Modelo de Gestión de Riesgo para Sistemas de Seguridad Electrónica para Entidades Financieras

Poly Lázaro Isaac Salazar Larico
Postgrado en Informática
Universidad Mayor de San Andrés
La Paz - Bolivia
salazarlaricopoly@gmail.com

***Resumen*—El presente artículo, constituye un estudio de gestión de riesgos sobre los sistemas de seguridad electrónica (sistemas de intrusión, control de accesos y sistemas CCTV) los cuales con el avance tecnológico deben alinearse a los estándares internacionales y el uso de buenas prácticas para un buen tratamiento de los riesgos identificados. De esa manera se pretende generar en la creación de un modelo análisis de riesgos para estos tipos de sistemas bajo la norma ISO 31000 el cual se podrá aplicar en entidades financieras.**

Palabras clave—ciberseguridad, mitigación, ISO, riesgos, seguridad de la información, seguridad electrónica.

I. INTRODUCCIÓN

En la actualidad toda empresa se basa en la información para tomar decisiones que permita la continuidad del negocio, transformándose así en un activo importante para las organizaciones, siendo necesario protegerla ante cualquier evento que puede causar corrupción en los datos. Dada la importancia de la información, organizaciones internacionales de estandarización han elaborado normas de buenas prácticas para el resguardo y buen uso de la información y de los activos en general.

La Organización de los Estados Americanos (OEA) el año 2018 presentó un reporte sobre el estado en el sector Bancario en América Latina y el Caribe donde recoge el trabajo de un año de análisis de las entidades bancarias, entre los principales hallazgos, el reporte señala que:

- Al menos 9 de cada 10 entidades bancarias sufrieron incidentes cibernéticos en el último año
- El 37% de los bancos de la Región fueron víctimas de ataques que resultaron efectivos.
- El 39% de los incidentes no son reportados, dato que en el caso de las entidades bancarias de mayor tamaño baja hasta el 19%
- 6 de cada 10 usuarios que no utilizan servicios de banca digitales lo hace por desconfianza sobre la seguridad de las transacciones.

Con este reporte, la OEA quiere ofrecer a los países de la región, y a sus entidades bancarias, una herramienta que les permita analizar y mejorar sus capacidades en la administración de riesgos que permitan mejorar y fortalecer sus sistemas de seguridad.

Actualmente es necesario garantizar un análisis de riesgos para los sistemas de seguridad electrónica acorde a las nuevas amenazas tecnológicas mejorando así los tratamientos de los riesgos asociados.

Los controles relacionados a la seguridad de la información se refieren al conjunto de normas, procedimientos y mecanismos utilizados para garantizar la confidencialidad, integridad y disponibilidad en los sistemas de procesamiento de datos y en la información utilizada por personal de las organizaciones.

Eloy Cestero de la Universidad Politécnica de Madrid, realizo una investigación de tesis doctoral que propone un enfoque borroso del Análisis y Gestión de Riesgos en los Sistemas de Información y toma como base la metodología MAGERIT para adoptar normas ISO, donde indica que es necesario facilitar a los expertos un método con el cual se pueda expresar de forma imprecisa juicios probabilísticos o sus valoraciones sobre activos de una organización, y una vez obtenidos tales valores, construir algoritmos que permitan establecer bajo tratamiento borroso indicadores de impacto y riesgo para las amenazas sobre los activos de información, encontrando un conjunto óptimo de salvaguardas que evite la materialización de una de una amenaza provocada sobre los activos reduciendo así el riesgo asociado al sistema.

Duvan y Ángela de la Universidad Católica de Colombia realizaron una investigación sobre los Riesgos, Amenazas y Vulnerabilidades de los Sistemas de Información, donde determinan realizar un análisis de riesgo de los sistemas de información, donde deben tratarse técnicas de seguridad según normas ISO y la gestión de riesgos tratamiento de los riesgos para establecer controles o medidas de protección correspondientes al riesgo para proteger los activos de la organización.

