Pobre Conciencia de los Usuarios de la Organización en el Cumplimiento de las Políticas de Seguridad de la Información

Corzo, Efraín. y Granados, Cesar.
efracorzo@hotmail.com, cagr821@gmail.com
Universidad Piloto de Colombia

Abstract -- This document contains the description and analysis of some relevant reasons as which the users of the organizations do not have a conscience adapted in the fulfillment of the politics of computer safety and how are you situations make difficult the protection of one of the most significant resources of the entities as it is the information. There is highlighted the importance of implementing strategies to achieve a suitable sensitization and the fundamental role that has the High Direction at the moment of implementing a system of safety management of the information (SGSI).

Index Terms – Cobit, Information Assets, ISO 27001, Risks.

Resumen -- Este documento contiene la descripción y análisis de causas relevantes por las cuales los usuarios de las organizaciones no tienen una conciencia adecuada en el cumplimiento de las políticas de seguridad de la información y cómo estas situaciones dificultan la protección del activo más significativo de las entidades como es la información. Se resalta la importancia de implementar estrategias para lograr una adecuada sensibilización y el papel fundamental que tiene la alta dirección al momento de implementar un sistema de gestión de seguridad de la información (SGSI).

Índice de Términos – Activos de Información, Cobit, ISO 27001, Riesgos.

I. INTRODUCCIÓN

Las políticas de seguridad de la información, cumplen un papel fundamental en la organización como herramienta para sensibilizar a cada uno de los usuarios en el uso de buenas prácticas, sin embargo, su implementación en muchas ocasiones no se realiza de la mejor manera. Este artículo está enfocado en el análisis de las causas por las cuales se presenta desinterés por parte de los usuarios internos de la organización a la hora de aplicar las políticas de seguridad de la información.

II. EL PAPEL QUE JUEGAN LOS USUARIOS EN LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.

Como bien se ha argumentado, ningún sistema es 100% seguro. Por esto, generalmente las organizaciones buscan aplicar las mejores estrategias a la hora de reducir, asumir o transferir los riesgos. Sin lugar a dudas los usuarios cumplen un papel importante a la hora de proteger los activos informáticos, pero surgen diferentes aspectos por los cuales se dificulta la aplicación de las políticas de seguridad de la información y que tienen que ver con las reacciones y actitudes de los usuarios frente al tema.

Una organización o empresa puede tener la mejor tecnología, la más actualizada, implementada en conjunto con las gigantes y reconocidas corporaciones a nivel internacional en temas de seguridad de la información, pero siempre existirá un brecha para penetrar esos sistemas, es aquí donde los usuarios son los protagonistas; de una u otra forma habrá que darle a los empleados las credenciales para administrar los sistemas, servicios informáticos y demás recursos de tecnologías de la información para cumplir con los objetivos del negocio o con la misión de la institución.

Sin embargo, si los usuarios no tienen una cultura bien definida de las políticas de seguridad de la empresa y una verdadera conciencia de seguridad de los recursos de TI que la entidad le proporciona para el cumplimiento de sus funciones, podría verse comprometida toda la inversión en infraestructura tecnológica de seguridad de la información a través de ataques informáticos de

Ingeniería Social (Phishing, Smishing, suplantación de identidad, entre otros) que le pueden entregar a un delincuente informático las llaves de acceso a los sistemas de la corporación.

"Las organizaciones gastan millones de dólares en firewalls y dispositivos de seguridad, pero tiran el dinero porque ninguna de estas medidas cubre el eslabón más débil de la cadena de seguridad: la gente que usa y administra los ordenadores", Kevin Mitnick [1]. La frase anterior es uno de los principales retos que tienen las empresas en sus sistemas de gestión de seguridad de la información (SGSI), no es suficiente blindar a la entidad de infraestructura de seguridad, también se debe fortalecer la cultura de buenas prácticas en el uso de las tecnologías de la información y comunicaciones a los usuarios de la empresa.

III. ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN Y LA SENSIBILIZACIÓN A LOS USUARIOS.

Estándares internacionales utilizados para la implementación de SGSI, como la norma ISO 27001:2005, en su Anexo 8, Seguridad del Personal, establece controles antes, durante y después de ser contratado un empleado; el objetivo de control para este anexo establece: *Asegurar que todos los usuarios empleados, contratistas y terceras partes tengan conciencia sobre las amenazas y problemas de seguridad de la información, sus responsabilidades y léxico, y que estén preparados para brindar apoyo a la política de seguridad de la información organizacional en el curso de su trabajo normal y para reducir los riesgos de error humano* [2].

