EL SER HUMANO: FACTOR CLAVE EN LA SEGURIDAD DE LA INFORMACIÓN

Javier Enrique Lizarazo Rueda[1]

Universidad Pontificia Bolivariana
Bucaramanga, Colombia
jaenliru@gmail.com

Resumen

El ser humano a través de sus acciones se convierte en un factor relevante en el mundo de la seguridad de la información. A medida que el hombre ha requerido indagar en la información resultante de sus actividades, le ha otorgado valor de acuerdo con la utilidad que le aporta a sus procesos; de ésta manera, nace la necesidad de protegerla en todos los entornos en los cuales sea generada y utilizada. El aseguramiento de los datos, que son la base de la información que nutre las actividades de las organizaciones, motiva a la implementación de los Sistemas de Gestión de la Seguridad de la Información y para ellos se requiere la vinculación activa de todo el recurso humano, quien es el responsable del uso de la información y las consecuencias del mismo. Por ello, deberá ser concientizado e instruido en el uso adecuado de las herramientas tecnológicas de gestión de la información, al igual que de todos los procesos que garanticen su seguridad. Dicho proceso formativo llevará a la generación de entornos seguros y una cultura orientada a la protección de los datos, en cada una de las actividades que desarrolle el ser humano.

Palabras claves

Información, Seguridad Informática, Tecnologías de la Información, Sistema de Gestión de la Seguridad de la Información, Inteligencia de Negocios y Programas de Intervención.

[1] Ingeniero de Sistemas Universidad Manuela Beltrán, Especialización en Seguridad Informática Universidad Pontificia Bolivariana, jaenliru@gmail.com

Abstract

The human being through his actions has become a relevant factor in the world of Information Security. He has given it value according to the usefulness that it brings to its processes. In this way, the need to protect the information in all the environments in which it is generated and used arises. The assurance of the data, which are the basis of the information that feeds the activities of organizations, motivates the implementation of Systems Management and Information Security and to obtain it, it is necessary the active involvement of all human resource, who is responsible for the use of the information and its consequences. Therefore, the human resource must be aware and educated in the proper use of technological tools with which information is managed, like all processes that ensure its safety, according to the role it plays in the company. Such learning process will lead to the creation of safe environments and a culture geared to the protection of data, in each and all the activities performed by the human being.

Keywords:
Information, Information Security, Information Technologies, Information Security Management Systems, Business Intelligence and Intervention Programs.

1. Introducción

En el entorno de la seguridad informática siempre se busca garantizar altos niveles de protección para la información, meta ideal que requiere aunar grandes esfuerzos tanto en recurso humano como en infraestructura tecnológica. Todo este trabajo es visto por los usuarios finales y la gente del común como barreras que dificultan la apropiación y uso de las Tecnologías de la Información y las Comunicaciones (TIC), ya que en cierto modo restringen y limitan las actividades que pueden ser desarrolladas con ellas y los resultados esperados. En la actualidad el acceso a las TIC se ha masificado, brindando con ello una serie de entornos que han facilitado el desarrollo de las actividades cotidianas; a su vez la gran acogida que ha tenido el desarrollo tecnológico abre las puertas a un gran cúmulo de conocimiento e información, la cual puede o no ser verdadera y exacta. Del uso que se dé a dicha información dependen los efectos que se generen, los cuales pueden afectar positiva o negativamente al usuario, la comunidad, las empresas y en general a su entorno. Dicho de otra manera, el ser humano es responsable del uso que hace de la información y las consecuencias que esto genera.

La falta de conciencia en el manejo y uso de la información individual o colectiva, conlleva a que se presenten incidentes de seguridad y posibles hechos delictivos que pueden afectar directa o indirectamente los intereses particulares, empresariales y de la vida cotidiana. Por ende, motivar el uso consiente y racional de la información en todas sus presentaciones, disminuirá la capacidad de que agentes externos puedan permear la privacidad de las personas y su entorno.

