CONCIENCIACIÓN EN SEGURIDAD DE LA INFORMACIÓN, LA ESTRATEGIA PARA FORTALECER EL ESLABÓN MÁS DÉBIL DE LA CADENA

Víctor Enrique Martínez Saravia

Proyecto Final para optar al Título de **ESPECIALISTA EN DIRECCIÓN ESTRATÉGICA DE EMPRESAS**

ÁREA DE EMPRESA, DESARROLLO DIRECTIVO Y RECURSOS HUMANOS, FUNDACIÓN UNIVERSITARIA IBEROAMERICANA

Lugar de Realización: Cartagena de Indias, Colombia.

BOGOTÁ D.C., COLOMBIA

ENERO DE 2010

CONCIENCIACIÓN EN SEGURIDAD DE LA INFORMACIÓN, LA ESTRATEGIA PARA FORTALECER EL ESLABÓN MÁS DÉBIL DE LA CADENA

Víctor Enrique Martínez Sarabia

……..

Director de Tesis: Andrés Alberto Osorio Londoño, Ingeniero Industrial, Ms. Recursos Humanos y Gestión del Conocimiento

Resumen

La Información es un fenómeno que proporciona significado o sentido a los elementos de la sociedad. Además de eso, la Información, después de las personas, es el tesoro más importante de toda organización y por lo tanto, se le debe dar un tratamiento seguro. Sin importar el cargo que se ocupe en una compañía, se maneja Información que es esencial para los intereses de la misma.

La seguridad se podría definir como la sensación de bienestar de algo; una propiedad intangible que nos indica que ese algo está libre de peligro, daño o riesgo. Ese algo, en este caso particular, es la Información.

Un usuario común puede ver la seguridad como una serie de barreras para hacer lo que considera que está bien y que probablemente puede afectar los intereses de la compañía. Es por esto que no se debe descuidar el hecho de que la inseguridad informática es un elemento propio de la dinámica de las organizaciones en cada uno de sus procesos.

La seguridad de la Información es para muchas organizaciones la asignatura pendiente, porque consideran prioritario invertir en estrategias de mercadeo y ventas, o quien sabe en qué. El hecho, es que la Seguridad de la Información es una estrategia tan necesaria como otras.

En este documento, se propone una solución a los problemas de seguridad de la información de una compañía, corresponde a la implantación de un programa de concienciación y sensibilización en Seguridad que incorpore buenas prácticas para que los usuarios en sus actividades diarias, se responsabilicen del cuidado de los activos de Información, previniendo y gestionando los riesgos de la organización en la vida digital y permitiéndole a la compañía diferenciarse de sus competidores.

Prefacio

Este trabajo es el resultado del proyecto final de especialización, llevado a cabo sobre la construcción de un modelo de Seguridad de la Información que permite adaptarse a las contingencias que en esta materia, enfrentan las organizaciones contemporáneas. También, esta tesis es el requisito último de la especialización en dirección estratégica de la Fundación Universitaria Iberoamericana.

Víctor Enrique, propone un modelo de Seguridad de la Información revolucionario, en donde se atacan todas las variables problemáticas que se desprenden dentro de la gestión de la información al interior de cualquier organización. Es de exaltar, el interés por parte del autor para generar una propuesta independiente, partiendo de todo el conocimiento tácito acumulado durante su experiencia profesional, que sumado a su interés y pasión dentro del área de estudio han generado como resultado un modelo de gestión de la Seguridad de la Información consistente, para ser aplicado dentro de cualquier giro de negocio.

En consecuencia, el proyecto presente tiene como característica fundamental la superación de los elementos técnicos dentro de la aplicación de la Seguridad de la Información, dejando claro que la Gestión del Talento Humano como ente forjador de cultura, tiene un rol crucial dentro de los planteamientos y criterios que deben proponerse a partir de cualquier modelo. Por otra parte, el autor domina satisfactoriamente las limitaciones de información que se presentaron en el camino, entrevistándose y generando contacto con expertos dentro del área, lo que a la postre se evidencia en resultado que se expone en las líneas siguientes.

TABLA DE CONTENIDO

CAPÍTULO 1

MARCO INTRODUCTORIO

1.1 Introducción

Cuando se habla de Seguridad de la Información (SI), es necesario tener en cuenta los tres pedestales vitales que la sostienen: los procesos corporativos, la tecnología que los soportan y las personas que los realizan. Pero, para la mayoría de las empresas, son solo dos, y esto hace que la estructura se vuelva frágil, resultando en que las personas se conviertan en el eslabón más débil de la cadena de seguridad dentro de las organizaciones.

Un usuario común puede ver la seguridad como una serie de barreras para hacer lo que considera que está bien y que probablemente puede afectar los intereses de la compañía. Además, puede llegar a pensar que los administradores de tecnologías de la información son paranoicos y se aprovechan para maximizar las contadas situaciones de riesgo dadas. En este orden de ideas, lo anterior puede resultar verídico; sin embargo, lo que acontece es que los administradores son conscientes de las amenazas que hay en el entorno, y por otra parte, entienden que la tecnología ha acortado las distancias.

¿Cuántos de esos usuarios no han pensado también que la máquina propia es poco importante para que un atacante pueda tener interés en ella? Por esta razón, a estos usuarios hay que hacerles ver que este atacante no sabe quién está al otro lado del monitor, por lo que cualquier objetivo (en principio) es tan importante o no como cualquier otro. También hay que hacerles ver, que estas

personas tienen un motivo para llevar a cabo la acción, unas creencias (lógicas o no) que tienen sentido para dicho atacante, que buscan una oportunidad, momento o situación para realizar la acción, y unos instrumentos que son los tres pilares mencionados anteriormente.

Tampoco se debe descuidar el hecho de que la inseguridad informática es un elemento propio de la dinámica de las organizaciones en cada uno de sus procesos. Mientras las empresas pretenden ser cada vez más seguras, la problemática de la inseguridad sigue creciendo. Durante los últimos años, los robos de información y la exposición de datos, fueron las manifestaciones más visibles de la inseguridad (Attriton, 2009). Y esto no se debe a falta de controles (puesto que los hay), sino a que nuestra estructura de seguridad tiene una base sobre la cual cojea.

Por lo anterior, se puede decir que para estudiar la seguridad, primero se debe entender la inseguridad, porque a diferencia de la seguridad, la inseguridad es objetiva. La forma mejor de entender la inseguridad es a través de un programa adecuado de concienciación de los usuarios en el tema de seguridad, debidamente apoyado en las políticas corporativas sobre el tema y con un adecuado proceso de seguimiento y actualización. En este documento se describen los diferentes aspectos que son necesarios afrontar para el diseño, la elaboración y la implementación de un programa de concienciación en seguridad que permita garantiza una ***Cultura de Seguridad de la Información.***

1.1. Justificación

Si se define textualmente, la Información es un fenómeno que proporciona significado o sentido a los elementos de la sociedad. En sentido general, la Información es un conjunto organizado de datos procesados, que constituyen un mensaje sobre un determinado ente. En consecuencia, un dato deja de serlo, una vez que establece un sentido, un valor semántico para el usuario, mediante asociaciones lógicas entre sí, y otros datos sueltos que a su vez carecen de valor individualmente. Por otra parte, los datos se perciben, se integran y generan la Información necesaria para producir el conocimiento que finalmente permite tomar decisiones para realizar las acciones cotidianas que aseguran la existencia. La Información por tanto, procesa y genera el conocimiento humano. En el proceso de toma de decisiones un dato no sirve, necesitamos Información (Melzner, 2009).

Además de la definición anterior, la Información, después de las personas, es el tesoro más importante de toda organización y por lo tanto, se le debe dar un tratamiento seguro. Sin importar el cargo que se ocupe en una compañía, se maneja Información que es esencial para los intereses de la misma.

Si nos atenemos a la definición de la Real Academia Española, seguridad es la "cualidad de seguro", siendo seguro "libre y exento de todo peligro, daño o riesgo". A partir de estas definiciones, se podría definir entonces la seguridad como la sensación de bienestar de algo; una propiedad intangible que nos indica que ese algo está libre de peligro, daño o riesgo. Ese algo, en este caso particular, es la Información. ***"Siempre hay que tener en cuenta que la Seguridad comienza y termina con personas"*** (Segu-info, sin fecha).

A través de un estudio de ***Datapro Research Corp.*** se pudo establecer que los problemas de seguridad en sistemas responden a la siguiente distribución:

- Errores de los empleados 50%.
- Empleados deshonestos 15%.
- Empleados descuidados 15%.
- Otros 20% (Intrusos ajenos a la Empresa 10%; Integridad física de instalaciones 10%).

