MAESTRÍA EN CIBERSEGURIDAD

PROYECTO DE TITULACIÓN

Modalidad Proyecto de Investigación y Desarrollo

Plan de migración de la Norma Internacional ISO 27001:2013 a la versión 27001:2022

Autor: Johanna Stepania Galarza Santana

Guía: Roque Jacinto Hernández Bustos

Presentando como parte de los requisitos para el título de magister en ciberseguridad.

Guayaquil, 4 de marzo del 2024

PROPUESTA DE CLÁUSULA DE AUTORIZACIÓN PARA LA PUBLICACIÓN DE TRABAJOS DE TITULACIÓN

Yo, GALARZA SANTANA, JOHANNA STEPANÍA, autor del trabajo de titulación “Plan de migración de la Norma Internacional ISO 27001:2013 a la versión 27001:2022”, certifico que el ensayo reflexivo es una creación de mi autoría, por lo que sus contenidos son originales, de exclusiva responsabilidad de su autor y no infringen derechos de autor de terceras personas. Con lo cual, exonero a la Universidad Casa Grande de reclamos o acciones legales.

Firmado electrónicamente por:
JOHANNA STEPANIA
GALARZA SANTANA

GALARZA SANTANA, JOHANNA STEPANÍA

0930931688

GALARZA SANTANA, JOHANNA STEPANÍA en calidad de autor y titular del trabajo de titulación “Plan de migración de la Norma Internacional ISO 27001:2013 a la versión 27001:2022” para optar por la **Maestría en Ciberseguridad**, autorizo a la Universidad Casa Grande para que realice la digitalización y publicación de este trabajo de titulación en su Repositorio Digital de acceso abierto, con fines estrictamente académicos, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

Asimismo, autorizo a la Universidad Casa Grande a reproducir, distribuir, comunicar y poner a disposición del público mi documento de trabajo de titulación en formato físico o digital y en cualquier medio sin modificar su contenido, sin perjuicio del reconocimiento que deba hacer la Universidad sobre la autoría de dichos trabajos.

Firmado electrónicamente por:
JOHANNA STEPANIA
GALARZA SANTANA

GALARZA SANTANA, JOHANNA STEPANÍA

0930931688

Introducción

La seguridad de la información constituye un pilar fundamental en el entorno empresarial contemporáneo, y las normativas que la rigen evolucionan para adaptarse a los desafíos y avances tecnológicos. En este contexto, la Norma ISO 27001 ha sido un referente crucial para las organizaciones que buscan establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI) manteniendo los 3 pilares fundamentales: Confidencialidad, Integridad, Disponibilidad. La edición más reciente, la ISO 27001:2022, ha introducido cambios significativos, planteando nuevos requisitos y enfoques para garantizar la protección efectiva de la información.

Este ensayo explora los cambios existentes en la Norma ISO 27001:2022, centrándose específicamente en su impacto en una entidad donde laboro, la cual se encuentra certificada con la versión previa, ISO 27001:2013.

A través de este análisis, se busca verificar el nivel de cumplimiento de los controles que se han establecido en la nueva versión de la norma internacional.

Desarrollo

Gerencia, Operación y Planificación de la Ciberseguridad, La Ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados. (UIT, 2008) . Esta asignatura ha enriquecido mis conocimientos sobre el Plan Estratégico de Ciberseguridad, así como la estructura que debe incorporar dicho plan. Se establece claramente, al menos, los siguientes apartados: misión, visión, introducción, gobernanza y objetivos estratégicos. Gracias a esta formación, tuve la capacidad de evaluar, en la fase inicial del proyecto, si el Plan Estratégico de la entidad cumplía con los elementos esenciales necesarios para su efectiva implementación y alineación con los estándares requeridos.

Estrategia y políticas multilaterales para la Ciberseguridad, ISO27k constituye un conjunto de normas internacionales (ISO/IEC) que establecen directrices para la gestión de riesgos asociados a diversos tipos de información, abarcando desde datos de clientes y propiedad intelectual hasta sistemas financieros y datos personales. Su objetivo fundamental radica en brindar orientación sobre la protección efectiva de la información valiosa, garantizando al mismo tiempo su utilización con fines comerciales legítimos. (I sec T Ltd, 2020).

