FORTALECIENDO LA SEGURIDAD DE LA INFORMACIÓN: UN CASO DE BUENA PRÁCTICA EN LA IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LA EMISIÓN DE TÍTULOS UNIVERSITARIOS BAJO LA NORMA ISO/IEC 27001

Resumen:

Este artículo presenta un caso de buena práctica en la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI) en el proceso de emisión de títulos de la Universidad Católica de Salta (UCASAL), bajo los criterios de la Norma ISO/IEC 27001. Esta norma proporciona una metodología sólida para el establecimiento, implementación, mantenimiento y mejora de este sistema en la universidad ayudando a identificar, evaluar y tratar los riesgos de seguridad de la información de manera sistemática, asegurando así la protección de los activos de información crítica. Se describen las medidas orientadas a proteger la información mediante la definición de una Política de Seguridad y el alcance del SGSI, el análisis y gestión de riesgos, la selección e implementación de controles de seguridad de la información, formación del personal y auditorías realizadas. Los resultados muestran una mejora significativa en la protección de la información, el cumplimiento de estándares internacionales, la reducción de incidentes de seguridad y una mayor conciencia de seguridad entre el personal. Se destacan los próximos pasos a seguir, incluyendo la mejora continua, la ampliación del alcance de la certificación, la actualización de políticas y procedimientos, entre otros. Este caso demuestra el compromiso de la Universidad con la seguridad de la información que administra y la protección de los datos en el camino de la transformación digital universitaria

INTRODUCCION

En el proceso de transformación digital de la gestión universitaria, la digitalización de procesos tradicionales a través de tecnologías de la información busca mejorar los servicios a alumnos y graduados, así como facilitar las operaciones a docentes y personal de gestión. Esta decisión implica gestionar documentos de forma electrónica, automatizar procesos académicos como matrículas y títulos, y manejar grandes volúmenes de datos, lo que representa un desafío en ciberseguridad si no se implementan medidas adecuadas. Este artículo presenta un caso de buenas prácticas en la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI) bajo la Norma ISO 27001 en la emisión de títulos, resaltando procedimientos, controles y medidas para garantizar la protección de la información y la confidencialidad.

Figura 1: Pasos en la Implementación de un SGSI en la Universidad

PLAN DE ACCION LLEVADO A CABO

Se eligió adecuar la seguridad de la UCASAL a la Norma ISO/IEC 27001 para preservar la integridad, confidencialidad e integridad de la información ya que se ha demostrado que no es suficiente la implantación de controles y procedimientos de seguridad realizados frecuentemente sin un criterio común establecido, en torno a la compra de productos técnicos y sin considerar toda la información esencial que se debe proteger. En este sentido, es necesario la identificación de definición y objetivos de la política de seguridad, su propósito, forma de comunicación, capacitación, confidencialidad, reglas y obligaciones de los usuarios, control de malware, uso de correo electrónico e Internet, datos personales, etc.

Fase 1: Definir la Política de Seguridad

Si bien existían documentos institucionales que detallaban procedimientos de uso de Internet, correo electrónico, contraseñas y asignación y uso de equipo de cómputo, quedaban pendientes definiciones relacionadas, entre otras, con relación a la conformación de un Comité de Seguridad y la estructura de Seguridad, la gestión de los datos personales, la definición de roles y permisos de los dueños de datos y la actividad a llevar a cabo por medio de la Auditoría Interna.

Se procedió entonces a la definición de una política de seguridad de manera general, citando o indicando procedimientos existentes o que se van a crear, sin entrar en el detalle de su implementación. Esto produjo una mejor lectura por personas no técnicas y a la vez permitió que la política se mantenga en el tiempo y sólo cambien los procedimientos o cómo se implementa cada subpolítica (o Norma).

En fecha 22/08/2023 se emitió la Resolución Rectoral N°: 761/2.023 con el objeto de "APROBAR LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD CATÓLICA DE SALTA" estableciendo así un marco formal de definiciones principales de la organización, planificación, comunicación, procedimientos, prácticas y controles para asegurar los activos de información de UCASAL en lo que respecta a la confidencialidad, integridad y disponibilidad y creando el "Comité de Seguridad de la Información" de UCASAL, con dependencia del Rectorado, y el puesto de "Administrador de Seguridad de la Información".