Se puede notar que el 80% de los problemas, son generados por los empleados de la organización, que se podrían tipificar en tres grupos grandes:

- Problemas por ignorancia.
- Problemas por haraganería.
- Problemas por malicia.

Entre estas razones, la ignorancia es la más fácil de direccionar. No obstante, desarrollando tácticas de entrenamiento y procedimientos formales e informales son fácilmente neutralizadas. Los usuarios, además, necesitan de tiempo en tiempo, que se les recuerden cosas que ellos deberían conocer (Manual de seguridad en Redes, ArCERT).

Pero el asunto no es tan fácil, porque en Colombia existen pocas organizaciones que cuenten con un programa concienciación de usuarios. En algunos casos, las intenciones son puntuales, por lo que no llegan a tener la continuidad necesaria como lograr algún cambio de actitud en los usuarios.

Como diría Christian Linacre, Gerente de Seguridad de Microsoft Latinoamérica: *"La seguridad es tan fuerte como el eslabón más delgado de la cadena"*. Por consiguiente, los usuarios son el punto más vulnerable en la cadena de seguridad, puesto que su desconocimiento de unas prácticas buenas de seguridad puede ocasionar incidentes que ponen en riesgo la confidencialidad e integridad de Información sensible. En consecuencia, los usuarios son la herramienta primordial para proteger la Información, porque se pueden establecer todo tipo controles técnicos. Sin embargo, sin la colaboración de los usuarios no se logrará la minimización los riegos.

Si bien la legislación ha mejorado a favor de los propietarios de la Información, se puede concluir que en un 100% no es específica y actualizada para las nuevas tecnologías. Por ejemplo, en las situaciones que aparecen, se aplica el código penal vigente y no siempre es posible ajustar o adaptar las leyes a los delitos informáticos nuevos. Los ***ciberdelincuentes*** no se sienten tan vigilados, pero sí más protegidos tras el anonimato que ofrece Internet.

Por las razones anteriores, se entiende que la solución a los problemas de seguridad de la información de una compañía, además de la aplicación de herramientas técnicas de control (antivirus, antispam o cortafuegos), corresponde a la implantación de un programa de concienciación y sensibilización en Seguridad que incorpore buenas prácticas para que los usuarios en sus actividades diarias, se responsabilicen del cuidado de los activos de Información, previniendo y gestionando los riesgos de la organización en la vida digital y permitiéndole a la compañía diferenciarse de sus competidores.

1.2.1 Viabilidad

Este proyecto se considera pertinente y relevante porque permite aprovechar en el terreno práctico lo aprendido durante el transcurso de la especialización y además, porque lo que se pretende realizar, proporcionará a diferentes empresas una herramienta económica para dar solución al problema de pérdida de Información. Se debe recordar, que la implementación de un sistema de gestión de seguridad de la información implica invertir tiempo y dinero en un marco de trabajo complejo, que si bien trae resultados benéficos y específicos, no todas las empresas lo entienden como una necesidad estratégica.

La seguridad de la Información es para muchas organizaciones la asignatura pendiente, porque consideran prioritario invertir en estrategias de mercadeo y ventas, o quien sabe en qué. El hecho, es que la Seguridad de la Información es una estrategia tan necesaria como otras.

En conclusión, la realización de este proyecto tiene total viabilidad, porque se basa en hechos reales, que se apoyan en la experiencia laboral del investigador, quien cuenta con los recursos de Información necesarios para la realización del mismo.

1.3 Descripción del área problemática

Con el paso del tiempo, se puede evidenciar que la mayor parte de las organizaciones, sin importar el tamaño, ni la industria en la que se desenvuelvan,

logran acumular gran cantidad de datos de sus empleados, proveedores, clientes, productos, proyectos investigación, su situación financiera, entre otros. El volumen más grande de estos datos, es recolectado, procesado, almacenado y puesto a la disposición de sus usuarios, como Información visible y disponible a través de redes de computadores.

Es preocupante entonces, como muchas empresas pueden perder el negocio e ir a la quiebra, gracias a la falta de credibilidad de sus clientes y a un sin número de demandas legales que pudieron evitarse controlando el manejo de la Información sensible como datos de clientes, decisiones estratégicas, estados financieros y estudios sobre líneas nuevas de productos, sin haber permitido que se volviera pública de forma no autorizada. Es por esto, que desde el punto de vista del investigador, proteger la Información confidencial es un requisito tan importante como cancelar la nómina o los impuestos de la compañía.

Como diría el Doctor Jeimy Cano, la única constante en el mundo de la seguridad de la información, es la ***inseguridad***. En este sentido, las organizaciones trabajan día tras día para tratar de eliminar o mitigar las vulnerabilidades posibles que se presentan en las infraestructuras tecnológicas o en los procedimientos que apoyan al negocio. Se hace evidente entonces, que la inseguridad informática es un elemento propio de la dinámica de las organizaciones en cada uno de sus procesos. Mientras las empresas buscan alcanzar un nivel superior de seguridad, cada vez más se encuentran con la problemática de la inseguridad, puesto que los procesos en sí mismos, al ser redes de comunicaciones y acuerdos entre personas, tecnologías y normas, establecen relaciones y distinciones que generalmente no son distinguibles, haciendo de la labor de aseguramiento de la Información más que una función

tecnológica, una función que corresponde a las acciones humanas y procesos administrativos y estratégicos.

Durante el 2006, los robos de Información y la exposición de datos (Attrition, 2009), fueron las manifestaciones más sobresalientes de la inseguridad. Si se mira con detalle estas dos consideraciones, este fenómeno no responde necesariamente a un problema de seguridad tecnológico, sino a una situación procedimental y de concienciación. Los intrusos saben y comprenden que detrás de las infraestructuras de seguridad de la información está ese elemento que las organizaciones hoy por hoy se resisten a entrenar, a formar, a hacer parte formal de su modelo de seguridad, los usuarios (Cano, 2007).

¿Cuántos de nosotros hemos visto a empleados escribir las contraseñas en un papel? ¿Cuántas veces se ha solicitado a compañeros digitar su contraseña en un sistema y en lugar de ponerla nos ha dicho “Es mi nombre” y después de algunos días al volver a pedírsela nos ha dicho “Sigue siendo la misma”? ¿Cuántas veces hemos pasado al lado de un computador libre, con la sesión iniciada o hemos ido a la impresora a recoger un documento y nos encontramos con documentación olvidada por algún compañero? ¿Cuántas veces hemos escuchado “Para qué tantos controles, a quién le va interesar lo que estoy haciendo”?.

Lo anterior, corresponden a ejemplos de cómo la seguridad en la mayoría de las empresas está siendo afectada desde los aspectos más ***básicos***, como las contraseñas, la protección de los puestos de trabajo y el cuidado de la Información.

Consecuentemente, la mayoría de los usuarios emplean hábitos de trabajo poco seguros que ponen en peligro la confidencialidad, disponibilidad e Integridad de la Información, por lo que muchas veces las organizaciones los consideran tan obvios y sencillos, que no hacen el mínimo esfuerzo por instruir a sus empleados.

Por otra parte, las compañías, delegando esta responsabilidad al departamento de Informática, suelen esforzarse en la adquisición de mecanismos y herramientas adecuadas para que un atacante no pueda dañar ningún equipo, colocando bloqueos a través de cortafuegos y herramientas de control de acceso, implementando los antivirus mejores, entre otros.

No obstante, algo curioso de todo esto, es que el conocimiento de los usuarios es algo que se supone, y se da por hecho que funciona según lo esperado: *¿Cómo no va a saber un usuario que su contraseña no debe ser escrita en un papel cuando se le ha dicho que es secreta? ¿Cómo no va a saber un usuario que su contraseña no puede ser su nombre o apellido?*

Aunque pueda parecer imposible, lo anterior sucede, pues la Información constituye un recurso que, en muchos casos, no se valora adecuadamente debido a su intangibilidad, cosa que no ocurre con los equipos, la documentación o las aplicaciones. Y es en este punto donde surgen creencias erróneas, muy comunes a la mayoría de usuarios: *"Mi sistema no es importante para un atacante"; "El antivirus me mantiene protegido"'; "Sé que tengo que bloquear mi sesión pero a mis compañeros no le interesa lo que yo hago"*.

Lo ideal sería que los datos no tuvieran ningún valor, sino que simplemente fueran entradas simples de un proceso productivo. Lamentablemente, esto es solo una utopía, por ejemplo: ¿Cómo le restamos el valor que tiene la Información financiera de una compañía o la vida crediticia de un ciudadano?

