos de solución de defectos y resolución de conflictos?	**SIN OBSERVAR**	
25	¿Los términos del contrato con proveedores señalan las obligaciones de cumplimiento de los requisitos de seguridad de la organización?	**SIN OBSERVAR**	
26	¿Los términos del contrato con proveedores señalan las condiciones de finalización del acuerdo en caso de incapacidad de suministrar los productos o servicios?	**SIN OBSERVAR**	
27	¿La organización analiza los riesgos asociados a la cadena de suministro de productos y servicios de las TICs?	**SIN OBSERVAR**	
28	¿La organización utiliza criterios de seguridad asociados a la cadena de suministro para la elección de proveedores de confianza?	**SIN OBSERVAR**	
29	¿La organización incluye en sus contratos con proveedores requisitos para abordar los riesgos de seguridad asociados a la cadena de suministro?	**SIN OBSERVAR**	
30	¿Se incluyen criterios de obsolescencia para cada servicio, producto o tecnología de comunicación a la hora de elegir o contratar un proveedor?	**SIN OBSERVAR**	

AUD-SGSI-29-2020	**Guía de Auditoría Evaluación del Sistema de Gestión de la Seguridad de la Información**

Nombre de la organización evaluada:

Área evaluada: **Fecha:**

Responsable de la evaluación:

Objetivo: Indagar si se mantiene un nivel de seguridad de la información y la entrega de servicios alineado con los acuerdos con proveedores.

Dominio ISO/IEC 27001: A.15 Relaciones con los proveedores

Guía de referencia ISO/IEC 27002: 15.2.1, 15.2.2 **Práctica de gestión:** No aplica

No.	Criterio a evaluar	Cumplimiento	Observaciones
1	¿La organización tiene asignada a una persona o equipo la responsabilidad de seguimiento de los niveles de servicio de los proveedores?	SI	
2	¿Se revisan los niveles de desempeño del servicio en relación con los acuerdos?	SI	
3	¿Se revisan los reportes de servicio del proveedor y concentran reuniones para revisar avances?	SI	
4	¿Las reuniones con proveedores se utilizan para resolver y gestionar cualquier problema o incumplimiento identificado?	SIN OBSERVAR	
5	¿Se generan informes o métricas relacionadas a las reuniones y las decisiones tomadas?	SIN OBSERVAR	
6	¿El proveedor suministra información acerca de incidentes de seguridad de la información y se revisan en atención a los acuerdos?	SIN OBSERVAR	
7	¿Se revisan los rastros de auditoría del proveedor, los registros de eventos de seguridad de la información o cualquier falla relacionado con el servicio entregado?	SIN OBSERVAR	
8	¿Se da seguimiento a las actividades del proveedor para monitorear aspectos de seguridad de la información y su capacidad de servicio?	SIN OBSERVAR	
9	¿Cuándo se modifican los servicios prestados por un proveedor, se aplica un nuevo análisis de riesgos al nuevo escenario?	SIN OBSERVAR	
10	¿Cuándo se modifican los servicios prestados por un proveedor, se cambian o amplían los acuerdos de prestación de servicios?	SIN OBSERVAR	

11	¿Cuándo se modifican los servicios prestados por un proveedor, se actualizan los acuerdos en concordancia con los cambios hechos en la organización?	**SIN OBSERVAR**	
12	¿Cuándo se modifican los servicios prestados por un proveedor, se considera el uso de nuevas tecnologías, productos, herramientas o mejoras en las redes?	**SIN OBSERVAR**	
13	¿Cuándo se modifican los servicios prestados por un proveedor, se considera el cambio del proveedor?	**SIN OBSERVAR**	

AUD-SGSI-30-2020	**Guía de Auditoría** **Evaluación del Sistema de Gestión de la Seguridad de la Información**

Nombre de la organización evaluada:

Área evaluada: **Fecha:**

Responsable de la evaluación:

Objetivo: Determinar la existencia y cumplimiento de un enfoque coherente y efectivo para la gestión de los incidentes de seguridad de la información, incluyendo la comunicación de los eventos y debilidades.