La seguridad electrónica en las entidades financieras son encargadas del control y monitoreo de los sistemas de intrusión física, control de accesos y video vigilancia tanto en la infraestructura de áreas restringida y otras instalaciones los cuales almacenan información confidencial y esta debe ser asegurada, resguardada y limitarse para evitar exponerla a personas ajenas a la utilización de la misma generando diversos riesgos cumpliendo con los mecanismos se seguridad de la información acorde a un análisis de riesgo elaborado de acuerdo a su contexto.

Para referenciar este artículo (IEEE):
[N] P. Salazar, «Modelo de Gestión de Riesgo para Sistemas de Seguridad Electrónica para Entidades Financieras» *Revista PGI. Investigación, Ciencia y Tecnología en Informática*, nº 7, pp. 80-82, 2020.

Las principales funciones de un Sistema de Seguridad Electrónica son: la detección de intrusos en el interior y exterior, el control de accesos y tráfico (personas, paquetes, correspondencia, vehículos, bóvedas, áreas de exclusión, rack de telecomunicaciones, etc.), la vigilancia óptica mediante fotografía o circuito cerrado de televisión (CCTV) y la intercomunicación por megafonía y protección de las comunicaciones.

Fig. 1. Sistemas de Seguridad Electrónica (José Miguel Roca Chillida, 2017)

Los controles relacionados a la seguridad de la información se refieren al conjunto de normas, procedimientos y mecanismos utilizados para garantizar la confidencialidad, integridad y disponibilidad en los sistemas de procesamiento de datos y en la información utilizada por personal de las organizaciones (Medina, 2006).

En Bolivia cada vez más se van identificando casos de vulneraciones y fraudes en diferentes sistemas de información en entidades bancarias, pese que se cuenta con un Reglamento de Requisitos Mínimos de Seguridad para el sector bancario, a raíz de estos eventos la Autoridad de Supervisión del Sistema Financiero boliviana emite la Circular II/CC-8188/2017 donde instruye que: “Fortalecer la gestión de riesgo operativo y el sistema de control interno, para adicionar e incorporar medidas de prevención, detección y respuesta”.

Bajo las consideraciones antes mencionadas es importante realizar un modelo de análisis de riesgos para los sistemas de seguridad electrónica. De esta manera se podría detectar mitigar posibles amenazas y vulnerabilidades bajo los lineamientos de la norma ISO 31000:2018.

A. Objetivos

1) Objetivo General

Plantear un modelo de gestión de riesgo para sistemas de seguridad electrónica para entidades financieras que mitiguen los mismos usando la norma ISO 31000.

2) Objetivos Específicos

- Identificar los riesgos de los sistemas de seguridad electrónica en entidades financieras.
- Evaluar los riesgos identificados para su tratamiento.
- Elaborar una propuesta de modelo de análisis de riesgos para los sistemas de seguridad electrónica en entidades financieras basado en la norma ISO 31000.
- Evaluar el modelo planteado en relación a los riesgos de los sistemas de sistemas de seguridad electrónica en una entidad financiera.

II. MÉTODOS

La gestión del riesgo es parte de la gobernanza y el liderazgo y es fundamental en la manera en que se gestiona la organización en todos sus niveles y que se puede aplicar en diferentes contextos, la gestión de la seguridad de la información permite identificar, analizar, valorar y clasificar el riesgo. La gestión de riesgo es un proceso dinámico y permanente que aporta a los procesos institucionales, se debe asegurar todos los elementos que procesan y guardan información conocidos como activos. Estos activos se los puede considerar en tres grupos: Datos e información, sistemas e infraestructura y personal.

En un mundo actual de constantes cambios tecnológicos, el manejo de la seguridad de información a todo nivel se convierte en un problema grave cuando no se le brinda el control y tratamiento apropiado. Una efectiva administración de los riesgos asociados y su tratamiento sobre este tema es un aspecto de negocio y regulación, no sólo de tecnología.

La norma ISO 31000 se aplicó para la identificación de riesgos. El estándar establece los principios, el marco de trabajo y el proceso que se debe seguir para gestionar cualquier tipo de riesgo de una forma transparente, sistemática y creíble dentro de cualquier contexto.