Otra alternativa constituye en que cada persona fuera consciente de la importancia que tienen los datos y la Información que maneja a diario, sin importar el entorno donde se desenvuelva. Para muchos es lógico que no se debe revelar Información personal por teléfono, pero para otros no. Lo mismo sucede en el campo laboral. Sería bueno que todos los empleados supieran que son responsables del trato que se le da a la Información que tienen a su alcance, pero como en el terreno práctico no sucede, es obligación de las directivas instruirlos con respecto a este tema.

Cuando se habla de seguridad de la información (SDLI), muchas son las propuestas que surgen como respuesta a la protección de la Información. Algunas de ellas, se describen a continuación.

ISO/IEC 27001:2005 (Information technology - Security techniques - Information security management systems - Requirements): es un estándar que especifica los requisitos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un sistema de gestión de seguridad de la información en el contexto de los riesgos de negocios generales de la organización. Especifica los requisitos para la aplicación de controles de seguridad adaptados a las necesidades de las organizaciones individuales o partes del mismo.

El *Intituto Nacional de Estandares y Tecnología* (*NIST*): hace parte del gobierno de los Estados Unidos y tiene por objetivo asegurar la competencia industrial a través de la elaboración de normas que permitan generar nuevos proyectos tecnológicos, y medir los ya existentes. La serie 800 de documentos del NIST, son dedicados a la protección de la Información.

COBIT (Control Objectives for Information and related Technology): es el resultado de una investigación con expertos de varios países, desarrollada por la *Information, Systems Audit and Control Association* (ISACA), y ha sido desarrollada como un estándar generalmente aplicable y aceptado para buenas prácticas de seguridad y control en tecnología de información (TI).

Ahora, siendo realistas, no todas las organizaciones marchan al ritmo de estas melodías.

Consiguientemente, una alternativa sencilla y económica, corresponde a un programa de concienciación que permita mostrar a los empleados con ejemplos del día a día, qué debería hacer y qué no, con la Información que se le ha suministrado para el cumplimiento de sus labores y aquella que si bien no se ha suministrado, está a su disposición, por cualquier motivo.

Por todas las situaciones mencionadas, y por muchas otras que no se alcanzan a caracterizar, es necesario que las empresas, además de definir políticas de seguridad de la información como herramienta de protección de su tesoro más preciado, implementen un programa de concienciación en seguridad de la Información, donde se sensibilice al usuario final, influenciándolo a sentirse

parte de esta seguridad. También, el programa debe hacerle saber al talento humano que sus actos son decisivos para que la seguridad se mantenga o se deteriore de forma catastrófica; pero sobre todo, que les haga entender que la seguridad no se consigue sólo con el departamento que lleva este nombre, sino que cada persona que trabaja en la compañía, hace parte de la seguridad de dicha organización, por lo que seguridad debe formar parte de su sistema de trabajo.

Para la realización de este proyecto, por haber hecho aportes importantes a esta temática, se seguirá la línea conceptual del Doctor Jeimy Cano, quien es miembro de la red Iberoamericana de Criptología y Seguridad de la Información, y quien además se desempeña como docente universitario, en las áreas de Seguridad informática, computación forense y derecho informático de la Universidad de los Andes, Colombia.

1.3.1 Proyección gráfica del problema

En la **figura 1.1**, se proyecta el problema antes descrito. Ésta, presenta un escenario real, muy frecuente y muchas veces no tan explícito, con respecto a cómo la fuga de Información, puede desencadenar en la pérdida de valor de una compañía.

También, permite demostrar que hay muchos medios por los cuales esta Información se puede perder, como son los clientes, los proveedores y los mismos empleados. Son estos últimos los directa o indirectamente responsables de la pérdida de Información. Está expresado de esta forma, pues si bien son los

autores materiales del hecho, tal vez la responsabilidad no recae completamente sobre ellos. Dicho por el mismo Doctor Cano:

> *"Los intrusos saben y comprenden que detrás de las infraestructuras de SDLI, está ese elemento que las organizaciones hoy por hoy se resisten a entrenar, a formar, a hacer parte formal de su modelo de Seguridad, los usuarios".*

Por consiguiente, la pérdida de valor de una compañía puede ser causada por situaciones tan simples y que se hubiesen podido evitar con un programa de concienciación, como son bloquear las sesiones de usuario al abandonar los equipos de cómputo, establecer contraseñas complejas cambiándolas periódicamente, el uso de dispositivos de almacenamiento extraíbles y el envío de Información propiedad de la compañía a correos personales; pero sobre todo, con la definición de políticas, normas, procedimientos, programas de control y herramientas que garanticen la confidencialidad, Integridad y disponibilidad de la Información.

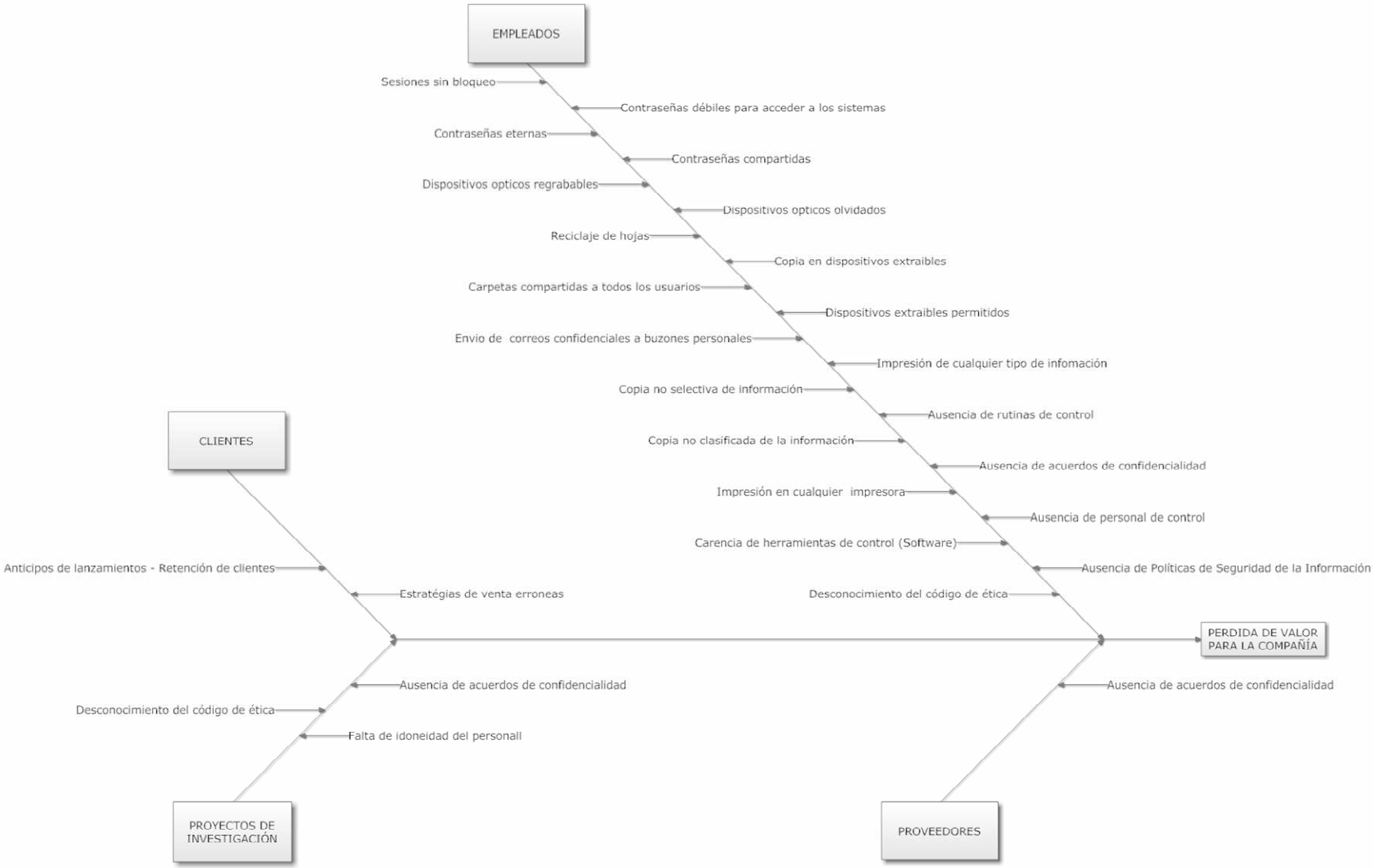

Figura 1.1: Proyección Gráfica del Problema, **Fuente:** Propia.

