ESCUELA DE POSGRADO NEWMAN

MAESTRÍA EN
GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

“Propuesta de diseño de un SGSI para la Agrupación Marista del Ecuador utilizando como marco de referencia la ISO27001”

Trabajo de Investigación
para optar el Grado a Nombre de la Nación de:

Maestro en
Gestión de Tecnologías de la Información

Autores:
Bach. Banda Yánez, Luis Fernando
Bach. Morejón Armijo, Victoria Estefanía

Docente Guía:
Mg. Moscoso Zegarra, Giomar Walter

TACNA – PERÚ

2022

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

Resumen

La Agrupación Marista del Ecuador se ve en la necesidad de implementar herramientas y estrategias que permitan proteger la información y los sistemas, que abarca datos financieros de los empleados de la institución y de las instituciones educativas que son parte de la agrupación a nivel nacional.

La agrupación no cuenta con un área que gestione, monitoree y determine acciones adecuadas para mantener la seguridad y privacidad de la información, así como también no cuenta con programas formativos de seguridad para sus empleados en políticas y buenas prácticas de manejo de información.

Es por esta razón es importante diseñar un Sistema de Gestión de Seguridad de la Información (SGSI) el cual se basa en la norma ISO27001, que establezca un proceso ordenado para la protección ante las amenazas que podrían llegar a afectar la confidencialidad, integridad o disponibilidad de la información, para minimizar y optimizando los riesgos informáticos en la Agrupación Marista del Ecuador.

Para el diseño de un SGSI es importante conocer el estado actual en temas de seguridad de la información, por lo que se realizó un diagnóstico a través de una auditoría tomando como marco de referencia los controles de la ISO 27001. Para realizar esta evaluación se realiza un análisis de brechas GAP, este método permite evaluar el nivel de cumplimiento de los controles de la norma ISO 27001.

Con los resultados obtenidos en la evaluación se puede conocer cuál es el grado de implantación de la norma, la brecha que actualmente existe y se puede establecer el punto de partida para la propuesta de creación del SGSI.

La agrupación Marista del Ecuador cumple parcialmente con el 14% de los controles, es decir 2 de los 14 dominios de la norma ISO 27001, estos controles corresponden a la Seguridad con las telecomunicaciones y relación con proveedores. Mientras que con el 86% de los controles no cumplen con los requisitos de la norma.

Introducción

La Agrupación Marista del Ecuador es una organización que tiene como misión contribuir a la formación espiritual, emocional y física de los niños, niñas, adolescentes y del recurso humano; por lo tanto, es necesario implementar herramientas y estrategias que permitan proteger la información y los sistemas, que abarca datos financieros, de los empleados de la institución y de las instituciones educativas que son parte de la agrupación a nivel nacional.

Se propone establecer un SGSI, en el que se determinen los lineamientos y controles necesarios que permitan a la organización identificar sus activos de información críticos, los riesgos de seguridad asociados a estos y por ende la protección adecuada que ayude a mantener la confidencialidad, disponibilidad e integridad de los datos.

El análisis que dé como resultado el estado actual de la seguridad de la información para procesos críticos de la agrupación Marista del Ecuador, permitirá definir una serie de recomendaciones de acuerdo a las necesidades de la organización, tomando como marco de referencia la norma internacional ISO27001.

El proponer un SGSI apoyará a mantener la confidencialidad, disponibilidad e integridad de la información, frente al avance tecnológico actual que incrementa los riesgos informáticos que afectan a los activos de información de la Agrupación Marista del Ecuador.

A través de la propuesta de un SGSI mejorará la gestión de los riesgos informáticos que atenten contra con confidencialidad, disponibilidad e integridad de los activos de información.

En la actualidad las empresas utilizas plataformas tecnológicas para la prestación de servicios, esto hace que sea necesario la pronta detección de amenazas

que puedan afectar al normal desarrollo de las operaciones y procesos. Adicional el avance acelerado de la tecnología y la variedad de herramientas informáticas disponibles que facilitan el acceso fraudulento, producen todo tipo de amenazas a los sistemas de información aumentando la brecha de los controles.

La organización no cuenta con el control suficiente para dar cumplimiento a los controles establecidos en la norma ISO27001, incrementando el riesgo en los activos de información. Por lo tanto, el diseño de un SGSI basado en esta norma proveerá un enfoque sistemático que permitirá establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información, con el fin de alcanzar los objetivos estratégicos.

Un SGSI permitirá a la organización contar con un gobierno de seguridad alineado a las necesidades y objetivos estratégicos, conformado por una estructura organizacional con roles y responsabilidades y un conjunto coherente de políticas, procesos y procedimientos con el objetivo de promover y extender una cultura de seguridad, permitiendo fortalecer integralmente a cada uno de sus colaboradores.

Las medidas de seguridad de la información que se implementen en la organización apoyarán no solo al cumplimiento de los objetivos establecidos, sino también a los cumplimientos regulatorios que se establecen en la nueva norma de protección de datos personales aprobada por la asamblea nacional del Ecuador.

