DOI: http://dx.doi.org/10.23857/dc.v8i3

Ciencias Tecnologías de la Información y la Comunicación
Artículo de Investigación

Aplicación de la Norma ISO 27001 para la seguridad de los Sistemas de Información

Application of the ISO 27001 Standard for the security of Information Systems

Aplicação da Norma ISO 27001 para a segurança de Sistemas de Informação

Juan Carlos Yungán-Cazar [I]
jyungan@espoch.edu.ec
https://orcid.org/0000-0001-5682-0399

Carina Valeria Narváez-Contero [II]
vale245773@gmail.com
https://orcid.org/0000-0002-8085-0288

Correspondencia: jyungan@espoch.edu.ec

*Recibido: 29 de mayo del 2022 *Aceptado: 02 de junio de 2022 * Publicado: 19 de julio de 2022

I. Magíster en Interconectividad de Redes, Ingeniero en Sistemas Informáticos, Escuela Superior Politécnica de Chimborazo. Riobamba, Ecuador.
II. Ingeniera en Electrónica Control y Redes Industriales, Escuela Superior Politécnica de Chimborazo. Riobamba, Ecuador.

Resumen

La seguridad de datos y la información de cualquier tipo en la actualidad se ha convertido en un reto dentro de una organización. Un SGSI (Sistema de gestión de la seguridad de la información) hace que los riesgos de seguridad de la información para las organizaciones sean calculables y manejables. Mientras que la norma ISO 27001 proporciona un conjunto de controles para la seguridad de la información que una organización debe implementar en función de los resultados de una evaluación de riesgos y los requisitos de las partes interesadas. Es decir, para cada riesgo a tratar se implementará una combinación de diferentes tipos de controles. Para la implementación de la norma ISO 27001 recurre a ciclo de Deming que se encarga en el continuo mejoramiento de la seguridad de la información. Podemos concluir que: un SGSI actúa como un eje centralizado para salvaguardar y gestionar toda la información de una organización en un solo lugar.

Palabras Claves: Norma ISO 27001; Seguridad de la Información; Ciclo de Deming; Auditoría de Sistemas; Seguridad.

Abstract

The security of data and information of any kind today has become a challenge within an organization. An ISMS (Information Security Management System) makes information security risks for organizations calculable and manageable. While the ISO 27001 standard provides a set of controls for information security that an organization must implement based on the results of a risk assessment and the requirements of interested parties. In other words, for each risk to be treated, a combination of different types of controls will be implemented. For the implementation of the ISO 27001 standard, it uses the Deming cycle that is responsible for the continuous improvement of information security. We can conclude that: an ISMS acts as a centralized hub to safeguard and manage all the information of an organization in one place.

Keywords: ISO 27001 standard; Security of the information; Deming cycle; Systems Audit; Security.

Resumo

A segurança de dados e informações de qualquer tipo hoje se tornou um desafio dentro de uma organização. Um ISMS (Sistema de Gerenciamento de Segurança da Informação) torna os riscos de segurança da informação para as organizações calculáveis e gerenciáveis. Enquanto a norma ISO

27001 fornece um conjunto de controles para segurança da informação que uma organização deve implementar com base nos resultados de uma avaliação de risco e nos requisitos das partes interessadas. Ou seja, para cada risco a ser tratado, será implementada uma combinação de diferentes tipos de controles. Para a implementação da norma ISO 27001, utiliza o ciclo Deming que é responsável pela melhoria contínua da segurança da informação. Podemos concluir que: um SGSI atua como um hub centralizado para salvaguardar e gerenciar todas as informações de uma organização em um só lugar.

Palavras-chave: norma ISO 27001; Segurança das informações; Ciclo de Deming; Auditoria de Sistemas; Segurança.

Introducción

La información es de vital importancia tanto para las personas como para las organizaciones, está más disponible y más expuesta por su digitalización. La información son datos muy valorados en las organizaciones por lo que debe protegerse correctamente. Para ello, las organizaciones deben recurrir a diferentes medidas de seguridad tanto técnicas como administrativas, gestionando controles de seguridad centrándose en el sistema de información y la gestión de riesgos.

La tecnología de la información se desarrolla a pasos acelerados, por lo que sigue siendo frágil a diversas amenazas. El sistema de gestión de seguridad de la información o SGSI se ha convertido en un asunto importante en la gestión de los sistemas de información ya que apuntan a su integridad, confidencialidad y disponibilidad.

Para ello, es necesario conocer y comprender el tema de la implementación de un Sistema de Gestión de la Seguridad de la Información según la norma ISO 27001, cuyo objetivo es proteger a cualquier institución u organización de posibles pérdidas, robos o alteraciones de datos. Este procedimiento no sólo defiende y preserva los sistemas informáticos frente a intrusiones o desastres, sino que asegura su supervivencia.