1.4 Objetivos

1.4.1. Objetivo General

Elaborar un programa de concienciación en Seguridad de la Información que pueda ser usado por las empresas, para garantizar un tratamiento seguro de la Información sensible y confidencial de la compañía, evitando se vuelva pública de una manera no autorizada.

1.4.2. Objetivos Específicos

- Identificar aquellas actuaciones que pueden provocar un problema de seguridad para la protección de los activos de Información de cualquier empresa, mostrando la forma correcta de actuar ante una lista de las situaciones habituales en el trabajo diario.

- Conocer las buenas prácticas para el uso seguro de la tecnología.

- Diseñar una forma de explicar a los funcionarios de la compañía, los principios fundamentales para el cuidado de la Información.

- Buscar la manera correcta de generar conciencia sobre la importancia de la seguridad de la Información de la compañía, basados en la premisa de que su protección es responsabilidad de todos.

- Divulgar las definiciones hechas por la dirección, a través de las Políticas de Seguridad de la Información.

- Adquirir técnicas para prevenir el acceso de terceros a Información confidencial.

- Reconocer situaciones donde se violan medidas de seguridad a través de técnicas de ingeniería social.

- Comprender las amenazas que acarrean los sistemas de mensajería instantánea y las redes P2P (Igual a Igual).

1.5 Antecedentes

Al realizar consultas en las bibliotecas de las Universidades de la región y bibliotecas virtuales (Internet), con respecto a las investigaciones previas, se encontraron los proyectos siguientes que aportan aspectos significativos relacionados con el presente proyecto de investigación:

HINSON, G. CONCIENTIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN EN SIETE PASOS

En el 2005, el Doctor Gary Hinson, quien se desempeña como consultor en Gobierno de IT publicó un artículo donde define un listado de etapas que sugiere seguir para asegurar un buen control de la seguridad de la información. Este

documento incentiva al desarrollo de este programa, proponiendo una guía a seguir para garantizar la efectividad y continuidad del mismo.

VILLALÓN, A. EL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN: CALIDAD DE LA SEGURIDAD

En 2005, Antonio Villalón, miembro del grupo español de monitorización de la Actividad de Negocio, s2grupo, concluye en su estudio que los problemas de seguridad informática de las empresas, rara vez son técnicos, por lo que suelen ser situaciones que corresponden a problemas de gestión. Concluye también, que la gestión debe contemplar la mejora continua del sistema porque todo evoluciona, y la seguridad no es un producto, es un proceso.

ARISTIZÁBAL, A y LÓPEZ, H. USING PROCESS CALCULI TO MODEL AND VERIFY SECURITY PROPERTIES IN REAL LIFE COMMUNICATION PROTOCOLS.

En 2006, estudiantes de la Pontificia Universidad Javeriana, contextualizaron en su proyecto, que la seguridad informática puede considerarse como una de las características más importantes en las comunicaciones actuales. La necesidad de transmitir Información crítica de manera segura utilizando canales públicos. ha cobrado especial importancia en el contexto de los sistemas de cómputo globales como Internet.

NIÑO D. y SIERRA, A. CENTRALIZACIÓN DE REGISTROS DE EVENTOS

En 2007, los estudiantes de la Pontificia Universidad Javeriana, Diana Mejía y Alejandro Sierra, propusieron una guía metodológica pensada para pequeñas y medianas empresas, que permite llevar al administrador de la red paso a paso, hacia la centralización de los registros de eventos de seguridad.

MIERES, J. ATAQUES INFORMÁTICOS, DEBILIDADES Y CONTRAMEDIDAS

En 2009, Jorge Mieres, miembro del grupo de Seguridad de *ESET* Latinoamérica, detalla varios de los ataques informáticos a los que se ven expuestos los usuarios, y explica que muchos de estos ataques son producto de la ingenuidad del usuario final, dentro de un proceso de persuasión conocido como Ingeniería Social.

1.6 Alcance

En la actualidad, Internet se ha convertido en el medio de comunicación masivo más poderoso y peligroso que existe. Es imposible saber a ciencia cierta la cantidad exacta de Información que viaja por Internet, y mucho menos la velocidad con que es transmitida.

Esto aumenta la posibilidad de que Información sensible, se propague sin los debidos controles, causando así, inconvenientes que en muchos casos se resumen en pérdidas de dinero.

En consecuencia, el trabajo se centrará en el campo de la seguridad de la Información, porque identificará aquellas actuaciones que pueden provocar un problema de seguridad para la protección de los activos de Información de cualquier empresa, estableciendo la forma correcta de actuar, ante una lista de las situaciones laborales habituales, a través de la elaboración de un manual de buenas prácticas para el uso seguro de las Tecnologías de la Información.

Por último, este proyecto permitirá a diferentes compañías, explicar a sus funcionarios los principios fundamentales para el cuidado de la Información, sensibilizándolos sobre la importancia de la seguridad de la información de la compañía, basados en la premisa de que su protección es responsabilidad de todos.

CAPÍTULO 2

REVISIÓN LITERARIA: ESTRATEGIA DE SEGURIDAD, LA ASIGNATURA PENDIENTE

2.1 Introducción

La teoría que explica el problema que se soluciona este proyecto final, se enmarca dentro de las temáticas de la administración y dirección de empresas, y gestión estratégica de los recursos humanos, parte de las cuales serán tomadas de los contenidos teóricos cursados dentro de la Especialización en Dirección Estratégica. Con respecto a la temática de la seguridad informática, es clave usar el aporte desarrollado por Antonio Villalón en su libro ***Seguridad de Unix y Redes***; llegando finalmente a enfatizar en el concepto de la Seguridad de la Información como eje central de este proyecto.

2.2 Teoría Empresarial

La empresa se puede definir como una unidad económica de producción, característica de la economía de mercado, en la cual, combinando los factores capital (herramientas, máquinas entre otros) y trabajo, se realizan actividades de producción, distribución o realización de servicios, organizados adecuadamente con objeto de obtener, con riesgo, un beneficio o renta.

Actualmente, se ha complementado su objeto único de obtener beneficios, por el de alcanzar unos objetivos globales determinados:

- Económicos: obtener beneficios.
- Técnicos: producir bienes necesarios a la sociedad y su entorno.
- Humanos: satisfacer a los trabajadores a través de retribuciones adecuadas, trato correcto, e integrar a los mismos en la empresa.
- Sociales: atender a las necesidades de la sociedad a través de los impuestos.

De forma general, las características principales que definen a toda empresa son:

- La empresa es un conjunto de factores de producción, entendiendo como tales los elementos necesarios para producir (bienes naturales o semielaborados, factor trabajo, energía, maquinaria y otros bienes de capital), factores mercadotécnicos, pues los productos no se venden por sí mismos, y factores financieros, pues para coordinar estos factores es preciso efectuar inversiones y éstas han de ser financiadas de algún modo.

- Toda empresa tiene fines u objetivos, que constituyen la propia razón de su existencia. Tradicionalmente, en el sistema de economía de mercado estos fines se han asociado a la maximización del beneficio.

- Los distintos factores que integran la empresa se encuentran coordinados para alcanzar sus fines. Sin esa coordinación, la empresa no existiría, puesto que se trataría de un mero grupo de elementos sin conexión entre sí

y por tanto, incapaces de alcanzar objetivo alguno. Esa coordinación hacia un fin, la realiza otro factor empresarial que es la dirección de la empresa. El factor directivo planifica la consecución de los objetivos, organiza el recurso humano, se encarga de que las decisiones se ejecuten y controla las posibles desviaciones entre los resultados obtenidos con respecto a los deseados.

2.2.1 Dirección estratégica

El concepto de "estrategia" es muy antiguo. El filósofo chino Sun Tzu, quien escribió Ping-fa en el año 300 A.C., describía el arte de la estrategia como aquel que se basaba en alcanzar victorias a través del análisis, el cálculo y las maniobras a realizar antes de la batalla.

Surgido en el ámbito militar desde tan antigua fecha, sin embargo, el concepto de estrategia es muy joven y reciente en el ámbito empresarial. Así, se reconoce que el primer modelo de análisis estratégico empresarial nace en la Harvard Business School en 1960. Y la concepción desarrollada de Dirección estratégica (Strategic Management), donde en esta contemporaneidad se inserta la estrategia, es apenas de la década del 70 del Siglo XX.