Basándome en estos conceptos, he utilizado como referencia para mi proyecto la norma ISO 27001, que aborda los Sistemas de Gestión de Seguridad de la Información, y la norma ISO 27007, que proporciona directrices específicas para la auditoría del SGSI. Durante la impartición de la clase por parte de la docente, tuve la oportunidad de evaluar el nivel de cumplimiento de los controles del EGSI vinculados a los procesos actuales de la entidad. Este análisis se llevó a cabo mediante el uso del Formato de Declaración de Aplicabilidad SoA-EGSI-V2, lo que resultó crucial para complementar el instrumento de diagnóstico utilizado en mi proyecto. De esta manera, pude evaluar el estado de los controles

que aún se encuentran en la versión 27001:2022.

Gestión Económica y Auditorías en la Seguridad de la información, un SGSI consiste en el conjunto de políticas, procedimientos y directrices junto a los recursos y actividades asociados que son administrados colectivamente por una organización, en la búsqueda de proteger sus activos de información esenciales. (ISO27000.ES, s.f.).

En esta materia, tuve la oportunidad de evaluar el estado y la aplicabilidad de los controles de Seguridad de la Información. Este conocimiento adquirido ha sido un valor añadido al desarrollar mi proyecto, ya que me permitió profundizar en la comprensión de cada control y entender las evidencias necesarias para considerar que un control se encuentra debidamente cumplido.

Hacking Ético y Análisis del Ciberataque, esta materia fue fundamental para ampliar mi comprensión acerca de las técnicas y herramientas utilizadas por los hackers en la ejecución de sus ataques. Gracias a esta formación, he adquirido conocimientos sobre las herramientas necesarias para realizar un Pentesting interno en la entidad donde trabajo, permitiéndome contribuir activamente a la identificación y verificación de vulnerabilidades presentes en nuestro sistema.

Continuidad de Negocio, gracias a la materia pude enlistar los procesos críticos de la entidad donde laboro, de esta forma pude contribuir con el conocimiento impartido en clases por la Docente, y llevarlo a mi vida profesional. Así también pude dejar evidenciada la importancia de un SGCN en la entidad donde laboro.

Implementación

A continuación, se exponen las etapas que he evaluado como esenciales para llevar a cabo la identificación de las modificaciones que han tenido lugar entre la normativa ISO 27001:2013 y la reciente ISO 27001:2022. He considerado este proceso como un componente integral la estrategia de gestión de la Seguridad de la Información, porque permite adaptar y fortalecer los controles ya implementados en concordancia con las últimas actualizaciones de esta norma.

La Primera Fase consiste en Identificar las Observaciones que se han tenido en la última Auditoría externa, posterior a eso ejecutar las acciones correctivas de acuerdo a los planes de acción.

Las observaciones encontradas fueron las siguientes:

11.2.3 Seguridad del cableado: En el centro de datos, se han encontrado cables de cableado estructurado sin identificar sueltos.

12.6.1 Control de las vulnerabilidades técnicas: Considerar realizar análisis de vulnerabilidades. Asegura las pruebas para los próximos años, tanto nivel de escaneo de vulnerabilidades con pruebas de Ethical hacking donde sea aplicable.

Las no conformidades se detallan a continuación:

9.4.1 Restricción de acceso a la información: Se pudo acceder a líneas de comando \CMD donde se permite ejecutar comando DOS. Las carpetas que se comparten se pueden renombrar y borrar.

A.11.2.9 Política de escritorio y pantallas limpias: Se observan accesos directos a documento PDF y documentos desde el escritorio, en varios computadores de la entidad.

11.2.4 Mantenimiento de los equipos: Se encontró que no se ha realizado el mantenimiento preventivo a los componentes tecnológicos firewall.

