GESTIÓN DEL RIESGO EN LA SEGURIDAD INFORMÁTICA: "CULTURA DE LA AUTO-SEGURIDAD INFORMÁTICA"

Duver Augusto Parra Moreno

Ensayo para optar al título de Especialización en Control Interno

Presentado a

Luz Mery Guevara

Profesora Seminario de Grado

Universidad Militar Nueva Granada

Especialización en Control Interno

Bogotá

2012

GESTIÓN DEL RIESGO EN LA SEGURIDAD INFORMÁTICA: “CULTURA DE LA AUTO-SEGURIDAD INFORMÁTICA”

Duver Augusto Parra Moreno

Universidad Militar Nueva Granada

Especialización en Control Interno

Bogotá

2012

INDICE

INTRODUCCIÓN

Antes de iniciar la búsqueda para profundizar sobre el tema de la gestión del riesgo en la seguridad informática, quise darme primero a la tarea de tratar de definir de una forma genérica y sencilla lo que hasta este momento para mí, es la seguridad informática vista desde la gestión del riesgo, para luego entrar a compararla con la definición que algunos autores dan al respecto. El objetivo era ver qué tan lejos o tan cerca estaba de su concepto principal, sin la profundidad que el tema lo amerita. Quise analizar hasta dónde he llegado y qué tanto conocimiento he podido alcanzar sobre el tema de la seguridad informática en la experiencia de alrededor ya de 15 años trabajando en el mundo de los sistemas; experiencia que ha estado siempre alejada de la participación directa en la delicada misión de resguardar adecuadamente la seguridad de la informática y la documentación electrónica, comité de seguridad, llamado por algunos autores (Honorato, s.f.).

Durante mi experiencia laboral, en la cual he visto varios de los cambios que la empresa ha tenido que efectuar para estar a la vanguardia de las nuevas exigencias que requiere la gestión del riesgo de la seguridad informática y garantizar la confidencialidad, la integridad y la disponibilidad de la información, considero, me da ciertas bases conceptuales para aventurarme a dar una definición inicial de lo que es la gestión del riesgo de la seguridad informática; puedo decir hasta estas instancias que la gestión del riesgo de la seguridad informática es el conjunto de acciones que una organización sin importar su naturaleza (pública o privada) desarrolla e implementa para proteger y salvaguardar uno de sus tesoros más valioso como lo es la información, ya que, se encuentra constantemente en riesgo de sufrir ataques; éstos pueden ser tanto internos como externos a la organización. Usurpación de identidad, uso inapropiado de datos o venta de información confidencial son algunos de los ataques considerados riesgos internos; virus, troyanos, ataques procedentes de

hackers, piratas informáticos, están dentro de los riesgos externos que pueden atacar a la organización.

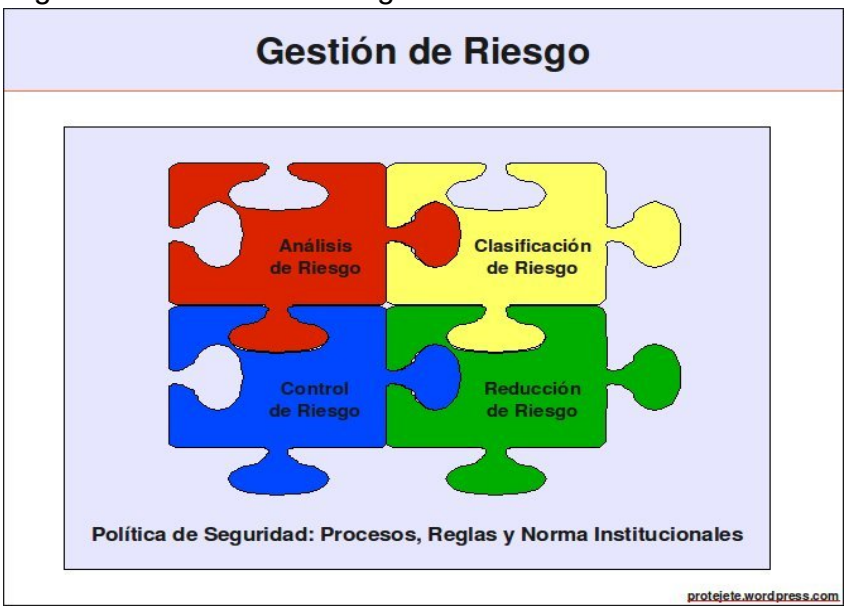
Y por qué surge la necesidad de asegurar la información… Considero que principalmente es para que la organización pueda garantizar la continuidad operacional; para proteger la documentación electrónica de un uso no autorizado; de qué se protege… De los virus, gusanos, caballos de troya, que lo que pretenden es dañar los datos, generar problemas en la prestación de los servicios, violar la seguridad, afectar la imagen de las organizaciones; de quienes… Los intrusos malintencionados, piratas informáticos, del cybercrimen, nombres que se dan para referirse a las especies de ladrones y merodeadores de la información que buscan hurtar la información con fines malintencionados (secuestro, extorsión, estafa, entre otros) y de otros tantos individuos e incluso ya hasta organizaciones que día a día, aparecen para atentar contra las tecnologías de la información y la comunicación (TIC); hasta aquí es lo que puedo agregar con respecto al tema.