El estudio de la estrategia y la dirección estratégica hoy día constituye un aspecto fundamental en todo el sistema de cualquier organización, no sólo por lo que representa para su estructura organizacional interna, sino también por lo que le permite obtener con relación al conocimiento y trabajo en su entorno.

La Dirección estratégica puede ser entendida como *"Una estructura teórica para la reflexión de las grandes opciones de la empresa, que se sustenta en una nueva cultura y una nueva actitud de los directivos, que escapa de la improvisación en busca de lo analítico y que integra el paso de lo estratégico a lo operativo de forma sistemática y coherente"* (Menguzzato, 1991). La Dirección estratégica está ligada al cambio, al mejoramiento continuo organizacional o empresarial. La Dirección estratégica configura un ciclo comprendiendo tres procesos fundamentales: planeación, implantación y control.

2.2.2 Estrategia y gestión de Recursos Humanos

Por gestión estratégica de recursos humanos se entenderá el conjunto de decisiones y acciones directivas en el ámbito organizacional que influyan en las personas, buscando el mejoramiento continuo, durante la planeación, implantación y control de las estrategias organizacionales y considerando las interacciones con el entorno.

La gestión de recursos humanos rechaza el enfoque que mutila al empleado su potencial de multihabilidades o multicompetencias, devenido en sustento de los sistemas de trabajo flexibles. Demanda la acción de diferentes disciplinas científicas, errando quien pretenda sesgarla con el predominio de alguna. Comprende la cada vez más creciente influencia de los empleados en las actividades de GRH y de toda la organización, y en especial en la toma de decisiones. Señala la actuación anticipada, contraria a la reactiva caracterizada por accionar cuando se presenta el problema o la dificultad, o peor aún, después de su manifestación.

2.2.3 Los ocho pecados mortales de la dirección

Si bien en los libros hay mucha información sobre el liderazgo y sobre cómo hacer las cosas de forma correcta para alcanzar el éxito buscado, a veces también es bueno observar cuáles son las cosas incorrectas y cómo evitarlas.

Para el autor, a continuación se presentan los pecados mortales y de mayor frecuencia que tienen los Directivos, en donde la gran mayoría tiene que ver con los empleados:

Asumir que sus empleados conocen los objetivos y el propósito de la compañía: toda empresa tiene un equipo directivo, y este a su vez tiene un gran plan estratégico diseñado. La pregunta es *¿Quién ejecutará ese plan?* Incluso el mejor plan deja de tener valor a menos que se entienda y se acepte como propio en todos los niveles. Su mano de obra es el motor que acciona su plan. Usted debe integrar su plan estratégico que le permita asegurarse de que TODOS están en sintonía con el Plan de la Empresa.

Dejar el proceso de selección y contratación al azar: en el mejor de los escenarios, conseguirá en un 14% de los casos un empleado acorde con las necesidades de la organización. Un buen sistema de contratación y selección a todos los niveles mejora el rendimiento global y ayuda a evitar pleitos. Una definición clara y precisa de los que buscamos y para qué lo buscamos es clave.

Asumir que su gente está entrenada adecuadamente: no poder desarrollar los talentos de las personas con el entrenamiento apropiado, es una pérdida

masiva de recursos. Muchas compañías dedican más tiempo y dinero a negociar y pagar los contratos de mantenimiento de sus equipos y máquinas, de lo que dedican al entrenamiento de su personal.

No poder evaluar y medir: es fácil caer en el hábito de ***"seguir el negocio como de costumbre"***, realizando tareas de memoria o haciendo las cosas de la misma manera simplemente porque ésa es la forma en que se han hecho siempre. Usted debe medir continuamente sus actividades clave para el negocio. *¿Son necesarias y relevantes?* Si es así entonces estas actividades se deben medir y seguir para determinar su eficacia así como eficiencia. Si usted no puede medirla, no la haga.

El no poder proporcionar el feedback adecuado: el miedo al conflicto puede llevar a los líderes a evitar mencionar un comportamiento inaceptable o a requerir responsabilidades. La retroalimentación sistemática y constructiva, orientada a objetivos, mediante evaluaciones de desempeño o con conversaciones en el curso de las actividades diarias, es necesaria para asegurar un buen funcionamiento y ayudar al desarrollo de carrera de los empleados.

Asumir que se están haciendo las cosas bien y que los clientes están contentos: ¿Les ha preguntado? Si se asume que sus clientes están satisfechos simplemente porque no ha recibido quejas, no es necesariamente un medidor exacto. Su negocio debe tener mecanismos y sistemas en marcha para favorecer la retroalimentación del cliente. Usted debe escuchar, y actuar en función de esa información.

No entender la relación entre ventas y marketing: incluso los negocios con una fuerza de ventas excelente deben ayudarse del marketing. El marketing, a través de sus disciplinas de relaciones públicas, investigación y publicidad, es una herramienta clave para identificar mercados nuevos, comunicarse con su mercado potencial y con sus clientes y difundir y consolidar su marca de fábrica y su mensaje entre todos sus actores.

Tratar a empleados como si fueran un material más: una compañía que haya experimentado el alto costo de la rotación de empleados, entiende lo que significa pagar este peaje: costes de reemplazo, pérdida de productividad y moral baja. Si tratan los empleados como un material ellos le responderán de la misma forma, es decir, dejándole cuanto antes por la mejor oferta siguiente.

Es importante saber en qué posición se encuentra la empresa respecto a los ítems anteriores, y sobre todo, cómo se está valorando al factor humano. Es importante tener claro, que los empleados, son el principal recurso de la organización. Es vital también, ser conscientes de que la mejor definición aceptada actualmente es ***Talento Humano***, porque se valora a cada empleado como persona, y se tiene claro que posee un talento que debe ser explotado para el bienestar de la compañía.

La Administración de personal se ha realizado desde los tiempos inmemoriales en que las personas necesitaron trabajar en grupos, hasta algo más de la segunda mitad del siglo XX, cuando ya no se considera un costo al factor humano, sino un recurso para el cual se asumen un gran cúmulo de actividades relacionadas con la organización laboral en su interacción con las personas, destacándose actividades clave como: selección, evaluación del desempeño,

planes de comunicación, planes de capacitación y de formación, estudios de clima y motivación, etcétera (Harper, 1992).

Es tal la importancia que hoy se le está otorgando a la GRH, que se le considera la esencia de la dirección o gestión empresarial. Así lo reafirma la experiencia de empresas de punta de Alemania y Japón (Thurow, 1992), donde el segundo hombre del gerente general es el gerente de recursos humanos, y no se arriba a ese primer cargo directivo si antes la persona no ha experimentado la gerencia de recursos humanos.

La responsabilidad y ejecución de la GRH es de todos, pero principalmente de la Alta Dirección. Asumir el criterio de garantizar la participación de todos en la GRH y comprender que la responsabilidad principal corresponde a la Alta Dirección, posee un sentido práctico ineludible. Ello debe ser una constante en la mente de los directivos.

Las Nuevas Tecnologías de la Información y las Comunicaciones (NTIC) han impactado con fuerza a la GRH, potenciándose la gestión de la información y llegando a acuñar la gestión del conocimiento en la década del 90 del pasado Siglo XX, a partir del tratamiento de los intangibles y la consideración del capital intelectual (Davenport, 1998; Edvinsson, 1999; Gates, 1999; Norton, 2001)/

Las NTIC agilizan las interacciones, posibilitan el tratamiento automatizado de todos los datos y sus relaciones y sirven de catalizador de las inferencias sobre las personas, promueven la eficiencia de la formación y configuran el teletrabajo

llamado a intensificarse, por tal, se deben propiciar los recursos necesarios, para que se haga de forma Segura.

2.2.4 Seguridad Informática

2.2.4.1 Concepto de seguridad

Se puede entender como Seguridad una característica de cualquier sistema (Informático o no) que indica que tal sistema está libre de todo peligro, daño o riesgo, y que es en cierta manera, infalible. Como esta característica, particularizando para el caso de los sistemas operativos o redes de computadores, es muy difícil de conseguir (según la mayoría de expertos imposible) se suaviza la definición de seguridad y se pasa a hablar de fiabilidad (probabilidad de que un sistema se comporte tal y cómo se espera de él) más que de seguridad; por tanto, se habla de sistemas fiables en lugar de sistemas seguros (Villalón, 2002).