Sin embargo, la implementación de estándares de seguridad de la información no es una tarea fácil. Dado que la mayoría de las normas proporcionan los requisitos sobre lo que se requiere, pero no sobre cómo implementarlos, lo que ha generado dificultad en las organizaciones. Por lo tanto, se recomienda implantar un SGSI basado en la norma ISO 27001 cuando puedan surgir riesgos relacionados con la seguridad de los datos de la empresa.

Desarrollo

Toda organización cuenta con información en diversas formas como: información personalizada, información económica, correos electrónicos, etc. La información es una recopilación de datos a través de una comunicación, una entrevista, una investigación, la enseñanza o la educación, la cual puede ser procesada para darle un fin en la organización.

ISO/IEC define la información como un activo que se puede almacenar en muchas formas, por ejemplo, forma digital, formas en papel y conocimiento de los empleados. En muchas organizaciones, la información depende de la tecnología de la información y las comunicaciones. Esta tecnología a menudo ayuda a facilitar la creación, procesamiento, almacenamiento, transmisión, protección y destrucción de información. Debido al alto valor de la información en las organizaciones, esta puede ser altamente crítica (dependiendo de qué información) si es incorrecta o no está cuando se necesita (ISO/IEC, 2018). (*FULLTEXT01.pdf*, s. f.)

La información de una organización puede verse afectada por amenazas las cuales pueden llegar a causar daño o perdidas de la información. Si su sistema de seguridad es vulnerable las amenazas aprovechan y pueden obtener acceso no autorizado a un activo dentro de la organización. Hay varios tipos de amenazas contra la información como, por ejemplo: las amenazas deliberadas causan un daño a propósito, las amenazas accidentales causadas por enlaces maliciosos y por último las amenazas ambientales como un incendio.

La seguridad de la información puede definirse como la protección de la información y los sistemas contra el acceso, la modificación, el uso, la descripción y la divulgación no autorizados, con el fin de proteger la integridad, la confidencialidad y la disponibilidad de los sistemas y los datos. La incapacidad de una organización para elegir y aplicar las directrices, la política y los procedimientos de seguridad adecuados puede tener un grave impacto en la misión de la empresa en lo que respecta a las normas y los procedimientos de seguridad bien elegidos para proteger los activos. (Ramadhan & Rose, s. f.)

El sistema de gestión de seguridad de la información (SGSI), es un sistema de gestión documentado que consta de un conjunto de controles de seguridad que protegen la confidencialidad, disponibilidad e integridad de los activos frente a amenazas y vulnerabilidades. La confidencialidad es la propiedad de la información en la que no se pone a disposición ni se revela a personas, entidades o procesos no autorizados. La disponibilidad es la propiedad de ser accesible y utilizada a pedido de una entidad autorizada. La integridad es la propiedad de la exactitud y la integridad. (*FULLTEXT01.pdf*, s. f.)

Al diseñar, implementar, administrar y mantener un SGSI, las organizaciones pueden proteger sus datos confidenciales y personales para que no se vean comprometidos. Proporcionando muchos beneficios a una empresa, ya que en el panorama actual se encuentra lleno de amenazas, donde tener una sólida seguridad de la información es una necesidad absoluta.

Para que un sistema de seguridad llegue a tener el éxito esperado deber ser revisado y mejorado constantemente.

Implementando un SGSI

Existen numerosas formas de abordar la implementación de un SGSI. El método más común a seguir es un proceso de "Plan Do Check Act"'. El proceso Planificar-Hacer- Verificar- Actuar (PDCA) se origina en el aseguramiento de la calidad y ahora es un requisito en la norma ISO 27001, ya que ayuda a tener una mejor visión de la implementación del sistema de seguridad. (*PDCA*, 2020)

Gestión de la calidad PDCA

La ISO 27001 se basa en la teoría de gestión de la calidad PDCA (también conocida como ciclo de Deming), como se podrá observar en la estructura de esta. (*ISO 27001 ¿En qué consiste esta norma de seguridad?*, s. f.)

- Planificar ("Plan"): etapa inicial de diseño del SGSI en la que se realiza la identificación inicial de los riesgos asociados con la Seguridad de la información. Esta cuestión se complementa con un análisis cualitativo y cuantitativo (si es necesario) de los riesgos identificados y la planificación de la respuesta y los controles necesarios para la mitigación de estos. Al efectuar la fase de la planificación, se debe analizar los problemas externos e internos de la organización. Los problemas externos son las amenazas que podrían ser la parte externa de la organización, como los requisitos legales, económicos y políticos. Los problemas internos son: estructura organizacional, valores, culturas, infraestructura TIC, recursos disponibles, etc.
- Hacer ("Do"): implantación y operación del Sistema de Gestión de Seguridad de la Información definido y desarrollado. La organización crea una evaluación de riesgos y evalúa las razones detrás de cada estructura. Se debe realizar una serie de procedimientos indicando los riesgos y su tratamiento. Asegurar que los documentos de procedimientos y políticas estén

disponibles y adecuadamente protegidos, distribuidos y almacenados en el sistema gestionado. Los documentos de origen externo deben ampararse bajo el alcance del SGSI 27001.

