Implementación de un SGSI en una empresa del sector exportador de camarón del cantón Durán

Wimper Fernando Cifuentes Moreira

Guía: Roque Hernández Bustos

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: cifuentesm.fernando@outlook.com

Guayaquil, 4 marzo del 2023

Introducción

En la actualidad los ataques informáticos se han convertido en actividades continuamente ejecutadas por agentes externos o internos a nivel mundial, en cualquier tipo de negocio o empresa. En muchos de estos casos los atacantes en sus diferentes vectores de ataque piden diferentes formas de rescates.

Este proyecto de titulación tiene como objetivo la implementación de un SGSI en una empresa del Sector Exportador de Camarón en el cantón Durán. En la actualidad, los ataques informáticos pueden ser orientados a cualquier tipo de organización, por lo que las mismas deben estar preparadas para poder responder en el caso de un ataque y así proteger sus activos de información.

Ecuador no se aísla de estos tipos de ataques informáticos, ya que en otros tipos de negocios se han presentado ocasionando malestar interno en la organización, a los usuarios y problemas reputacionales.

La competitividad empresarial exige a las organizaciones, que la información esté disponible en el momento que se la requiera, manteniendo su integridad y confidencialidad.

Para esta implementación se apoyó en las asignaturas de Seguridad de Base de datos y Aplicaciones Web, Estrategias y Políticas Multilaterales, Hacking Ético y Análisis de Ciberataques, Continuidad del Negocio y Ciberseguridad Industrial porque brindan un gran aporte en este proceso.

Desarrollo

Seguridad de Aplicaciones web y bases de datos

En esta asignatura se realizaron pruebas de diferentes ataques y se establecieron qué tipos de consideraciones debemos tener para evitarlos. En la actualidad, la gran mayoría de empresas ofrecen servicios tecnológicos. Dentro de estos servicios se encuentran las aplicaciones web siendo una de las más importantes porque permiten una fácil comunicación e interacción del usuario con la organización y en ellas puede realizar diferentes tipos de transacciones ya sean: compras, ventas, etc.

Es importante que las organizaciones realicen pruebas de seguridad en sus aplicaciones web para evitar que los servicios tecnológicos se vean afectados, ocasionando así molestias a los usuarios de estos servicios.

Las bases de datos son un recurso esencial dentro de la diversidad de recursos tecnológicos que poseen las organizaciones. Por su importancia se deben establecer planes de respaldos, pruebas y recuperación en casos de incidentes.

Por otro lado, para el desarrollo de software seguro existen lineamientos de buenas prácticas llamado OWASP, las cuales nos ayudan a mejorar la calidad de software, y de esta manera minimizar o mitigar el riesgo de seguridad en las aplicaciones.

Para evaluar la calidad de software se utilizó la herramienta SonarQube, la cual nos brinda reportes del estado del código fuente y poder tomar decisiones de cambios o realizar mejoras al desarrollo de software.

Estrategias y políticas multilaterales

Esta asignatura permitió definir estrategias para implementar medios de prevención de ciberataques, enfocándose en políticas, procedimientos, cultura, normativas y el seguimiento para el control adecuado y la ejecución de las estrategias.

Adicionalmente, existen normativas internacionales que nos ayudan a establecer políticas y procedimientos basados en las mejores prácticas para la seguridad de la información como lo es la ISO 27001. Este estándar internacional se puede aplicar a cualquier tipo de institución ya sea pública o privada y así garantizar la seguridad de la información (ISO 27001:2013, 2015).

Enfocándonos en el ámbito nacional, en Ecuador existen entes reguladores especializados en normativas para el control de la ciberseguridad entre ellos: el Ministerio de Telecomunicaciones y de la Sociedad de la Información y la Superintendencia de Bancos. Estos tienen como objetivo establecer lineamientos que nos ayudan a tener un ciberespacio seguro y de esta manera contribuir al desarrollo del país; ya que, se puede crear un ecosistema confiable de seguridad digital para el intercambio de información y poder generar transacciones de bienes y servicios online (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2021).

Ante esta iniciativa, también se agrega la Ley Orgánica de Protección de Datos Personales que fue enviada mediante la Asamblea Nacional del Ecuador en mayo del 2021 para el Registro Oficial. La cual se establece que sea ejecutada en todo tipo de institución pública y privada (Asamblea Nacional del Ecuador, 2021).

Ciberseguridad en entornos industriales

Por la diversidad de dispositivos y programas computacionales que forman parte del proceso de control y automatización industrial, estos necesitan compartir o intercambiar su información. Para estas actividades se han desarrollado diversos medios, métodos y protocolos de comunicación.