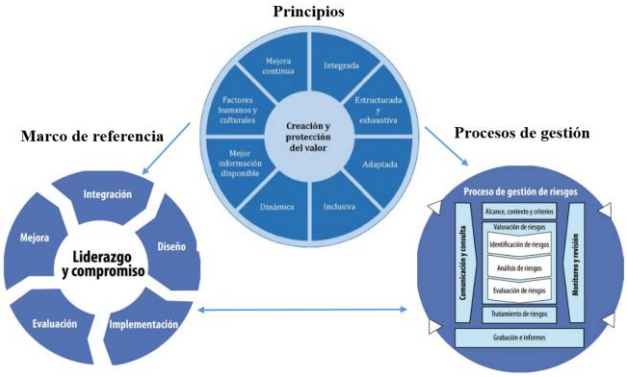

Fig. 2. Principios, marco de referencia y proceso ISO 31000:2018

La investigación también utiliza el método hipotético-deductivo, que consiste en hacer observaciones manipulativas y análisis, a partir de las cuales se formulan hipótesis que serán comprobada en base a sus fases metodológicas de acuerdo con los objetivos planteados en la investigación.

En este sentido, en la presente investigación se utilizó el diseño Experimental, debido a que se desea analizar el posible grado de contribución que puede tener el Modelo de análisis de riegos para sistemas de seguridad electrónica basado en la norma ISO 31000. (variable independiente) en mitigar los riesgos en los sistemas de seguridad electrónica en entidades financieras (variable dependiente).

Las técnicas aplicadas para la recolección de información se basaron en: encuestas, entrevistas, consultas, observación revisión de documentación entre otros.

En el presente trabajo de investigación tuvo como universo de estudio las entidades financieras de la Asociación de Bancos Privados de Bolivia (ASOBAN), con autorización vigente por la Autoridad de Supervisión del Sistema Financiero (ASFI) en Bolivia y que cuenten con los sistemas de seguridad electrónica propia y que hacen un total de 7 hasta el 2019.

La muestra de estudio tiene como como objeto de estudio se tuvo una entidad financiera de ASOBAN y supervisada por la Autoridad de Supervisión del Sistema Financiero (ASFI) siendo así una muestra sesgada para mejorar la investigación.

III. Resultados

En la investigación realizada de acuerdo con el diseño y contexto dentro de seguridad electrónica se elaboró una matriz de riesgo con la identificación de los riesgos y evaluación de los mismos, se identificó los siguientes vectores de ataques que a su vez genera la matriz de riesgo las cuales son: Dispositivos de suplantación de identidad, Manipulación de la ubicación, Fraude de identidad, Amenazas/bots y Hardware en los sistemas electrónicos.

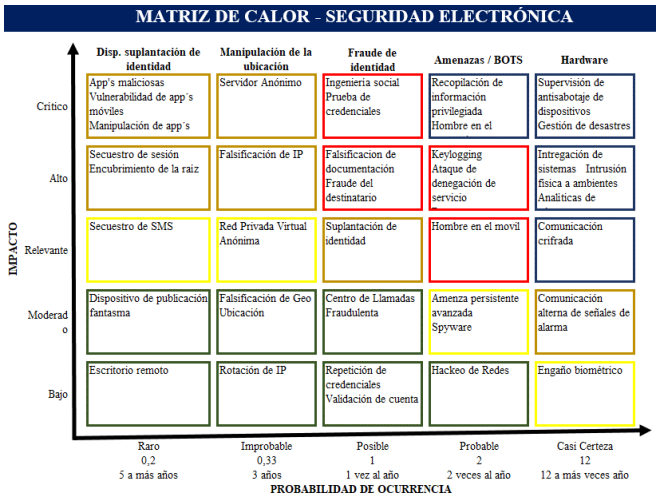

Fig. 3. Matriz de riesgos seguridad electrónica (Elaboración propia).

