Afrontando los Desafíos de la Seguridad de la Información: Implementación de un SGSI en un Instituto Superior Universitario.

Edel Moreira Alvarez

Presentado como parte de los requisitos para el título de magíster en ciberseguridad.

CES: RPC-SE-01-N˚.014-2020. COHORT2 2022 - 2023.

Correo electrónico del autor: edelmoreiraalvarez@gmail.com

GUAYAQUIL, 2 DE ABRIL DEL 2023.

Keywords: Information security, ISMS, challenges of information security.

Resumen

El Instituto Superior Universitario está planificando implementar un Sistema de Gestión de Seguridad de la Información (SGSI) para proteger sus activos de información, incluyendo los datos de estudiantes, docentes, administrativos, propiedad intelectual y otros activos importantes. La implementación de este sistema se justifica por varios puntos, como la protección de la información, el cumplimiento legal, la protección de la reputación, la reducción de costos y la mejora continua. La implementación de un SGSI ayudará a garantizar el cumplimiento de los requisitos legales y regulatorios, así como a reducir el riesgo de violaciones de seguridad y, por lo tanto, a proteger la reputación y reducir los costos asociados con ellas. Además, será un sistema de mejora continua que ayudará a identificar, evaluar y mitigar los riesgos de seguridad de la información en curso. Los conocimientos adquiridos durante la Maestría en Ciberseguridad, impartido por la Universidad Casa Grande, fueron valiosos para la implementación del SGSI. Cuatro materias en particular jugaron un papel importante: Gerencia, Operación y Planificación de la Ciberseguridad; Estrategias y Políticas Multilaterales para la Ciberseguridad; Marco Legal y Análisis Forense; y Tecnología, Modelos y Técnicas de Ciberseguridad.

Afrontando los Desafíos de la Seguridad de la Información: Implementación de un SGSI en un Instituto Superior Universitario.

Actualmente el Instituto Superior Universitario no cuenta con los mecanismos y procedimientos necesarios para evaluar y mitigar los riesgos asociados a los activos de seguridad informática. Tampoco cuenta con equipos de colaboradores que pueda dirigir a la Institución en materia de seguridad informática, quedando de esta forma, expuesto a disimiles ciberataques.

Este trabajo está enfocado en la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) dentro de un Instituto Superior Universitario. En esta ocasión se consultaron diversas fuentes bibliográficas para resumir los principales puntos que justifican la implementación de este sistema. (EXCELLENCE)

1. Protección de la información: Esta implementación ayudará a proteger la información de la Institución, incluyendo los datos de los estudiantes, docentes, administrativos, los secretos comerciales, la propiedad intelectual y otros activos importantes.
2. Cumplimiento legal: Muchas leyes y regulaciones requieren que la Institución proteja la información que manejan. (NACIONAL, 2021) Este SGSI ayudará a garantizar que se cumpla con estos requisitos legales y regulatorios.
3. Protección de la reputación: Una violación de seguridad puede tener un impacto significativo en la reputación de la Institución. Implementar un SGSI ayudará a reducir el riesgo de violaciones de seguridad y, por lo tanto, protege la reputación.
4. Reducción de costos: Una violación de seguridad puede ser costosa para las Institución. La implementación de este SGSI ayudará a reducir el riesgo de violaciones de seguridad y, por lo tanto, reducir los costos asociados con ellas.

5. Mejora continua: Este SGSI será un sistema de mejora continua que ayudará a identificar, evaluar y mitigar los riesgos de seguridad de la información en curso. Al hacerlo, la Institución podrá mejorar constantemente su postura de seguridad y reducir el riesgo de violaciones de seguridad en el futuro.

También fueron muy valiosos los conocimientos adquiridos durante el cursar de la Maestría en Ciberseguridad, impartido por la Universidad Casa Grande. Se debe resaltar cuatros materias que jugaron un papel muy importante: Gerencia, Operación y Panificación de la Ciberseguridad; Estrategias y Políticas Multilaterales para la Ciberseguridad; Marco Legal y Análisis Forense; Tecnología, Modelos y Técnicas de Ciberseguridad.

Desarrollo

La materia Gerencia, Operación y Planificación de la Ciberseguridad jugó un papel fundamental dentro de la implementación del SGSI. Brindando herramientas que aseguran que la organización tenga una estrategia sólida de seguridad de la información, alineada con los objetivos del negocio.

Esta materia brindó las pautas para identificar los riesgos que puedan afectar a la Institución y sus activos informáticos. La evaluación de riesgos es un paso clave en la implementación del SGSI y ayudará a comprender los riesgos potenciales y su impacto.

