La política de seguridad de la información y la conciencia humana

*Efraín Cuevas Riaño**

Resumen

Toda vez que la información es uno de los activos más importantes de cualquier persona o empresa, es fundamental que se garantice su protección. En la época contemporánea, este presupuesto ha llevado a que la seguridad de la información sea un tema álgido en todos los contextos; así, es común que se implementen procesos con los que se cree estar protegido de posibles infiltraciones. Con esto en mente, en este artículo se busca evaluar la manera en que se ven afectados los mecanismos de seguridad de la información por la falta de conciencia de las personas respecto a comportamientos personales que pueden poner en riesgo la información a la que tienen acceso.

Palabras clave: conciencia, información, seguridad

Abstract

Since information is one of the most important assets of any person or company, it is essential to guarantee its protection. Nowadays, this requirement has led to information security being an unavoidable topic in all contexts; thus, it is common to implement processes that are believed to be protected from possible infiltrations. In this sense, this article seeks to assess the way in which information security mechanisms are affected by the lack of awareness of people regarding personal behaviors that may put in risk their information.

Keywords: Consciousness, Information, Safety

* Ingeniero de sistemas. Docente de la Corporación Unificada Nacional de Educación Superior (CUN). Contacto: efrain_cuevas@cun.edu.co

Introducción

En la época contemporánea, llena de cambios y avances tecnológicos, la información se ha establecido como uno de los aspectos más importantes para las personas y organizaciones. Esto se debe a la creciente necesidad de manipular las variables del entorno que permiten la adecuada toma de decisiones y protegen el procesamiento, almacenamiento, uso, creación y transmisión de la información. Lo anterior ha impulsado la creación e implementación de mecanismos para protegerla; aun así, es fundamental que los individuos tomen conciencia[1] de la información que conocen y se apropien de las políticas de seguridad (pasos a seguir) para que se garantice su correcto manejo. Con esto en mente, en este artículo se muestran los principios fundamentales de la seguridad de la información, se explican las buenas prácticas en su manejo y en la implementación de un sistema de gestión de la seguridad de la información (SGSI), y, finalmente, se presentan las conclusiones.

Principios fundamentales de la seguridad de la información

La seguridad de la información es un tema recurrente en las investigaciones de este siglo. En estas es usual encontrar el famoso aforismo atribuido a Gene Spafford[2] (director y auditor de seguridad de Coast Technology) referente a la imposibilidad de confiar en un sistema de seguridad:

> el único sistema que es realmente seguro es aquel que está apagado y desenchufado, encerrado en una caja forrada de titanio, enterrado en un bunker de hormigón y está rodeado de gas nervioso y guardias armados muy bien pagos. Incluso entonces no me jugaría la vida en ella.

Con esta frase se resume lo delicada que es la seguridad de la información y la imposibilidad de hablar de esta si no hay parámetros definidos para mitigar las posibles amenazas y vulnerabilidades. Por ejemplo, un sistema *seguro* puede ser vulnerado por sus propios creadores, ya que ellos tienen las pautas, normas, reglas y contraseñas que, de ser mal utilizadas, les permitirán acceder, manipular o convertir un sistema confiable en uno no confiable o inutilizable. Las amenazas (agentes internos o externos) son capaces de explotar los fallos de seguridad, producir debilidades y causar pérdidas de los activos de las organizaciones o personas.

Entre los puntos susceptibles a un ataque se encuentran el almacenamiento, las vulnerabilidades físicas y las comunicaciones humanas; estas últimas son la amenaza más grande: si los individuos involucrados no conocen las normas de seguridad, puede que estas no se adopten de manera eficiente y surjan insatisfacciones, errores e infracciones al sistema. Así, es posible que

1 Para la construcción de este artículo se entiende *concientizar* como el hecho de reconocer una falta o carencia, aunque esta no se corrija, y *tomar conciencia* como la acción que determina que se tomen medidas o se modifiquen las estrategias y enfoques para superar alguna problemática.

2 Ejemplos de esto son los libros *Cisco Secure Internet Security Solutions* (2001, p. 73) de Andrew Mason y Mark Newcomb, *Issues for Libraries and Information Science in the Internet Age* (2001, p. 129) de Bruce Shuman y *Technological Turf Wars* (2009, pp. 46-47) de Jessica Johnston.

se presenten impactos en la estructura de seguridad o se materialicen las amenazas; entonces, para mitigar estos impactos, es necesario priorizar el conocimiento de los fundamentos de la seguridad de la información. Estos últimos, a través de acciones diarias como auditorias, análisis de incidentes, políticas claras de seguridad, resiliencia ante desastres, entre otros, sostienen la seguridad de las organizaciones.