La teórica del proceso abordando fundamentos, normas y modelos referenciales, así como, su alcance y diseño para la gestión de la seguridad de la información, que nos ayuden a la interpretación adecuada de los resultados en el presente trabajo de investigación. Cada uno de ellos son activos de información que son necesarios para los objetivos que se quiere alcanzar como empresa u organización.

Las gerencias de las organizaciones buscan estrategias adecuadas para reducir el nivel de exposición de los activos de información, con medidas factibles en coste/eficacia considerando las ya existentes. El objetivo era proporcionar a cualquier empresa -británica o no- un conjunto de buenas prácticas para la gestión de la seguridad de su información (iso27000.es, 2022).

Con el propósito mejorar la competitividad, las organizaciones están más enfocadas en el proceso que permite obtener conocimiento, para incrementar la eficiencia de las operaciones de la empresa, incorporando principios corporativos asociados a su cadena de valor sistémica, garantizando la disponibilidad de recursos y el cumplimiento de sus indicadores de logro.

Los métodos que incorporan el desarrollo tecnológico y la congruencia organizacional, llevando a cabo procesos de creación, transformación, entrega de valor a clientes y consumidores; los esfuerzos que las empresas realicen para agregar valor a sus productos o servicios.

La tecnología es un medio que incrementa las oportunidades para el desarrollo a través del conocimiento, con el objetivo de alcanzar una administración competitiva para la empresa. Las innovaciones y los cambios tecnológicos son necesarios para el desarrollo y mejoramiento de la producción, sistemas de gestión, estructuras, planes o programas para los miembros de la empresa.

La Información en una organización o empresa es el activo más importante, por esta razón es necesario mantener un sistema sólido para administrarla y protegerla. Un sistema de información (SI) es un conjunto de procesos ordenados que tiene como fin la administración de los datos y de información, para que de esta manera sea posible recuperarlos y sean procesados de manera fácil y rápida. Las empresas se enfrentan a la transformación digital sin un proceso adecuado que dé garantías para

digitalizar sus archivos y automatizar las tareas mediante nuevos sistemas. Estos cambios para ordenar más y mejor su información, volcando toda en la red, provoca que estemos más vulnerables a los ciberataques y cualquier otro tipo de amenaza digital.

Los cibercriminales en el mundo hiperconectado actual se han convertido en un problema, por lo que es necesario que todas las empresas cuenten con un plan estratégico de ciberseguridad para de esta manera evitar al máximo posibles ataques. Las empresas deben conocer las actividades que se están produciendo en su red informática, para detectar movimientos sospechosos realizados por los ciberdelincuentes.

Es necesario contar con un plan adecuado de ciberseguridad en las empresas, pues los ataques virtuales pueden llegar a ser catastróficos como un robo o un incendio. Para tener esta seguridad es necesario mantener tecnologías de hardware y software que este orientada a diversas amenazas, evitando que ingresen o se multiplique en la red.

Un SGSI desde la visión del estándar internacional ISO/IEC 27001 es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización y lograr sus objetivos comerciales y/o de servicio. Hablar de un SGSI es respetar parámetros, que ligados al estándar internacional ISO/IEC 27001, permitirá proporcionar en una organización buenas prácticas para la gestión de la seguridad de su información almacenada y procesada, que a su vez está expuesta ante amenazas de ataque, riesgos y vulnerabilidades que abren brechas de seguridad que ponen en peligro los activos de información de la organización.

El avance tecnológico genera preocupaciones y por ende altos desafíos para garantizar un nivel máximo de disponibilidad, integridad y confidencialidad de la información manejada diariamente, este es un aspecto de gran importancia que se tiene en cuenta dentro de las labores empresariales. Es por esta razón que es importante la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) el cual está establecido sobre la norma ISO27001, que establece un proceso ordenado para la protección ante las amenazas que podrían llegar a afectar la confidencialidad, integridad o disponibilidad de la información.

Las mejores prácticas aplicadas de manera adecuada o correcta proporcionan una mejora continua y apropiada para evaluar los riesgos y establecer controles, mejorando la protección del activo más valioso dentro de la organización, la información. Para las empresas u organizaciones es importante certificar bajo la norma ISO 27001 de su Sistema de Seguridad de la Información, ya que sus beneficios aportan.

En definitiva, es beneficioso el mantener un SGSI basado en la ISO 27001, para reducir las probabilidades de que ocurran incidentes que afecten a la información que maneja la empresa u organización. En qué nivel de cumplimiento y controles se encuentra la empresa u organización es lo que nos indica el análisis de brechas en ISO 27001, informando sobre los problemas que se pueda presentar.

Es importante realizar la evaluación de riesgos, ya que sin ella no se podría dar por completo el análisis de brechas que es necesario para escribir la declaración de aplicabilidad.

El análisis de brechas GAP es un procedimiento que permite evaluar el rendimiento de los sistemas de información de una empresa u organización, de las aplicaciones que gestione para de esta manera determinar si cumple con los requisitos deseados

para el negocio, y de no cumplirlos determinar los pasos para garantizar que se cumplan con éxito.