La implementación del SGSI es un proceso complejo que requiere de la consideración de múltiples factores, entre ellos el marco legal, por esto la importancia de la materia: Marco Legal y Análisis Forense. A continuación, se indica cómo influyen estos dos aspectos en la implementación de nuestro SGSI:

- Marco Legal: El marco legal incluye leyes, regulaciones, políticas y estándares que establecen las obligaciones y requisitos que la Institución debe cumplir para proteger la seguridad de la información. La implementación de un SGSI debe considerar y cumplir con los requisitos legales pertinentes, como la protección de datos personales, la privacidad, la confidencialidad y la integridad de la información. (telecomunicaciones)

Además, el marco legal también establece las sanciones y las consecuencias de no cumplir con los requisitos de seguridad de la información. Por lo tanto, la implementación de un SGSI debe considerar estas sanciones y consecuencias para asegurar que se estén cumpliendo los requisitos legales y evitar posibles multas o daños a la reputación de la Institución.

- Análisis Forense: El análisis forense es el proceso de recolección, análisis y preservación de evidencia digital con el objetivo de determinar la causa de un incidente de seguridad de la información y, en última instancia, identificar al responsable del mismo. La implementación de un SGSI debe considerar la posibilidad de incidentes de seguridad de la información y cómo la organización va a manejarlos.

El análisis forense puede ser una herramienta importante para la gestión de incidentes de seguridad de la información, permitiendo a la organización determinar la causa raíz del incidente y tomar medidas para prevenir incidentes similares en el futuro. Además, el análisis forense puede ser útil para la resolución de disputas legales o para proporcionar pruebas en caso de litigios.

Dentro de la materia Tecnología, Modelos y Técnicas de Ciberseguridad se vieron aspectos de vital importancia para la implantación de un sistema de gestión de seguridad de la información. La implementación de soluciones de seguridad

informática adecuadas garantiza la integridad, confidencialidad y disponibilidad de la información.

Como última materia analizada para el desarrollo de este trabajo se encuentra: Estrategias y Políticas Multilaterales para la Ciberseguridad, la cual proporcionar una comprensión de las políticas y estándares internacionales de seguridad, como la Norma ISO 27001. Además, comprensión de los marcos de gobernanza de la ciberseguridad, como el Marco de Ciberseguridad Nacional de los Estados Unidos, que pueden ser útiles en la implementación de políticas de seguridad de la información y en la gestión de incidentes de seguridad.

Implementación

La implementación de este Sistema de Gestión de Seguridad de la Información será un proceso clave para garantizar la protección y confidencialidad de los datos de la Institución. Considerando la relevancia de este proceso, se propuso definir los siguientes puntos dentro de la implementación:

1. Se definirá el alcance y objetivos del SGSI, determinando qué áreas de la Institución estarán incluidas en el SGSI y qué objetivos se quieren alcanzar. Esto permitirá establecer un marco de referencia para la implementación.

2. Se establecerá un equipo de implementación, encargado de liderar la implementación del SGSI. Este equipo estará conformado por personas con conocimientos técnicos, representantes de las principales áreas de la Institución y experiencia en seguridad de la información. (Información, 2020)

3. Se identificarán los activos críticos de la institución, los cueles necesitan ser protegidos. Estos activos pueden ser datos, sistemas, procesos, entre otros.

4. Se realizará una evaluación de los riesgos a los que están expuestos los activos críticos de la institución. Esta evaluación permitirá establecer las medidas necesarias para minimizar los riesgos.

5. Se definirán políticas y procedimientos de seguridad para garantizar la seguridad de los activos críticos de la institución. Estas políticas y procedimientos estarán basados en estándares reconocidos de seguridad de la información.

6. Serán implementados los controles de seguridad necesarios para proteger los activos críticos de la empresa. Estos controles pueden ser tecnológicos, físicos, administrativos, entre otros. (Empresa, 2017)

7. Se establecerá un sistema de monitoreo y revisión que permita asegurarse de que los controles de seguridad están funcionando de manera efectiva y de que se están cumpliendo las políticas y procedimientos establecidos.

8. Se realizarán pruebas de seguridad periódicas para asegurarse de que el SGSI está funcionando de manera efectiva y de que se pueden detectar y corregir posibles fallas.

9. Se capacitará al personal de la Institución en cuanto a las políticas y procedimientos de seguridad de la información y en la importancia de proteger los activos críticos.

10. Se establecerán procesos de mejora continua que permita identificar áreas de oportunidad y hacer ajustes necesarios en el SGSI para mejorar su eficacia y eficiencia.

