https://doi.org/10.22201/dgtic.ctud.2024.2.2.52

Vol. 2, Núm. 2. abril-junio 2024, págs. 33 - 38

Recertificación del ISO/IEC 27001 de un área universitaria

Información del reporte:

Para citar este reporte técnico:

Lugo Rojas, E. (2024). Recertificación del ISO/IEC 27001 de un área universitaria. Cuadernos Técnicos Universitarios de la DGTIC, 2 (2) páginas (33 - 38).

https://doi.org/10.22201/dgtic.ctud.2024.2.2.52

Esther Lugo Rojas

Dirección General de Cómputo y de Tecnologías de Información y Comunicación

Universidad Nacional Autónoma de México

esther.lugo@unam.mx

ORCID: 0009-0003-6823-3943

Resumen

El estándar ISO/IEC 27001 es uno de los estándares en seguridad de la información que más se utiliza en las organizaciones debido a que proporciona un marco de trabajo para la adopción de un sistema de gestión de seguridad de la información. Este estándar indica los requerimientos mínimos para establecer, implementar, mantener y mejorar los procesos, actividades, funciones, infraestructura, roles organizacionales, activos y todos aquellos elementos que forman parte del sistema de gestión de seguridad de la información. En el área universitaria que recientemente se recertificó con éxito en el estándar ISO/IEC 27001, se implementó una metodología que consistió en alinear las siete cláusulas del estándar en las cuatro fases del ciclo de mejora continua y ser ejecutadas en ese orden. Las cláusulas de contexto de la organización, liderazgo, planeación y soporte forman parte de la fase del ciclo de mejora continua denominada como Plan; la cláusula operación en la fase de Hacer; a la fase de Verificación le corresponde la cláusula de evaluación del desempeño y finalmente, en la fase de Actuar se identifica la cláusula de mejora. El apoyo de la alta dirección es fundamental para conseguir buenos resultados en la implementación del Sistema de Gestión de Seguridad de la Información (SGSI).

Palabras clave:

SGSI, seguridad de la información, ciclo de mejora continua, ISO/IEC 27001.

https://doi.org/10.22201/dgtic.ctud.2024.2.2.52 Vol. 2, Núm. 2. abril-junio 2024, págs. 34 - 38

1. INTRODUCCIÓN

La rápida evolución de las tecnologías de la información hace imprescindible hoy día la incorporación de la seguridad de la información (SI) en cualquier proceso de valor que la organización lleve a cabo sin importar su giro. En dicho proceso estará implícita la generación, uso, transformación y eliminación de información valiosa que requiere ser protegida. "La información corresponde a los datos que se han organizado de modo que tengan significado y valor para el receptor [...]" (Nolasco et al., 2023, p. 30).

La SI comprende la "preservación de la confidencialidad, integridad y disponibilidad de la información" (ISO, 2018). Existen variadas herramientas y mecanismos para su protección.

La Organización Internacional de Normalización (*International Organization for Standardization*, *ISO*) y la Comisión Electrotécnica Internacional (*International Electrotechnical Commission*, *IEC*) cuentan con la norma ISO/IEC 27001 que "proporciona los requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un Sistema de Gestión de Seguridad de la Información" (SGSI) (ISO, 2022). El SGSI se usa para proteger la confidencialidad, integridad y disponibilidad de la información. El estándar ISO/IEC 27001 provee un marco para la SI que ayuda a reconocer y administrar sus riesgos de forma efectiva.

Los marcos de trabajo "[...] dan una serie de pautas y medidas que se han desarrollado a través de la experiencia y el conocimiento de la industria, es decir, que se ha probado y se ha demostrado que son efectivos" (Caballero et al., 2023, p. 112).

Para obtener la certificación en ISO/IEC 27001, el área universitaria debe contar con un SGSI implementado y apegado a dicho estándar, así como a la normatividad interna establecida por ella misma. Los organismos certificadores son entidades independientes y especializadas que evalúan y verifican el cumplimiento de algún estándar. Específicamente sobre el estándar ISO/IEC 27001 se encuentran, entre otros, la BSI (*British Standards Institution*) y la Asociación Española de Normalización y Certificación (AENOR).