Fase 2: Definir el Alcance del SGSI

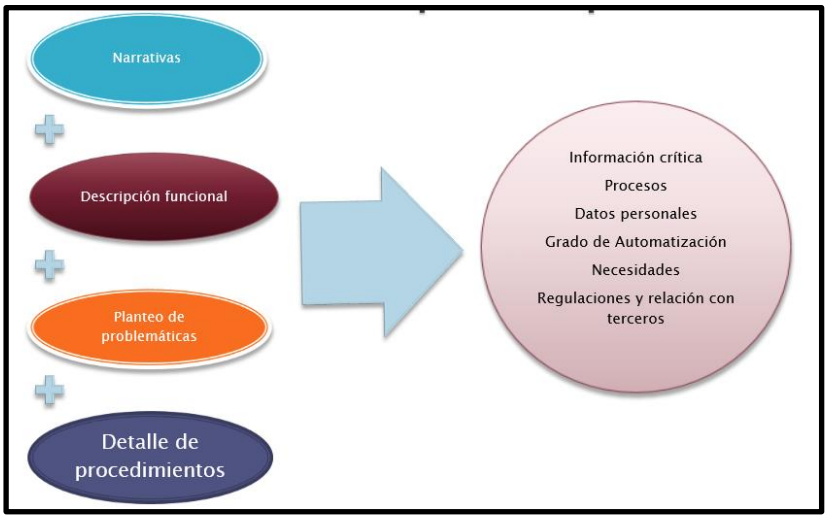
Es necesario definir el alcance del SGSI (Figura 2), ya que no toda la información de la organización tiene los mismos niveles de criticidad y, por lo tanto, de economicidad en la implementación de los controles. Para definir el alcance a través de los dueños de los procesos y los datos se realizaron las actividades de relevamiento general de la Universidad a fin de conocer las diferentes áreas y organización existente, coordinación de visitas a los diferentes Vicerrectorados y el relevamiento más detallado, a nivel de Dirección, en cada Vicerrectorado y otras áreas estratégicas. Estas actividades se desarrollaron utilizando las técnicas de Entrevistas presenciales y virtuales, revisión de documentación, confección de minutas resumen y Validación de información con los entrevistados.

El resultado de esta fase permitió definir la Información crítica respecto a la confidencialidad, integridad y disponibilidad, los procesos que se gestionan, activos tecnológicos en general, datos personales, grado de automatización de las tareas que se realizan, necesidades y el cumplimiento de regulaciones y relación con terceros.

Para prevenir las consecuencias de los ataques cibernéticos en la universidad, es necesario contar una estrategia de ciberseguridad sólida que aborde los riesgos específicos contemplando a la Institución como un todo, pero particularizando cada parte.

Atendiendo a nuestra experiencia en gestión universitaria y luego de revisar propuestas interesantes para el ámbito universitario, como las de Choi y Kim (2021) , Krombholz, K., Kieseberg, P., & Weippl, E. (2021) , Sánchez-Arias, J. A., & Ochoa-Arias, A. M. (2021) y Zhu, Y., Wang, X., Guo, L., Huang, X., & Xu, R. (2021) entre otros, decidimos adoptar como guía de nuestro trabajo en esta área la propuesta realizada por Rizk y Zohdy (2021) para las instituciones de educación superior, la cual ofrece un marco de evaluación de riesgos

Figura 2: Definición del Alcance y sus resultados



Fase 3: Análisis de Riesgo:

A continuación, se procedió a realizar un análisis exhaustivo de riesgos asociados al proceso de emisión de títulos, tras un relevamiento integral de los activos. Identificamos las posibles vulnerabilidades y amenazas, realizamos un análisis de impacto integral y sugerimos medidas para mitigarlos. Como mencionamos anteriormente, en esta fase complementamos la tarea con la guía realizada por Rizk y Zohdy (2021), orientada a las instituciones de educación superior, para enriquecer el marco que le dimos a las tareas en esta etapa. (Figura 3)

Figura 3: Método de Evaluación y Tratamiento de Riesgo

Destacamos que al proceso de Confección y Emisión de Títulos está certificado con la Norma Iram ISO 9001, lo cual facilita la tarea en términos de definición de procesos claves relacionados con este proceso crítico. Queremos reforzar este proceso con el aseguramiento de calidad que propone la Norma ISO 27001. Actualmente, estamos trabajando en el desarrollo e implementación de la fase 4, referente a la gestión del riesgo, y la Fase 5, sobre la selección de los controles de seguridad tanto técnica como organizativa, para avanzar en la certificación de la Norma Internacional. Paralelamente, estamos elaborando un plan de formación y concientización sólido sobre la seguridad de la información, dirigido principalmente al personal involucrado en el proceso de

confección y emisión de Títulos, con el fin de aumentar la conciencia sobre los riesgos y las mejores practicas de seguridad. Con la conformación del comité de seguridad, se pretende responder eficaz y rápidamente ante cualquier incidente de seguridad que pueda ocurrir durante el proceso de emisión de títulos.