Cronograma de implementación del SGSI

Nota: Se muestra el cronograma de implementación del Sistema de Gestión de Seguridad de la Información dentro de la institución. Se tiene previsto comenzar a mediados del mes de abril y finalizar a finales del mes de julio. El proceso de implementación fue dividido en doce etapas.

Conclusiones

La implementación de un Sistema de Gestión de Seguridad de la Información dentro de nuestra Institución será esencial para garantizar la protección de los datos y sistemas de información. A lo largo del proceso de implementación, se deben considerarán diversos aspectos, como la identificación de los activos críticos, la evaluación de riesgos, la implementación de controles de seguridad y la capacitación del personal.

La implementación de este SGSI no solo es importante para proteger la información, sino que también mejorará la eficiencia de los procesos y optimizará los recursos. Además, que podrá ayudar a mantener la confianza de los estudiantes, docentes, administrativos y cumplir con los requisitos normativos dispuestos por las instituciones rectoras del sistema académico en el país.

La mejora continua será un elemento clave en la implementación de este SGSI y permitirá identificar oportunidades de mejora en el sistema de seguridad, implementar soluciones y medir el impacto de las mejoras. La mejora continua no

será un proceso único, sino que será parte de la cultura organizacional y evolucionará junto con los cambios y avances en la tecnología y las amenazas de seguridad.

Limitaciones

Con la implementación del SGSI se prevén varios desafíos entre los que destacan la falta de conciencia sobre la importancia de la seguridad de la información y la resistencia al cambio por parte de estudiantes, docentes y administrativos. Además, la falta de recursos adecuados, incluyendo presupuesto, personal capacitado y herramientas de seguridad, lo que puede retrasar la implementación y limitar la eficacia del SGSI. La complejidad del entorno tecnológico en nuestro Instituto, con múltiples sistemas, plataformas y dispositivos, puede dificultar la implementación.

Recomendaciones

Se agradece a todos los docentes y al coordinador de la Maestría por la paciencia y los conocimientos transmitidos. Para todo aquel profesional del área que desean cursar la Maestría en Ciberseguridad, se dejan las siguientes recomendaciones:

- Existen muchas herramientas y recursos en línea que pueden ser útiles para estudiar ciberseguridad, desde foros de discusión hasta cursos en línea. Investiga y familiarízate con estos recursos antes de comenzar tu programa de maestría.
- Configurar un entorno de pruebas en tu propia computadora o dispositivo móvil para practicar y experimentar con diferentes herramientas y técnicas de ciberseguridad.
- Forma un grupo de estudio con otros estudiantes de ciberseguridad para discutir temas, practicar habilidades y resolver problemas juntos.

- Aprovecha al máximo las oportunidades de realizar proyectos prácticos durante el programa de maestría. Trabaja en proyectos que involucren la identificación y resolución de problemas reales de seguridad de la información.
- Busca oportunidades para realizar prácticas profesionales en empresas, organizaciones que se especialicen en ciberseguridad
- Asistir a conferencias y eventos de ciberseguridad para aprender de expertos en el campo, conocer las últimas tendencias y tecnologías, y establecer contactos con profesionales de la industria.

Referencias

Empresa, S. G. (2017). *ISO/IEC 27002:2013 - Código de Prácticas para los Controles de Seguridad de la Información.*

EXCELLENCE, I. (s.f.). *La Norma ISO 27001: Aspectos Claves de su Diseño e Implantación.*

Información, M. d. (2020). *Guía para la Implementación del Esquema Gubernamental de Seguridad de la Información.* Gobierno Electrónico.

NACIONAL, A. (2021). *LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES.* Registro Oficial - Ógano de la Republica del Ecuador.

telecomunicaciones, c. o. (s.f.). *Guía de Iniciación a Actividad Profesional Implantación de Sistemas de Gestión de la Seguridad de la Información (SGSI) según la norma ISO 27001.*

Anexos

Anexo1: Notion, Propuesta

https://shiny-bobcat-1dd.notion.site/Implementar-un-Sistema-de-Gesti-n-de-Seguridad-de-la-Informaci-n-en-el-Instituto-Superior-Universita-aea78a0cd917411d9794c5fc35ccb3e9

Anexo2: Propuesta de implementación

https://www.notion.so/Implementar-un-Sistema-de-Gesti-n-de-Seguridad-de-la-Informaci-n-en-el-Instituto-Superior-Universita-aea78a0cd917411d9794c5fc35ccb3e9?pvs=4#fbfcf7558eab4692884c38841d2b165b