El modelo de referencia Cobit 4.1, presenta procesos detallados sobre la importancia del entrenamiento y capacitación de los usuarios en la administración adecuada de TI y de la comunicación al interior de la entidad de las políticas de seguridad de la información. En el marco de trabajo de Cobit 4.1, en el dominio de Planear y Organizar (PO), cuenta con un proceso llamado Administrar los recursos humanos de TI (PO07), con la actividad PO7.4 Entrenamiento del personal de TI que cita: *Proporcionar a los empleados de TI la orientación necesaria al momento de la contratación y entrenamiento continuo para conservar su conocimiento, aptitudes, habilidades, controles internos y conciencia sobre la seguridad, al nivel requerido para alcanzar las metas organizacionales* [3].

El anterior estándar y guía de referencia, de ser implementados por la organización, obligan a la creación de un procedimiento que permita mantener una cultura de seguridad en los usuarios internos, induciéndoles en todo momento el empleo de buenas prácticas de seguridad de la información y el conocimiento permanente de los diferentes métodos que utilizan los delincuentes informáticos para cometer fraudes, obtener información confidencial o afectar la continuidad de los servicios informáticos e inclusive la continuidad del negocio.

IV. PRINCIPALES CAUSAS DE LA POBRE CONCIENCIA DE LOS USUARIOS EN EL CUMPLIMIENTO DE LAS POLITICAS DE SI.

Las empresas al realizar los planes de entrenamiento y sensibilización de las Políticas de seguridad de la información deben poder medir la cultura o el ambiente de seguridad para poder determinar si verdaderamente se está cumpliendo con el objetivo del entrenamiento. Puede ocurrir que los usuarios no estén recibiendo adecuadamente la formación y concienciación, en este sentido se pueden presentar varias causas que afectarían de forma directa el Sistema de Gestión de Seguridad de la Información. Entre los métodos que se utilizan para medir el nivel de entrenamiento de los usuarios se encuentran las encuestas, evaluaciones o pruebas de penetración a través de técnicas de ingeniería social.

Cuando los usuarios no están recibiendo la sensibilización de las políticas de forma adecuada, puede deberse a las siguientes causas:

A. Sensibilizaciones esporádicas o poco frecuentes.

Sin dejar de lado la importancia que tiene implementar políticas de seguridad de la información, ésta debe ir de la mano con la socialización adecuada de las mismas hacia el personal. Es importante que los usuarios entiendan y apliquen cada una de las políticas establecidas y para ello las organizaciones pueden hacer uso de diferentes estrategias para este fin; las capacitaciones, conferencias, publicaciones, realización de talleres, hacking en vivo, evaluaciones al personal, entre otras, son algunas alternativas para hacer tomar conciencia sobre el tema.

La mejor manera para que los usuarios tomen conciencia, es demostrándoles a través de técnicas de hacking en vivo de los principales fraudes electrónicos o robo de credenciales que se realizan en la actualidad, si ellos ven en tiempo real, comprenderán mejor el concepto del fraude o delito informático que se quiere explicar; si revisamos el cono del aprendizaje de Edgar Dale, podemos comprobar que después de recibir una demostración, las personas logran retener el concepto de mejor manera.

Fig. 1 Cono del Aprendizaje de Edgar Dale [4]

Es importante tener en cuenta que las socializaciones deben realizarse constantemente ya que en temas de tecnología los cambios surgen en periodos de tiempo muy cortos y hay que mantener los conocimientos actualizados.

B. Se piensa que es responsabilidad únicamente del área de tecnología.

Las áreas de tecnología o las dependencias con funciones afines al tema, cumplen un papel muy importante como apoyo para lograr de forma automatizada las metas del negocio y por necesidad se afectan cada una de las áreas que componen la organización ya que todas ellas deben hacer uso de las tecnologías. Pero cuando se habla de seguridad de la información hay una tendencia a pensar que es un tema estrictamente bajo la responsabilidad de TI. Este pensamiento dificulta que las demás áreas asuman con propiedad y responsabilidad el tema ya que se cree que existe solamente un doliente para desarrollar esa actividad.

