Sistema de Seguridad electrónica basada en la norma ISO 27001

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 sobre los sistemas de seguridad electrónica (Sistemas de Control de Acceso, Video-Vigilancia y Alarmas Contra Intrusión Física) los cuales con el avance tecnológico deben alinearse a los estándares internacionales y el uso de buenas prácticas para un buen tratamiento de las amenazas y vulnerabilidades asociadas, basados y alineados a la seguridad de la información y estándar ISO 27001, el cual tiene una estructura robusta que ayuda, fortalece y minimiza las brechas de los sistemas de seguridad electrónica en entidades financieras en base al Reglamento para la Gestión de Seguridad Física.**

Palabras clave—buenas prácticas, estándares, intrusión, seguridad de la información, seguridad electrónica.

I. INTRODUCCIÓN

La seguridad informática en las empresas es implementada con el fin de asegurar la información y actualmente está vista como un gasto para la empresa, pero con el avance tecnológico y los nuevos riesgos que vienen asociados se tiene que cambiar de visión ya que estos lineamientos de seguridad son una inversión que guardan lo esencial que es la información y que en base a esta ayuda bastante en la toma de decisiones para la empresa.

La seguridad de la información se refiere 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).

Bajo las consideraciones antes mencionadas es importante realizar un modelo de seguridad para los sistemas de seguridad electrónica. De esta manera se podría mitigar amenazas y vulnerabilidades bajo los lineamientos de la norma ISO 27001.

Falta de actualización de lineamientos en los sistemas de seguridad electrónica basados en buenas prácticas y/o estándares internacionales no permite tener el control adecuado del manejo y los accesos a los sistemas de procesamiento de información, abriendo la posibilidad de que la información manejada sea utilizada para fines que perjudiquen a la empresa en relación en cumplimiento normativo y gestión de incidentes adecuados.

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.

Contexto Nacional

A raíz de eventos de fraudes internos identificados en una entidad financiera, la Autoridad de Supervisión del Sistema Financiero (ASFI), el 9 de octubre emitió la Circular II/CC-8188/2017 donde instruye que: "Considerando los últimos acontecimientos relacionados con hechos delictivos, se instruye fortalecer la gestión de riesgo operativo y el sistema de control interno, a fin de incorporar medidas de prevención, detección y respuesta".

La seguridad de la información no es sólo técnica y por tanto sólo compete a los equipos, recursos humanos y sistemas informáticos, procedimientos, normas, buenas prácticas entre otros, esto conduce a descuidar aspectos tan importantes como los sistemas de seguridad electrónica que realizan el control y monitoreo de las entidades y sus instalaciones acorde a un modelo de análisis de riesgo en el contexto en el cual trabajan dichos sistemas.

Contento Internacional

En países de Latinoamérica los Ministerios de seguridad son conformados por autoridades estatales y privadas con el fin de realizar comisiones de supervisión y/o seguridad siendo su función principal establecer políticas estratégicas, programas, normas y procedimientos generales.

Tras investigación realizada en Costa Rica el Ministerio de Seguridad Publica conformo una comisión de seguridad privada en el ámbito financiero, garantizando la seguridad del usuario y de la entidad, de forma que sea ejecutada según las normas y leyes del estado, así como que velando la estandarización de prácticas que vayan siempre hacia la mejora continua y gestión de modelos de seguridad integral.

Esta comisión fue conformada por miembros de ministro de seguridad pública, bancos privados, cooperativas, mutuales, bancos del estado, empresas de seguridad, asesores legales, donde gracias al esfuerzo, dedicación y compromiso mediante la experticia y conocimiento en la materia plasmaron las mejores prácticas y medidas utilizadas hoy en día en ese país; con el fin

Para referenciar este artículo (IEEE):
[N] P. Salazar, «Sistema de Seguridad electrónica basada en la norma ISO 27001», *Revista PGI. Investigación, Ciencia y Tecnología en Informática*, nº 8, pp. 156-159, 2020.

de minimizar los riesgos que se presentan a nivel de seguridad de información sobre los sistemas de seguridad electrónica de todas las entidades financieras y bancarias, y con ello velar por el cumplimiento de la Ley 8395 "Ley de Regulación de Servicios de Seguridad Privados" en el país de costa Rica.