La industria en su proceso de evolución no se queda atrás, actualmente se habla de la Industria 4.0. En estos, los dispositivos cada vez reducen su tamaño, son más inteligentes, con gran capacidad de almacenamiento de datos, así como su procesamiento y con la capacidad de conectarse a la red (Joyanes Aguilar, 2018).

La industria en la actualidad es vulnerable basado en dos tipos de amenazas informáticas, la primera es la relacionada a la tecnología de la información TI. Siendo esta una de las más atacadas, comprometiendo los equipos de cómputo con el objetivo de robos o perdida de datos. La segunda es la Tecnología Operacional (TO), la cual se relaciona con los sistemas de control y producción (Ayerbe, 2019).

Ciberseguridad Industrial está dentro del entorno de la Seguridad Industrial, debido a que generan gran cantidad de datos y su procesamiento nos da como resultado información valiosa, esta información debe ser protegida de ataques mediante medios tecnológicos. Los métodos orientados a mitigar las amenazas deben considerar que no pueden interrumpir la disponibilidad de las operaciones y los sistemas de control como son: (PLC,DCS,RTU, HMI, MES, etc), estos se comunican mediante protocolos establecidos como: (Modbus, Profibus, OPC, Ethernet/IP,DNP3, etc) (Centro de Ciberseguridad Industrial, 2014) .

Hacking Ético y Análisis de Ciberataque

Hacking tiene como actividad principal poder acceder desde cualquier sitio del ciberespacio hacia un equipo computacional privado, aprovechándose de la vulnerabilidad en los sistemas de seguridad y de esta manera obtener accesos privilegiados para hacerse pasar por usuarios legítimos (Sánchez Avila, 2019).

Hacking Ético es la definición asignada por los profesionales a una actividad de evaluación del estado actual de un sistema informático ya sea este software, redes e infraestructura tecnológica. El Hacker ético es un profesional de la informática que tiene como habilidades evaluar la seguridad de los sistemas informáticos e identificar sus vulnerabilidades y explotarlas en algunos casos para poder tomar las medidas preventivas y así poder reducir el riesgo a ataques o accesos no autorizados (Erickson, 2008).

Una vez ya establecido los conceptos de Hacking, Hacking Ético. Esta asignatura permitió identificar la diferencia entre seguridad de la información y seguridad informática. La seguridad de la información se enfoca en establecer técnicas de implementación para la protección de la información basado en normativas y buenas prácticas. Mediante el análisis de riesgos de las posibles amenazas que puedan afectar a las organizaciones, se establecen planes de acción para minimizar el riesgo y poder incrementar la confianza en el mantenimiento, almacenamiento, recuperación y uso de la información. La Seguridad de la Información tiene como objetivo principal garantizar la disponibilidad, integridad y confidencialidad de la información (Figueroa-Suárez et al., 2017). Seguridad Informática es la encargada de proteger las diferentes herramientas tecnológicas que comprenden un sistema informático en una organización, y de esta manera reducir los riesgos sobre los recursos informáticos para garantizar la continuidad de las operaciones (Romero Castro et al., 2018).

Podemos definir que la seguridad de la información está orientada a proteger los activos de información ya sean estos físicos o digitales, usando metodologías, técnicas, normas y herramientas, para poder tomar las medidas adecuadas en el tratamiento de la información. La seguridad de la información contiene a la seguridad informática. Pero la seguridad informática se orienta a proteger los sistemas informáticos los cuales procesan, almacenan los activos de información digitalmente sin importar que se encuentren interconectados.

Existen diferentes tipos de ciberatacantes que tienen como objetivo vulnerar las seguridades de las organizaciones o personas y obtener algún beneficio en esa actividad, entre ellos están: Black Hat, White Hat, Gray Hat, Crackers, Script Kiddies, Newbie, Lammer, Phreaker (Flores Quispe, 2018). En el análisis de ciberataques es importante conocer las etapas que se cumplen cuando se realiza el ataque, e identificar como pueden evolucionar para tomar las medidas preventivas o correctivas. Según (The Mitre Corporation, 2023) las etapas son: exploración, desarrollo de recursos, acceso inicial, ejecución, persistencia, escalada de privilegios, evasión de defensa, acceso a credenciales, descubrimiento, movimientos laterales, colección, comando y control, extra filtración e impacto.