Para solventar las observaciones y no conformidades se han definidos los siguientes planes de acción:

Figura 1

11.2.3 Seguridad del cableado - Plan de Acción

N°	TIPO	ACTIVIDAD	RESPONSABLE	PLAZO	
				DESDE	HASTA
1	AC	Realizar cableado estructurado en centro de Datos y etiquetar cables de comunicación.	Analista de Infraestructura	29/1/2024	9/2/2024
2	AP	Revisar periódicamente que el cableado del Centro de Datos se encuentre ordenado.	Analista de Infraestructura	12/2/2024	21/2/2024

Figura 2

12.6.1 Control de las vulnerabilidades técnicas – Plan de Acción

N°	TIPO	ACTIVIDAD	RESPONSABLE	PLAZO	
				DESDE	HASTA
1	AC	Gestionar documentación para servicio de Ethical Hacking	Técnico de Infraestructura	29/1/2024	9/2/2024
2	AC	Gestionar fechas de análisis de vulnerabilidades con el proveedor contratante	Técnico de Infraestructura	11/3/2024	15/3/2024
3	AP	Gestionar el plan de análisis de vulnerabilidades durante los próximos 3 años	Arquitecto de TIC	11/3/2024	15/3/2024

Figura 3

9.4.1 Restricción de acceso a la información – Plan de Acción

N°	TIPO	ACTIVIDAD	RESPONSABLE	PLAZO	
				DESDE	HASTA
1	AC	Configurar permiso de solo lectura a los usuarios que comparten carpetas	Técnico de Infraestructura	30/1/2024	2/2/2024
2	AC	Configurar el acceso a CMD solo a usuarios específicos (administradores)	Técnico de Infraestructura	30/1/2024	2/2/2024
3	AP	Capacitar a los usuarios para que utilicen OneDrive institucional y evitar el acceso a carpetas compartidas.	Arquitecto de TIC	30/1/2024	2/2/2024

Figura 4

A.11.2.9 Política de escritorio y pantallas limpias– Plan de Acción

N°	TIPO	ACTIVIDAD	RESPONSABLE	PLAZO	
				DESDE	HASTA
1	AC	Actualización de la política de puesto de trabajo despejado y pantalla limpia	Arquitecto de TIC	5/2/2024	9/2/2024
2	AP	Verificar que los computadores de la organización no tengan documentos PDF y WORD en el escritorio	Asistente de TIC	5/2/2024	9/2/2024
3	AP	Gestionar la socialización de la política actualizada de puesto de trabajo despejado y pantalla limpia	Técnico de Infraestrutura	6/2/2024	8/2/2024

Figura 5

11.2.4 Mantenimiento de los equipos – Plan de Acción

N°	TIPO	ACTIVIDAD	RESPONSABLE	PLAZO	
				DESDE	HASTA
1	AC	Gestionar la obtención de presupuesto para la adquisición de nuevos equipos firewall	Arquitecto de TIC	29/1/2024	9/2/2024
2	AC	Gestionar la obtención de cotizaciones	Técnico de Infraestructura	29/1/2024	9/2/2024
3	AC	Realizar los trámites respectivos para la aprobación de Mintel	Técnico de Infraestructura	9/2/2024	15/2/2024
4	AC	Gestionar la compra del equipo firewall con el área de compras	Técnico de Infraestructura	16/2/2024	15/3/2024
5	AP	Realizar la planificación de los mantenimientos futuros del nueco equipo	Técnico de Infraestructura	29/1/2024	9/2/2024

Los resultados de la ejecución de los planes de acción pueden ser verificados en el **anexo 2** Propuesta de implementación, en la fase 1 “solventar hallazgos en la auditoría externa”.

La segunda Fase consiste en identificar los cambios que existen entre las versiones 2013 y 2022, tales como cambios de redacción, cambios de controles del anexo. En esta etapa también se comparará lo implementado en la entidad vs controles que son necesarios implementar con la actualización 2022.