Después de revisar varios artículos y documentos que encontré en el maravilloso mundo de la internet; Harold F. Tipton, *Information Security Management Handbook*, 5th Ed.(2006); Leonardo Sena y Simón Mario Tenzer, *Introducción a Riesgo Informático* (2004); Microsoft, *Disciplina de administración de riesgos de seguridad* (2004); Isaca, *Definición de Gerencia de la seguridad de la información* (2010); me quedé con dos de las tantas definiciones que se pueden encontrar al respecto y que a mi parecer, son las que resumen la seguridad informática en una corta pero muy práctica y entendible definición; la primera de ellas es: “Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos. Según [ISO/IEC Guía 73:2002]: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo” (ISO27001, 2005). La segunda fue:

Método para determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo. Está compuesta por cuatro fases: Análisis, Clasificación, Reducción y Control de Riesgo.

a. ***Análisis**: Determina los componentes de un sistema que requiere protección, sus vulnerabilidades que lo debilitan y las amenazas que lo ponen en peligro, con el resultado de revelar su grado de riesgo.*
b. ***Clasificación**: Determina si los riesgos encontrados y los riesgos restantes son aceptables.*
c. ***Reducción**: Define e implementa las medidas de protección. Además sensibiliza y capacita los usuarios conforme a las medidas.*
d. ***Control**: Analiza el funcionamiento, la efectividad y el cumplimiento de las medidas, para determinar y ajustar las medidas deficientes y sanciona el incumplimiento (ver Figura 1).*

Figura 1. Gestión del Riesgo.



(Erb, s.f.)

Comparando mi definición con las encontradas, siento gran tranquilidad al ver que no estaba tan lejos de lo que en sí es la gestión del riesgo en la seguridad de la informática. El título del ensayo surge de la reflexión a la que he llegado empíricamente

después de estos 15 años de compartir de una y otro forma, vivencias cercanas con el tema, y de lo que me impulsa a considerar es vital, para que el modelo que se decida implantar tenga un factor clave de éxito en su objetivo; con el debido respeto por otras opiniones, más allá de la urgente necesidad de disponer de las últimas soluciones, herramientas y equipos de software y hardware para tales efectos, que no obstante son necesarios y requeridos, la seguridad informática es responsabilidad de ***todos***, lo esencial es crear y desarrollar, al interior de la organización, una cultura de la seguridad que encamine al capital humano por la ruta de la **cultura de la auto-seguridad**, tema que trataré de sustentar y demostrar pretendiendo dar un aporte útil y, una contribución que anime el interés de los estudiosos y expertos en el tema, para profundizar los comentarios y alcances que se han incluido.

La intensión es mostrar, en su mayoría con escenarios empíricos, vividos desde mi sitial de Ingeniero de sistemas, que sin importar las políticas, normas y procesos que se desarrollen e implementen en la organización, sea pública o privada, pequeña o grande, la ausencia de la cultura de la auto-seguridad, propende por la ocurrencia de riesgo aun mayor. “En las decisiones de SW y HW, poner la carreta delante de los bueyes puede ser fatal**”** (Honorato, s.f.)**.**

La seguridad total o 100 por ciento no es posible, pues no existe ningún elemento que no esté expuesto a situaciones no controladas o inesperadas, que alteren su funcionamiento bien sea de manera positiva o negativa (Cano, 2006). Con esto en mente, se presenta este ensayo que busca contextualizar brevemente los distintos escenarios presentes en el modelo de seguridad informática, para terminar con el tema central que evoca el ensayo cultura de la auto-seguridad, que no es más que la activa participación de capital intelectual de la organización con un compromiso y empoderamiento en las políticas, normas y procesos establecidos para la seguridad de la información.

Creo firmemente que definir una estrategia para crear la cultura de la auto-seguridad informática, debidamente difundida, conocida y apoyada por todos en la organización, puede contribuir eficazmente y en gran manera a mitigar el riesgo.

ORÍGENES DE LA SOCIEDAD DE LA INFORMACIÓN

Durante los últimos años de la década de los sesenta y principios de los setenta, investigadores como Alain Touraine (La societé post-industrielle, 1969) o Daniel Bell (The coming of post-industrial society: a venture in social forecasting, 1973). Ambos investigadores indicaron que una nueva era estaba surgiendo, una nueva etapa influenciada por el conocimiento, un conocimiento fruto de la aparición de nuevas fuentes de información y de la posibilidad de acceso a ellas.

