Fortalecimiento de la ciberseguridad en una PYME mediante la aplicación de controles de la norma ISO 27001:2013

Barba Salazar Joel Alejandro

Guía: Hernández Roque

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: joelbarba18@outlook.com Guayaquil, marzo,2023.

Fortalecimiento de la ciberseguridad en una PYME mediante la aplicación de controles de la norma ISO 27001:2013

Introducción

En la actualidad, el activo más importante de las empresas es su información, debido a esto, es fundamental la implementación de controles de ciberseguridad que les permita asegurar la disponibilidad, confidencialidad e integridad de su información. Sin embargo, la mayoría de empresas esperan a pasar por eventos desfavorables para recién tomar decisiones correctivas en los procesos que realizan. Estas falencias tienen como resultado la aparición de crisis que pudieron ser perfectamente evitadas. (Peralta y Aguilar, 2021)

Por lo mencionado, surge la necesidad de que el personal a cargo del área de tecnología de una empresa esté capacitado en distintos contenidos sobre ciberseguridad. Una de las mejores opciones para cumplir esto es la preparación académica brindada en la maestría de ciberseguridad de la Universidad Casa Grande donde se brinda conocimiento normativo, teórico y práctico sobre ciberseguridad. El conocimiento aprendido por los estudiantes les permite implementar una variedad de proyectos de ciberseguridad en sus lugares de trabajo o de manera independiente.

El presente proyecto está basado en el conocimiento aprendido en cinco materias de la maestría de ciberseguridad. Como conocimiento teórico y normativo se incluye tres materias: "Gerencia, Operación y Planificación de la ciberseguridad", "Estrategias y Políticas Multilaterales para la Ciberseguridad" y "Continuidad de Negocio", mientras que como conocimiento práctico se incluye dos materias: "Tecnología, Modelos y Técnicas de Ciberseguridad" y "Hacking Ético y Análisis del Ciberataque".

El objetivo del proyecto es fortalecer la ciberseguridad en una PYME mediante la implementación de controles de la norma ISO 27001, estos controles se enfocarán en

dos frentes: el desarrollo de políticas de seguridad de información y la implementación de herramientas de seguridad. Se eligió esta normativa ya que nos muestra cómo adoptar estándares de seguridad de la información, construyendo una cultura de seguridad y continuidad del negocio. (Martínez, 2019)

Desarrollo

A continuación, se resumen los conocimientos impartidos en cada una de las materias mencionadas que son usados para el desarrollo del presente proyecto.

Gerencia, Operación y Planificación de la Ciberseguridad

Esta materia se enfocó en un concepto: el riesgo, el cual se define como la posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información (Santiago y Sánchez, 2017, p. 9). A través de las clases esta asignatura muestra cómo identificar los riesgos asociados a los procesos en una organización, así como implementar controles de la norma ISO 27001 para mitigar el nivel del riesgo.

A través de casos reales de ciberataques que tuvieron éxito durante la pandemia se analizó la importancia de la implementación de controles para mitigar los riesgos. Como conclusión de este análisis se obtuvo que la aplicación de controles internos brinda a la empresa una protección a su información y la disminución de la posibilidad de que un ataque informático tenga éxito. Se resaltó que el éxito de un ciberataque puede ocasionar grandes pérdidas económicas y la interrupción indefinida de las operaciones de la organización.

Estrategias y Políticas Multilaterales para la Ciberseguridad

Esta materia se orientó en la importancia de que los controles que se implementen en una empresa estén diversificados entre las diferentes aristas de la seguridad integrada, sin embargo, se resaltó lo fundamental que es abordar el eslabón

más débil: la cultura de ciberseguridad. Es todo un reto conseguir que el colaborador esté plenamente identificado con acciones para la protección de los datos de la organización, pero se puede lograr a través de la sensibilización, la capacitación, divulgación y mejora continua (Bustillos y Rojas, 2022, p. 178).

Como proyecto final de esta materia se procedió a dar sesión a un comité de administración de seguridad de información en la cual se mostró a los estudiantes de qué forma conseguir la aprobación de los directivos de una empresa para implementar controles de ciberseguridad.