Dominio ISO/IEC 27001: A.16 Gestión de incidentes de seguridad de la información

Guía de referencia ISO/IEC 27002: 16.1.1, 16.1.2, 16.1.3, 16.1.4, 16.1.5, 16.1.6, 16.1.7

Práctica de gestión: APO13.02, APO13.03 y DSS05.07

No.	Criterio a evaluar	Cumplimiento	Observaciones
1	¿La organización tiene acordado objetivos, directrices y prioridades para la gestión de incidentes de seguridad de la información?	**SI**	
2	¿La organización ha designado un responsable oresponsables para la gestión de incidentes de seguridad de la información?	**SI**	
3	¿Existen procedimientos para la planificación y preparación de respuesta a incidentes?	**SI**	
4	¿Cada empleado asido informado sobre su responsabilidad en la comunicación de eventos o incidentes de seguridad?	**SI**	
5	¿Existen procedimientos para el seguimiento, detección, análisis y reporte de eventos e incidentes de seguridad de la información?	**PARCIAL**	
6	¿Existen procedimientos para el manejo de evidencia forense?	**SI**	
7	¿Existen procedimientos para la valoración y toma de decisiones sobre eventos de seguridad de la información?	**SIN OBSERVAR**	
8	¿Existen procedimientos de respuesta a incidentes, que incluyan la recuperación y comunicación del incidentes?	**SIN OBSERVAR**	
9	¿El perfil del puesto de los responsables de manejar incidentes es acorde a las actividades de gestión de incidentes?	**SIN OBSERVAR**	
10	¿Se tiene asignado un punto de contado para la detección y reporte de incidentes de seguridad?	**SIN OBSERVAR**	

11	¿Los responsables de la gestión de incidentes mantienen contacto con autoridades, grupos de interés o foros relacionados con incidentes de seguridad?	**SIN OBSERVAR**	
12	¿Se han establecido formatos uniformes para el reporte de eventos de seguridad?	**SIN OBSERVAR**	
13	¿Se tienen establecido los pasos a seguir en caso de un evento de seguridad de la información?	**SIN OBSERVAR**	
14	¿Se dispone de un proceso disciplinario formal para empleados que cometen violaciones a la seguridad?	**SIN OBSERVAR**	
15	¿Se dispone de procesos de retroalimentación después de que un evento haya sido tratado y cerrado?	**SIN OBSERVAR**	
16	¿Se dispone de contactos externos para aquellos casos de incidentes de seguridad que no puedan manejarse internamente?	**SIN OBSERVAR**	
17	¿Se dispone de herramientas tecnológicas para la detección, análisis, seguimiento, evaluación y reporte de eventos de seguridad de la información?	**SIN OBSERVAR**	
18	¿Existe evidencia de la notificación, registro, clasificación, tratamiento y cierre de incidentes de seguridad de la información?	**SIN OBSERVAR**	
19	¿Existen vías de comunicación para que todos los empleados puedan informar sobre posibles eventos o incidentes de seguridad? Por ejemplo, email, mesa de ayuda, persona de contacto.	**SIN OBSERVAR**	
20	¿Todos los usuarios (empleados y proveedores) han recibido formación para identificar un evento o incidente en la seguridad y los pasos para reportarlo?	**SIN OBSERVAR**	
21	¿Se ha comunicado a todos los usuarios las posibles situaciones que se deberían considerar para el reporte de eventos de seguridad de la información?	**SIN OBSERVAR**	
22	¿Se ha comunicado a todos los usuarios la exigencia de observar y reportar cualquier debilidad de seguridad vista o sospechada en los sistemas de información de la organización?	**SIN OBSERVAR**	
23	¿Se prohíbe explícitamente a todos los usuarios verificar, explotar o poner a prueba las debilidades de seguridad sospechadas?	**SIN OBSERVAR**	