En la figura 6 se puede apreciar los cambios en números que presenta la nueva versión. Los 114 controles se convirtieron en 93 controles. Los controles ahora se dividen en cuatro temas : organizativos (37) , personas (8) físicos (14) y tecnológicos (34). Hay 56 controles ISO 27001:2013 fusionados en 24 controles en ISO 27001:2022 y un total de 11 controles nuevos.

Figura 6

ISO 27001:2022 en números

A continuación, se presentan las modificaciones de redacción de la norma ISO 27001:2022:

Figura 7

ISO 27001:2022 cambios de redacción

4.2 Comprender las necesidades y expectativas de las partes interesadas: Se agrega literal c: “Cuáles de estos requisitos se abordarán mediante el Sistema de Gestión de Seguridad de la Información”

4.4 Sistema de gestión de seguridad de la información: Se agrega línea que indica: “incluyendo los procesos necesarios y sus interacciones, de acuerdo con los requisitos de esta Norma Internacional”

5.3 Roles, responsabilidades y autoridades organizacionales: Se cambió la redacción: estén asignadas y comunicadas dentro de la organización.

6.2 Objetivos de seguridad de la información y planificación para conseguirlos:

1. e) ser comunicados;

2. g) estar disponible como información documentada.

6.3 Planificación de cambios: Se agrega cláusula 6.3 “Cuando la organización determina la necesidad de cambios en el sistema de gestión de la seguridad de la información, los cambios deben ser llevados a cabo de manera planificada.”

7.4 Comunicación: Ante indicaba “quién debe comunicar”, ahora indica “como comunicarse”, en la nueva versión se elimina el literal e).

8.1 Planificación y control operacional: Se extiende a procesos. Se agrega una solicitud para establecer criterios para los procesos del Sistema.

9.3 Revisión por la dirección: Se detalla 9.3.1, 9.3.2, 9.3.3**.** Adición de numeral c) cambios en las necesidades y expectativas de las partes interesadas que son relevantes para el sistema de gestión de seguridad de la información.

Cambios de controles de anexo:

Hay 37 controles organizativos del 5.1 al 5.37, 8 controles “personas” del 6.1 al 6.8, 14 controles físicos del 7.1 al 7.14, 34 controles tecnológicos del 8.1 al 8.34.

Figura 8

ISO 27001:2022 controles del anexo

Porcentaje de cumplimiento de los controles:

Para determinar el nivel de cumplimiento de los controles, se empleó el Instrumento de Diagnóstico Posterior a la Declaración de Aplicabilidad. Este instrumento se presenta como una matriz que enumera los 93 controles junto con sus descripciones detalladas. A través de esta matriz, se evaluó el grado de cumplimiento de los controles ya implementados en la entidad.

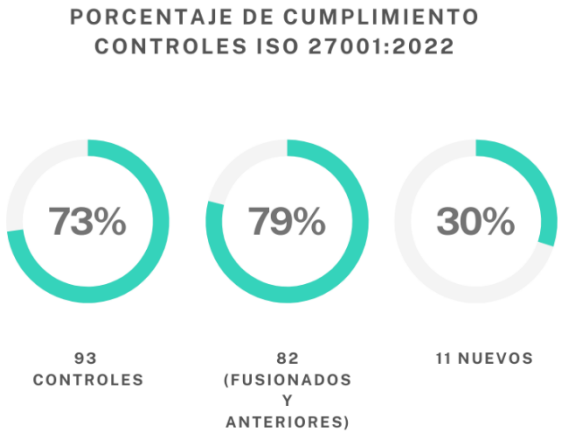
Es fundamental destacar que este proceso de evaluación se basa en una escala específica de valores predefinidos, diseñada para brindar una representación clara del estado de cada control. Los valores asignados para evaluar el estado de los controles son los siguientes:

- Valor 0: Sin documentar, ni implementar.
- Valor 1: Implementado, pero no documentado.
- Valor 2: Implementado, documentado, pero requiere mejoras.
- Valor 3: Implementado y listo para auditar.

Esta metodología estructurada permite una clasificación precisa de cada control, proporcionando una visión integral del nivel de preparación y cumplimiento en la implementación de los mecanismos de seguridad.