A grandes rasgos, se entiende que mantener un sistema seguro (o Fiable) consiste básicamente en garantizar tres aspectos (Pfleeger, 1997): confidencialidad, integridad y disponibilidad. Algunos estudios (Laprie, 1991; Olovsson, 1992), integran la seguridad dentro de una propiedad más general de los sistemas, la confiabilidad, entendida como el nivel de calidad del servicio ofrecido. Consideran la disponibilidad como un aspecto al mismo nivel que la seguridad y no como parte de ella, por lo que dividen esta última en solo las dos facetas restantes, confidencialidad e integridad. En este trabajo no se seguirá esa corriente por considerarse minoritaria.

La confidencialidad (C) dice que los objetos de un sistema solo han de ser accedidos por usuarios autorizados, y que esos funcionarios autorizados no van a convertir esa Información en disponible para otras entidades. La integridad (I) significa que los objetos solo pueden ser modificados por funcionarios autorizados y de forma controlada. La disponibilidad (D) indica que los objetos del Sistema tienen que permanecer accesibles a los funcionarios autorizados.

El objetivo de la Seguridad Informática será mantener la integridad, disponibilidad, privacidad (sus aspectos fundamentales), control y autenticidad de la Información manejada por computadora (Aldegani, 1997).

2.2.4.2 ¿Qué se quiere proteger?

Los tres elementos principales a proteger en cualquier sistema informático son el hardware, el software y la información. El hardware corresponde a todos los elementos físicos que conforman el Sistema, desde los dispositivos que se encuentran dentro de la torre (memorias, unidades, tarjetas, entre otros) hasta los que se encuentra por fuera de ella (teclado, mouse, pantalla, entre otros). El Software hace alusión a todos aquellos componentes lógicos (Sistemas Operativos y Aplicaciones) que le dan funcionamiento al hardware. La información corresponde a todos aquellos datos procesados y organizados que se almacenan en un Sistema Informático.

¿De qué se quiere proteger?

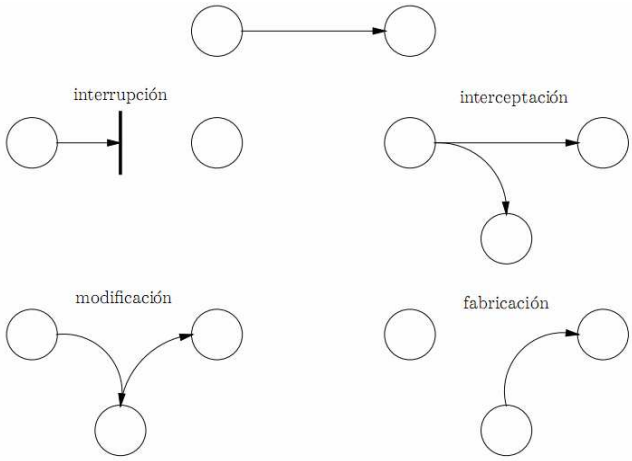

Figura 2.1: Flujo normal de información entre emisor y receptor, y posibles amenazas, **Fuente:** Villalón, 2002.

En la gran mayoría de documentos relacionados con Seguridad Informática, se intentan clasificar en grupos los posibles elementos que pueden atacar un sistema. Con frecuencia, especialmente en las obras menos técnicas (Meyer, 1989; Icove, Seger y Vonstorch, 1995), se suelen identificar a los atacantes únicamente como personas. Esto tiene sentido si se habla por ejemplo de responsabilidades de delito informático. Pero en este trabajo, será preferible hablar de ***"elementos",*** porque un sistema puede ser afectado por elementos diferentes a las personas, como por ejemplo programas o entes externos.

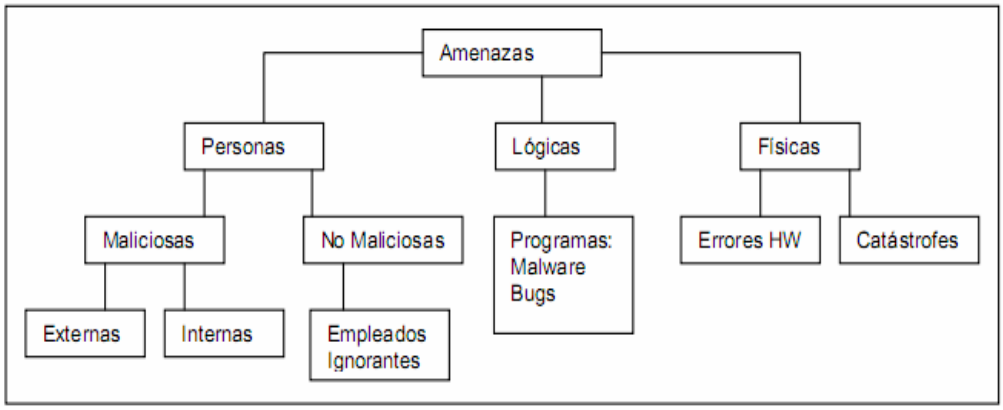

Figura 2.2: Amenazas para la Seguridad, **Fuente:** Villalón, 2002.

La mayoría de ataques a un sistema van a provenir en última instancia de personas que, de forma intencional o no, pueden causar enormes pérdidas. Generalmente, se tratará de piratas que intentan conseguir el nivel máximo de privilegio posible, aprovechando las debilidades del mismo. Sin embargo, con frecuencia se acostumbra a olvidar que los piratas ***"clásicos"*** no son los únicos que amenazan los equipos.

Es especialmente preocupante, que hoy en día cualquier administrador preocupado mínimamente por la seguridad va a conseguir un sistema relativamente fiable de una forma lógica, en donde pocos administradores tienen en cuenta factores como la Ingeniería Social, que afecta a los usuarios.

Ante la pregunta de los tipos de intrusos existentes actualmente, Julio C. Ardita[1] contesta lo siguiente: los tipos de intrusos podrían clasificarse desde el punto de vista del nivel de conocimiento, formando una pirámide, así:

- Clase A: es el 80% en la base, son los nuevos intrusos que bajan programas de internet y prueban, están jugando (…) son pequeños grupitos que se juntan y dicen vamos a probar.

- Clase B: es el 12% son más peligrosos, saben compilar programas aunque no saben programar. Prueban programas, saben cómo detectar qué sistema operativo está usando la víctima, prueban las vulnerabilidades del mismo e ingresan por ellas.

- Clase C: es el 5%, es gente que sabe, que conoce y que define sus objetivos. A partir de aquí buscan todos los accesos remotos e intentan ingresar.

- Clase D: es el 30% restante. Cuando entran a determinados sistemas, buscan la información que necesitan.

Para llegar desde la base hasta el último nivel, se tarda de 4 a 6 años, por el nivel de conocimiento que se requiere asimilar.

[1] Ardita, J. (2001). Director de Cybsec S. A. Security System y ex-hacker [En línea], disponible en: http://www.cybsec.com, recuperado: 30 de enero de 2010.

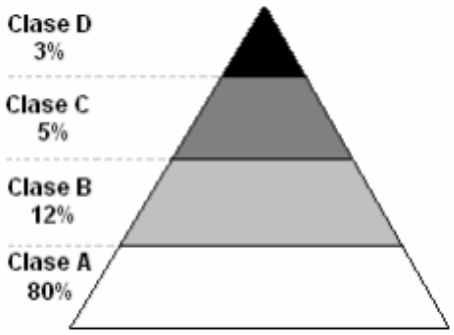

Figura 2.3: Tipos de Intrusos, **Fuente:** CybSec S.A., 2001.

A continuación, se describen brevemente los dos tipos de Atacantes que de una u otra forma pueden constituir un riesgo para los sistemas: los atacantes pasivos, que son aquellos que fisgonean por el sistema, pero no lo modifican (o destruyen), y los activos, que son aquellos que dañan el objetivo atacado, o lo modifican a favor de sí mismos. Habitualmente, los curiosos realizan ataques pasivos (que se pueden convertir en activos), mientras que los malintencionados, realizan ataques activos puros.

Las amenazas a la seguridad de un sistema provenientes del personal de la propia organización rara vez son tomadas en cuenta. Puesto que se presupone un entorno de confianza que en ciertos casos no existe, por lo que se pasa por alto el hecho de que casi cualquier persona de la organización, incluso el personal ajeno a la infraestructura informática (secretariado, personal de seguridad, personal de limpieza y mantenimiento, entre otros) puede comprometer la seguridad de los equipos. Aunque los ataques pueden ser intencionados (en cuyo caso sus efectos son extremadamente dañinos, recordemos que nadie mejor que el propio personal de la organización conoce mejor los sistemas y sus debilidades), lo normal es que más que de ataques se trata, las situaciones corresponden a accidentes causados

por un error o por desconocimiento de las normas básicas de seguridad. Debemos recordar siempre, que decir ***"No lo hice a propósito",*** no va a servir para recuperar datos perdidos, ni para restaurar un hardware dañado o robado.

