Implementación de Controles de Ciberseguridad recomendados por Estándares Internacionales ISO 27001 en una PYME

Vicente Gregorio Quiñónez Vera

Guía: Roque Hernández Bustos

Presentado como parte de los requisitos para el Título de Magíster en Ciberseguridad.

CES: RPC-SE-01-N°.014-2020. Cohorte 2022 - 2023.

Correo electrónico del autor: vicente.quinonez@casagrande.edu.ec

Guayaquil, 03/03/2023

Implementación de Controles de Ciberseguridad recomendados por Estándares Internacionales ISO 27001 en una PYME

Una de las más grandes motivaciones del Maestrante de este ensayo para ingresar a la Maestría de Ciberseguridad fue justamente el poder aprender las mejores recomendaciones y técnicas que pudieran ayudarlo a crecer profesionalmente, además de poner en práctica todo lo aprendido en su lugar de trabajo.

Es un verdadero reto hoy en día estar preparado para enfrentarse a los grandes desafíos que se presentan en el área de TI de las empresas, debido a la gran proliferación de atacantes y el desarrollo continuo de la economía de la ciberdelincuencia. Quienes buscan lucrarse extorsionando por rescates de información (ransomware) u ofreciendo servicios especializados en el uso de exploits para dar acceso a redes privadas a cualquier delincuente que esté dispuesto a pagar por estos servicios. (Sophos Ltd., 2023)**.**

La Maestría en Ciberseguridad ha ayudado mucho en el crecimiento que el maestrante buscaba y en ser el punto de partida para adentrarse aún más en las diferentes opciones que existen dentro de este maravilloso mundo de la ciberseguridad.

Este proyecto de titulación está enfocado en la implementación de controles de ciberseguridad recomendados por estándares Internacionales (ISO 27001) para el área de TI de una PYME, y así salvaguardar el bien más valioso de toda organización que es su información. Algo que también es de vital importancia es la correcta identificación y valoración previa de los riesgos de ciberseguridad en la organización. Esta valoración debe ser la base para luego empezar a adoptar los controles. Para esto las materias que jugaron un papel muy importante fueron **Gerencia, Operación y Planificación de la Ciberseguridad**, que fue el punto de partida en la carrera y la base para una correcta

identificación de los riesgos del área. La materia **Tecnología, Modelos y Técnicas de Ciberseguridad** para reforzar lo aprendido anteriormente en pregrado en cuanto a redes y las técnicas para su securización. Otra materia muy importante fue **Estrategias y Políticas Multilaterales para la Ciberseguridad** porque muchas veces se piensa que la responsabilidad del departamento de TI de las organizaciones debe recaer solo sobre el encargado de esa área. Debido a los grandes desafíos que existen actualmente esta responsabilidad debe ser compartida para poder enfrentarlos en un Comité de Administración de Seguridad de la Información y ahí establecer en conjunto un Plan Estratégico de Seguridad de Información.

Finalmente, pero no en menor importancia tenemos a las materias **Seguridad de Aplicaciones y Bases de Datos** y **Hacking Ético y Análisis del Ciberataque**, con cada una de ellas, se lograron tomar estrategias necesarias que hacían falta en el Departamento de TI de la PYME y estas estrategias se expandirán en la sección de Implementación.

Desarrollo

Gerencia, Operación y Planificación de la Ciberseguridad, fue el punto de partida para saber qué se necesita mejorar en las políticas y procedimientos del área. Antes de implementar esas mejoras debe existir una planificación del área, empezando por un análisis completo de los riesgos y el tratamiento que se debe darles. Otro concepto importante es cómo se implementa para este aspecto el uso de estándares internacionales para una correcta adopción de controles que ayuden a que los riesgos sean gestionados adecuadamente (ICONTEC, 2013). Además, como el establecer políticas y procedimientos claros, logra que el área de TI pueda contribuir a "generar valor al negocio con las inversiones de TI" (ISACA, 2012).

Tecnología, Modelos y Técnicas de Ciberseguridad, reforzó lo que normalmente se aprende en una carrera de Telemática en el tema de redes y su importancia para la seguridad de los sistemas de información. También se analizaron las tecnologías y técnicas de ciberseguridad. Se revisó un tema de mucha consideración como es la criptografía. Este concepto se utiliza para asegurar que la información no pueda ser accesible por terceros no autorizados, mediante un criptoanálisis que "consiste en comprometer la seguridad de un criptosistema" (López, 2021)

Estrategias y Políticas Multilaterales para la Ciberseguridad, enseñó como la definición correcta de estrategias mediante un Comité de Administración de Seguridad de la Información ayuda a la prevención de ciberataques. Adicionalmente se analizó cómo se deben definir políticas, procedimientos y campañas de concientización para una correcta cultura organizacional en ciberseguridad. Este comité en algunos

casos, es de cumplimiento normativo obligatorio por los entes de control gubernamentales.