- Verificar ("Check"): revisar y evaluar su eficacia y eficiencia. Si el desempeño no es el esperado analizar las causas y determinar las mejoras. Esta fase cubre controles de seguimiento, medición, análisis y evaluación dentro de la organización. Las personas responsables deben medir el desempeño de los procesos contra las políticas, objetivos y experiencia práctica en un procedimiento documentado establecido en la fase anterior. Los líderes responsables deben presentar cualquier resultado seguido de la implementación de estos resultados de política. Es la mejor manera de verificar dónde se han identificado, tratado, eliminado y requerido revisar y mejorar los problemas.
- Actuar ("Act"): mejora continua del SGSI. Una organización debe emprender acciones correctivas y preventivas basadas en los resultados de la auditoría interna y la revisión de la gestión del SGSI. Se puede nombrar un Director de Información que será responsable de monitorear y medir la seguridad de la información. El CIO debe actuar sobre cualquier hallazgo que se relacione con la violación de la seguridad de la información. La mejora continua es una parte integral de la norma ISO 27001. La norma requiere que las organizaciones mejoren continuamente para eliminar futuras amenazas. (*SGSI*, s. f.)

El método PDCA se puede usar cuando en una organización se desee realizar un cambio: al instalar nuevos firewalls, contenido de una capacitación, nuevas políticas o solicitar a las personas que cambien la forma de instalar los dispositivos. Como se puede observar en la figura 1, después de un cambio exitoso, alcanza un nivel de calidad superior y el nuevo nivel se convierte en la línea de base para evaluar las próximas propuestas de cambio.

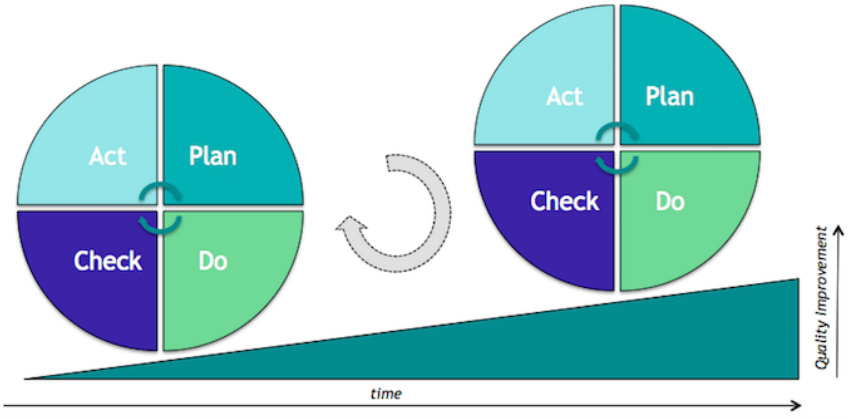


Figura 1. Ilustra la idea de ajustar las métricas en cada paso.

Fuente: https://ictinstitute.nl/pdca-plan-do-check-act/

Norma ISO 27001

ISO 27001 es el estándar de seguridad internacional que detalla los requisitos de un SGSI. ISO 27001, junto con las pautas de mejores prácticas contenidas en ISO 27002, sirven como dos guías excelentes para comenzar a implementar un SGSI.

Un SGSI certificado, auditado de forma independiente por un organismo de certificación aprobado, puede servir como la garantía necesaria para los clientes y clientes potenciales de que la organización ha tomado las medidas necesarias para proteger sus activos de información de una variedad de riesgos identificados. La solidez de un SGSI se basa en la solidez de la evaluación de riesgos de seguridad de la información, que es clave para cualquier implementación.(*What is an Information Security Management System (ISMS)? | Myra*, s. f.)

La capacidad de reconocer la gama completa de riesgos que la organización y sus datos pueden enfrentar en el futuro previsible es un precursor para implementar las medidas de mitigación necesarias (conocidas como 'controles').