Continuidad del negocio

La asignatura hace referencia a la importancia de implementar un plan de continuidad del negocio orientado a los objetivos de la organización, y de esta manera reducir el tiempo de interrupción de los servicios, los cuales pueden ser ocasionados por diferentes tipos de amenazas ya sean estos biológicas, meteorológicas, eventos accidentales, tecnológicos, geológicos para lograr que la organización retome sus actividades normales en el menor tiempo posible.

Como apoyo a la continuidad del negocio se establecen normativas de buenas prácticas que ayudan a mitigar el tiempo de interrupción llamados Sistemas de Gestión de la Continuidad del Negocio (SGNC), los cuales pueden ser adaptados a cualquier tipo de organización. Este sistema utiliza un modelo llamado PHVA (Planificar-Hacer-Verificar-Actuar) (ISO 22301:2019).

Se debe tener en cuenta que la continuidad del negocio es lo más importante para una eficiente gestión de riesgos, ya que los riesgos no se los puede eliminar sino minimizar, con esto la continuidad del negocio tiene como objetivo mitigar el riesgo lo máximo posible (Rodríguez Pinilla, 2017). Para la gestión de la continuidad del negocio hay que tener presente: El análisis de riesgo, análisis de impacto de negocio, plan de recuperación ante desastres, plan de continuidad de negocio, estrategia para crisis (Laserfiche, 2020).

Implementación

La organización dentro de su organigrama no tiene un área de Ciberseguridad, sólo posee el área de Sistemas, dentro de su estructura contiene un Gerente de Sistemas, un jefe de Software, un jefe de Infraestructura, equipo de programadores y el equipo de infraestructura.

Dentro de su arquitectura tecnológica mantienen una infraestructura híbrida, en su infraestructura on-premise poseen un Firewall encargado de recibir todo el tráfico de internet y realizar el filtrado mediante reglas para limitar los accesos de navegación al personal. Internamente tiene diferentes segmentos de redes, para personal administrativo, invitados, corporativos, telefonía ip, cámaras de video vigilancia.

Su arquitectura Cloud está soportada mediante la herramienta de Microsoft en la nube conocida como Azure, en esta plataforma la organización posee servidores virtuales, storage, portal web, sistema web, servicios de office 365 y su dominio.

Sus sistemas de información están en un proceso de migración tecnológica, un sistema legado en Visual Fox Pro hacia C# con SQL Server lo cual les está ayudando a mejorar los procesos y controles. Con este antecedente, esta organización puede ser blanco de ciberataques lo cual puede afectar gravemente a sus procesos y ser perjudicial para sus actividades normales. Se procedió a organizar una reunión para conformar el comité de Ciberseguridad, definir una persona encargada de Ciberseguridad y establecer políticas para la salida de empleados.

Como resultado del comité se designó a un responsable de Ciberseguridad y políticas para empleados cesantes de la organización. Dada la necesidad de reducir el riesgo a las amenazas, se realizó un análisis de riesgo inicial ya que no se ha desarrollado porque se estaba manejando en función a la experiencia, se procedió a realizar un documento identificando los riesgos tecnológicos posibles en la organización e identificar sus activos críticos.

Posterior a esto, se realizó la creación de políticas y procedimientos de sistemas que deben ser implementados y ejecutados en la organización, con el apoyo de los directivos para establecer sanciones en el caso de no aplicarlos.

Por la necesidad de tener un mejor análisis y seguimiento de las actividades en la infraestructura tecnológica se procede a realizar la implementación de herramientas que ayudan en el control. Esta implementación se lleva a cabo en conjunto con Telconet y dirigida por el encargado de Ciberseguridad. Entre las herramientas en el proceso de implementación se establece Firewalls, Protección de Mail, EDR, concientización a los usuarios, Pentesting. SOC.

La organización tiene como actividad económica la exportación de camarón, para esta industria es importante proteger los equipos de operaciones de la planta. Para

esto la organización amplía el análisis a Ciberseguridad Industrial y de esta manera cubrir todos sus puntos vulnerables.

Conclusiones

La implementación de estrategias de Ciberseguridad en una organización es muy importante para garantizar la disponibilidad, confidencialidad e integridad de la información. Dentro de este proceso se evaluaron diversos aspectos como conocer su estado actual tecnológico, sus políticas y el nivel de conocimiento del personal. Las organizaciones suelen tomar muy a la ligera estos aspectos pensando que nunca sufrirán algún ataque; por lo tanto, en el caso que le suceda no están preparados para afrontar y reaccionar ante estos incidentes.