Continuidad de Negocio

Esta asignatura se basó en cómo elaborar un plan de continuidad de negocio y los beneficios que brindan a las empresas de tenerlo. Se destaca que un plan de continuidad del negocio es principalmente operativo y debe contemplar todas las medidas preventivas y acciones necesarias para mantener la operatividad de la organización a un nivel mínimo aceptable durante una contingencia. (Oneto,2020)

A través de la práctica se observó que la implementación de controles de seguridad y de buenas prácticas aumentan las posibilidades de recuperarse ante un desastre. Uno de los controles más importantes es el respaldo de la información, por lo que es vital que se hagan respaldos periódicos de la información de la organización tanto físicamente como en la nube. Esto está directamente relacionado a un término visto en clase el cual es el RPO (Recovery Point Objective) el cual es el rango de tolerancia que la entidad puede tener sobre la pérdida de sus datos.

Tecnología, Modelos y Técnicas de Ciberseguridad

En esta materia se impartieron conocimientos muy importantes sobre la informática enfocados en la ciberseguridad. Se estableció que la ciberseguridad es un conjunto de procesos y tecnologías diseñadas con el objetivo de proteger programas,

ordenadores, redes de comunicación y también datos ante ataques, y/o accesos no autorizados, asegurando de esta manera la confidencialidad, integridad y disponibilidad de los sistemas (Jove et. al, 2021).

Habiendo conocido la parte teórica se procedió a entrar a la parte más técnica de la ciberseguridad en la cual se repasó los conceptos básicos de las tecnologías de red (Switch, IP, Máscara de Red, Gateway, Puertos, Protocolos, DNS, etc.). Repasar los conocimientos esenciales del área sirve de antecedente para conocer las diversas técnicas de seguridad de red que se implementan actualmente en las empresas. Entre las técnicas vistas resaltan las siguientes: Segmentación de red, Firewalls, Sistemas IDS e IPS, Honeypots, Servidores proxy y VPNs.

Hacking Ético y Análisis del Ciberataque

El hacking ético se define como la rama de la seguridad tecnológica dirigida a prevenir, erradicar, estabilizar y contraatacar vulnerabilidades de software o de hardware (Rodríguez, 2020). Debido a esto el hacking ético se presenta como una herramienta muy útil para que las empresas puedan detectar vulnerabilidades en sus sistemas informáticos y corregirlas a tiempo antes de recibir un ciberataque.

Finalmente, en esta materia se realizaron diversas prácticas sobre hacking en la cual los estudiantes pueden observar lo vulnerables que son los sistemas de las empresas y lo fácil que es para un ciber atacante realizar un ataque, de esta forma se concientiza de la importancia de mantener a los sistemas seguros y actualizados, así como de tener buenas prácticas de seguridad informática. Es fundamental que las empresas no tengan una postura reactiva en la seguridad informática, sino una postura preventiva, es decir no esperar a sufrir un ciberataque para comenzar a implementar los controles.

Implementación

El presente proyecto utilizará como base los conocimientos aprendidos durante la maestría y consiste en tres fases: La primera fase se centrará en la creación de una matriz de riesgos, para esto se procederá a identificar riesgos que afecten a la seguridad de la información de la PYME, luego de identificarlos se procederá a calcular el nivel del riesgo inherente. El siguiente paso será elegir controles que permitan mitigar los riesgos y con esto disminuir el nivel del riesgo residual, estos controles serán elegidos de la norma ISO 27001:2013 en su Anexo A.

La segunda fase se orientará a la implementación de los controles elegidos, estos controles se dividirán en dos tipos. El primer tipo de control serán herramientas de seguridad que se aplicarán en la PYME (Ej. Firewall, Antivirus, IPS, etc.), mientras que el segundo tipo de control se centrará en la elaboración de políticas de seguridad de información.

Finalmente la tercera fase consistirá en la socialización de la matriz de riesgos desarrollada, así como de los controles implementados, la socialización será dirigida a los directivos de la organización y a los jefes de los departamentos. Con la implementación de controles de seguridad se busca fortalecer la ciberseguridad de la PYME y con esto asegurar la confidencialidad, integridad y disponibilidad de la información.