Uno de ellos es el MINTEL que menciona en su Política de Ciberseguridad: “La política establece directrices que buscan afianzar un ciberespacio seguro para contribuir al desarrollo social, económico y humano del país” (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2021, 17 de Mayo)

Seguridad de Aplicaciones y Bases de Datos, afianzó aún más el tema de una Matriz de Riesgos, incluyendo la categorización, el tipo de control y si es de requerimiento regulatorio o no. El uso de Inteligencia de Amenazas a los sistemas para comprobar que tan eficiente son los controles empleados y la definición de una superficie de ataque e indicadores de compromiso (IOCS) que ayudan a gestionar de una manera correcta la seguridad de las aplicaciones. Finalmente se aprendió en esta materia la Matrix Mitre Att&ck que contiene técnicas y tácticas que pueden usar los atacantes para vulnerar los sistemas de las organizaciones. (MITRE Corporation, 2015-2022)

Hacking Ético y Análisis del Ciberataque, fue la materia que permitió conocer de primera mano cómo se desarrolla un ciberataque, las “más grandes amenazas digitales” a las que estamos expuestos (Eidam, 2021). Las técnicas y herramientas que usan los hackers para llevar a cabo sus incursiones y las repercusiones que pueden tener en una organización al no tener identificadas y controladas esas amenazas. Con la ayuda de esta materia se logró poner en práctica lo aprendido para evaluar si los nuevos controles implementados en la organización están cumpliendo o no y si es necesario mejorarlos.

Implementación

Dentro de la PYME sobre la cual se basa este ensayo, existe un Departamento de TI constituido por el jefe del departamento y dos analistas, uno en la ciudad matriz que es Guayaquil y otro en Quito.

El Departamento de TI cuenta con una Política del área, varias guías o instructivos de los procesos que se efectúan y un Plan de Contingencia Informático, toda esta documentación está clasificada y ordenada en un árbol de Gestión ISO 9001:2015.

Como parte de la Implementación lo primero que se consideró fue lo aprendido en la Materia de **Gerencia, Operación y Planificación de la Ciberseguridad** que fue la identificación de los riesgos de la organización y su adecuada clasificación por el apetito de riesgo establecido por la organización, es así que se creó el documento ESPN G.SIS 12 MATRIZ DE EVALUACIÓN DE RIESGOS Y MEDIDAS DE CONTROL, donde se analizaron todos los riesgos del área y la creación de sus controles en caso de no existir, con la ayuda de la ISO 27001.

Después de tener definido los riesgos y controles, lo siguiente que se realizó fue la revisión de las Políticas del Departamento definidas en el documento ESPN N.SIS 01 POLÍTICAS INFORMÁTICAS EESACI, aquí se pudo determinar que muchas de las políticas definidas en el documento ya no se ajustaban a las recomendaciones actuales en Gestión de la Seguridad de la Información y se realizaron todas las actualizaciones sugeridas. Estas recomendaciones pueden ser apreciadas a mayor detalle en la propuesta de implementación.

Junto con la revisión de las Políticas y con los conocimientos adquiridos de la materia **Tecnología, Modelos y Técnicas de Ciberseguridad** se aplicaron cambios a la red de la empresa, se definieron controles de seguridad a los switches administrables de

la organización, se etiquetó nuevamente el cableado que ya no se veían las etiquetas anteriores y se presentó una propuesta de una herramienta SIEM (Security Information and Event Management) o de un SOC (Security Operation Center) gestionada por un proveedor de Seguridad Informático y está todavía en análisis de la Gerencia ya que no se ha definido los presupuestos de las áreas. Por el momento se implementó una herramienta open source Wazuh, que ha resultado muy eficiente para la supervisión de equipos en las dimensiones de una PYME y se dejó definido dentro de las políticas informáticas el uso de esta herramienta.

Gracias a la información adquirida en la materia de **Estrategias y Políticas Multilaterales para la Ciberseguridad** se revisaron nuevamente las políticas informáticas del área anteriormente definidas y ver si faltaba alguna que sea de cumplimiento regulatorio y no haya sido definida, es así que se elaboró el documento FOR G.SIS 02 PLAN ANUAL DE CONCIENTIZACIÓN EN CIBERSEGURIDAD. En este documento se definen las campañas de prevención de ciberseguridad que serán impartidas a los empleados de la organización durante todo el año y que pueden ser sujetas a evaluaciones posteriores para comprobar su eficacia.

Una parte muy importante y que además es de cumplimiento regulatorio y que debe estar correctamente definida en las organizaciones es la identificación de sus Activos de Información, es por esto que se creó el documento ESP G.SIS 13 ACTIVOS DE SEGURIDAD DE INFORMACIÓN que es la matriz que contiene esta información y que fue realizado mediante entrevista a los empleados claves de cada departamento de la organización y posteriormente aprobado por la Gerencia.

Como parte final de este proyecto y con la ayuda de las materias **Seguridad de Aplicaciones y Bases de Datos** y **Hacking Ético y Análisis del Ciberataque** se realizaron valiosas revisiones a los controles antes implementados en la organización.

Primero se revisó la matriz MITRE para ver las técnicas que pueden usar los atacantes para tratar de ingresar a la red y con el uso de una de las herramientas vistas, Metasploit, se realizaron varias técnicas para tratar de explotar esos activos y parte de los resultados de los mismos están dentro de la propuesta de Implementación.