RECURSOS UTILIZADOS

Para llevar a cabo las tareas relacionadas con la implementación del SGSI, se conformó un equipo multidisciplinario de profesionales expertos en procesos digitalizados, procesos académicos y seguridad. Asimismo, se utilizaron diversas herramientas y tecnologías de seguridad de la información, como sistemas de detección de phishing, cifrado de datos, entre otros, para garantizar la inviolabilidad de los sistemas y protección de los datos. Cabe destacar que se asignó una partida presupuestaria especial para la compra de tecnologías de seguridad, la capacitación del personal, auditorias externas e internas y otras actividades relacionadas con la implementación de la ciberseguridad.

RESULTADOS ALCANZADOS

Entre los logros alcanzados hasta el momento, se destaca que pudimos identificar ciertas amenazas y vulnerabilidades a nivel de sistemas en nuestro camino hacia la Transformación Digital. Esto nos permitió implementar medidas que mejoran la protección de los datos y la información sensible y critica asociada al proceso de emisión de títulos, como la autenticación de dos factores (2FV) y la tecnología blokchain, reduciendo así el riesgo de exposición a amenazas cibernéticas. Además, logramos instaurar una mayor conciencia sobre la seguridad de la información entre el personal involucrado en el proceso de emisión de títulos,lo que ha contribuido a la adopción de mejores prácticas de seguridad.

PRÓXIMOS PASOS

Nuestro objetivo es ampliar el alcance de la certificación ISO 27001 a otros procesos importantes del quehacer universitario, garantizando una protección integral de la información en toda la Institución. Mantendremos un enfoque de mejora continua en el sistema de seguridad de la información, identificando áreas de mejora e implementando acciones correctivas y preventivas. Al mismo tiempo, iremos incorporando nuevas tecnologías emergentes, como la inteligencia artificial, para mejorar la detección y respuesta ante amenazas cibernéticas, promoviendo constantemente la cultura de la seguridad donde la protección de los datos sea una prioridad en el quehacer universitario.

CONCLUSIONES

Los aprendizajes que esta experiencia brinda a la UCASAL son innumerables, destacando principalmente la comprensión de los riesgos de seguridad asociados con el uso de la tecnología y el desarrollo de estrategias para abordarlos, garantizando la protección de datos sensibles y la confiabilidad de los procesos críticos, como la confección y emisión de títulos, en una institución educativa. La certificación ISO 27001 nos asegura cumplir con estándares internacionales de seguridad, la auditoria permanente y la mejora continua, lo cual añade un importante plus a la eficiencia operativa y la confianza de los stakeholders.

Estos logros demuestran el compromiso de la UCASAL con la ciberseguridad de la información y la excelencia en la gestión, sentando un sólido precedente para futuras implementaciones y mejoras en la institución.

REFERENCIAS BIBLIOGRAFICAS

Choi, Y. J., & Kim, S. S. (2021). Cybersecurity Awareness and Education in Higher Education Institutions. Journal of Education for Library and Information Science, 62(2), 80-91. https://doi.org/10.3138/jelis.62.2.03

ISO/IEC 27001:2022 (2022). Information security, cybersecurity and privacy protection. Information security management systems. Requirements.

ISO/IEC 27001:2022 (2022). Information security, cybersecurity and privacy protection. Information security controls.

Krombholz, K., Kieseberg, P., & Weippl, E. (2021). Protecting Academic Research and Intellectual Property from Cyber Attacks. ACM SIGCAS Computers and Society, 50(1), 9-16. https://doi.org/10.1145/3454063.3454067

Rizk, R., & Zohdy, I. (2021). Towards a framework for assessing cyber security risk in higher education institutions. Computers & Security, 104, 102242. https://doi.org/10.1016/j.cose.2021.10224

Sánchez-Arias, J. A., & Ochoa-Arias, A. M. (2021). Security of Personal Data in Higher Education: Analysis of Technological Trends and Implications. Revista de Administração, Contabilidade e Economia da FUNDACE, 12(2), 117-133. https://doi.org/10.13071/recope-2021-0030

Zhu, Y., Wang, X., Guo, L., Huang, X., & Xu, R. (2021). A Lightweight and Secure Mobile Authentication Protocol for University E-Campus. IEEE Access, 9, 61658-61668. https://doi.org/10.1109/ACCESS.2021.3075581