C. Falta de compromiso por parte de la alta dirección.

Actualmente muchas organizaciones no tienen conciencia sobre la importancia de resguardar su información. Desafortunadamente los temas relacionados con la seguridad de este activo se empiezan a tener en cuenta cuando ocurre un evento que lo afecte o cuando la normatividad vigente lo exija, lo que se traduce en la implementación de sistemas de seguridad de la información de manera correctiva. Adicionalmente, que “nunca ocurra nada”, puede hacer pensar que los costos que conlleva la implementación de un SGSI sean innecesarios.

Es vital que en la alta dirección de las organizaciones tomen conciencia sobre la importancia que tiene la información para el logro de los objetivos y que se adopten medidas preventivas para mantener el resguardo de este activo.

D. Empleo de un vocabulario técnico para los usuarios.

Para realizar una sensibilización exitosa es necesario utilizar un lenguaje apropiado y entendible para los diferentes tipos de usuarios de la organización. Es inadecuado asumir que todos los usuarios deban entender el tema de seguridad de la información sin que se les haga comprender su importancia y además utilizando un vocabulario técnico. Esto crea una brecha que dificulta la comunicación y termina haciendo que se le pierda importancia al tema o que se vea como algo muy complicado de adoptar.

Los ingenieros de tecnología de la información, generalmente se expresan con términos muy específicos de herramientas o equipos de TI como por ejemplo, router, Firewall, dirección IP, Core, vlan, subred, switch, dirección MAC, Botnet, malware, phishing, FTP, telnet, ssh, DNS, IPS, ipconfig, interfaz, entre otros términos que no son muy conocidos por los usuarios finales y que para grupos como las secretarias, fuerza de ventas o la sección logística y contable, se tornan sin sentido, complicados o difíciles de pronunciar en razón a que no tienen relación directa con su actividad específica o su formación académica y por lo tanto no hacen parte de su vocabulario cotidiano. Lo anterior dificulta en gran medida la sensibilización de las políticas y controles de seguridad establecidos en la institución.

E. Los usuarios no son conscientes de la importancia de la información para la organización.

La información es el activo vital para el desarrollo de las actividades de la organización y para mantener una alta competitividad en el mercado. No obstante, en muchas entidades, no se ha logrado crear una cultura sobre el adecuado tratamiento de la misma. Incluso en ocasiones de manera involuntaria se cometen errores que pueden llegar a afectar alguna de las características de la información (confidencialidad, disponibilidad e integridad).

Uno de los ataques que ocurre con frecuencia es el denominado Ingeniería Social, en donde el atacante utiliza mecanismos de persuasión ante los usuarios para lograr obtener información valiosa y confidencial que le puedan dar acceso a algún sistema. La falta de conciencia sobre la importancia de la información es la causa más clara para generar este tipo de ataques.

Mantener una cultura sobre buenas prácticas del manejo de la información es importante para reducir el riesgo de divulgación inadecuada o pérdida de información. Prácticas sencillas como la utilización de usuarios y contraseñas para el ingreso a los sistemas evitan este tipo de inconvenientes. Sin embargo nada asegura que estas credenciales son manejadas con la mayor cautela por parte de quien las utiliza. Debido a esto, hay que hacer uso de otras estrategias que fortalezcan este tipo de controles, por ejemplo inducir a que el usuario cambie su contraseña con frecuencia y que a su vez se haga uso de contraseñas robustas para minimizar la probabilidad de ser descifradas por el atacante.

F. Entrenamiento sin clasificar a los usuarios por su nivel de formación en el uso de TI.

Hay que tener en cuenta el grado de conocimientos que tiene cada usuario en el manejo de las tecnologías. No todas las personas gustan de este tema o a algunas se les dificulta, por lo que es importante clasificar los diferentes tipos de usuarios y los niveles de conocimiento de cada uno. De esta manera podremos enfocar la manera en que se va a sensibilizar la implementación de las políticas.

De acuerdo a esta clasificación se deben adoptar los temas a socializar ya que no todos van realizar la aplicación de la misma manera, por lo tanto no se requiere que todos conozcan del tema en el mismo nivel.

G. No existen o no se dan a conocer las sanciones o las posibles infracciones por incumplimiento de las políticas de seguridad de la información.

El incumplimiento de las políticas de seguridad de la información debe contener sanciones directas sobre quienes las aplican. De esta forma se crea una conciencia y un ambiente de responsabilidad en los usuarios. De igual manera es importante dar a conocer las posibles sanciones a las que se tendrían que someter un usuario al no aplicar adecuadamente las políticas, esto conlleva a que se le dé la importancia necesaria al tema de la seguridad de la información.