24	¿Se ha definido una escala de clasificación y priorización de eventos e incidentes de seguridad de la información?	SIN OBSERVAR	
25	¿La evaluación de eventos o incidentes es realizada por los responsables de la gestión de incidentes?	SIN OBSERVAR	
26	¿Se lleva un registro de la evaluación de eventos o incidentes para ser usado en el proceso de retroalimentación?	SIN OBSERVAR	
27	¿Se dispone de un plan de respuesta a incidentes de seguridad de la información?	SIN OBSERVAR	
28	¿La respuesta a incidentes considera la identificación, recolección, adquisición y preservación de evidencia.	SIN OBSERVAR	
29	¿La respuesta a incidentes señala la necesidad de análisis forense según se requiera?	SIN OBSERVAR	
30	¿La respuesta a incidentes considera las situaciones o parámetros en los cuales se requiere elevar incidentes a una instancia superior?	SIN OBSERVAR	
31	¿Se documentan todas las actividades de respuesta a incidentes y los resultados de las mismas?	SIN OBSERVAR	
32	¿La respuesta a incidentes tiene señalada la línea de comunicación y el responsable de informar cualquier detalle a las partes internas y externas pertinentes?	SIN OBSERVAR	
33	¿La respuesta a incidentes señala las condiciones de tratamiento de las debilidades para declarar el cierre formal del incidente?	SIN OBSERVAR	
34	¿Se emite un informe con el análisis del incidente para señalar las causas y los costos de la atención?	SIN OBSERVAR	
35	¿Se mantiene una base de conocimiento sobre los incidentes de seguridad de la información atendidos en la organización?	SIN OBSERVAR	
36	¿Se tienen identificados los incidentes más recurrentes y de alto impacto?	SIN OBSERVAR	
37	¿La atención a incidentes ha generado recomendaciones formales para la incorporación de nuevos controles o mejora de los existentes?	SIN OBSERVAR	
38	¿Los conocimientos adquiridos en la atención a incidentes se han usado dentro del proceso de toma de conciencia, formación y capacitación en seguridad de la información?	SIN OBSERVAR	

39	¿Se dispone de personal capacitado y confiable para el tratamiento de evidencia forense?	**SIN OBSERVAR**	
40	¿Se tienen procesos internos para el tratamiento de evidencia digital para propósitos de acciones legales y disciplinarios?	**SIN OBSERVAR**	
41	¿Se dispone de herramientas para la identificación, recolección, adquisición y preservación de evidencia digital?	**SIN OBSERVAR**	
42	¿Se tienen identificadas las situaciones en las cuales es necesario contratar un proveedor para el tratamiento de evidencia digital?	**SIN OBSERVAR**	

AUD-SGSI-31-2020	**Guía de Auditoría** **Evaluación del Sistema de Gestión de la Seguridad de la Información**

Nombre de la organización evaluada:

Área evaluada: **Fecha:**

Responsable de la evaluación:

Objetivo: Constatar si la continuidad de la seguridad de la información está integrada en los sistemas de gestión de la continuidad de negocio de la organización.

Dominio ISO/IEC 27001: A.17 Aspectos de seguridad de la información en la gestión de la continuidad del negocio

Guía de referencia ISO/IEC 27002: 17.1.1, 17.1.2 y 17.1.3

Práctica de gestión: DSS04.03, DSS04.04

No.	Criterio a evaluar	Cumplimiento	Observaciones
1	¿La organización dispone de un Programa de Continuidad del Negocio?	SI	
2	¿Los requisitos de la seguridad de la información están integrados en el Programa de Continuidad del Negocio?	NO	
3	¿Los aspectos de la seguridad de la información están incluidos en el análisis de impacto al negocio (BIA)?	PARCIAL	
4	¿El plan de recuperación de desastres (DRP) ha tomado en cuenta la seguridad de la información?	NO APLICA	
5	¿El análisis de riesgos tiene señalados riesgos que impacten a la seguridad de los sistemas de información?	SI	
6	¿La organización cuenta con una estructura de gestión para prepararse, mitigar y responder a un evento perturbador?	SIN OBSERVAR	
7	¿La organización cuenta con personal capacitado para manejar y mantener la seguridad de la información ante una situación adversa?	SIN OBSERVAR	
8	¿Los especialistas de la seguridad de la información apoyan la definición y aplicación de controles en las tareas de continuidad del negocio?	SIN OBSERVAR	
9	¿Se han definido los controles de la seguridad de la información dentro del plan de continuidad del negocio?	SIN OBSERVAR	
10	¿Se han definido los controles de la seguridad de la información dentro del DRP?	SIN OBSERVAR	