Yoneji Masuda de origen japonés, en 1980, publicó su libro "The Information Society as Post-Industrial Society". Popularizando la expresión "Sociedad de la Información". Así, Alvin Toffler con "La tercera ola" (“The third wave", 1981), en la que destacaba el uso de la tecnología para satisfacer necesidades de comunicación e información hacía del conocimiento. Para él la información estaba consolidando una sociedad moderna: "los generadores de información". Más recientemente, Nicholas Negroponte, con el "Mundo Digital" ("Being Digital", 1995), nos ofrece una visión optimista de cómo la tecnología digital puede transformar las vidas humanas. Anuncia que la fabricación de bits puede llegar a realizarse en cualquier lugar del mundo, en cualquier momento, anulando las limitaciones geográficas.

Todos estos autores han contribuido, con el aporte de sus obras, a la popularización de las ideas que habían introducido Touraine y Bell, esparciendo el concepto de

sociedad de la información así como algunos de los sinónimos que posteriormente también han gozado de una notable popularidad: sociedad digital, era digital, sociedad interconectada, sociedad inalámbrica, aldea global y otros términos de carácter similar. (ALFA-REDI, 2002)

Esta sociedad de la información, que desde su inicio ha buscado transformar de una forma positiva las vidas humanas, creando una aldea global de información e incrementando la velocidad en la cual la gente y los negocios pueden tener las cosas; facilita de manera rápida y eficiente los métodos para cometer delitos o crímenes conocidos como fraudes o robos. La aparición de las nuevas tecnologías provoca que una guerra suceda a diario en los escenarios de la economía, de la política o de la vida cotidiana. En el campo de las nuevas tecnologías ya no hay verdades sino una lucha por el poder (Bloom, 1988).

Las situaciones adversas (riesgos) a las pretendidas por la sociedad de la información; abren un capítulo en la seguridad de la información que se denomina gestión del riesgo, proceso que reconoce la presencia de situaciones no previstas y trata de identificar los posibles controles que mitiguen los mismos. Los subsiguientes párrafos pretenden mostrar de una forma breve los alcances de la gestión del riesgo; dejando claro eso sí, sin la profundidad que el tema lo requiere, y dado que el tema principal del ensayo es mostrar desde mi postura cómo la cultura de la auto-seguridad en la información se convierte en un factor clave de éxito; tanto o más importante que las soluciones de de SW o HW que podemos ver en la actualidad.

GESTIÓN DE RIESGO EN LA SEGURIDAD INFORMÁTICA

A continuación evoco algunos juicios encontrados con respecto a la gestión del riesgo en la seguridad informática; parte de ellos de documentos respaldados por organismos reconocidos por su labor investigativa y sus aportes a las tecnologías de la información (TI): normas ISO, alfa-redi, acis e isaca; y de algunos autores que también se destacan por su gran experiencia en TI: Jeimy J. Cano, Allan David Bloom, Enrique Dutra, Markus Erb y Juan Honorato. Los pensamientos que se traen a la memoria en este ensayo son el resultado de la investigación que realice de la gestión del riesgo en la seguridad informática.

La presencia de amenazas que comprometen el sistema deben ser analizadas y a su vez evaluadas las probabilidades de que una amenaza aproveche esas vulnerabilidades. Eugene Howard Spafford, profesor de la universidad de purdue, ubicada en indiana, EE.UU, dijo: "El único sistema verdaderamente seguro es aquél que está apagado, encerrado en un bloque de hormigón, y sellado en una habitación con guardias armados. E incluso así, tengo mis dudas". (s.f.)

La gestión del riesgo es un método para determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo (Erb, s.f.). Para comprender aun mejor la gestión del riesgo, se hace claridad de los siguientes conceptos:

a. ***Activo:*** *Como en los aspectos contables existe el activo y el pasivo, la información ahora posee un valor importante y por eso se lo considera un activo. Si un alumno posee el trabajo final de grado y no posee un backup o resguardo en otro dispositivo, ese activo corre un serio riesgo de sufrir algún daño irrecuperable.*

b. ***Amenaza:*** *todo aquello que pueda provocar un daño a nuestro activo. Por ejemplo, si un virus corrompe el ordenador en donde el alumno tiene su trabajo final, no podrá acceder al momento de presentarlo y tal vez lo pierda.*
c. ***Vulnerabilidad:*** *Son las inseguridades que posee el activo tanto por problemas tecnológicos, como problemas de procedimientos. Está demostrado que la gran mayoría de pérdidas de activos son por falta de procedimientos o desconocimiento. El alumno no ha realizado copias de su trabajo en otros medios.*
d. ***Riesgo:*** *es la probabilidad que una amenaza aproveche una vulnerabilidad. Siguiendo el caso del ejemplo, supongamos que el equipo no posee una descarga a tierra y en una noche tormentosa el equipo sufra una descarga y se queme el disco. (Dutra, 2008)*

En la NORMA ISO/IEC 27001:2005 los especialistas que encaran el proceso de análisis, revelan todos los recursos de HW y servicios de la compañía SW, haciendo un análisis de las vulnerabilidades de seguridad de la compañía y con base en esto verifican cuál es la brecha para lograr la normalización. Otra forma de gestionar el riesgo es: realizar test de vulnerabilidad o test de penetración; prácticas frecuentes como herramientas de evaluación para analizar el estado de seguridad de la infraestructura de la organización.