Buenas prácticas en el manejo de la información

Las buenas prácticas se basan en los tres principios fundamentales de la seguridad de la información: confidencialidad, integridad y disponibilidad (ISO 27000, s. f.). El primero autoriza a la persona u organización a acceder a la información que requiere; el segundo garantiza que los datos o recursos no hayan sido alterados en su contenido, y el último permite acceder de forma segura a la información y que esta pueda ser utilizada en el momento en que se solicite (Ministerio de la Presidencia, 8 de enero del 2010).

Para que lo anterior funcione adecuadamente es fundamental que se implemente un SGSI. Por ejemplo, el ISO 27001 está diseñado para proteger los activos de información con la implementación de políticas de seguridad, procedimientos y controles que, además, ofrecen ventajas competitivas, rentabilidad, acatamiento legal e imagen (ISO 27000, s. f.). Los activos de información pueden ser informativos, documentados, tecnológicos, medios, procedimentales y de personas; de esta manera, es fundamental que los individuos se capaciten de manera específica en la política de seguridad para mitigar los riesgos y amenazas. Igualmente, con el objetivo de evaluar los riesgos, es necesario tener en cuenta los procedimientos, las rutinas diarias del uso de la información y las actividades de todo el personal que tenga acceso a los activos de información y a los servicios que proporciona la organización.

Ahora bien, lo anterior no es viable si los individuos no toman conciencia de sus actos y hábitos frente a la información. Así, es importante adaptar las costumbres, comportamientos y decisiones que toman las personas frente a las políticas de seguridad de una organización si se quieren mitigar los riesgos. Por este motivo, el ser humano debe estar a la altura de los nuevos retos de la época contemporánea. En el siglo XXI, la conciencia y el pensamiento deben estar en estrecha relación con las normas y políticas de seguridad de las empresas, ya que la seguridad se clasifica como prioridad para las organizaciones. Esto ocurre porque los atacantes buscan infiltrarse en los sistemas privados y permanecer sin ser detectados durante largos períodos de tiempo, en los que pueden robar información, atacar la infraestructura o demandar rescates económicos para liberar las estructuras de las organizaciones. A su vez, esto lleva a que las empresas consideren fundamental fortalecer sus sistemas de seguridad, una vez que, si llegan a ser víctimas de *hackers,* serán criticadas públicamente por no proteger la información personal de sus clientes y empleados.

Conclusiones

En este mundo globalizado tecnológicamente es impensable que no se tengan unas normas claras frente a la seguridad de la información. Esto implica la necesidad de implementar un SGSI que ofrezca reglas transparentes, buenas practicas, políticas de seguridad acordes a las organizaciones y capacitaciones a las personas que hacen parte de estas. Solo así será posible alcanzar una conciencia ideal –frente a los diferentes riesgos que enfrentan las organizaciones y personas– que permita tener objetivos concretos sobre las políticas de seguridad y su implementación.

En este sentido, es importante entender que, para estar a la vanguardia de cualquier tipo de organización y tecnología, los sistemas de gestión de seguridad deben evolucionar según las necesidades de las organizaciones, así como actualizar sus políticas de seguridad y los métodos para realizar las auditorias. No en vano, cada vez se utilizan con mayor frecuencia sistemas de vigilancia de la información a través de sistemas de redes neuronales, ya que estos, entre otros aspectos, posibilitan la implementación de sistemas de reconocimiento de patrones faciales o de biométrica para manipular la alta densidad de información.

Referencias

ISO 27000. (s. f.). Sistema de Gestión de la Seguridad de la Información. Recuperado de https://bit.ly/2QT6gu3

Johnston, J. (2009). *Technological Turf Wars*. Filadelfia, Estados Unidos: Temple University Press.

Mason, A. y Newcomb, M. (2001). *Cisco Secure Internet Security Solutions*. Indianapolis: Cisco Press.

Ministerio de la Presidencia. (8 de enero del 2010). Real Decreto 3/2010, del 8 de enero: por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. BOE: 25. Recuperado de https://bit.ly/2QRYGjm

Shuman, B. (2001). *Issues for Libraries and Information Science in the Internet Age*. Englewood, Estados Unidos: Libraries Unlimited.