11	¿El DRP incluye las excepciones a los controles de seguridad durante y después de una situación adversa?	**SIN OBSERVAR**	
12	¿Se dispone de procesos, procedimientos y controles documentados requeridos durante una situación adversa, señalando los pasos de acción y los responsables de ejecutarlos?	**SIN OBSERVAR**	
13	¿Se dispone de un Plan de Pruebas para el Programa de Continuidad del Negocio que incluya los procedimientos y controles de la seguridad de la información?	**SIN OBSERVAR**	
14	¿Los resultados de las pruebas son discutidos y generan oportunidades de mejora para la gestión de la continuidad?	**SIN OBSERVAR**	
15	¿Se revisa la validez y eficacia de las medidas de continuidad, cuando hay cambios en sistemas y procesos?	**SIN OBSERVAR**	

AUD-SGSI-32-2020	**Guía de Auditoría Evaluación del Sistema de Gestión de la Seguridad de la Información**

Nombre de la organización evaluada:

Área evaluada: **Fecha:**

Responsable de la evaluación:

Objetivo: Constatar la implementación de los recursos de procesamiento de información con redundancia suficiente para asegurar ladisponibilidad.

Dominio ISO/IEC 27001: A.17 Aspectos de seguridad de la información en la gestión de la continuidad del negocio

Guía de referencia ISO/IEC 27002: 17.2.1 **Práctica de gestión:** DSS04.03, DSS04.04 y DSS04.07

No.	Criterio a evaluar	Cumplimiento	Observaciones
1	¿Los requisitos del negocio justifican la necesidad de sistemas de procesamiento de información redundantes?	SIN OBSERVAR	
2	¿Se puede garantizar la disponibilidad de los sistemas de información con la arquitectura existente?	SIN OBSERVAR	
3	¿Se tienen identificado los sistemas de información críticos que no pueden garantizar la disponibilidad exigida por los procesos de negocio?	SIN OBSERVAR	
4	¿Los sistemas de procesamiento de información redundantes corresponden a una arquitectura interna?	SIN OBSERVAR	
5	¿Los sistemas de procesamiento de información redundantes externos están dentro del territorio nacional?	SIN OBSERVAR	
6	¿Los sistemas de procesamiento de información redundantes tienen pruebas a la integridad y confidencialidad de la información?	SIN OBSERVAR	
7	¿Los sistemas de procesamiento de información redundantes están incluidos en un plan de pruebas?	SIN OBSERVAR	
8	¿El plan de pruebas a los sistemas de información redundantes cumple con las fechas programadas?	SIN OBSERVAR	
9	¿Se genera evidencia de los resultados de las pruebas a los sistemas de información redundantes?	SIN OBSERVAR	
10	¿La transición entre el sistema principal y el sistema redundante ocurre sin interrupciones?	SIN OBSERVAR	

AUD-SGSI-33-2020	**Guía de Auditoría Evaluación del Sistema de Gestión de la Seguridad de la Información**

Nombre de la organización evaluada:

Área evaluada: **Fecha:**

Responsable de la evaluación:

Objetivo: Identificar y verificar la legislación aplicable para evitar brechas entre las obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con seguridad de la información y cualquier requisito de seguridad.