Figura 9

Porcentaje de cumplimiento de los controles ISO 27001:2022



El instrumento de diagnóstico se lo puede revisar en el **anexo 2** Propuesta de implementación, en la fase 2 “Comparar lo implementado 27001:2013 vs 27001:2022”.

En la tercera fase, se lleva a cabo la elaboración del plan de actualización para aquellos controles (11 nuevos) que, según el instrumento de diagnóstico, han sido valorados con 0, indicando que aún no han sido implementados ni documentados.

Los resultados obtenidos se los representa en la figura 10:

Figura 10

Controles con valor 0

PROCESO	CONTROL	NOMBRE CONTROL	DESCRIPCIÓN	SGSI
SI	5.7	Inteligencia de amenazas	La información relativa a las amenazas a la seguridad de la información se recopilará y analizará para producir información sobre amenazas.	0
SI	5.23	Seguridad de la información para el uso de Servicios en la nube	Los procesos de adquisición, uso, gestión y salida de los servicios en la nube se establecerán de acuerdo con los requisitos de seguridad de la información de la organización.	0
TIC	8.10	Eliminación de información	La información almacenada en sistemas de información, dispositivos o en cualquier otro medio de almacenamiento se eliminará cuando ya no sea necesaria.	0
TIC	8.11	Enmascaramiento de datos	El enmascaramiento de datos se utilizará de acuerdo con la política específica del tema de la organización sobre control de acceso y otras políticas específicas de temas relacionados, y los requisitos comerciales, teniendo en cuenta la legislación aplicable.	0
TIC	8.12	Prevención de fuga de datos	Se aplicarán medidas de prevención de fuga de datos a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información sensible.	0
TIC	8.16	Actividades de supervisión	Se supervisarán las redes, los sistemas y las aplicaciones para detectar comportamientos anómalos y se adoptarán las medidas adecuadas para evaluar posibles incidentes de seguridad de información.	0

Para los controles con valor 0, se ha elaborado el siguiente cronograma:

Figura 11

Cronograma para el plan de actualización de controles con valor 0

Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin
1		**5.7 Inteligencia de Amenazas**	**25 días**	**lun 11/3/24**	**vie 12/4/24**
2		Actualización de Procedimiento de Gestión de Incidentes	15 días	lun 11/3/24	vie 29/3/24
3		Política de inteligencia de amenazas	10 días	lun 1/4/24	vie 12/4/24
4		**5.23 Seguridad de la información para el uso de Servicios en la nube**	**30 días**	**mar 12/3/24**	**lun 22/4/24**
5		Política de seguridad con proveedores	15 días	mar 12/3/24	lun 1/4/24
6		Política de servicios en la nube	10 días	mar 2/4/24	lun 15/4/24
7		Acuerdos de servicios en la nube	5 días	mar 16/4/24	lun 22/4/24
8		**8.10 Eliminación de información**	**10 días**	**lun 18/3/24**	**vie 29/3/24**
9		Política de eliminación y destrucción de información	10 días	lun 18/3/24	vie 29/3/24
10		**8.11 Enmascaramiento de datos**	**9 días**	**lun 18/3/24**	**jue 28/3/24**
11		Política de desarrollo seguro	5 días	lun 18/3/24	vie 22/3/24
12		Política de protección de la información	3 días	lun 25/3/24	mié 27/3/24
13		**8.12 Prevención de fuga de datos**	**24 días**	**mar 19/3/24**	**vie 19/4/24**
14		Actualización de procedimiento de Seguridad de la Información	4 días	mar 19/3/24	vie 22/3/24
15		Política de protección de la información	5 días	lun 25/3/24	vie 29/3/24
16		Actualización de matriz de riesgo	11 días	lun 1/4/24	lun 15/4/24
17		Capacitación	4 días	mar 16/4/24	vie 19/4/24
18		**8.16 Actividades de supervisión**	**30 días**	**mié 20/3/24**	**mar 30/4/24**
19		Actualización de procedimiento de Seguridad de la Información	4 días	mié 20/3/24	lun 25/3/24
20		Política de registro u monitoreo	4 días	mar 26/3/24	vie 29/3/24
21		Gestión para implementación de SIEM	22 días	lun 1/4/24	mar 30/4/24

En la cuarta fase, se detallan los pasos a seguir para llevar a cabo una auditoría interna con el propósito de evaluar la eficacia de los recién implementados controles. Este proceso no solo tiene como meta verificar la conformidad con los estándares establecidos, sino que también desempeña un papel esencial en la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).