ISO 27001 proporciona una lista de controles recomendados que pueden servir como una lista de verificación para evaluar si ha tomado en cuenta los controles necesarios para fines legislativos, comerciales, contractuales o reglamentarios. La clave para un SGSI eficaz es una evaluación de riesgos. Después de todo, solo cuando sabe a qué amenazas se enfrenta puede implementar las defensas adecuadas. (Dutton, 2021)

Contar con un sistema de gestión de seguridad de la información (SGSI) efectivo en una organización puede:

- Proteger los activos de información de su organización
- Facilitar la demostración de la seguridad de su información
- Mostrar la seriedad con la que su organización se toma la seguridad de la información
- Ayudarlo a anticiparse a los nuevos riesgos y oportunidades de seguridad de la información
- Apoyar el desarrollo y crecimiento de su organización (Dutton, 2021)

Estructura de la Norma

1. Objeto y campo de aplicación: objetivos y uso de la norma en el contexto de las diferentes organizaciones.
2. Referencias normativas del estándar.
3. Términos y definiciones utilizados en el desarrollo de la norma.
4. Contexto de la organización: requisitos y expectativas de los interesados tanto a nivel interno como externo y que influirán en el SGSI y determinación del alcance de este.

4.1 Entender la organización y su contexto

4.2 Comprender las necesidades y expectativas de las partes interesadas

4.3 Determinación del alcance del SGSI

4.4 Sistema de gestión de seguridad de la información (SGSI)

5. Liderazgo: importancia de la implicación de la gerencia con el sistema, mediante el establecimiento de políticas, integrando el SGSI en los procesos de la organización, y asegurando los recursos necesarios.

5.1 Liderazgo y compromiso

5.2 Política de Seguridad de la Información

5.3 Funciones, responsabilidades y autoridades de la organización

6. Planificación: es imprescindibles detectar, analizar y valorar los riesgos de seguridad de la información tomando como referencia los umbrales aceptables de riesgo de la organización (apetito al riesgo), así como planificar estrategias de respuesta (mitigación).

6.1 Acciones para abordar riesgos y oportunidades

6.2 Objetivos de seguridad de la información y planificación para lograrlos

7. Soporte: recursos necesarios para la capacitación y concienciación del personal, además de la importancia de la comunicación y la propia información.

7.1 Recursos

7.2 Competencia

7.3 Conciencia

7.4 Comunicación

7.5 Información documentada

8. Operación: cómo operar el sistema e implantar la respuesta a los riesgos.

8.1 Planificación y control operativo

8.2 Evaluación de riesgos de seguridad de la información

8.3 Tratamiento de riesgos de seguridad de la información

9. Evaluación de desempeño: pautas para la monitorización, seguimiento y control del SGSI y la evaluación de su eficiencia y eficacia.

9.1 Seguimiento, medición, análisis y evaluación

9.2 Auditoría interna

9.3 Revisión por la dirección

10. Mejora: se centra en cómo abordar las no conformidades con la norma, las acciones correctivas que hay que implementar y la mejora periódica del Sistema de Gestión de Seguridad de la Información. (*ISO_IEC_27000_2018.pdf*, s. f.)

10.1 No conformidad y acción correctiva

10.2 Mejora continua

11. Anexo A: definición de los controles para mejorar la seguridad de la información.

Controles del Anexo A ISO 27001

A.5 Políticas de seguridad de la información: gestionar la dirección y el apoyo para la seguridad de la información de acuerdo con los requisitos de la organización, así como de acuerdo con las leyes y reglamentos pertinentes.(*NQA-ISO-27001-Guia-de-implantacion.pdf*, s. f.)

A.6 Organización de la seguridad de la información: establecer un marco de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.

A.7 Seguridad de los recursos humanos: asegurar que los empleados y contratistas entiendan sus responsabilidades y sean aptos para las funciones para las que están considerados. También cubre lo que sucede cuando esas personas se van o cambian de roles.

A.8 Gestión de activos: identificar los activos de información en el alcance del sistema de gestión y definir las responsabilidades de protección apropiadas.

A.9 Control de acceso: salvaguardar el acceso a la información y garantizar que los empleados solo puedan ver la información que es relevante para su trabajo.

A.10 Criptografía: garantizar el uso adecuado y efectivo de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.

A.11 Seguridad física y ambiental: evitar el acceso físico no autorizado, el daño y la interferencia a la información de la organización ya las instalaciones de procesamiento de información.

A.12 Seguridad de las operaciones: garantizar operaciones correctas y seguras de las instalaciones de procesamiento de información.

A.13 Seguridad de las comunicaciones: garantizar la protección de la información en las redes y sus instalaciones de procesamiento de información de apoyo.

A.14 Adquisición, desarrollo y mantenimiento del sistema: garantizar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que brindan servicios a través de redes públicas.

A.15 Relaciones con proveedores: protección de los activos valiosos de la organización que son accesibles o afectados por los proveedores.