2. El ser humano, el eslabón más débil

El ser humano por su naturaleza y carácter social es en esencia influenciable en mayor o menor proporción. Éste factor convierte al hombre en: "*El eslabón más débil en la cadena de la seguridad de la información…*"[2]; no obstante él también interviene de manera activa y permanente en los procesos que nacen de las áreas o departamentos encargados de las Tecnologías de la Información (TI) que están orientados a garantizar y conservar la seguridad de la información. Las TIC han abierto un universo de posibilidades de acceso a la información sin límites, como lo pueden ser la ubicación geográfica, la disponibilidad, los formatos de presentación y almacenamiento de los datos. La falta de formación en el uso apropiado de las herramientas informáticas, ha puesto de manifiesto una de las debilidades más grandes en cuanto a la preservación de la seguridad de la información se trata, ya que el primer paso utilizado por los atacantes para obtener acceso indebido a la información es a través de un usuario inexperto en el uso de las TIC. La información y la comunicación son herramientas que han permitido la evolución y el desarrollo del ser humano; a medida que el hombre avanza en conocimiento, lo apropia y lo comunica, genera información; proceso que inicialmente se convirtió en la tradición oral de los pueblos y con el paso del tiempo en escritos que hoy son la base documental de la humanidad. Los escritos por si solos no tienen valor, éstos son valorados por el significado que les proporciona el hombre, lo que representan para él; esto quiere decir que el hombre cualifica, cuantifica y valora la información.

Actualmente en el mundo del marketing y los negocios se resalta el principio que "*quien tiene la información tiene el control*"[3] ; pero no solo el tener la información es suficiente, se debe saber qué hacer con ella, cuándo y de qué forma utilizarla para lograr su mayor aprovechamiento, en pro de mantener la continuidad del negocio.

Al convertirse la información en un elemento tan importante en el entorno empresarial, de igual forma se deben definir los lineamientos que se han de tener en cuenta al momento de cuidarla y conservarla para mantener vigentes sus atributos más importantes como son: la confidencialidad, la integridad y la disponibilidad.

El ser humano, es quien necesita de la información para poder realizar sus tareas, alcanzar sus metas, ser competitivo y tener éxito, por ello es el directo responsable de su cuidado y conservación, para ello debe estar preparado.

[2] http://www.borrmart.es/articulo_redseguridad.php?id=1137&numero=24

[3] Material elaborado por: Francisco Samper Programa Gobierno en línea. Seminario Marketing Gubernamental y la redes sociales Agosto 25 de 2009. http://programa.gobiernoenlinea.gov.co/apc-aafiles/Cursos/Dos/Presentacion_Francisco_Samper.

3. Es ser Humano y la Seguridad de la Información [1]

Ante el auge tecnológico y el gran valor que adquiere la información como activo primordial de las organizaciones y del hombre, se debe iniciar el fomento de una Cultura de la Seguridad de la Información, que no es más que unir esfuerzos encaminados a la formación integral del ser humano para lograr su correcto desarrollo y desenvolvimiento en todos los aspectos y escenarios de la vida (personal, académico, laboral, social, cultural, entre otros); para esto se debe tener en cuenta la fundamentación en los principios éticos y morales, que le permitan discernir claramente entre lo bueno y lo malo en su entorno cotidiano.

En todo momento el ser humano tiene a su alcance información de diversos orígenes como son académicos, laborales, públicos, entre otros; de acuerdo con la valoración que se le haya otorgado a la misma, ésta debe ser resguardada. Éste proceso de salvaguarda de la información va encaminado en los ámbitos empresariales y corporativos a la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI)[4], el cual busca garantizar la protección de los activos de información que en determinadas circunstancias pueden ser los más valiosos para la compañía.