Un proceso de gestión de riesgo va a permitir a la organización entender cuál es su situación de seguridad actual, le va a facilitar tomar decisiones adecuadas para mitigar los riesgos; también evaluar qué medidas se implementan a largo y corto plazo y al final precisará si las decisiones fueron las correctas. Según Enrique Dutra, argentino, consultor de IT & seguridad y certificado en seguridad de Windows desde el 2005 durante los últimos 6 años por Microsoft; afirma que en la gestión de riesgos se involucran 4 estadios:

a. ***Situación actual****: Un análisis de la situación de seguridad de la compañía para entender cómo se están tratando los activos, que niveles de seguridad existen, que leyes se están cumpliendo y cuáles no. Es lo que denominamos l*a foto*.*
   En esta etapa, suele llevarse a la práctica los clásicos test de vulnerabilidad o test de penetración. Los mismos deben ser rigurosos y muy bien planificados, ya que muchas veces, hay profesionales con el afán de demostrar todos sus conocimientos de intrusión provocan caídas de servicios que ponen en riesgo a la compañía a nivel funcional.
b. ***Definir pasos a seguir****: En base a un informe detallado de la situación actual, un comité formado por los responsables de sistemas, RRHH, legales y la gerencia, deberán definir cuáles son los pasos a seguir para atacar el riesgo.*
c. ***Implementación:*** *en base a las decisiones tomadas, se implementan las normas, procedimientos, actualizaciones y ajustes que sean requeridos y que fueron aprobados por el comité. La misma debe ser rigurosamente planificada, ya que hay puntos que deben ser tenidos en cuenta para no impactar en los procesos de negocios.*
d. ***Monitorear****: Analizar el éxito de la implementaciones llevadas a cabo, verificar qué desvíos surgieron y planificar un nuevo análisis en un periodo acorde en la compañía (2008).*

Los factores críticos de éxito para que el proceso de la gestión de riesgos cumpla los objetivos establecidos, requieren de: apoyo incondicional de la gerencia desde el inicio y durante todo el proceso; involucrar a todo el capital intelectual de la organización con participación activa y compromiso hacia la seguridad de la informática; conocer los procesos críticos de negocio de la organización y que activos intervienen en los mismos; implementar los cambios sugeridos que permitan mitigar los riesgos; Dar a conocer a toda la organización el proceso de la gestión de riesgo (Dutra,

2008). Además Isaca resalta la importancia de la alta gerencia en la gestión del riesgo:

> *La práctica ha demostrado que la función de TI y los riesgos de TI a menudo no son bien comprendidos por las principales partes interesadas de una organización, entre ellos los miembros de la junta y la dirección ejecutiva. Sin embargo, estas son las personas que dependen de TI para alcanzar los objetivos estratégicos y operativos de la organización y, en consecuencia, deberían ser los responsables de la gestión de los riesgos. Sin una clara comprensión de la función y de los riesgos asociados a TI, los ejecutivos de alto rango no tienen un marco de referencia para priorizar y administrar los riesgos de TI. Los riesgos de TI no son puramente una cuestión técnica. A pesar de que se necesita de expertos en la materia para entender y gestionar los aspectos de los riesgos de TI, el conocimiento sobre la gestión del negocio es lo más importante. Los gerentes del negocio han de determinar lo que se debe hacer para apoyar su negocio y establecer los objetivos de TI. Por consiguiente, son responsables de la gestión de los riesgos asociados (2009, pág. 12).*

La gestión eficaz de los riesgos promueve la mejora continua y es una parte de las actividades diarias. Debido a la naturaleza dinámica del riesgo, gestión de riesgos es un iterativo y perpetuo proceso en curso. Cada cambio conlleva riesgos y/o oportunidades. Se presta atención a la evaluación del riesgo mediante métodos, funciones y responsabilidades, herramientas, técnicas y criterios en toda la organización (Isaca, 2009).

La aplicación de mejores prácticas para la gestión de los riesgos, proporcionará beneficios tangibles de negocios; por ejemplo, un menor número de eventos inesperados y fracasos, el aumento de la calidad de la información, una mayor confianza de las partes interesadas, menos preocupaciones de carácter regulatorio y nuevas iniciativas para el negocio apoyadas por aplicaciones innovadoras. Al igual que

cobit y val it, risk it, son un marco, no una norma. Esto significa que las organizaciones pueden y deben personalizar los componentes previstos en el marco para adaptarlos a la organización y su contexto (Isaca, 2009).