A.16 Gestión de incidentes de seguridad de la información: garantizar un enfoque coherente y eficaz para el ciclo de vida de incidentes, eventos y debilidades

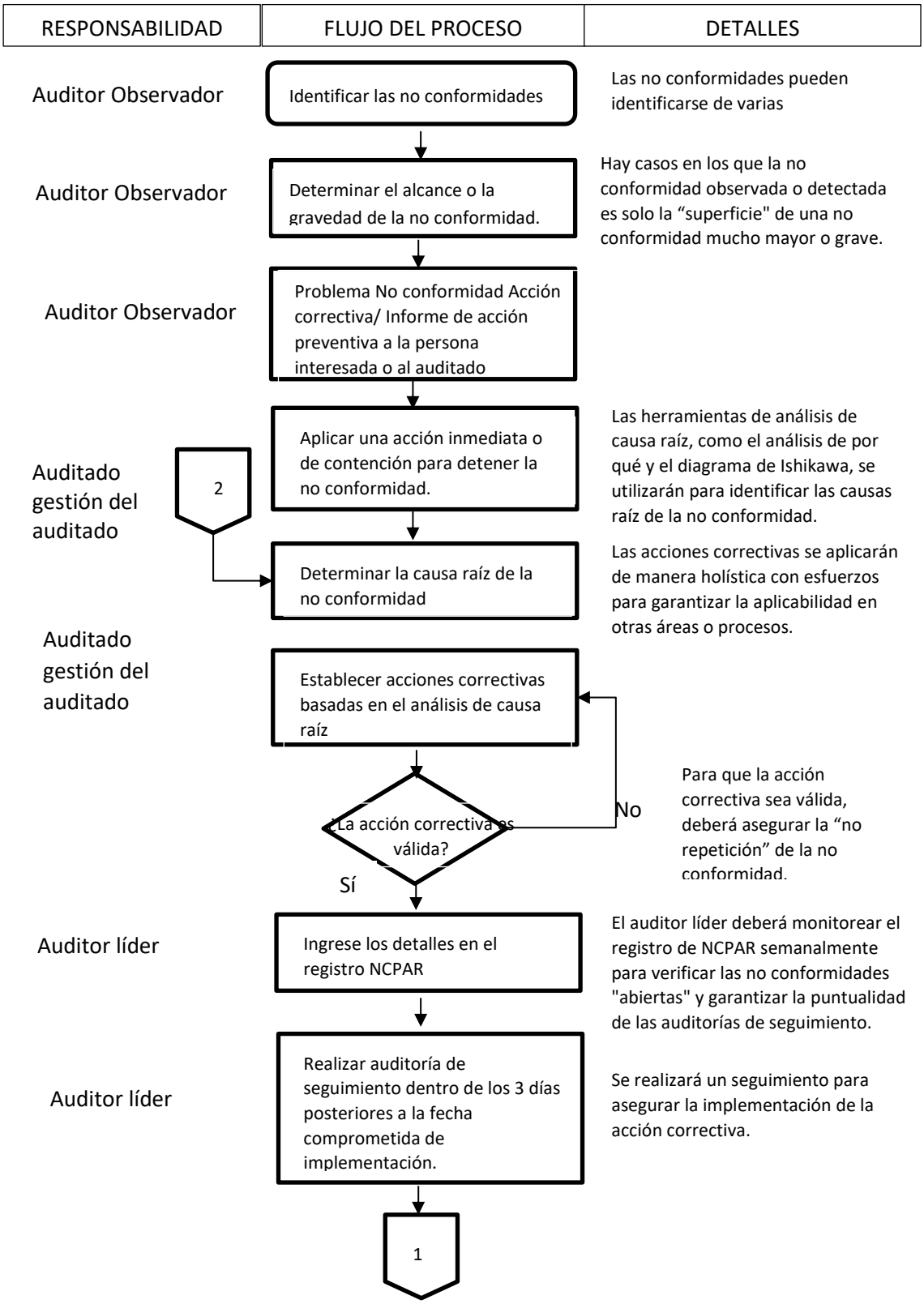
A.17 Aspectos de seguridad de la información de la gestión de la continuidad del negocio: continuidad de la seguridad de la información se incorpore a los sistemas de gestión de la continuidad del negocio de la organización.

A.18 Cumplimiento: evitar el incumplimiento de las obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y de cualquier requisito de seguridad. (*Business-case-for-an-ISMS-Whitepaper.pdf*, s. f.)

Sin duda, la ISO 27001 es fundamental para gestionar la seguridad de la información en organismos y empresas independientemente de su tamaño, objetivos o estructura. (*ISO 27001 ¿En qué consiste esta norma de seguridad?*, s. f.)