4. Las Empresas y la Información

Citando a Marion Jarper Jr. en el libro Nueve Claves para el Éxito, “Administrar un negocio bien es administrar su futuro; y administrar el futuro es administrar información”, (Calder, A., 2006) [2]. En el mundo de los negocios, desde los más pequeños hasta los más grandes deben procurar un muy buen manejo y control de la información ya que ésta es de vital importancia para lograr altos niveles de competitividad y productividad, “Una organización puede ser rica en datos y pobre en información, si no sabe cómo identificar, resumir y categorizar los datos”, (Madnick, S., 1993). Lo anterior es la base de la Inteligencia de Negocios, que busca obtener de los datos la más valiosa información que permita a las empresas alcanzar el éxito.

Algunas organizaciones se ven motivadas a la búsqueda y adquisición de los datos o información de sus competidores, para poder superarlos o no quedarse rezagados en el mercado; de aquí que se animen a la realización de espionaje corporativo, el cual ataca inicialmente al equipo humano de las empresas objetivo y luego a los componentes tecnológicos que gestionan ese anhelado recurso. De esta manera, quienes se quieren mantener vigentes en éste entorno se ven en la necesidad de proteger su información y para lograrlo deben implementar un SGSI; éste objetivo requiere de una serie de actividades y procesos, todos ellos basados en una norma de carácter internacional como lo es la ISO/IEC 27001, que sirve de base para que la empresa logre los niveles de seguridad deseados de acuerdo con los alcances y objetivos proyectados por la Alta Dirección [3].

[4] NTC ISO 27001:2005 numeral 0.1 Generalidades.

La implementación del SGSI debe estar estrechamente ligada a los lineamientos de la organización y a los objetivos del negocio, con el fin de lograr atacar los riesgos a los que se enfrenta. El compromiso de la Alta Dirección es de vital importancia, ya que es quien define los parámetros que se han de tener en cuenta para lograr el éxito en el proceso. De igual manera todo el recurso humano se debe vincular activamente al proceso para fortalecerlo.

De acuerdo con los lineamentos planteados por la NTC ISO/IEC 27001:2005 en el numeral 5.1 "COMPROMISO DE LA DIRECCIÓN" literal (c) "estableciendo funciones y responsabilidades de seguridad de la información", se denota que es fundamental para el correcto funcionamiento del SGSI, la correcta, clara y específica definición de roles y responsabilidades respecto a la Seguridad de la Información. Cada miembro de la organización, debe estar al tanto del papel que desempeña dentro del proceso del SGSI y las obligaciones que ello conlleva. Estos roles se definen como parte de la política del SGSI y su conocimiento debe formar parte del entrenamiento que recibe el personal al iniciar en su cargo o al momento de realizar la implementación del SGSI; lo que quiere decir que éstos deben formar parte del manual de funciones de cada cargo existente en la organización.

Es importante el reconocimiento y apropiación de cada uno de los roles y las tareas que ellos llevan implícitos dentro de la organización; para generar un clima laboral favorable que facilite la gestión eficiente de los procesos corporativos.

El establecimiento de roles es positivo en cuanto a que genera orden en los procesos de la empresa y mejores resultados en producción; sin embargo, deben ser definidos de manera tal, que no se subestime o sobrevalore a ningún trabajador, siendo justos con las aptitudes y habilidades de cada persona y los requerimientos de los cargos.

5. Sensibilización Organizacional [4][5][6]

La sensibilización organizacional busca despertar y fortalecer sentimientos éticos y morales dentro de todos los miembros de la organización, logrando un alto sentido de pertenencia con la misma, que contribuya significativamente a su propio bienestar y a la generación de un ambiente seguro para el procesamiento y gestión de la información. Este proceso hace más fácil la implantación de las políticas de seguridad planteadas por la Alta Dirección. Como parte del proceso de sensibilización, se deben definir programas de intervención con los trabajadores, en los cuales obtengan un mayor conocimiento de la empresa, para que de este modo se desarrolle un sentido de pertenencia y solidaridad para con ella. Hay que tener en cuenta también, que antes de aplicar un programa de intervención, se debe realizar una investigación profunda de la población que caracteriza a la empresa y sus diferentes puestos de trabajo. Al ejecutar un plan de intervención se deben tener en cuenta algunas estrategias existentes, que sirven de base para el desarrollo de actividades de motivación al personal con respecto a los procesos de gestión de la seguridad de la información, entre ellas se pueden destacar:

- *Generación de expectativa:* Llamar la atención del personal hacia el nuevo proceso que se va a iniciar (implantación del SGSI). El trabajador que se sienta intrigado respecto a un tema, como sería el del manejo de la seguridad de la información en el sitio de trabajo, se interesará en preguntar y averiguar, estará listo para recibir la información que le sea dada, puesto que tendrá interés en ello y será proactivo durante todo el proceso.

- *Despertar el interés acerca de la seguridad de la información:* mediante la utilización de estrategias publicitarias como banners, carteleras, protectores de pantalla, pequeñas notas, entre otras; en el manejo de las imágenes es primordial, los colores que se usan y los logotipos. El cerebro humano tiene que adaptarse día a día a los nuevos esquemas que se presentan; así, los trabajadores deben empezar a percibir en la empresa que existe la posibilidad de algo nuevo, preparándose para ello.

- *Juego y actividades lúdicas:* para lograr el objetivo de la sensibilización del recurso humano, pueden realizarse jornadas recreativas que involucren actividades lúdicas, con el fin de enseñar patrones básicos de comportamiento, que fortalezcan los esquemas de seguridad de la información, estas se pueden llevar a cabo durante las pausas activas, luego de la hora de almuerzo o durante actividades de recreación creadas con este fin.

- *Seguimiento:* se debe aplicar encuestas a los participantes para evaluar las actividades y el conocimiento adquirido en ellas. De esta forma, se tiene una herramienta objetiva para verificar la efectividad y detectar oportunidades de mejora en el proceso de sensibilización y toma de conciencia en lo que a Seguridad de la Información se refiere.

- *Simulacros:* así como en las jornadas de prevención de desastres se emplean los simulacros, para verificar la efectividad de los procedimientos que se ejecutan durante una emergencia; éstos también se pueden emplear, para constatar la reacción y forma de proceder del personal en el momento que ocurra un incidente de seguridad de la información.

En los procesos de intervención la obtención de resultados varía de acuerdo con cada persona y su participación en el grupo. Hay que resaltar la existencia de un margen de error que caracteriza toda investigación y sus herramientas de trabajo, para determinar la flexibilidad de la misma y no crear expectativas que se alejen de la realidad.

Del mismo modo, se deben reforzar aquellas actividades observadas que propician la generación de resultados positivos en los funcionarios de la empresa con respecto a los objetivos propuestos. El fin mismo de estas actividades, es crear una cultura organizacional que con el menor número de restricciones o cambios que afecten la armonía del entorno laboral, brinden la mayor protección y seguridad a los activos de información que sustentan a la empresa.

Como complemento a las estrategias empleadas, se deben incorporar componentes comportamentales en cada una de ellas y con ello crear nuevas actitudes en respuesta a las

eventualidades que afectan la seguridad de la Información. Algunos detalles que deben ser tenidos en cuenta para fortalecer la toma de conciencia son:

- Llevar a comprender cuál es el verdadero significado y valor de la información.
- Creación de contraseñas seguras.
- Utilización de los recursos tecnológicos como equipos de cómputo, dispositivos móviles y unidades de almacenamiento.
- Importancia de la retención documental.
- Disposición de documentación impresa.
- Conocimiento en cuanto a clasificación de la información, por ejemplo: pública, confidencial y estrictamente confidencial.
- Uso de la información personal, que tanta información se puede hacer pública en los entornos virtuales, redes sociales y correo electrónico.
- Detección y reporte de incidentes de seguridad.

6. Seguridad de da Información, “Una Cultura de Vida”.[7]

La meta de todo el proceso es crear una cultura al interior de la organización que brinde la confianza en la efectividad de los procedimientos encaminados a la conservación de la seguridad de la información de acuerdo con el SGSI establecido por la Alta Dirección.