A. Objetivos

1) Objetivo General

Determinar la contribución de un modelo de seguridad de información basado en la norma ISO 27001 en las vulnerabilidades de sistemas de seguridad electrónica.

2) Objetivos Específicos

- Determinar el estado actual de los sistemas de monitoreo y control de áreas físicas.
- Fundamentar una propuesta para un modelo de seguridad de la información basada en la norma ISO 27001 para los sistemas de monitoreo y control de áreas físicas restringidas.
- Evaluar el modelo propuesto de seguridad de información basada en la norma ISO 27001.

B. Marco teórico

1) Seguridad

Seguridad es el conjunto de acciones enfocadas a la protección, defensa y preservación de las personas y su entorno frente a amenazas externas que atenten contra su integridad.

De todas formas, cabe decir que la seguridad es un concepto amplísimo, aplicable a muchas situaciones y contextos, que van desde la tecnología hasta el derecho.

2) Electrónica

Finalizando la década de los cuarenta, la electrónica no tenía mayor consideración que la de ser una rama secundaria de la electricidad cuya función principal era reducir el volumen de los elementos eléctricos tradicionales; esta concepción cambia radicalmente al descubrirse el uso de los semiconductores, tales materiales permitieron la creación de dispositivos (siendo el primero el transistor) capaces de manipular la energía para el transporte de la información.

De esta manera se concibe a la electrónica de una nueva forma, como la ciencia que permite obtener, controlar y utilizar información (en forma de energía eléctrica) procedente de la naturaleza o del ser humano.

3) Arquitectura de un Sistema de Seguridad Electrónica

El concepto de seguridad es amplio y aplicable a un gran número de situaciones, por esta razón para alcanzar una seguridad integral es necesario utilizar medios de diversa naturaleza cuyo uso conjunto permite una mejor aproximación al bajo riesgo. La clasificación de tales medios se muestra a continuación:

- Recursos o medios humanos: Constituidos por personal capacitado de seguridad pública (Policía Nacional) o privada.
- Medios Técnicos: Todo recurso físico encaminado a mantener a la seguridad de sitios y personas, pueden ser de tipo pasivo (construcciones, vallas, etc.) o activo (dispositivos electrónicos).
- Medios Organizativos: Todas las herramientas utilizadas en la organización y coordinación en el uso de recursos, como la planificación, asignación de recursos, normas de seguridad, aplicación de los medios técnicos activos.

4) Sistemas de Seguridad electrónica

Tomando en cuenta las consideraciones anteriores podemos decir que un sistema de seguridad electrónica será la interconexión de recursos, redes y dispositivos (Medios técnicos activos) cuyo objetivo es precautelar la integridad de las personas y su entorno previniéndolas de peligros y presiones externas.

El uso de estos recursos, dependerá (como ya se dijo) de la características y necesidades de aquello que se va a proteger, considerándose el número de sitios a proteger, los riesgos potenciales de los mismos y necesidades especiales que se puedan presentar.

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. Dispositivos de Seguridad Electrónica (J. M. Roca Chillida, 2017)

5) Sistemas de control de accesos

La seguridad electrónica también ofrece importantes recursos en el control de accesos a través de la instalación de monitores. Con ellos puede controlarse el flujo de personas, vehículos y cualquier tipo de activo en un ámbito determinado o en diferentes localizaciones de la misma empresa.

Habitualmente cuenta con tecnologías de control, tanto para fábricas como para edificios, sistemas de tarjeta de proximidad y de lectura, control inalámbrico, sistemas biométricos de

reconocimiento facial o por huella digital, integración con redes IP, cerraduras electromagnéticas, etc.

6) Sistemas de circuito cerrado de televisión

CCTV (Circuito Cerrado de Televisión) una herramienta esencial dentro del sistema de control y vigilancia para las empresas, que cuenta con cámaras, tanto para el interior como para el exterior, Domos y controladores, grabadoras digitales DVR/NVR, equipos PCI, tecnología coaxial e IP, etc.