AENOR indica dos tipos de auditorías que dan lugar a la certificación de seguimiento (anual) y a la recertificación o renovación (trianual). La primera consiste en "contrastar la adecuación del sistema implantado a la norma y ayudar a la empresa a detectar las posibles desviaciones", en la segunda "se evalúan los requisitos con mayor profundidad que en el seguimiento anual" (AENOR, 2024).

Desde 2010 el área universitaria encargada de la SI en la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC) de la Universidad Nacional Autónoma de México (UNAM) está certificada con el estándar ISO/IEC 27001 para el servicio de respuesta a incidentes (DGTIC UNAM, 2020). En el año 2023 se realizó la recertificación y se obtuvo la renovación vigente.

Este reporte técnico está organizado como sigue: Desarrollo técnico explica la implementación del SGSI en el área universitaria referida, sus propósitos y procedimientos; Metodología muestra las fases de dicha implementación; Resultados indica los logros alcanzados por la recertificación del área universitaria; y finalmente, el documento cierra con las Conclusiones. El objetivo consiste en reportar el proceso para obtener la recertificación de un SGSI con ISO/IEC 27001 de un área universitaria.

https://doi.org/10.22201/dgtic.ctud.2024.2.2.52 Vol. 2, Núm. 2. abril-junio 2024, págs. 35 - 38

2. DESARROLLO TÉCNICO

La implementación del SGSI que llevó a la recertificación en 2023, consistió en la actualización y ejecución de políticas, procedimientos, guías, manuales, registros y documentación que dicta los lineamientos en SI para las actividades centrales en el alcance del SGSI. Dicha implementación consistió en: ejecutar los preceptos en SI para los activos críticos determinados por el área universitaria; gestionar las interacciones con la infraestructura tecnológica; e identificar las acciones de aquellos roles organizacionales involucrados que llevarán a mantener con un nivel de seguridad acorde al área universitaria dentro del alcance del SGSI.

Es necesario partir de la identificación de la información como principal valor del área universitaria, qué personas la conforman y qué funciones desempeñan, con qué tecnología se trabajó y por dónde viajaron los principales flujos de datos, identificar las amenazas, los escenarios de preocupación, probabilidades, impactos, y escenarios futuros para gestionar estas amenazas incorporando las medidas de seguridad más oportunas (Caballero et al., 2023).

En este proceso, el repaso minucioso de cada elemento de la metodología empleada fue muy importante para verificar su cumplimiento y obtener la recertificación.

2.1 METODOLOGÍA

La implementación del SGSI contempla la administración de proyectos (de la cual se retoma centralmente la planeación) y el ciclo de mejora continua. El ciclo de mejora continua (PDCA del inglés *Plan, Do, Check, Act*), desarrollado por Edward Deming, (Montesinos et al., 2020) se compone de cuatro fases: planear, hacer, verificar y actuar.

Incrementar la productividad, eficiencia y calidad exige mayores esfuerzos para la mejora continua del proceso, producto o servicio que se ofrece; incluye la infraestructura, equipos o herramientas disponibles dentro de la organización, en específico del área universitaria (Montesinos et al., 2020).

La recertificación del SGSI considera la implementación de las cláusulas del estándar ISO/IEC 27001 alineadas y repartidas en las cuatro fases del PDCA, como se muestra en la Tabla 1.

Tabla 1

La recertificación del SGSI contempla la implementación de las siete cláusulas operacionales del estándar ISO/IEC 27001 (las tres primeras son teóricas) alineadas y repartidas en las cuatro fases del PDCA

Fase PDCA	Cláusula ISO/IEC 27001
I. Plan	4. Contexto de la organización
	5. Liderazgo
	6. Planeación
	7. Soporte
II. Hacer	8. Operación
III. Verificar	9. Evaluación del desempeño
IV. Actuar	10. Mejora

https://doi.org/10.22201/dgtic.ctud.2024.2.2.52 Vol. 2, Núm. 2. abril-junio 2024, págs. 36 - 38

Para la recertificación se realizaron reuniones con la alta dirección para evaluar: a) la disponibilidad de los integrantes involucrados en la implementación; b) la fecha de entrega de proyectos; y c) proyectos adicionales a cargo de la responsable del SGSI.