El objetivo de lograr una cultura de vida enfocada a la Seguridad de la Información, es brindar fortalezas a quienes producen, manipulan, procesan y mantienen la información, para que fortalezcan la cadena de la Seguridad.

¿Por qué Cultura de Vida? Se define de esta manera ya que ha de crearse un patrón de comportamiento en el recurso humano, que lo motive a seguir los lineamientos del SGSI dentro y fuera de la organización, reduciendo al máximo los riesgos que puedan afectar los activos de información del negocio (ver figura #1).

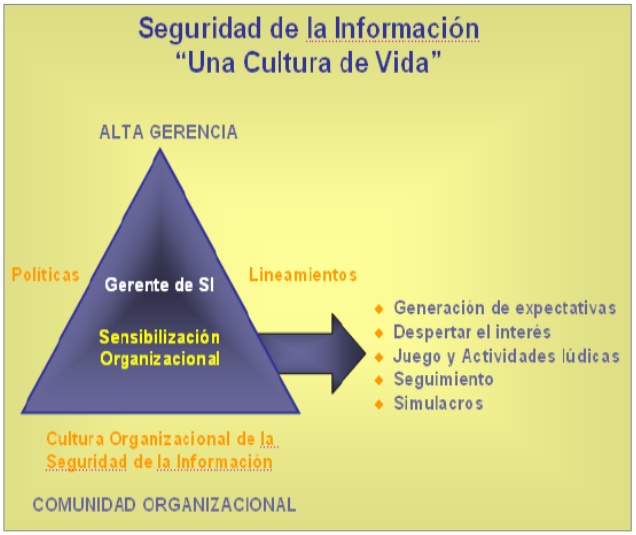


Figura #1. Seguridad de la Información “Una Cultura de Vida” Fuente: Lizarazo, J., 2012.

Los procesos encaminados hacia la generación de ésta cultura de vida, son aplicables a todos los entornos en los cuales se involucra el ser humano.

7. Conclusiones

La falta de conocimiento en gestión segura de la información, hace vulnerable al recurso humano de las organizaciones. Debido al componente subjetivo en el comportamiento del ser humano, éste se convierte en un factor vulnerable para la seguridad de la información; por tal razón se debe aprovechar este factor en beneficio de las organizaciones capacitando e instruyendo en las buenas prácticas del manejo de la información.

El buen manejo de la información ha sido un pilar fundamental en el desarrollo del ser humano y por ello ha sido merecedora de un alto nivel de valoración. Las organizaciones deben contar con programas de capacitación y entrenamiento para todo su personal, en cuanto a la seguridad de la información se trata; para con ello generar entornos laborales más seguros.

La alta competitividad en los negocios la logra quién posee la información, sabe cómo y cuándo usarla y sobre todo la protege. La implementación de un Sistema de Gestión de Seguridad de la Información – SGSI es una herramienta de gran importancia para las empresas que quieren lograr latos niveles de competitividad y mantenerse vigentes en el mercado.

Durante la implementación y el funcionamiento de un SGSI es de vital importancia la vinculación de todo el recurso humano, con el fin de obtener los mejores resultados y garantizar altos niveles de seguridad para la información. Se debe buscar la generación de una cultura organizacional en torno a la seguridad de la información que apalanque todos los procesos del SGSI; ya que son aplicables a todos los entornos en los cuales se involucra el ser humano.

De manera continua, se deben ejecutar programas de intervención con el personal de la organización, tendientes a fortalecer los conocimientos en los procesos y la gestión segura de la información. Las organizaciones deben estar completamente alineadas con las directrices de la alta gerencia y los procesos del Sistema de Gestión de la Seguridad de la Información.