H. *El personal que imparte la sensibilización y entrenamiento no posee las habilidades requeridas.*

En las sensibilizaciones no hay nada más aburrido y tedioso para los usuarios que el orador se limite únicamente a leer diapositivas, emplear slide recargados con demasiado texto, pronunciar términos técnicos suponiendo que el público ya los conoce, no aterrizar el tema con la realidad actual o cotidiana, emplear un tono de voz inadecuado, demostrar nerviosismo o no tener el dominio suficiente del tema, aulas incomodas para realizar la sensibilización, entre otros, puede provocar que los usuarios asistentes se duerman durante la charla, se dediquen hablar por celular y chatear o se ausenten durante la jornada de concienciación.

El Instituto Nacional de Estándares y Tecnología, NIST, en su documento NIST Special Publication SP800-50 [5], presenta una guía para la construcción de programas de sensibilización y entrenamiento en tecnologías de seguridad de la información y hace una diferencia entre el entrenamiento y la concienciación, indicando que el objetivo de la capacitación es proporcionar un conjunto de conocimientos, mientras que la concienciación busca conseguir que los usuarios cambien su comportamiento. Muchos de los responsables de los planes de sensibilización no comprenden la diferencia que hay entre los dos términos y por lo tanto sus actividades no conducen a cambiar el comportamiento de las personas, afectando de manera directa la cultura del SGSI.

V. CONCLUSIONES

- ✓ Actualmente se vienen incorporando nuevos mecanismos para asegurar la información, los cuales son muy efectivos si se implementan de forma adecuada. Sin embargo esto debe ir ligado a la razón social de cada organización ya que dependiendo de esto se establecerán los niveles de seguridad que se requieran, lo que ayudará a no incurrir en gastos innecesarios. Estos mecanismos disminuyen en gran medida los riesgos informáticos a los que está expuesta la organización, pero no hay que dejar de lado el factor humano. Tanto usuarios externos como internos deben conocer y ser consientes del tratamiento que se le debe dar a la información y además deben existir mecanismos que permitan mantener en evaluación las acciones que estos realicen ya que los incidentes no siempre se generan desde afuera, incluso los usuarios internos pueden atentar contra la seguridad de la información ya sea de forma intencional o por falta de conocimiento.

- ✓ Las técnicas de ingeniería social son los mayores problemas que enfrentan las empresas que administran un sistema de gestión de seguridad de la información, los delincuentes informáticos constantemente buscan a través de distintas maneras persuadir a los usuarios para obtener las credenciales de acceso a los sistemas corporativos. Por esta razón, los empleados deben estar adecuadamente formados para enfrentar estos riesgos, de modo tal que le permita identificar cuando está haciendo víctima de un ataque de este tipo y poderlo manejar de la mejor manera sin afectar el SGSI. Promover el cambio de comportamiento en los usuarios es el mayor reto que tiene la alta gerencia y el oficial de seguridad de la información de la entidad; para lograrlo, se deben realizar demostraciones en vivo de los principales incidentes, tener talleres de lecciones aprendidas tomadas de casos ocurridos en otras entidades y realizar constantemente pruebas o simulaciones de ataques para comprobar la formación y el comportamiento de los usuarios frente al tema.

RECONOCIMIENTO

Un especial reconocimiento a cada uno de los docentes de la especialización y el diplomado, ya que con sus valiosos aportes hacen que el tema de la Seguridad de la Información empiece a tomar un grado de importancia muy alto en nuestro país.

REFERENCIAS

[1] K. Mitnick, frase célebre sobre el factor humano, [En línea], Disponible en: http://www.proyecto-cero.com/?categoryid=20
[2] ISO/IEC 27001:2005, Information security management systems – Requirements, 2005, pp.16.
[3] Marco de trabajo Cobit 4.1, 2007, pp. 61.
[4] Cono del aprendizaje de Edgar Dale, [En línea], Disponible en: http://enmarchaconlastic.educarex.es/2009/01/27/el-cono-del-aprendizaje-y-las-tic/
[5] NIST Building an Information Technology Security Awareness and Training Program, NIST Special Publication, SP800-50, Oct. 2003.

Autores

Efraín Corzo García, Ingeniero de sistemas, estudiante de especialización en Seguridad Informática, con 6 años de experiencia en el sector de las fuerzas militares de Colombia.

Cesar Augusto Granados Rivera, Ingeniero de sistemas, estudiante de especialización en Seguridad Informática, con 7 años de experiencia en el sector público en entidades del orden territorial.