Posteriormente, se planteó un diagrama de Gantt de la planeación del SGSI que integró la identificación de las actividades y sus dependencias, los tiempos destinados para hacer las actividades y los responsables que están involucrados en la implementación del Sistema.

2.2 FASE I. PLANEAR (PLAN)

En esta fase se desarrollaron las actividades relacionadas con el contexto interno y externo del área universitaria e incluyó aquellas situaciones que pudieron afectar positiva o negativamente al SGSI, asimismo, se consideraron las expectativas y necesidades de las partes interesadas en el Sistema y determinadas según su alcance.

También se integró el liderazgo, que implica el compromiso y apoyo de la alta dirección hacia la implementación del SGSI. Se revisó el contenido de la política de SI y se incorporaron los ajustes provenientes del análisis del contexto y del alcance. Se revisaron y actualizaron los roles y responsabilidades del área universitaria.

En la cláusula del estándar denominada Planeación, se realizó la revisión de las acciones para tratar los riesgos y oportunidades, su apreciación y tratamiento, y la revisión de los objetivos de SI en el alcance del Sistema.

Se revisó y actualizó la documentación derivada de los cambios detectados en el contexto. Ejemplo de este tipo de cambios es la actualización de infraestructura y roles organizacionales. Se contribuyó con la identificación y el análisis de las dependencias entre documentos del SGSI, y en la verificación, control y resguardo de registros, disminuyendo la generación de estos.

Adicionalmente, se dio el seguimiento y verificación de tareas de conservación de integridad de la información como el estatus del alta, baja y cambio de responsables de tareas, sus cuentas de correo, de sistema operativo, entre otros. Se actualizaron los planes de concientización y comunicación, y las competencias laborales.

2.3 FASE II. HACER (DO)

Esta fase corresponde operativamente con la implementación del SGSI. Se llevaron a cabo los lineamientos establecidos en la documentación, se ejecutaron las acciones para cumplir los objetivos, se realizó el análisis y evaluación de riesgos, el plan de tratamiento de riesgos y la identificación de controles para atender los riesgos identificados. Derivado de la fase previa (Plan), se revisaron los elementos que pudieran afectar al análisis de riesgos, como nuevos activos o integrantes dentro del alcance del SGSI.

También se enriqueció el análisis de riesgos al incorporar nuevos escenarios. Se mejoró el plan de tratamiento de riesgos para aumentar su trazabilidad con los riesgos residuales. Finalmente, se realizó un comparativo histórico de los resultados del análisis de riesgos para observar tendencias.

https://doi.org/10.22201/dgtic.ctud.2024.2.2.52 Vol. 2, Núm. 2. abril-junio 2024, págs. 37 - 38

2.4 FASE III. VERIFICAR (CHECK)

Se realizó la evaluación del desempeño de la SI y de la eficacia del SGSI. La medición de variables es una herramienta clave para identificar los aspectos que llevaron al cumplimiento de las métricas, se generó un comparativo histórico de éstas que condujo a la identificación de su aplicabilidad. Ejemplos de estas métricas son el porcentaje de cumplimiento de los objetivos, políticas y procedimientos del SGSI.

La auditoría interna revisó tanto la alineación de la implementación del SGSI al estándar ISO/IEC 27001 como a la normatividad interna del área universitaria. Finalmente, con los resultados se generó el informe que concentra los datos más destacables en un formato ejecutivo para la alta dirección. En el informe se identificaron las métricas cumplidas, pero también se reconoce aquellas que no cumplieron, esto no es necesariamente malo para el SGSI, sino por el contrario, una vez identificadas se estudian las razones que impidieron su cumplimiento y se destacaron como áreas de oportunidad para el Sistema.

2.5 FASE IV. ACTUAR (ACT)

En esta última fase se implementaron medidas para mejorar el SGSI. Estas mejoras procedieron principalmente de los resultados de la auditoría interna y externa, del análisis y evaluación de riesgos y de las métricas. A partir del análisis de los resultados en conjunto, se propusieron acciones de mejora y planes para su ejecución. Por ejemplo, la realización de formatos para los riesgos residuales, de comunicaciones internas y de acciones para la mejora continua.