Dominio ISO/IEC 27001:A.18 Cumplimiento

Guía de referencia ISO/IEC 27002: 18.1.1, 18.1.2, 18.1.3, 18.1.4, 18.1.5 **Práctica de gestión:** No aplica

No.	Criterio a evaluar	Cumplimiento	Observaciones
1	¿Están identificados todos los requisitos legales y contractuales aplicables a la organización y a los sistemas de información?	SI	
2	¿Están definidos los responsables para el cumplimiento de los requisitos legales y contractuales?	SI	
3	¿Están definidos los controles para el cumplimiento de los requisitos legales y contractuales?	SIN OBSERVAR	
4	¿Se tiene publicada una política para el cumplimiento de los derechos de propiedad intelectual en el uso legal de software y productos informáticos?	SIN OBSERVAR	
5	¿Se revisa periódicamente que solo se utilice software con licencia?	SIN OBSERVAR	
6	¿Se controla el número máximo de usuarios por licencia?	SIN OBSERVAR	
7	¿Se mantiene un registro con todos los activos que tienen requisitos para proteger los derechos de propiedad intelectual?	SIN OBSERVAR	
8	¿Se a comunicado a los usuarios la lista de software y productos informáticos para uso legal?	SIN OBSERVAR	
9	¿Se han publicado directrices sobre la retención, almacenamiento, tratamiento y eliminación de registros y información?	SIN OBSERVAR	
10	¿Se mantiene un calendario de retención que señale los registros y el periodo por el cual se deben retener?	SIN OBSERVAR	

11	¿Se mantiene un inventario de los registros con base en el esquema de clasificación de la organización?	**SIN OBSERVAR**	
12	¿Se garantiza la privacidad y protección de los datos personales que maneja la organización?	**SIN OBSERVAR**	
13	¿Se ha designado un responsable para el manejo de la privacidad de los datos personales?	**SIN OBSERVAR**	
14	¿Se conocen las normativas vigentes para el uso de controles criptográficos?	**SIN OBSERVAR**	
15	¿Existen limitaciones o restricciones legales para el uso de medios o funciones criptográficas?	**SIN OBSERVAR**	
16	¿Existen requisitos legales de cifrado de información que deba cumplir obligatoriamente la organización?	**SIN OBSERVAR**	

AUD-SGSI-34-2020	**Guía de Auditoría Evaluación del Sistema de Gestión de la Seguridad de la Información**

Nombre de la organización evaluada:

Área evaluada: **Fecha:**

Responsable de la evaluación:

Objetivo: Verificar que la seguridad de la información fue implementada y opere de acuerdo con las políticas y procedimientos de la organización.

Dominio ISO/IEC 27001: A.18 Cumplimiento

Guía de referencia ISO/IEC 27002: 18.2.1, 18.2.2 , 18.2.3

Práctica de gestión: APO01.08 y APO13.03

No.	Criterio a evaluar	Cumplimiento	Observaciones
1	¿La organización ha contratado revisiones independientes de cumplimiento de la seguridad de la información?	**SI**	
2	¿Los objetivos y alcance de la revisión de la seguridad de la información son autorizados por la Junta directiva?	**SI**	
3	¿Los resultados de la última revisión independiente han generado acciones correctivas?	**PARCIAL**	
4	¿Se controla el acceso a las herramientas de auditoría de los sistemas de información?	**SI**	
5	¿Cada área dispone de un plan anual de revisiones de cumplimiento de políticas y procedimientos de seguridad de la información?	**SI**	
6	¿Se dispone de diferentes métodos para realizar las revisiones de cumplimiento de políticas y procedimientos de seguridad de la información?	**SI**	
7	¿Se dispone de herramientas automáticas de medición y generación de informes de cumplimiento?	**NO**	
8	¿Se informan los resultados de las revisiones a los usuarios involucrados?	**SI**	
9	¿Existen incentivos para motivar el cumplimiento de las políticas y procedimientos de seguridad de la información?	**NO**	
10	¿Se mantienen registros de los resultados de las revisiones y de las acciones correctivas realizadas?	**SI**	

11	¿Se revisa periódicamente la configuración de los sistemas de información?	**SI**	
12	¿Se realizan periódicamente escaneos de vulnerabilidades?	**SI**	
13	¿Las revisiones de cumplimiento técnico son llevadas a cabo por personal conforme su rol y responsabilidades?	**SI**	

Estado de Cumplimiento Total

Dominios	SI	NO	PARCIAL	NO APLICA	SIN OBSERVAR
Total AUD-SGSI	99	38	30	11	508