La matriz mostrada en la tabla anterior se realizó en base al requerimiento de reglamento de Seguridad Física de la ASFI y Resolución Ministerial 153/15 cumpliendo con los requisitos establecidos en dichos documentos de los reguladores.

El modelo reflejado en la matriz fue a partir de los criterios de la norma ISO 31000, para obtener una mejora continua, integración, estructura, adaptación, dinámica, para una mejora continua. El modelo contempla también la integración de los sistemas de seguridad bajo el contexto y ambiente adecuado realización una relación de cooperación entre sistemas de acceso, alarmas y circuito cerrado CCTV.

Esta conjunción y controles y mitigaciones elaboradas para cada amenaza o vulnerabilidad se basa también con los nuevos retos de la actualidad que viene asociado con la tecnología, como los nuevos ataques como, por ejemplo, ransomware, ataques de denegación de servicio, ingeniería social, hackeo de redes, intrusiones físicas, servidores anónimos, aplicaciones maliciosas, fuga de información, engaño de biométrico, gestión de desastres, recopilación de información privilegiada entre otros.

IV. Conclusiones

Con la presente investigación se podrá identificar los criterios en base al contexto descrito en el presente artículo que ayudará relevar la información para generar un análisis de riesgos para los sistemas de seguridad electrónica. De esta manera el modelo de gestión de riesgos para el tratamiento de los riesgos identificados en base a la norma ISO 31000 que podrá aplicarse en entidades financieras.

En base a lo expuesto anteriormente se logró alcanzar los objetivos planteados en la investigación.

- Se lo lograron identificar los riesgos asociados a los sistemas de seguridad electrónica en una entidad financiera.
- Se estableció los criterios en los riesgos para la asignación de valores en su impacto y probabilidad de ocurrencia en cada activo.
- Se elaboró una propuesta de modelo de análisis de riesgos para los sistemas de seguridad electrónica en entidades financieras basado en la norma ISO 31000.
- El modelo planteado en relación a los riesgos de los sistemas de seguridad electrónica en una entidad financiera permite el tratamiento de los riesgos minimizando considerablemente los mismos.

Referencias

[1] M. Aguilar, Sistemas de gestión de seguridad de información para una institución financiera., Lima, 2006.

[2] OEA, «Estado de la ciberseguridad en el sector Bancario en América Latina y el caribe,» 2018.

[3] M. A. V. Aguilar, Sistema de Gestión de Seguridad de Información para una Institución Financiera, Lima, 2006.

[4] J. Bertolin, Seguridad de la información, Redes, informática y sistemas de información, Madrid: Paraninfo, 2008.

[5] A. Emilio, Nuevas tendencias y Otros Procesos de BI, Barcelona: Oberta UOC Publishing, 2013.

[6] J. C. Estévez, Metodología de la investigación, La Paz, 2008.

[7] J. M. Roca Chillida, «http://www.informeticplus.com/,» 2018. [En línea]. Available: http://www.informeticplus.com/que-es-la-seguridad-electronica.

[8] E. Hernández, Auditoria en Informática, México: CECSA, 2005.

[9] D. E. Castro Bolañoz y Á. D. Rojas Mora, Riesgos, amenazas y vulnerabilidades de los sistemas de información, Bogotá: Universidad Católica de Colombia, 2013.

[10] E. Vicente Cestero, Análisis y gestión del riesgo en los sistemas de información, Madrid: Universidad Politécnica de Madrid, 2016.

Breve CV del autor

Poly Lazaro Isaac Salazar Larico es Licenciado en Informática, mención Ingeniera de Sistemas Informáticos por la Universidad Mayor de San Andrés, La Paz. Actualmente realiza la Maestría en Informática Forense, Seguridad de la Información y Auditoría Informática en el Postgrado en Informática UMSA. Trabaja como Supervisor Nacional de Seguridad Electrónica en el Banco de Crédito de Bolivia S.A. y es Presidente del Comité Mixto de Trabajadores A. Centro (parte Patronal). Banco de Crédito de Bolivia S.A. Email: salazarlaricopoly@gmail.com.