Conclusiones

En conclusión, el presente estudio sobre el plan de migración de la Norma Internacional ISO 27001:2013 a la versión 27001:2022 ha proporcionado una visión integral y detallada sobre los aspectos clave involucrados en la transición hacia los estándares más recientes en seguridad de la información. La evaluación de los cambios en los requisitos, la implementación de un instrumento de diagnóstico posterior a la Declaración de Aplicabilidad, y la ejecución de una auditoría interna han destacado la importancia de adaptarse a las últimas actualizaciones.

La migración exitosa no solo implica la modificación de procesos y controles, sino también la promoción de una cultura organizacional centrada en la seguridad. La incorporación de nuevas estrategias y enfoques, así como la identificación y actualización de controles que no estaban implementados, demuestran el compromiso continuo con la mejora y la adaptación a los desafíos cambiantes en el ámbito de la seguridad de la información.

Este plan de migración no solo se concibe como una obligación normativa, sino como una oportunidad para fortalecer y optimizar el Sistema de Gestión de Seguridad de la Información (SGSI). La comprensión profunda de los cambios, la metodología de evaluación rigurosa y la auditoría interna sistemática son elementos fundamentales para garantizar la conformidad y la efectividad en la gestión de la seguridad de la información.

En resumen, este plan de migración se erige como un paso estratégico hacia la mejora continua, la resiliencia organizacional y el mantenimiento de estándares de seguridad robustos en consonancia con los avances en el panorama de amenazas y la evolución de la normativa internacional.

Limitaciones

Dentro de las limitaciones para la ejecución de este proyecto, se destaca el aspecto presupuestario. Es necesario justificar y explicar las razones por las cuales se requiere realizar una inversión considerable para mantener los tres pilares fundamentales de la seguridad de la información: confidencialidad, integridad y disponibilidad. Es crucial que toda la organización comprenda la importancia de la seguridad de la información, y también se valora que el compromiso de la alta dirección se mantenga.

Recomendaciones

En vista de la crítica importancia de la seguridad de la información, es esencial seguir rigurosamente el plan de actualización de controles, implementando y documentando aquellos que aún no lo están. La medición efectiva de la eficacia de estos controles se logra a través de auditorías internas y externas. Las auditorías internas permiten evaluaciones sistemáticas internas, identificando áreas de mejora, mientras que las auditorías externas, realizadas por expertos independientes, brindan una validación objetiva del cumplimiento con estándares externos. La combinación de estas auditorías garantiza no solo el cumplimiento de los controles, sino también la mejora continua, fortaleciendo la resiliencia y la capacidad de adaptación a los cambios en amenazas y regulaciones. Este enfoque integral no solo protege la integridad, confidencialidad y disponibilidad de la información, sino que también refuerza la credibilidad de la organización.

Referencias

I sec T Ltd. (2020). *Introduction to the ISO27k standards.* Obtenido de https://www.iso27001security.com/html/iso27000.html

ISO27000.ES. (s.f.). Obtenido de https://www.iso27000.es/sgsi.html

UIT. (2008). *Aspectos generales de la ciberseguridad.* Suiza.

Anexo 1

Evidencia de aprendizaje.

https://www.notion.so/839ebc9465db4f63ae01f4d1ecd755cf?v=2c77311368e14c89986c1b1f80b6e7a7&pvs=4

Anexo 2

Propuesta de implementación.

https://www.notion.so/Propuesta-de-implementaci-n-2d16aea82ed2435383ca4a5d3384a781?pvs=4