Un apartado fundamental de la tecnología de seguridad electrónica es la capacidad de visualizar las cámaras desde la oficina o a través de la red desde cualquier punto y a cualquier hora. Es clave para la tranquilidad en el entorno laboral. (Jordi Gutiérrez, 2016).

7) Norma ISO 27001

Es una norma internacional que detalla lineamientos de seguridad de la información, los cuales permiten implementar en la gestión de seguridad de la información de cualquier empresa controles para mejorar continuamente la seguridad física y lógica de la información, ayudando así a proteger la información de posibles robos o daños.

La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2. (Kosutic, 2014) hasta llegar a su versión 2013 el cual aborda esta investigación.

II. MÉTODOS

El diseño metodológico implica descripción de cómo se va a realizar la presente investigación, dicho de otro modo, el plan de acción que permitirá llegar a los objetivos maximizando la información y reduciendo errores en los resultados. Según Hernández y Fernández (Hernández & Fernández, 2010), se define al diseño como el plan o estrategia concebida para obtener la información que se desee. Clasifican al diseño de Investigación en experimental y no experimental.

El diseño experimental, como su nombre lo indica es una situación de control, en la cual se manipulan de manera intencional, una o más variables independientes (causas), para analizar las consecuencias de tal manipulación sobre una o más variables dependientes (efectos).

El diseño no experimental, se define como la investigación que se realiza sin manipular deliberadamente variables y en los que se observan los fenómenos en su ambiente natural para después analizarlos.

En este sentido, en la presente investigación se utilizará el diseño No experimental, debido a que se desea analizar el posible grado de contribución que puede tener el Modelo de seguridad para sistemas de seguridad electrónica basado en la norma ISO 27001. (variable independiente) en mitigar los riesgos en los sistemas de seguridad electrónica en entidades financieras (variable dependiente).

Método de investigación

La investigación utilizará el método hipotético-deductivo, que consiste en hacer observaciones manipulativas y análisis, a partir de las cuales se formulan hipótesis que serán comprobada.

Fases metodológicas

Objetivos	Fases metodológicas
Determinar el estado actual de los sistemas de monitoreo y control de áreas físicas restringidas en entidades financieras.	Levantamiento de información Clasificación de la información Registro de la información Análisis de la información Verificación de la información Archivo de la información
Fundamentar una propuesta para un modelo de seguridad de la información basada en la norma ISO 27001 para los sistemas de monitoreo y control de áreas físicas restringidas en entidades financieras.	Revisión teórica Identificar la arquitectura, pasos, herramientas adecuadas para elaborar el modelo de seguridad de información basada en la ISO 27001, que se ajuste a las entidades financieras.
Evaluar el modelo propuesto de seguridad de información basada en la norma ISO 27001 una vez implementado.	Probar la hipótesis bajo el desarrollo del modelo elaborado en la investigación

Fig. 2. Fases metodológicas (Elaboración Propia)

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 2020.

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 ESPERADOS

El modelo de seguridad de información desarrolla los controles consistentes y mecanismos efectivos para su implementación dirigidos a los riesgos presentes y las acciones que se deben implementar para reducirlos en relación al contexto.

Los controles están alineados a la norma ISO 27002 donde se tiene una guía de acuerdo a los dominios de la norma 27001 los cuales son:

- Políticas de seguridad
- Organización de la información
- Seguridad de los recursos humanos
- Gestión de los activos
- Control de accesos
- Criptografía
- Seguridad Física y ambiental
- Seguridad en las operaciones
- Transferencia de información
- Adquisición de sistemas, desarrollo y mantenimiento
- Relación con los proveedores
- Gestión de incidentes
- Continuidad de negocio

- Cumplimiento con requerimientos legales y contractuales

En base al análisis de riego y evaluación de los mismos permite generar una matriz de riesgo en base al modelo propuesto.