Los análisis de resultados utilizaron técnicas de causa-raíz para identificar las razones origen de las observaciones, y a partir de éstas se propusieron acciones que corrigieron dicha observación. También se plantearon acciones inmediatas ejecutadas al término de las auditorías.

Para efectuar las acciones correctivas e inmediatas, fue necesaria la coordinación de grupo, asignación y seguimiento de tareas, actividades facilitadas por la experiencia acumulada en los procesos del SGSI relacionados con los roles y responsabilidades.

3. RESULTADOS

Con base en la implementación del SGSI apegada a la metodología de mejora continua que se ha descrito, se obtuvo la recertificación con el estándar ISO/IEC 27001. Esto denota que el área universitaria implementó mejoras, como el análisis de potenciales riesgos tecnológicos (fallas de *hardware* y *software*, entre otros) y no tecnológicos (como los relacionados con desastres naturales) en sus activos críticos (servidores, bases de datos, documentación, entre otros); se validaron los mecanismos y actividades de protección de seguridad de la información; y el personal adoptó los lineamientos y son conscientes de su aplicación.

Es un logro confirmar que la implementación cumple con los lineamientos establecidos en el estándar y por el área universitaria, no obstante, se detectaron observaciones relacionadas con algunos aspectos de la documentación y seguimiento de ciertos procedimientos. Estas observaciones son valiosas porque ayudan a identificar áreas de oportunidad en la implementación del SGSI y forman parte de la propia metodología de mejora continua que se efectúa en el área universitaria. Así, el área universitaria cuenta con la certificación por tres años más.

https://doi.org/10.22201/dgtic.ctud.2024.2.2.52 Vol. 2, Núm. 2. abril-junio 2024, págs. 38 - 38

La certificación otorga reputación al área universitaria y la coloca en una mejor posición de competitividad por sobre otras organizaciones, e incentiva el compromiso institucional para propiciar consistentemente las acciones requeridas para mantener su certificación.

4. CONCLUSIONES

El estándar ISO/IEC 27001 puede ser adoptado por cualquier organización interesada en proteger su información; el establecimiento de un Sistema de Gestión de Seguridad de la Información proporciona un marco de referencia para instaurar, implementar y mantener de manera adecuada los lineamientos para la seguridad de la información.

El caso que aquí se presenta, sobre el área universitaria encargada de la seguridad de la información de la DGTIC UNAM, representa la consolidación de un proceso que por años se ha mantenido en dicha área, la cual ha enfrentado exitosamente los nuevos retos que imponen los cambios organizacionales, la actualización de la tecnología y los procesos de soporte.

Elaborar las actividades de cada fase de la metodología planteada para la recertificación del SGSI con el estándar ISO/IEC 27001 implica actualizar el contexto en el que se encuentra el área universitaria. Con esa base se habrá de hacer frente a las siguientes actividades planteadas por cada fase de la metodología, concluyéndola y preparándose para volver a iniciarla dentro de un ciclo de mejora continua.

REFERENCIAS

AENOR México. (2024). *Proceso de certificación.* https://www.aenor.com/certificacion/certificacion-de-organizaciones-servicios-y-sistemas/proceso-de-certificacion.

Caballero, M., Baus, L., Cilleros, D. (2023). *Ciberseguridad paso a paso. Diseña tu estrategia.* Anaya.

DGTIC UNAM. (2020). *Se renueva certificación internacional.* https://www.tic.unam.mx/se-renueva-certificacion-internacional/

Montesinos, S., Vázquez, C., Maya, I., Gracida, E. (2020). *Mejora continua en una empresa en México: estudio desde el ciclo Deming.* 25(92), 1863-1883. https://www.redalyc.org/journal/290/29065286036/html/

Nolasco, J., Gamboa, J., Dextre, J., Nolasco, L., Pal (2023). *Tecnologías disruptivas. Comprende las herramientas de la sociedad digital.* Ra-Ma.

Organización Internacional de Normalización. (2018). *Sistema de Gestión de Seguridad de la Información. ISO 27000:2018*.

Organización Internacional de Normalización. (2022). *Tecnología de la información. ISO 27001:2022*.