8. Referencias

[1] GÓMEZ, Álvaro, Enciclopedia de la Seguridad Informática. Primera Edición. Alfaomega Ra-Ma. México 2007. ISBN: 978-970-15-1266-1

[2] CALDER, Alan, Nueve Claves para el éxito. Una visión general de la implementación de la norma NTC-ISO/IEC 27001. ICONTEC. Colombia 2006. ISBN: 958-9383-62-9

[3] ICONTEC, Compendio. Sistemas de Gestión de la Seguridad de la Información (SGSI). Segunda Edición. ICONTEC. Colombia 2009. ISBN:978-958-9383-93-3

[4] ROBBINS, Stephen P. Comportamiento Organizacional, Conceptos, Controversias y Aplicaciones. Tercera Edición. 1987. PHH Prentice Hall. ISBN 0-13-64'549-0.

[5] MUGNY, Gabriel, PÉREZ, Juan A. Psicología Social del Desarrollo Cognitivo. Primera Edición. Anthropos. Barcelona 1998. ISBN: 84-7658-099-1.

[6] MYERS, David G. Psicología Social. Segunda Edición. Panamericana. Madrid 1991. ISBN: 84-7903-010-0.

[7] SANCHEZ, José C. Psicología de los Grupos, Teorías, Procesos y Aplicaciones. 2002. Mc Graw Hill. ISBN 84-481-3658-6.

[8] KRIEGER, Mario. Sociología de las organizaciones, Una introducción al comportamiento organizacional. 2001. Prentice Hall. ISBN 987-9460-65-0.

[9] BLOGG, Keith. "Espionaje Corporativo". Disponible en Web: http://www.seguridadla.com/artic/segcorp/7208.htm

[10] CARUANA, Pablo, "Breves conceptos sobre la Ingeniería Social" Disponible en Web: http://www.rompecadenas.com.ar/ingsocial.htm

[11] SAPRONOV, Konstantin, "El factor humano y la seguridad de la información" Disponible en Web: http://www.viruslist.com/sp/analysis?pubid=176195190

[12] MERCADO, Claudia, "Factor humano, principal amenaza para la seguridad" Disponible en Web: http://www.iworld.com.mx/iw_SpecialReport_read.asp?iwid=4233&back=2&HistoryParam=F

[13] GALLEGO, Ramsés, "LA SEGURIDAD, UNA ACTITUD" Disponible en Web: http://www.borrmart.es/articulo_redseguridad.php?id=1004

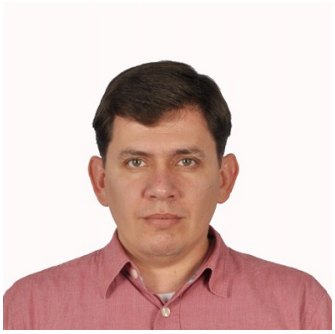
[14] "Uso de la Ingeniería Social" Disponible en Web: http://www.seguinfo.com.ar/cruzada/consejo-01.html

[15] REVILLA, Olga, 06 Abr 2006, “Ingeniería social: cuando la cadena de seguridad se rompe en el usuario” Disponible en Web: http://www.laflecha.net/articulos/seguridad/ingenieria_social/

[16] BENNIS, Warren. Cómo llegar a ser líder.1995. Grupo Editorial Norma. ISBN 958-04-1986-8

[17] MARTÍNEZ, Alfonso. Robo de información: La amenaza viene de dentro. Enero 2009. Red Seguridad. Disponible en Web: http://www.idn.es/novedades_ver.php?ref=128

9. Biografía



Javier Enrique Lizarazo Rueda Colombiano nacido en Barrancabermeja en 1976, mayor de tres hermanos e hijo de Luis A. Lizarazo J. y Ana María Rueda de Lizarazo. Casado. Ingeniero de Sistemas de la Universidad Manuela Beltrán - UMB (2002), con estudios para optar al título de Especialista en Seguridad Informática de la Universidad Pontificia Bolivariana. Auditor Interno en ISO-27001. Profesional interesado en los comportamientos humanos que originan los altos niveles de inseguridad de la información. Coordinador Técnico UNIRED, Ex-Coordinador Programa Ingeniería de Sistemas UMB.