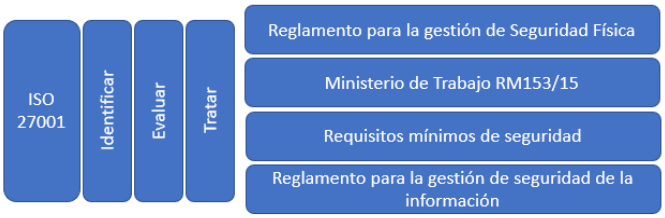

Fig. 3. Modelo seguridad de seguridad de información para sistemas de electrónica (Elaboración propia).

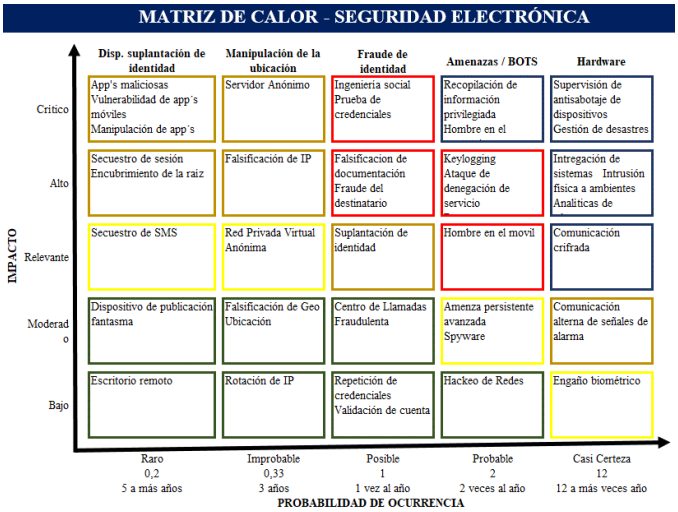

Fig. 4. Matriz de riesgos seguridad electrónica (Elaboración propia).

IV. CONCLUSIONES

Con la presente investigación se podrá fortalecer los criterios en base al contexto descrito en el presente artículo que ayudará relevar la información para generar un modelo de seguridad de información para los sistemas de seguridad electrónica. De esta manera se generará un modelo seguridad de información para el tratamiento amenazas y vulnerabilidades en base a la norma ISO 27001 que podrá aplicarse en entidades financieras o instituciones que trabaje con estos sistemas.

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

- Se identifica el estado actual de los sistemas de monitoreo y control de áreas físicas restringidas.
- El modelo de seguridad de la información basada en la norma ISO 27001 para los sistemas de monitoreo y control de áreas físicas restringidas en entidades financieras cumple con los 14 principios de la norma.
- El modelo propuesto de seguridad de información basada en la norma ISO 27001 permite el tratamiento de los riesgos y vulnerabilidades minimizando considerablemente los mismos.

REFERENCIAS

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

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

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

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

[5] Fundación UNIR, «Unir Revista,» Fundación UNIR, 11 Diciembre 2019. [En línea]. Available: https://www.unir.net/ingenieria/revista/noticias/iso-27001/549204720236/. [Últ. acceso: 20 sep. 2020].

[6] I. R. Narváez Barreiros, Artist, *Aplicación de la norma ISO 27001 para la implementación de un SGSI en la fiscalía general del estado.* [Art]. Universidad Católica del Ecuador, 2013.

[7] vJ. A. Angariat Leiva y C. L. Bautista Bojorques, Artists, Diseño de un sistema de gestión de la seguridad de la información ISO27001 para la Alcaldía de Florida Blanca y plan de acción para su implementación según la guía PMBOX. [Art]. Universidad Industrial de Santander, 2014.

[8] D. E. Santos Llanos, Artist, Establecimiento, implementación, mantenimiento y mejora de un sistema de gestión de seguridad de la información, basado en la ISO/IEC 27001:2013, para una empresa de consultoría de software. [Art]. Pontificia Universidad Católica del Perú, 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. Actualmente realiza la Maestría en Informática Forense, Seguridad de la Información y Auditoria Informática en el Postgrado en Informática UMSA.
Tiene experiencia como Supervisor Nacional de Seguridad Electrónica.
Email: salazarlaricopoly@gmail.com.