Conclusiones

La implementación de controles de la norma ISO 27001 le brinda a las PYMES una línea de defensa vital contra los ciberatacantes, sin embargo, la tendencia de las organizaciones es de tener un comportamiento reactivo y no preventivo. Debido a esto es muy importante que las empresas concienticen sobre el establecimiento de la ciberseguridad como una prioridad, teniendo como pilares los siguientes aspectos:

- Es vital que el personal encargado de un departamento de tecnología o de seguridad de información conozca ampliamente sobre ciberseguridad ya que de esta forma podrá implementar las herramientas y estrategias necesarias para defender la información e infraestructura de las empresas de un ciberataque.
- Es importante que los directivos de una empresa, ya sea una PYME o una transnacional, conozcan de la importancia de implementar medidas de ciberseguridad en sus empresas, lo cual les permitirá recuperarse de una crisis o un desastre dándole ventaja competitiva en el mercado.
- La implementación de controles de la norma ISO 27001 permite fortalecer el nivel de ciberseguridad de las empresas por lo que es fundamental que las PYMES implementen todos los controles que estén dentro de sus posibilidades.

Limitaciones

La implementación de controles de ciberseguridad en las empresas hace un gran uso de recursos económicos y humanos, por lo que el fortalecimiento de ciberseguridad en PYMES presenta las siguientes limitaciones:

- Debido a que se desarrolló el proyecto sobre una PYME, no se tuvo un presupuesto muy elevado para la ciberseguridad, por lo cual gran parte de los controles implementados fueron utilizando herramientas open source las cuales no son tan avanzadas y eficientes como las herramientas de pago.
- Debido al corto tiempo del proyecto se tuvo que descartar controles que llevan un gran tiempo para ser implementados los cuales también benefician a la PYME.

Recomendaciones

- Concientizar a los directivos de las empresas sobre ciberseguridad previo a la presentación de los proyectos, así como socializar de forma periódica sobre los avances de los proyectos con el objetivo de aumentar el compromiso de los directivos.
- Invertir los recursos necesarios para implementar un SGSI (Sistema de Gestión de Seguridad de la Información) utilizando la norma ISO 27001 y utilizar la norma ISO 27002 como guía de implementación de todos los controles.

Anexos

Anexo 1: **Evidencias de Aprendizaje**

https://rich-fenugreek-820.notion.site/Evidencias-de-aprendizaje-5acff984dcc34996a6a81c8d91e9d412

Anexo 2: **Propuesta de Implementación**

https://rich-fenugreek-820.notion.site/Propuesta-de-implementaci-n-b9e9ca2aa0894c9eb6751815b32d91fc

Referencias

Bustillos Ortega, O., & Rojas Segura, J. (2022). Protocolo básico de ciberseguridad para pymes. Interfases, (016), 168-186. https://doi.org/10.26439/interfases2022.n016.6021

Jove, E., Calvo-Rolle, J. L., Urda, D., Herrero, Á., Zurutuza, U., & Casola, V. (2021). Avances recientes en la aplicación de la ciencia de datos a la ciberseguridad industrial. Revista DYNA, 96(3), 231-232.

Martínez, A. M. (2019). Importancia de la implementación de un sistema de gestión de seguridad de la información (SGSI) en las empresas bajo la ISO 27001. Recuperado de: http://hdl.handle.net/10654/34863.

Oneto, A. (2020) COVID-19: Continuidad del negocio, gestión de crisis y gobierno corporativo. Caracas: CAF. Retrieved from http://scioteca.caf.com/handle/123456789/1596

Peralta Zuñiga, M., & Aguilar Valarezo, D. (2021). La ciberseguridad y su concepción en las PYMES de Cuenca, Ecuador. Contabilidad Y Auditoría, (53), 99 - 126. Recuperado a partir de https://ojs.econ.uba.ar/index.php/Contyaudit/article/view/2061

Rodríguez, A. (2020). Herramientas fundamentales para el hacking ético. Revista Cubana de Informática Médica, 12(1), 116-131.

Santiago Chinchilla, E., & Sánchez Allende, J. (2017). Riesgos de ciberseguridad en las empresas. Tecnología y desarrollo, 15.