Otro gran grupo de personas potencialmente interesadas en atacar el sistema son los empleados antiguos, especialmente los que no abandonaron el entorno por voluntad propia (y en el caso de redes de empresas, los que pasaron a la competencia). Por lo general, son personas descontentas con la organización que pueden aprovechar debilidades de un sistema que conocen perfectamente para dañarlo, como venganza por algún hecho que no consideran justo.

¿Cómo se puede proteger?

Hasta ahora, se ha hablado de los aspectos que engloban la Seguridad Informática, de los elementos a proteger, de los tipos de amenazas que contra ellos se presentan y del origen de tales amenazas. Parece claro que, para completar esta visión de la seguridad, hay que hablar de las formas de protección de los sistemas.

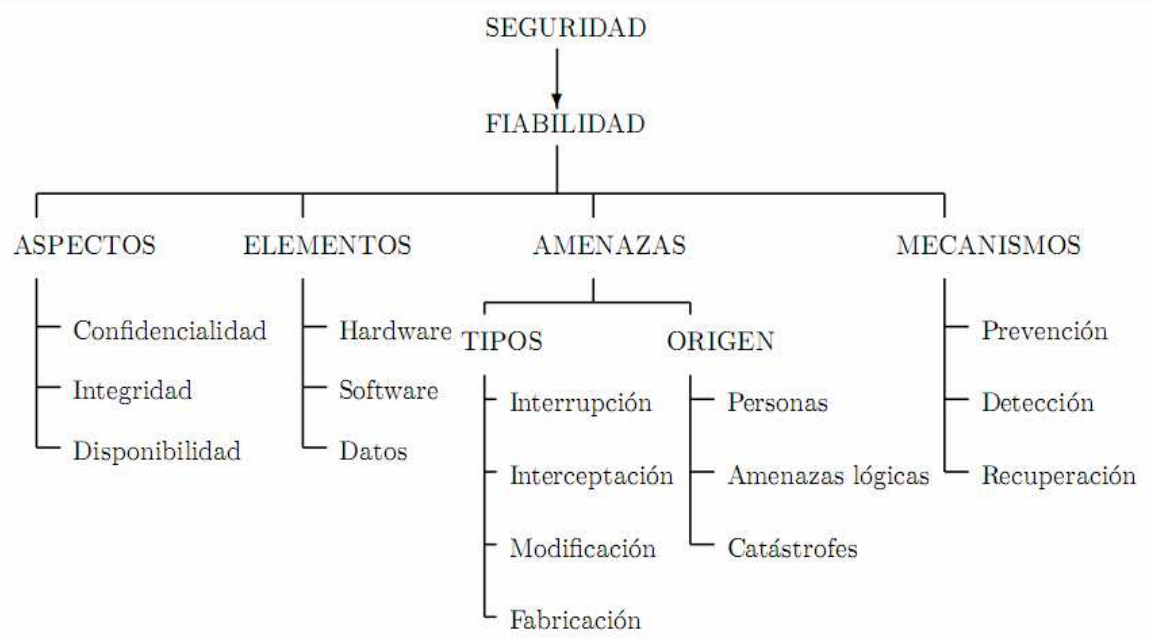

Figura 2.4: Visión global de la Seguridad Informática, **Fuente:** Villalón, 2002.

Para proteger el Sistema, se debe realizar un análisis de las amenazas potenciales que puede sufrir, las pérdidas que se podrían generar, y la probabilidad de su ocurrencia; a partir de este análisis, se ha de diseñar una política de seguridad que defina responsabilidades y reglas a seguir para evitar tales amenazas o minimizar sus efectos en caso de que se produzcan. A los mecanismos utilizados para implementar esta política de seguridad, se les denomina ***Mecanismos De Seguridad***. Tales mecanismos corresponden a la parte más visible del Sistema de Seguridad, y se convierten en la herramienta básica para garantizar la protección de los sistemas o de la red propia.

Los Mecanismos de Seguridad se dividen en tres grandes grupos: mecanismos de prevención, de detección y de recuperación. Los mecanismos de prevención, son aquellos que aumentan la Seguridad de un Sistema durante el

funcionamiento normal de éste, previniendo la ocurrencia de violaciones a la Seguridad; por ejemplo: *el uso de cifrado en la transmisión de datos se puede considerar un mecanismo de este tipo, porque evita que un atacante posible escuche las conexiones hacia o desde un sistema en la red.*

Por mecanismos de detección, se conocen a aquellos que se utilizan para detectar violaciones de la seguridad o intentos de violación; ejemplos de estos mecanismos son los *programas de auditoría*. Finalmente, los mecanismos de recuperación, son aquellos que se aplican cuando una violación del sistema se ha detectado, para retornar a éste a su funcionamiento correcto; ejemplos de estos mecanismos son: *la utilización de copias de seguridad o el hardware adicional*. Dentro de este último grupo de mecanismos de Seguridad, se encuentra un subgrupo denominado mecanismos de análisis forense, cuyo objetivo no es simplemente retornar al sistema a su modo de trabajo normal, sino averiguar el alcance de la violación, las actividades de un intruso en el sistema, y la puerta utilizada para entrar. Así, se previenen ataques posteriores y se detectan ataques a otros sistemas de nuestra red.

Aunque los tres tipos de mecanismos son importantes para la seguridad del sistema, se ha de enfatizar en el uso de mecanismos de prevención y de detección. La máxima popular ***"más vale prevenir que curar"*** se puede aplicar a la seguridad: *para nosotros, evitar un ataque, detectar un intento de violación, o detectar una violación exitosa inmediatamente después de que ocurra, es mucho más productivo y menos comprometedor para el sistema, que restaurar el estado tras una penetración de la máquina.*

Igualmente, sí se consiguiera un sistema sin vulnerabilidades y cuya política de seguridad se implementara mediante mecanismos de prevención, no se necesitarían mecanismos de detección o recuperación.

Una muy buena forma de prevenir, es la concienciación de usuarios y administradores de que ellos también son parte del problema, pero mejor aún pueden ser parte de la solución (Villalón, 2002).

¿Por qué es importante la Seguridad de la Información en las empresas?

En este punto, se empezará a hacer énfasis en el tema en cuestión, y para esto, se tomará un documento titulado: *Seguridad de la información* (Sandoval, 2005).

La información cuesta, la información se compra, la información se roba, la información se pierde…

Imaginemos, que la organización Chicolastic[2] tuviera acceso a la estrategia de mercado de Kimberly Clark, productora de Huggies o de Procter & Gamble, productora de Pampers; que Renato Cantarelli, Gerente General de Unilever, supiera que productos están desarrollando o la estructura de costos de sus principales competidores. O que se supiera hoy, cuál es el nuevo desarrollo turístico del gobierno con el objetivo de comprar terrenos a precios bajos y venderlos en un par de años en cientos de veces su valor.

[2] Marca de pañales desechables

De la misma forma, la Información de las empresas representa un activo muy importante para las mismas: desarrollos tecnológicos, patentes, fórmulas, estrategias o planes de inversión tienen un valor muy importante. Una fuga de información crítica puede representar incluso la bancarrota para una empresa.

¿Por qué se intensifica a partir de finales de los 80´s? ¿Por qué mientras duró la guerra fría entre Estados Unidos y sus aliados contra la Unión Soviética y los suyos, muchos de los activos empresariales estratégicos como bancos, empresas petroleras, farmacéuticas o industria aeroespacial eran protegidas por el propio ejército? Con el cambio de enfoque el ejército se retira y las empresas deben intensificar la Seguridad de su Información sensible.

La petrolera Shell por su parte, es una de las pioneras en desarrollar políticas estrictas para proteger la información y es adoptada por Inglaterra para desarrollar la norma de SDLI, BS 7799, la cual fue tomada como base para el surgimiento de la norma ISO 27001:2005 para Sistemas de Gestión de Seguridad de la Información.

Para que una información se considere segura, tiene que cumplir con cuatro características: que tenga los niveles de confidencialidad adecuados, que sea integra, que esté disponible y que sea auténtica.

