El Arte de la Seguridad de la Información en la Globalización

Germán Alberto Saba Carrasco
Postgrado en Informática
Universidad Mayor de San Andrés
La Paz - Bolivia
german.saba@gmail.com

***Resumen*—El presente artículo presenta el replanteo del cambio de los modelos de seguridad que se centran en las amenazas externas a los nuevos modelos que ven la seguridad de manera predictiva y para todas las empresas, esto debido a las tendencias de uso de las redes sociales y dispositivos móviles en la empresa que cambio el entorno del riesgo en toda la empresa.**

Palabras Clave—seguridad, redes sociales, dispositivos móviles.

I. INTRODUCCIÓN

El cambio y evolución de las tecnologías, así como las facilidades junto con las comodidades que le brindan la tecnología al usuario repercute de manera directa en el entorno de riesgos normal que se tenía en una empresa. Sin embargo, de la mano de dicha expansión tecnológica y el aumento del uso de servicios de Internet surgen nuevos retos y desafíos para las organizaciones. Así, una de las principales amenazas que han traído consigo estos avances es la proliferación de acciones delictivas en el ciberespacio.

Debido a estas nuevas amenazas es que se debe plantear un cambio en los programas de seguridad de la información, este cambio debe centrarse en alinearse con la agenda de negocio y poder lidiar y acomodarse a los nuevos riesgos presentes en la entidad.

Viendo así la necesidad de contar con un modelo estándar que toda entidad pueda aplicar para desarrollar una cultura de Seguridad de la Información, que pueda ser aplicado de manera sencilla en toda Entidad, permitiendo a las mismas estar preparadas ante los cambios que la globalización trae.

II. MARCO TEÓRICO

Mancera, S.C. Seguridad de la información [1], postula que la Seguridad de la Información en el marco de la Globalización e incremento de la Tecnología que esta presenta actualmente en todos los niveles jerárquicos institucionales; teniendo que lidiar con constantes alteraciones de la complejidad en los elementos de amenaza que el entorno interno y externo, conlleva a que el personal encargado de la Seguridad de la Información debe tener presente en la actualidad una serie de nuevos entornos de amenaza ajenos a los tradicionales y sobre todo portátiles, siendo de uso común que pueden causar daño en la imagen institucional, fuga de información e incluso pérdidas económicas.

Los puntos descritos a continuación son un punto de vista de aquello que se debe tener presente al hablar de Seguridad de la Información en la actualidad.

A. Predictivo y para Toda la Empresa, Consejo de normas de seguridad PCI

Se debe cambiar la perspectiva de la seguridad de la información está ya no es solo el cumplimiento de normativa y ya no depende solamente de TI. Este cambio es predictivo y transversal a toda la empresa, se hace de manera proactiva [2].

Esta nueva perspectiva está basada en la confianza por lo que acepta algunos elementos en vez de prohibirlos. La siguiente figura nos presenta una estrategia que se puede utilizar para fomentar la confianza y así evitar entrar a la paranoia.

B. Identificar los Riesgos Reales, Consejo de normas de seguridad PCI

La cantidad de problemas que se suscitan cotidianamente y necesitan atención inmediata evitan que el profesional pueda prestar atención y anticiparte a problemas futuros. Para proteger los activos críticos de la empresa todos en la empresa deben conocer donde reside la información que manejan. Se debe comprender que es la información más importante para la empresa, donde se encuentra, quienes necesitarían acceso a ella y así saber qué áreas son las más vulnerables a ataques [2].

Según OWASP, las amenazas más relevantes a las que uno se debe enfrentar en una organización son [5][6]:

- *Amenazas Internas*, prevalecen más que las amenazas externas estas pueden ser accidental o intencionalmente, este riesgo seguirá en aumento si es que no se controla a tiempo.
- *Computación en la Nube*, es un término general para denominar cualquier cosa que tenga que ver con la provisión de servicios de hospedaje a través de Internet, esto brinda diversas ventajas en cuestión a costos, pero incrementan los riesgos en la empresa.
- *Dispositivos Móviles*, la utilización de los mismos por los empleados conlleva al incremento de los riesgos en la empresa.
- *Ciberataques*, este tipo de ataques se está volviendo más especializado en la actualidad de lo que estaban acostumbras las empresas.