Conclusiones

En la implementación de todos estos controles para proteger a la organización se encontraron muchos desafíos, por una parte, la falta de presupuesto que fue informada a la Gerencia de la Organización. Hay cambios importantes que se deben realizar como la segmentación de redes, el uso de equipos centralizados para Wifi y la renovación de varios equipos obsoletos que pueden ser una brecha de seguridad en todo lo implementado. Otro gran desafío fue la falta de apoyo de varias personas de la organización, que no le dan la debida importancia al respecto. Contra todo eso se lograron hacer muchos cambios y sobre todo ejecutar controles que ya fueron definidos en un estándar y que están probados internacionalmente. Es importante señalar que todo este esfuerzo no sirve de nada, si la Alta Directiva no supervisa y sanciona por incumplimiento de las nuevas políticas establecidas en la organización y si no están en constante revisión y actualización estos controles.

El trabajo inicial está hecho, pero depende de todos en la organización que permanezcan funcionando en el tiempo y adaptándose a las nuevas amenazas que puedan aparecer.

Limitaciones

Dentro de las limitaciones como se dijo anteriormente fue la falta de apoyo del personal de la organización, no brindaban la información que se les solicitaba, o faltaban a las reuniones con sus áreas de trabajo, indicando que no tenían tiempo y la Gerencia no daba el apoyo necesario para que cumplan, esto impedía el realizar un levantamiento correcto de la información, para posteriormente sugerir los controles adecuados.

La obsolescencia de la infraestructura tecnológica es un componente a tener en cuenta, ya que de nada nos sirve poner controles eficientes, si los equipos informáticos

pierden por ejemplo el soporte tecnológico del fabricante y quedan expuestos a nuevos ataques que se mitigaría si tuvieran sus actualizaciones.

Recomendaciones

Exponer a la alta directiva la importancia de tener en la organización una cultura en ciberseguridad, que conozcan de las amenazas actuales y futuras, de las pérdidas económicas que pueden llegar a tener en caso de un incidente y de las regulaciones que se deben cumplir en materia de ciberseguridad.

Establecer el Comité de Administración de Seguridad de la Información en la organización, esto hubiera permitido que toda la organización se involucre de manera más eficiente, ya que se cuenta con el apoyo de la alta dirección desde el inicio, ya que forma parte de este comité.

Tener definido un presupuesto anual del área para poder invertir en las herramientas tecnológicas necesarias para el correcto funcionamiento de los controles implementados.

Referencias

Eidam, B. (2021). *The 116 Best Cybersecurity Tools & Tactics.*

ICONTEC. (2013). *Norma Técnica Colombiana NTC-ISO-IEC 27001* . Bogotá: Instituto Colombiano de Normas Técnicas y Certificación .

ISACA. (2012). *Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa.* Madrid.

López, M. J. (2021). *Criptografía y Seguridad en Computadores.* CC-BY NC SA / 2021.

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2021, 17 de Mayo). *Acuerdo-No.-006-2021-Politica-de-Ciberseguridad.* Obtenido de https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Acuerdo-No.-006-2021-Politica-de-Ciberseguridad.pdf

MITRE Corporation. (2015-2022). *MITRE ATT&CK*. Obtenido de https://attack.mitre.org/matrices/enterprise/

Sophos Ltd. (2023). *Informe de Sophos sobre amenazas 2023.* Inglaterra.

Glosario de Términos

TI: Tecnologías de la Información

Hacker: Persona con grandes conocimientos en informática que se dedica a detectar fallos de seguridad en sistemas informáticos.

Securización: Hecho de dotar de la seguridad necesaria a algo, de hacerlo seguro o protegerlo con los medios pertinentes.

Ciberseguridad: Es la práctica de proteger tu información digital, dispositivos o activos de información.

Ciberdelincuencia: es una actividad delictiva que tiene como objetivo principal un ordenador, una red asociada a este o un dispositivo conectado.

Criptografía: Técnica de escribir con procedimientos o claves secretas, de tal forma que el escrito solamente sea inteligible para quien sepa cómo descifrarlo.

Criptoanálisis: Es una parte de la criptología que se dedica al estudio de los sistemas criptográficos con el fin de encontrar sus debilidades y romper su seguridad sin el conocimiento de la clave secreta.

Ransomware: Es un ataque mediante un código malicioso que causa daños en los datos críticos de una organización, los cifra con un cifrado de alta seguridad, que no se puede deshacer e impide el acceso a ellos.

Exploits: es cualquier ataque que aprovecha las vulnerabilidades de las aplicaciones, las redes, los sistemas operativos o el hardware.

Anexo 1

Evidencias de Aprendizaje

https://band-booth-990.notion.site/67033e23060d4bfaa600efb310245c26?v=ad95996f2d634e3b89da8e0c4627db84

Anexo 2

Propuesta de Implementación

https://www.notion.so/Propuesta-de-Implementaci-n-2c3861f79f1f4b8eb366dc4e48555a5e?pvs=4