Como mejora a este proceso se implementó una matriz de riesgo de activos críticos, sistemas de monitoreo continuo de los activos, honeypot, honeyfiles, y se está analizando servicios de Ciberseguridad Industrial. Se logró alinear los objetivos de la empresa a los de ciberseguridad y así obtener todo el apoyo de los directivos en este proceso de implementación.

Recomendaciones

Con la implementación del SGSI en la organización se recomienda mantener actualizado el análisis de riesgo, tener al personal interno capacitado, en especial al usuario final que es el más susceptible a ser influenciado por Ciber atacantes. Las organizaciones por su crecimiento e innovación realizan cambios en sus arquitecturas tecnológicas, brindan nuevos servicios, y los tipos de ataques informáticos también evolucionan. Por esto, es importante que estén preparados ante cualquier incidente que se pueda dar.

Limitaciones

La compleja situación económica que atraviesan las organizaciones en el Ecuador las encamina a priorizar sus necesidades que incidan en el giro del negocio, pero es importante tomar medidas preventivas ante los ciberataques para reducir el impacto y poder controlarlo. Debido a esto, se ha priorizado proteger los activos esenciales que afecten gravemente a la continuidad del negocio y mediante etapas lograr cubrir la mayoría de las brechas de seguridad que se tenga en la organización.

Referencias

ISO 22301:2019. (s.f.). *GUÍA DE IMPLANTACIÓN DE LA CONTINUIDAD DE NEGOCIO.*

Asamblea Nacional del Ecuador. (2021). *Ley de Protección de Datos Personales.*

Ayerbe, A. (2019). *Hablemos de la ciberseguridad industrial.* Real Instituto Elcano.

Centro de Ciberseguridad Industrial. (2014). *Guia para la construcción de un SGCI. Sistema de Gestión de la Ciberseguridad Industrial.*

Erickson, J. (2008). *Hacking : The Art of Exploitation.* No Starch Press, Inc. https://doi.org/ISBN-10: 1-59327-144-1,ISBN-13: 978-1-59327-144-2

Figueroa-Suárez, J. A., Rodríguez-Andrade, R. F., Bone-Obando, C. C., y Saltos-Gómez, J. A. (2017). La seguridad informática y la seguridad de la información. *Polo del Conocimiento*. https://doi.org/10.23857/pc.v2i12.420

Flores Quispe, C. A. (2018). *TIPOS DE HACKERS.* TIPOS DE HACKERS: http://www.revistasbolivianas.ciencia.bo/scielo.php?script=sci_arttext&pid=S1997-40442013000100008&lng=es&nrm=iso

ISO 27001:2013. (2015). *Sistemas de Gestion de la Seguridad de la Información.*

Joyanes Aguilar, L. (2018). *Industria 4.0. La cuarta revolución industrial.* Alfaomega Grupo Editor. https://doi.org/ISBN: 978-84-267-2568-4

Laserfiche. (2020). *Guía práctica para la Continuidad de Negocio.*

Loján Granda, E. M. (2017). *Modelo de Evaluación de Gestión de Continuidad del Negocio basado en la norma ISO 22301:2012.*

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2021). *Política de Ciberseguridad.*

Quiroz-Zambrano, S. M., y Macías-Valencia, D. (2017). Seguridad en informática: consideraciones. *Dominio de las Ciencias, 3(3), 676-688.*

Rodríguez Pinilla, O. J. (2017). *CONTINUIDAD DEL NEGOCIO.* Bachelor's thesis, Universidad Piloto de Colombia.

Romero Castro, M. I., Figueroa Morán, G. L., Vera Navarrete, D. S., Álava Cruzatty, J. E., Parrales Anzúles, G. R., Álava Mero, C. J., . . . Castillo Merino, M. A. (2018). *INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES.* Área de Innovación y Desarrollo, S.L.

Sánchez Avila, M. A. (2019). *Hacking ético: impacto en la sociedad.*

Superintendencia de Bancos. (2021). *Normativa de la Superintendencia de Bancos.*

The Mitre Corporation. (2023). *MITRE ATT&CK*. https://attack.mitre.org/

Zhang, X., y McMurray, A. (2013). Embedding Business Continuity and Disaster Recovery within Risk Management. *World Journal of Social Sciences*, 61-70.

ANEXOS

Anexo de Aprendizaje

https://nickel-background-b4d.notion.site/750248679dd742f89aba3f26939e6f7f?v=468cc422fbb749b8996ff7484473cb46

Anexo de Implementación

https://nickel-background-b4d.notion.site/fc8f7605eb7b408297a0769c163ee03a?v=3464118f532a4f5b8e0145163a288127