Considero importante, hacer mención especial a la posición de Isaca, frente al discernimiento de marcos y no de normas, caso contrario de: ISO 27001:2005 que sí es una norma. Los modelos o métodos que se han presentado son eso, un marco; la organización debe adaptarla a sus necesidades, no copiarlos. Esa debe ser la virtud que debe mostrar el gerente de seguridad; tener el suficiente conocimiento de la organización para implementar un modelo conforme y adecuado a las necesidades de la organización. En el tema de gestión de riesgos no todo está dicho; es un proceso que evoluciona constantemente y de forma rápida paralelo a las nuevas TI.

Ya para finalizar con el asunto de la gestión del riesgo, considero importante concluir con las estrategias más utilizadas para reducir (mitigar) el riesgo:

a. **Evitar riesgos:** Se debe salir de las actividades o de las condiciones que dan lugar a riesgo; eliminar la causa raíz. Se puede aplicar cuando no hay otra respuesta adecuada.
b. **Reducción de Riesgos / Mitigación:** Corresponde a las medidas tomadas para detectar el riesgo, seguido por la acción para reducir la frecuencia y/o el impacto de un riesgo. Al aplicar los controles sobre las causas del riesgo, se reduce la frecuencia del mismo o su materialización futura. La eficacia de esta estrategia, se puede medir por medio de los indicadores establecidos en los planes de control.
c. **Riesgo Compartido / Transferencia:** Transferencia o distribución de una parte del riesgo. Las técnicas más comunes son los seguros y la subcontratación. Sin embargo, el riesgo no se transfiere por completo al subcontratista o aseguradora, la empresa sigue asumiendo parte del riesgo y además se expone a otros riesgos relacionados con la subcontratación o aseguramiento.
d. **Aceptación del riesgo:** No se toman medidas relativas con un riesgo particular, y la pérdida es aceptada cuando se produce. Esto es diferente de ignorar el

riesgo. En ocasiones, se considera aceptar el riesgo cuando mitigarlo resulta más costoso que el mismo impacto que este pueda producir a la organización (Fernández, 2010) (Isaca, 2009).

CULTURA DE SEGURIDAD INFORMÁTICA

Antes de entrar en la cultura de la seguridad informática, me di a la tarea de buscar el significado de la palabra cultura. Wikipedia define cultura como: Término que tiene muchos significados interrelacionados. Alfred Kroeber y Clyde Kluckhohn (1952) compilaron una lista de 164 definiciones. Sin embargo, se asocia en dos sentidos básicos: Excelencia en el gusto por las bellas artes y las humanidades, también conocida como alta cultura; y conjuntos de saberes, creencias y pautas de conducta de un grupo social, incluyendo los medios materiales (tecnologías) que usan sus miembros para comunicarse entre sí y resolver sus necesidades de todo tipo. El diccionario de la lengua española (Espasa-Calpe, 2005) define cultura como el resultado o efecto de cultivar los conocimientos humanos; Conjunto de modos de vida y costumbres de una época o grupo social (cultura egipcia, popular…).

La cultura también se demuestra a través de valores, ideas, actitudes, principios, conocimientos, creencias y comportamientos adquiridos por los individuos, implícitos y explícitos que, se trasmiten de generación en generación. Ahora bien, ¿Cómo se puede aplicar a la seguridad informática?: Considero, debe estar conformada por un sentido de responsabilidad, respecto y cumplimiento de las normas y políticas definidas por la organización; que a la larga, lo que buscan es garantizar la confidencialidad, la integridad y la disponibilidad de la información. Marcos Gómez - (2008) subdirector de e-confianza del Instituto Nacional de Tecnologías de la Comunicación (INTECO), cree que la cultura de la seguridad informática tiene que formar parte de la política de actuación de nuestro entorno corporativo; considera además que: los componentes de

esta sociedad de la información tienen el deber de conocer el entorno tecnológico, sus usos y costumbres.

La principal preocupación que ve es: la de poder explicar y hacer comprender al capital intelectual, el por qué de las decisiones adoptadas en la seguridad informática, para que se entiendan como una mejora y no como un impedimento. Velar por la seguridad no tendría que ser una prioridad y una necesidad, sencillamente tendría que ser una mejora en la calidad ofrecida. No tendríamos que estar pendientes del mal que alguien interna o externamente pudiera causar. Por desgracia, la seguridad hoy es una prioridad y una necesidad que se le exige a las TI para ofrecer un servicio de calidad (Sebastia, s.f).

Se debe enfatizar en explicar el por qué, el cuándo y el cómo de la seguridad; en definitiva, crear una cultura de la Seguridad, inculcar unos conocimientos que actualmente son indispensables para realizar correctamente el trabajo de las personas que manejan herramientas informáticas y trabajan con datos e información. No se debe caer en la tentación de hacer cumplir las directrices de seguridad sin saber dar una explicación convincente, sin saber escuchar otras opiniones y sin analizar los inconvenientes que se pueden generar.