Para referenciar este artículo (IEEE):

[N] G. Saba, «El Arte de la Seguridad de la Información en la Globalización», *Revista PGI. Investigación, Ciencia y Tecnología en Informática*, nº 8, pp. 77-79, 2020.

- *Redes Sociales*, gracias al crecimiento de las redes sociales la interconexión entre las personas pone en peligro información tanta personal como de la organización.

C. Consejo de normas de seguridad PCI, Adelantarse a las Amenazas

El mundo de seguridad de hoy necesita que se conozcan las debilidades del programa de seguridad y así adelantarse a amenazas internas o externas que pudieran explotar estas debilidades [4]:

- ISO/IEC. ISO/IEC 31000:2018 "Gestión de Riesgos", *Definir la Inclinación de Riesgo de la Empresa*, se tiene que entender a fondo la cultura de la organización para realizar la alineación al riesgo a enfrentar.
- ISO/IEC. ISO/IEC 31000:2018 "Gestión de Riesgos", *Identificar la Información más Importante*, se debe identificar, inventariar y priorizar el valor de la información para poder priorizar las acciones a tomar en seguridad.
- ISO/IEC. ISO/IEC 31000:2018 "Gestión de Riesgos", *Evaluar el Panorama de las Amenazas*, se debe identificar quien puede tener acceso a la información para poder identificar amenazas contra la misma.
- ISO/IEC. ISO/IEC 31000:2018 "Gestión de Riesgos", *Desarrollar Modelos de Amenazas Predictivos*, una vez identificado el riesgo se deben crear escenarios que ayuden a entender y cuantificar la probabilidad de que ocurra una violación.
- ISO/IEC. ISO/IEC 31000:2018 "Gestión de Riesgos", *Determinar los Mecanismos de Protección Adecuados*, se utiliza el modelo de amenazas para generar los mecanismos adecuados de protección.

D. Consejo de normas de seguridad PCI, Proteger la Información más Importante

El concepto de estar 100% seguros ya no existe por lo que ahora es necesario determinar la información más importante para poder planear y realizar las acciones necesarias rápidamente si sucede alguna violación [2].

- ISO/IEC 270002:2013/Cor 2:2015, *Detectar y monitorear*, es necesario tener áreas de detección y reacción ante incidentes [8].
- ISO/IEC 270002:2013/Cor 2:2015, *Prevenir la Pérdida de Datos*, se tiene que utilizar herramientas de prevención de perdida de tatos (PPD) para prevenir que personas con acceso a la información copie la misma en dispositivos externos o envié archivos por correo al competidor [8].
- ISO/IEC 270002:2013/Cor 2:2015, *Optimizar los Controles*, no basta con realizar solo el cumplimiento de las normas la seguridad debe ir revisando los controles y mejorándolos para proteger la empresa [8].

E. Consejo de normas de seguridad PCI, Equilibrar los Fundamentos

Se debe alinear todos los aspectos de seguridad con la organización, optimizando el uso de recursos y pudiendo así invertís en el control de nuevos riesgos [2].

- *Equilibrar las Prioridades e Inversiones*, se tiene que encontrar un equilibrio entre la inversión en los procesos de la empresa y la inversión en seguridad de la empresa.
- *Invertir de Manera Prudente*, se requieren nuevas tecnologías para adelantarse a las amenazas recientes.
- *Realizar Subcontrataciones Selectivas*, Subcontratar de manera selectiva libera recursos para aquellas tareas de más alto valor.
- *Utilizar la Tecnología Adecuadamente*, no basta solo con la adquisición de tecnología se debe utilizar al máximo las capacidades de la tecnología.