Procedimiento de Acción Correctiva

Dentro de un sistema de gestión de seguridad de la información puede darse las no conformidades, por lo que se debe realizar una acción correctiva del mismo. Contar con un procedimiento de acciones correctivas ayudará a eliminar la causa de las no conformidades en el sistema de gestión de seguridad de la información (SGSI) establecido. Este procedimiento (Figura 2) abarca la recopilación de datos sobre no conformidades, el análisis de la causa de las no conformidades y la planificación de las acciones para evitar la recurrencia de problemas. (Richard O. Regalado & ISO27k implementers' forum, s. f.)


RESPONSABILIDAD
FLUJO DEL PROCESO
DETALLES
Auditor Observador
Identificar las no conformidades
Las no conformidades pueden identificarse de varias
Auditor Observador
Determinar el alcance o la gravedad de la no conformidad.
Hay casos en los que la no conformidad observada o detectada es solo la “superficie" de una no conformidad mucho mayor o grave.
Auditor Observador
Problema No conformidad Acción correctiva/ Informe de acción preventiva a la persona interesada o al auditado
Auditado gestión del auditado
2
Aplicar una acción inmediata o de contención para detener la no conformidad.
Las herramientas de análisis de causa raíz, como el análisis de por qué y el diagrama de Ishikawa, se utilizarán para identificar las causas raíz de la no conformidad.
Determinar la causa raíz de la no conformidad
Las acciones correctivas se aplicarán de manera holística con esfuerzos para garantizar la aplicabilidad en otras áreas o procesos.
Auditado gestión del auditado
Establecer acciones correctivas basadas en el análisis de causa raíz
¿La acción correctiva es válida?
No
Para que la acción correctiva sea válida, deberá asegurar la “no repetición” de la no conformidad.
Sí
Auditor líder
Ingrese los detalles en el registro NCPAR
El auditor líder deberá monitorear el registro de NCPAR semanalmente para verificar las no conformidades "abiertas" y garantizar la puntualidad de las auditorías de seguimiento.
Auditor líder
Realizar auditoría de seguimiento dentro de los 3 días posteriores a la fecha comprometida de implementación.
Se realizará un seguimiento para asegurar la implementación de la acción correctiva.
1