El desarrollo de la cultura debe llegar a toda la estructura de la organización, empezando por la alta gerencia, que es la que tiene que apoyar sin vacilaciones las políticas a seguir en materia de seguridad informática. Sus políticas deben ser flexibles, para ir adaptándola a los cambios de la propia organización, a la evolución de las tecnologías que el mercado cada día pone a nuestra disposición, y a las nuevas vulnerabilidades que puedan surgir en un mundo cambiante y evolutivo como el que hoy vivimos. Una vez establecidas las políticas, la cultura de seguridad exige que se den a conocer a la organización; es aquí donde se debe tener el conocimiento y la diligencia de saber explicar y hacer comprender el por qué se ha marcado esa política concreta y no otra. Una persona informada, formada y educada, sabrá comprender por qué se dictan ciertas normas y por qué es necesario cumplirlas, y no sólo por el único

motivo de: *porque alguien lo ha dicho*, *porque así está escrito*, o peor todavía, *porque sí* (Sebastia, s.f).

En la cultura de la seguridad informática no se trata de saber, como ocurría en la escuela, colegio o universidad para simplemente aprobar; lo que sugiere la cultura de la seguridad informática es el saber para poder razonar, valorar y, en consecuencia, actuar freten a las TI. Considero sumamente importante, que la organización vea, la cultura de la seguridad informática como una ayuda y no como una traba. El camino puede ser escabroso y hasta en ocasiones llegar a generar uno que otro disgusto dentro de la organización; pero creo firmemente, que es lo adecuado y conveniente junto a las soluciones de SW y HW para conseguir mejores resultados en la seguridad informática.

Finalizo el tema de la cultura de seguridad informática con este juicio: “Fuerza, valor, equilibrio y sensatez. Fuerza, para poder implantar las medidas de seguridad necesarias. Valor, para hacer que todos las cumplan. Equilibrio, para conseguir que estas medidas compaginen la seguridad con la agilidad en el trabajo. Sensatez, para que sean sólo las necesarias para conseguir los objetivos definidos en la política de seguridad” (Sebastia, s.f).

AUTO-SEGURIDAD INFORMÁTICA

El concepto de auto-seguridad informática, surgió inicialmente, de las vivencias laborales experimentadas desde mi sitial de ingeniero de sistemas, y continúo con la investigación y el análisis realizado de lo que es, y de lo que aporta la cultura de la seguridad y la gestión del riesgo, a la seguridad informática. Es un aporte personal de

lo que considero, es un tema, que debe formar parte junto al SW y HW; para mejorar el proceso de la seguridad informática en las organizaciones.

Como lo he mencionado durante el desarrollo del ensayo, las decisiones tomadas por la organización frente al SW y HW; son necesarias, indispensables, y se requieren para blindar a las organizaciones de los ataques a los cuales está expuesta la información; pero, me inquieta la idea qué, sin importar las acciones de seguridad que una organización pueda llegar a implementar y que involucran SW y HW; sin una cultura de la auto-seguridad informática que las complementen; dichas acciones, pueden llegar a perder el sentido para lo cual se desarrollaron.

Para soportar mi juicio sobre la auto-seguridad informática, considero primordial abarcar el tema del *autocontrol*, como fuente de mi discernimiento; tema que hizo parte, o en su defecto fue mencionado por todas las asignaturas vista durante la especialización en control interno y qué, despertó en mi gran interés, pues; lo considero uno de los factores a destacar para el logro de los objetivos de cualquier proceso.

Según Alfonso Alonso Parga Beatriz y Becerro de Bengoa - (2008) Editores y Coordinadores de la sección: Salud Mental en el Trabajo, de la revista de la salud mental - : El autocontrol, ¿autorregulación?, ¿autodisciplina?, ¿fuerza de voluntad?, todos ellos son conceptos nombrados a lo largo de nuestras vidas por muchos de nosotros, cada uno con una acepción distinta. Pero, ¿qué es exactamente el autocontrol?; los autores comienzan exponiendo el autocontrol como una *conducta controladora*, cuyo fin principal, es el de alterar la probabilidad de aparición de una *conducta problemática*, es decir, la capacidad que tiene el individuo de transformar una situación crítica que puede terminar en un problema, en una situación controlada. El autocontrol es una habilidad que perfectamente se puede formar, susceptible de aprendizaje, *siempre incitada y puesta en marcha por uno mismo* y nunca incitada por

otros, ya sean agentes externos o sociales. El autocontrol en una medida adecuada conduce al individuo hacia el bienestar, la seguridad y el equilibrio emocional. En definitiva, teniendo en cuenta todo lo anterior, podemos decir del autocontrol que:

a. Llevado a cabo de forma coherente y saludable facilita un completo equilibrio emocional.
b. Es autogenerado, es decir, no está incitado por variables externas (otras personas o situaciones), sino por uno mismo.
c. Conlleva el inicio de una conducta controladora cuyo principal objetivo es alterar la aparición de la conducta no deseada.
d. Es una habilidad que se puede formar
e. Y por supuesto, no supone restricción o evitación alguna

El Autocontrol lo definen también como: conjunto de prácticas que pueden aprenderse y desarrollarse con la experiencia. Por ello, el autocontrol es como un proceso a través del cual el individuo llega a ser el principal agente en la guía, regulación y dirección de las características de su propio comportamiento. El desarrollo de este comportamiento traerá consecuencias positivas que generan beneficios en donde se apliquen (USCO, s.f.).