F. Consejo de normas de seguridad PCI, Ir más allá del Cumplimiento para Lograr una Seguridad Sustentable

- *Conseguir la Atención del Consejo para Fines de Gobierno y Determinar la Tolerancia al Riesgo*, la atención del consejo es necesaria, así como que tenga las funciones adecuadas asegura que el consejo determine el alineamiento de la seguridad de la información y el cumplimiento de la misma, ellos también ayudaran con la determinación del riesgo aceptable para el funcionamiento normal de la empresa.
- *Permitir que la Seguridad Impulse el Cumplimiento*, realizar solo el cumplimiento de regulaciones produce en carencias de seguridad, los nuevos atacantes buscan mejores formas de poder vulnerar la seguridad de la empresa eludiendo las normas establecidas.
- *Medir los Indicadores Líderes*, las métricas tradicionales tienden a mirar hacia atrás tomando en cuenta hechos sucedidos y no así diversos factores que lograrían detectar incidentes cuando aún son pequeños y así atender con mayor eficacia a las áreas que representan el peligro más grande [2].

G. Consejo de normas de seguridad PCI, No Prohibir las Cosas Nuevas – Aceptar el Cambio

Se debe apoyar la aceptación del cambio debido a que tan rápido se realiza el cambio en la organización y así crear políticas de seguridad que permitan el uso de nuevas tecnologías [2].

- *Garantizar que la Seguridad sea Responsabilidad de Todos*, la forma de lograr un entorno de seguridad mucho más seguro es logrando hacer que los empleados entiendan que la seguridad de la empresa es responsabilidad de todos.
- *Habilitar Tecnologías más Nuevas*, los usuarios cada vez están más relacionados con nuevas tecnologías, más sofisticadas, móviles y con mayores capacidades, es por esto que en lugar de poner políticas que eviten o prohíban las tecnologías, se deben poner controles para proteger y optimizar la seguridad y acceso en la empresa.

- *Extender los Programas e Seguridad en toda la Empresa*, La seguridad de la Información debe ser la base de la estrategia general de administración de riesgos de la empresa. Fomentando a que todos en la empresa trabajen conjuntamente y así proteger a la empresa de amenazas existentes y emergentes.
- *Establecer Métricas del Programa de Seguridad que Impacten el Desempeño del Negocio*, los programas deben enfocarse en la medición del valor y la responsabilidad, mediante métricas que midan el impacto que tiene el programa de seguridad en el negocio.

III. Resultados esperados

Con todo lo expuesto se pretende presentar un modelo estándar que toda entidad pueda aplicar para desarrollar una cultura de Seguridad de la Información, basada en estándares, preparada para el cambio en todo momento y tratando de estar siempre adelantado a toda amenaza que se puede presentar.

Si bien se exponen una serie de puntos y parámetros a tener presente, estos no son los únicos o absolutos ya que todo anda en constante cambio y pueden aparecer nuevos parámetros a tomar en cuenta o desaparecen de la lista a medida que la Tecnología y la Globalización avance.

IV. Conclusiones

La Seguridad de la Información en la Globalización, está replanteando la estrategia para poder hacer frente a los nuevos riesgos que conlleva la interconexión que se tiene actualmente a nivel mundial, impulsando la madurez en el entendimiento de que es seguridad y concientizando de lo que conlleva el resguardo de la información en el presente al mismo tiempo que se debe estar preparado para el futuro.

Si bien los estándares internacionales nos brindan un marco normativo que cubre la seguridad de la información de manera global y transversal, los mismos deben ser manejados por personal capacitado para lograr efectividad en la utilización de estos y a su vez adecuarlos al entrono que se quiere utilizar o que se va a manejar al utilizar un servicio de manejo de información.

Referencias

[1] Mancera, S.C. Seguridad de la información, Integrante de Ernst & Young Global, 2011

[2] Consejo de normas de seguridad PCI [En línea] https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

[3] ISO/IEC 27001:2013 “Tecnología de la información – Técnicas de seguridad – Sistemas de gestión de la seguridad de la información – Requisitos - Anexo E: Enfoques de la evaluación de riesgos de la seguridad de la información”, 2013

[4] ISO/IEC. ISO/IEC 31000:2018 “Gestión de Riesgos”, 2018.

[5] OWASP [En línea] http://www.owasp.org/index.php/OWASP_Top_Ten_Project

[6] OWASP [En línea] http://www.owasp.org/index.php/Category:OWASP_Guide_Project

[7] ISO/IEC 270002:2013/Cor 2:2015 Tecnología de la información – Técnicas de la seguridad – Código de buenas prácticas para la gestión de la seguridad de la información, 2015.