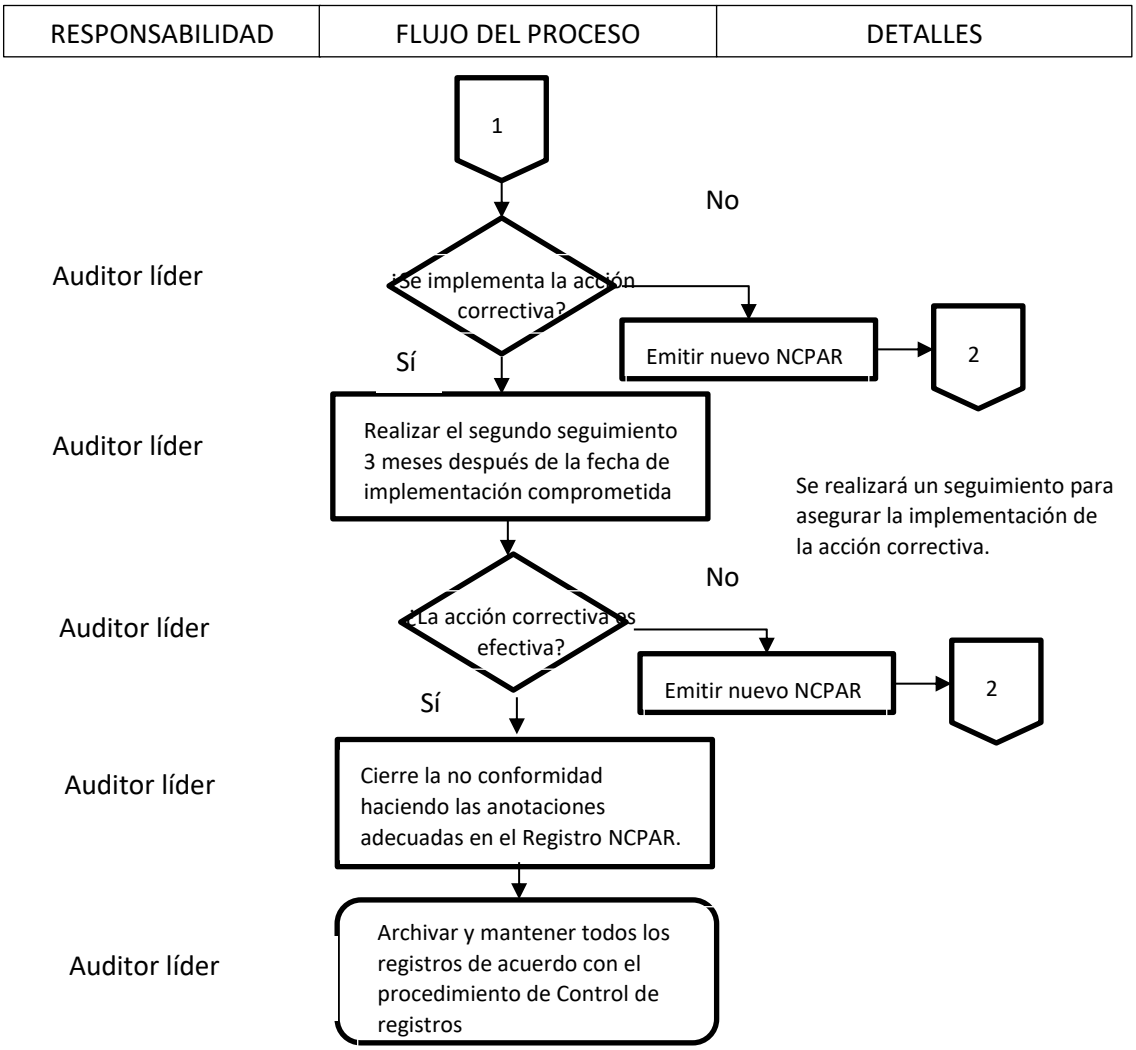


Figura 2. Procedimiento de acción correctiva

Casos en los que se pueden encontrar no conformidades: (tabla 1)

SITUACIONES	DESCRIPCIÓN
como resultado de la Auditoría interna SGSI	Todas las no conformidades y observaciones observadas ameritarán acciones correctivas por parte del auditado y de la dirección del auditado.
Proceso de no conformidad	No conformidades relacionadas con desviaciones del proceso. Los ejemplos serían: no actualizar las definiciones de virus, no monitorear los registros requeridos, no implementar un

	procedimiento de seguridad. Las no conformidades del proceso pueden ser planteadas fuera de las actividades de auditoría interna por cualquier miembro del personal que haya observado el evento.
Producto no conforme	Una desviación o error en la salida de un proceso que compromete la integridad. Los ejemplos serían errores en la codificación descubiertos por el cliente, incumplimiento de los acuerdos de nivel de servicio. Las no conformidades del producto pueden ser planteadas fuera de las actividades de auditoría interna por cualquier miembro del personal que haya sido testigo de la no conformidad.
Quejas de clientes	Quejas válidas provenientes de los clientes.
incidentes de seguridad de la información	La acción correctiva se establecerá en todas las infracciones de seguridad de la información válidas después de que se hayan llevado a cabo los pasos de remediación (consulte el formulario de investigación de SI)

Tabla 1: Casos de conformidades

Fuente: (Richard O. Regalado & ISO27k implementers' forum, s. f.)

Metodología

El uso de un método de investigación es fundamental porque permite alcanzar un fin, para su elección se ha considerado la naturaleza del problema que se está abordando. Se ha estimado el método de investigación descriptiva a través de observaciones cualitativas.

Además de las competencias de hablar y escuchar que se utilizan en las entrevistas, observar es otra destreza de la vida cotidiana que se sistematiza metodológicamente y aplica en la investigación cualitativa. Se integran no sólo las percepciones visuales, sino también las basadas en la audición, el tacto y el olfato. (Flick, U. 2012).

La observación cualitativa permite observar, interactuar y obtener una imagen amplia en el entorno natural de esta investigación. Este método de recopilación de datos permite comprender mejor los procesos en estudio.

La observación cualitativa en esta investigación es subjetiva, ya que tiene un enfoque que depende exclusivamente de la observación.

Discusión

La norma ISO/IEC 27001 apoya a las organizaciones en la creación de una mejor eficiencia comercial, salvaguarda los activos valiosos como los datos personales, protege la reputación del personal y de las organizaciones y, al mismo tiempo, facilita el logro de los objetivos de cumplimiento. (Lopes et al., 2019)

Las organizaciones que ya están implementando la norma ISO/IEC 27001 abarcan una amplia gama de sectores del mercado, que incluyen: telecomunicaciones, servicios financieros y de seguros, sectores manufactureros, servicios públicos (electricidad, gas, petróleo, agua), industria minorista, industria de servicios, salud, policía y servicios de emergencia, universidades y departamentos gubernamentales. (Fomin et al., 2008)

PDCA se basa en la idea de mejora continua. Esta idea de mejora continua es en realidad más importante que los pasos exactos de PDCA. El modelo PDCA/PDSA fue desarrollado para ayudar a mejorar los procesos de producción. (*PDCA*, 2020)

Para aplicar PDCA, primero debe asegurarse de que la seguridad de la información se vea como una actividad recurrente y no como un proyecto. Por lo que se recomienda para la seguridad de la información crear un equipo permanente de seguridad de la información y así se implemente PDCA. (*Information security and PDCA (Plan-Do-Check-Act)*, 2017)

La certificación ISMS ha sido diseñada para la protección de SI. Por lo tanto, de manera similar a los estándares QMS, la cuantificación de los beneficios de la adopción del estándar ISMS es problemática. El interés de un estándar de sistema de gestión de seguridad de la información es prevenir las fallas de seguridad y mitigar sus consecuencias.