El autocontrol, desde el punto de vista del sector público, lo definen como: control realizado por uno mismo. Implica dirigir la mirada hacia nosotros mismos, hacia nuestros comportamientos y actitudes, dejar atrás la tendencia de atribuir a las circunstancias externas, a las demás personas, al destino y al azar de las causas de nuestras decisiones, acciones y de los resultados que alcanzamos. Podría definirse el autocontrol como toda acción operativa ejecutada por los funcionarios, en el marco de la ética, la legalidad y la efectividad, tendiente a garantizar el cumplimiento de las políticas y estrategias de una organización (Aburrá, s.f.)

Con base a las conceptos expuestos hasta aquí de lo que es el autocontrol; se podría concluir que: la auto-seguridad aplicada a la informática es: el correcto comportamiento de los individuos frente a las TI; comportamiento que es formado por el propio individuo, y que nos debe llevar a una conducta controlada, para evitar situaciones de riesgo que pongan en peligro la conservación de la información de la organización. La auto-seguridad es además, una actitud, que debemos como seres inteligentes asumir con compromiso, ética y responsabilidad.

La auto-seguridad podría traer beneficios a las organizaciones tales como: mejora del nivel de convivencia, regulación y optimización de resultados en los procesos, trabajo con responsabilidad, fomento de la disciplina, la organización, la excelencia y el sentido de pertenencia; calidad de vida personal y laboral, y otras tantas mas. La auto-seguridad también promueve: hacer las cosas con calidad, oportunidad, transparencia y participación; mejoramiento continuo en la forma de realizar nuestra labor diaria; respeto por las normas y los demás.

Es tiempo de profundizar y de iniciar el trabajo, encaminado al desarrollo de una cultura de la auto-seguridad en las organizaciones; considero que un buen comienzo para este fin, se puede dar: dándola a conocer a todo el capital intelectual a través de escenarios de capacitación, inducción y re-inducción; generando los espacios de participación y reflexión; creando conciencia positiva por medio de: motivación, estímulos y reconocimientos. De la misma manera que el autocontrol exige valores; la auto-seguridad debe fomentarse bajo los valores como: compromiso, pertenencia, responsabilidad, solidaridad, lealtad, confianza, participación, honestidad, entre otros.

Para mostrar y evidenciar lo que la falta de auto-seguridad puede causar al interior de una organización, se describe a continuación, una situación que se presentó, donde se evidencia la falta de auto-seguridad en el no cumplimiento de las normas de seguridad que se establecen en las organizaciones; llegando incluso en ocasiones a pensarse, que sólo están para entorpecer y demorar nuestra labor. En cierto momento, dentro de una empresa dedicada al mercado bursátil; un corredor de bolsa (muy cercano a la familia) no siguió las normas de seguridad y consideró, que no veía problema alguno en darle a conocer, y permitirle el uso del usuario y la clave personal a su asistente. Era tanta la confianza que tenía depositada en él asistente, que no sólo le dio su usuario y clave, sino que tampoco se dio a la tarea al final del día, de revisar las transacciones de negociación realizadas en la bolsa a nombre de él. Las transacciones realizadas por el asistente eran de clientes que habían depositado su confianza en el corredor para que administrara sus recursos monetarios. Después de un tiempo, y cuando se presentó una crisis en las bolsas a nivel mundial, la gente por miedo fue a retirar sus inversiones, pero no estaban donde las habían dejado. El asistente, abusando de la confianza del corredor, utilizó el usuario y la clave, para desviar las inversiones de algunos clientes, a mercados de alto riesgo como se dice en el argot del medio bursátil. No sólo se habían perdido los recursos, sino qué, los clientes debían saldos a la misma entidad bursátil, ya que se había utilizado la figura de apalancamiento que consiste en realizar operaciones de inversión superiores a los recursos disponibles, con líneas de crédito hechas por la misma bolsa. Las inversiones no contaban con la autorización y el aval de los clientes.

Después de descubierto el fraude, finalmente la aseguradora, la compañía y el corredor tuvieron que responder por las pérdidas ocasionadas a los clientes. El asistente fue retirado de su trabajo sin ninguna falta, por miedo a demandas que clientes pudieran hacer en contra de la compañía, por haber permitido que una persona sin el perfil de corredor hubiese manejado sus recursos. Las consecuencias de esta falta de auto-seguridad fueron: Problemas de imagen y credibilidad frente a sus clientes, pérdidas económicas, demandas, pérdida de clientes, en fin.