Los altos costos en dinero y tiempo de la implementación de las normas SGSI son definitivamente barreras para la adopción de la norma por parte de las empresas de menor tamaño. (Fomin et al., 2008)

Conclusiones

- Un SGSI garantiza que los activos de información de propiedad (p. ej., propiedad intelectual, datos personales o datos financieros), así como los datos confiados por los clientes o terceros, estén adecuadamente protegidos contra todas y cada una de las amenazas.
- Mediante el uso de un SGSI para hacer que la seguridad de la información sea una parte integral de sus procesos comerciales, las empresas pueden aumentar continuamente su nivel de seguridad y mitigar los riesgos de seguridad de la información. De esta forma, contrarrestan el riesgo de que incidentes de seguridad interrumpan la continuidad del negocio.
- Para organizaciones que son altamente regulados como finanzas el SGSI ayudan a cumplir con todos los requisitos normativos y contractuales, concediendo una mayor seguridad operativa y jurídica.
- Implementar un SGSI en una empresa u organización, pueden verificar ante terceros que la información confidencial se maneja de forma segura. Esto contribuye a una mejor imagen externa y a generar confianza, lo que se considera una ventaja competitiva.

En cuanto a costos, el invertir en un sistema de gestión de la seguridad de la información permite utilizar los recursos de manera eficiente y realizar inversiones en lugares correctos. Sus costos de inversión se pueden reducir a largo plazo.

Referencias

1. Business-case-for-an-ISMS-Whitepaper.pdf. (s. f.). Recuperado 25 de junio de 2022, de https://www.isms.online/app/uploads/2018/08/Business-case-for-an-ISMS-Whitepaper.pdf
2. Dutton, J. (2021, agosto 23). What is an ISMS (Information Security Management System)? IT Governance USA Blog. https://www.itgovernanceusa.com/blog/what-exactly-is-an-information-security-management-system-isms-2
3. Fomin, V., de Vries, H. J., Nl, hvries@rsm, & Barlette, Y. (2008, septiembre 17). ISO/IEC 27001 Information Systems Security Management Standard: Exploring the reasons for low adoption.
4. FULLTEXT01.pdf. (s. f.). Recuperado 24 de junio de 2022, de https://www.diva-portal.org/smash/get/diva2:1580053/FULLTEXT01.pdf

5. Information security and PDCA (Plan-Do-Check-Act). (2017, febrero 8). ICT Institute. https://ictinstitute.nl/pdca-plan-do-check-act/
6. ISO 27001 ¿En qué consiste esta norma de seguridad? (s. f.). UNIR. Recuperado 24 de junio de 2022, de https://www.unir.net/ingenieria/revista/iso-27001/
7. ISO_IEC_27000_2018.pdf. (s. f.). Recuperado 25 de junio de 2022, de https://akela.mendelu.cz/~lidak/IPI/ISO_IEC_27000_2018.pdf
8. Lopes, I., Guarda, T., & Oliveira, P. (2019). Implementation of ISO 27001 Standards as GDPR Compliance Facilitator. Journal of Information Systems Engineering & Management, 4. https://doi.org/10.29333/jisem/5888
9. NQA-ISO-27001-Guia-de-implantacion.pdf. (s. f.). Recuperado 25 de junio de 2022, de https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf
10. PDCA: An Implementation Guide to ISO 27001:2013. (2020, diciembre 8). Best Practice. https://bestpractice.biz/pdca-an-implementation-guide-to-iso-270012013/
11. Ramadhan, N., & Rose, U. (s. f.). Adapting ISO/ IEC 27001 Information Security Management Standard to SMEs. 78.
12. Richard O. Regalado, & ISO27k implementers' forum. (s. f.). CORRECTIVE ACTION PROCEDURE. www.ISO27001security.com
13. SGSI. (s. f.). Recuperado 25 de junio de 2022, de https://www.iso27000.es/sgsi.html
14. What is an Information Security Management System (ISMS)? | Myra. (s. f.). Recuperado 24 de junio de 2022, de https://www.myrasecurity.com/en/information-security-management-system-isms/