Así como este caso, hay muchas historias que por la falta de auto-seguridad, ponen en riesgo la estabilidad de las organizaciones. El siguiente informe, nos habla del porcentaje de ataques que se presentan desde el interior de las mismas organizaciones:

> *Un estudio publicado en 2005 por PricewaterhouseCoopers y CIO, The Global State of Information Security 2005, reveló que el 33 % de los ataques contra la seguridad de la información fueron perpetrados por empleados internos, mientras que el 28 % procedían de antiguos empleados y socios. Dar más importancia a las amenazas externas que a los peligros internos es un error, y puede acrecentar sobremanera la vulnerabilidad de las defensas de una organización. La empresa HSBC Electronic Data Processing (India) Private, de servicios de asistencia al cliente y procesamiento de tareas administrativas, informó en 2006 que un empleado, como parte de una red de ladrones más grande, había accedido a información de tarjetas de débito de clientes y la utilizó para defraudar 425.000 dólares EE.UU. a 20 clientes del Reino Unido. Este incidente es uno solo de los muchos que se produjeron en los últimos escasos años. La Privacy Rights Clearinghouse mantiene una lista con cientos de violaciones de datos ocurridas en Estados Unidos desde el caso flagrante de infracción que tuvo lugar en ChoicePoint en febrero de 2005. Muchas de estas infracciones se cometieron desde dentro de la organización, por personas a las que la lista se refiere como miembros que no son honrados (IBM, 2006).*

Definitivamente, y después de realizada la investigación de la gestión de riesgos y de la cultura de la seguridad en la informática; puedo afirmar desde mi perspectiva personal, teniendo eso sí, respeto por lo que puedan pensar otros, qué: por más decisiones que se tomen en cuanto a SW y HW para proteger uno de los activos más valioso de las organizaciones, como lo es la información; nada puede garantizar en un 100, qué no se presenten situaciones de riesgo que puedan atentar contra la confidencialidad, la integridad y la disponibilidad de la información. Situación de riesgo que se puede elevar aún más, si no se cuenta con una política que fomente la cultura de la auto-seguridad a todo nivel dentro de la organización. Fomentar la cultura de la auto-seguridad debe estar principalmente influenciada por el compromiso indispensable de la alta dirección, quienes deben estar comprometidos en todo momento, siguiendo con el resto del capital humano como: supervisores, coordinadores y demás empleados. La clave del éxito en la cultura de la auto-seguridad no depende exclusivamente del apoyo de la alta dirección, sino qué, es fundamental que nosotros, con seres pensantes e inteligentes, la asumamos como propia, y necesaria para el fortalecimiento de la seguridad informática en la TI. Finalizo retomando el juicio: “En las decisiones de SW y HW, poner la carreta delante de los bueyes puede ser fatal**”** (Honorato, s.f.)

REFERENCIAS

Aburrá, Á. M. (s.f.). *areadigital*. Recuperado el 03 de 2012, de www.areadigital.gov.co

ALFA-REDI. (2002). *Construyendo la Sociedad de la información*. Recuperado el 03 de 2012, de www.alfa-redi.org

Bloom, A. D. (1988). *The Closing of the American Mind.*

Cano, J. J. (Abril-Junio de 2006). *Asociación Colombiana de Ingenieros de Sistema*s, Revista SISTEMAS, Asociación Colombiana de Ingenieros de Sistemas (ACIS), No. 96. Recuperado el 03 de 2012, de Inseguridad Informática y Computación Anti-Forense: Dos Conceptos Emergentes en Seguridad de la Informacion: www.acis.org.co

Dutra, E. (2008). Gestión de Riesgo en Procesos de Negocios. *Revista Hakin9* (33).

Erb, M. (s.f.). *WordPress.com*. Recuperado el 2012, de Gestión de Riesgos en la Seguridad Informática: http://protejete.wordpess.com

Fernández, L. A. (2010). *La Gestión del Riesgo Operacional-De la teoría a su aplicación.* Mexico: Limusa - Noriega Editores.

Honorato, J. (s.f.). *Gestión del Riesgo en la Seguridad Informática: El Nuevo Escenario del Control.* Recuperado el 03 de 2012, de www.cidemconsult.cl

IBM. (09 de 2006). *IBM*. Recuperado el 03 de 2012, de Detener los ataques internos: cómo pueden proteger las organizaciones su información confidencial: www.-05.ibm.com

Isaca. (2009). *Marco de Riesgos de TI.* Recuperado el 03 de 2012, de ISACA: www.isaca.org

ISO27001, N. (2005). *ISO 27001 - Sistemas de Gestión de la Seguridad de la información.* Recuperado el 03 de 2012, de www.iso27000.es

Sebastia, J. S. (s.f). La seguridad Informatica: ¿Qué preocupa? *SIC* (61).

USCO. (s.f.). *Oficina de Control Interno*. Recuperado el 03 de 2012, de www.usco.edu.co