En datos recientes, el pentágono en Estados Unidos de América recibe al año 79 mil intentos de penetrar sus sistemas de Seguridad para obtener o dañar información. Un hacker experimentado requiere de menos de 4 segundos para entrar a una maquina desprotegida. El promedio de pérdidas por robo de

información en 2003 de información propietaria, superó los 6 mil seiscientos millones de dólares

Parecería que sólo las grandes corporaciones están expuestas a perder la Seguridad de su Información clave del negocio, pero no es así. Hace un mes una empresa buscó a la consultora ***Denegocio*** para apoyarla en un proyecto de certificación de calidad; la semana anterior revisando el estado de la empresa, se identificó que había una similitud extraordinaria entre lo que habían desarrollado junto con sus asesores anteriores y una metodología que hacía cinco años ***Denegocio*** había propuesto para alguno de sus clientes. La similitud rayaba en el fusil: los códigos, la redacción del sistema, los registros, los nombres empleados eran un ***Copy-paste*** de cinco años atrás. Inclusive, hasta los errores que se identificaron a posteriori los habían cometido de la misma manera. *¿Quién no ha tenido un virus que se come sus bases de datos o máquinas que dejan de funcionar contaminadas por cientos de bichos raros que circulan por la red? ¿Cuántos documentos no se traspapelan o caen en las manos inadecuadas dentro de las mismas empresas?*

No es posible poner controles a todo para que nunca se fugue información. La nueva norma ISO 27001, propone que a través de un análisis de riesgo las organizaciones pueden identificar su exposición a perder la SDLI con la que cuentan y en función de ello, proponer acciones para disminuir el grado de riesgo.

¿Cómo medir el riesgo que se tiene respecto a la SDLI? Primero, Identificando cuál es la información crítica, aquella que hace que se tenga una ventaja competitiva sobre la competencia, como podría ser en el caso de Hylsa, el proceso de reducción directa del cual venden tecnología en todo el mundo por

ejemplo, el plan de promoción del nuevo vehiculo de VW, los descuentos a que se tienen acceso en el caso de almacenes de cadena o los prototipos nuevos de vivienda de una Constructora.

Segundo, determinando qué amenazas a la información crítica existen, desde que se la roben, hasta inclusive que caiga un rayo y dañe la base de datos en la que está; que alguien más la patente o haga un desarrollo similar, que fallezca el científico que tiene el conocimiento, que le caiga café encima y muchas más, por simples que puedan parecer algunas.

Tercero, evaluando cuál es la probabilidad y la consecuencia de que la amenaza se torne real. *¿Qué probabilidad y consecuencia tiene que caiga un rayo, que el científico fallezca o que le caiga café al documento?*

Este análisis permitirá centrar a las organizaciones hacia los riesgos más importantes y en función de ellos, determinar los controles adecuados. Seguramente no todos los riesgos estarán cubiertos, por lo que algunos tendrán que ser aceptados. Sin embargo, la tendencia mundial en las empresas se dirige hacia mantener la Seguridad de su Información, aquella que finalmente hace que marcas como Disney, Pepsi, Ferrari, Levi´s o Goodyear valgan miles de millones de dólares (Sandoval, 2005).

CAPÍTULO 3

MARCO CONCEPTUAL

3.1 Inseguridad informática

La Seguridad Informática como concepto ha venido evolucionando a lo largo del tiempo. La necesidad de protección, de controlar el acceso a la información, de la confidencialidad y disponibilidad de la misma, han marcado una manera de comprender las posibilidades de la seguridad informática en las empresas (Parker, 1998; Krause y Tipton, 1999; Hancock y Rittinghouse, 2003).

En este sentido, las organizaciones desde sus inicios han buscado la manera de aumentar la certeza y el seguimiento adecuado de las actividades de los usuarios y procesos en los diferentes sistemas de información, con el fin de mantener un adecuado control (comprendido como capacidad de regulación) de la evolución del sistema y un manejo óptimo de los recursos de información disponibles para soportar la operación de las organizaciones (Carlson, Green y Schetina, 2002; Byrnes y Proctor, 2002).

Al terminar un año e iniciar el siguiente, generalmente se presentan los resultados de la gestión del que concluye y se establecen los pronósticos sobre el venidero. El tema de Seguridad Informática no es ajeno a esta dinámica del mundo, es probablemente uno de los tópicos donde los especialistas en el área buscan afanosamente establecer líneas de acción sobre características especiales de los acontecimientos que pasaron y podrán ser influyentes en el futuro.

Revisando algunos de los pronósticos se encuentra que temas como: el SPAM, los firewalls personales, los dispositivos de almacenamiento USB, organizaciones criminales en Internet, las crecientes regulaciones en el ámbito tecnológico, entre otros; serán elementos importantes donde muchos cambios y actividades tomarán lugar y generarán eventos que impactarán las organizaciones y la operación de las mismas.

En tal sentido, la Seguridad Informática, por una tradición académica y científica, fundada en un contexto histórico donde la inversión en protección y control de Información son los factores comunes, se ha confinado al contexto de dispositivos, iniciativas y estrategias técnicas y experimentales para elevar cada vez más los niveles de control sobre los datos disponibles, sabiendo que ellos, son parte esencial de la razón de ser de los proceso de negocio. Esta realidad, se ha afirmado a lo largo del tiempo en las organizaciones, generando un paradigma eminentemente técnico alrededor del tema de seguridad informática, generalmente de dominio de los profesionales de la ingeniería, donde el espacio para individuos de otras disciplinas generalmente no es muy amplio.

Observando las reflexiones sobre las predicciones y concentrándose en la estructura de pensamiento plasmada en las mismas, es frecuente observar que estos pronósticos muchas veces responden a eventos que en el pasado han ocurrido y se manifiestan como posibles tendencias, reflejando un pensamiento lineal que sugiere continuidad y avance, pero algunas veces negación de los temas en sí mismos. Es decir, las predicciones responden a causas y efectos que pueden ser establecidos y revisados. Sin causas no habría efectos, lo que se conoce en el pensamiento filosófico como dualismo.

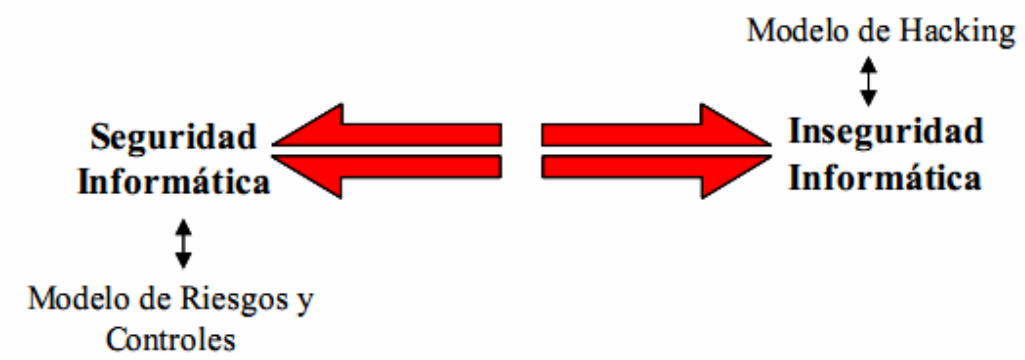

Figura 3.1: Dualismo de la Seguridad Informática, **Fuente:** Cano, 2004.

El dualismo, ha sido factor clave para el desarrollo de muchos conceptos que hoy en día son fundamentales para el avance de la tecnología y la seguridad informática, pero no es la única estrategia para abordar los fenómenos de nuestra realidad. Desde la perspectiva del dualismo, un sistema es seguro o inseguro, lo que implica reconocer y profundizar en un lado de la línea de pensamiento. Es decir, o aplicamos técnicas de seguridad informática para reducir los riesgos e implementar controles, ó vemos como podemos saber que tantas vulnerabilidades tenemos que nos hacen inseguros, para tomar medidas correctivas.

En este sentido, se presenta la estrategia de la dualidad, como una manera complementaria de explorar los hechos mismos en el mundo, para reconocer las causas y los efectos en su contexto, sin negar la posibilidad de considerar que uno surge a partir del otro, significando, reconocer que la Seguridad Informática surge a partir de considerar la Inseguridad Informática y viceversa; un continuo de aprendizaje que muchas veces no corresponde a una causa específica sino a la relaciones existentes entre los componentes objeto del análisis. (ver Figura 3.2).

Con estas ideas planteadas, se desarrolla este documento breve donde se revisa el concepto de Inseguridad Informática desde una perspectiva dual como

una manera complementaria de comprender los elementos, relaciones y efectos de la Seguridad Informática en el contexto de una realidad cambiante y dinámica. Los planteamientos sugeridos en este apartado, responden a reflexiones recogidas de la experiencia de la industria al tratar de enfrentar la variabilidad de los escenarios y sus vulnerabilidades y, las ideas de la academia para profundizar en eventos predecibles e inesperados de la dinámica entre la tecnología, la organización y los individuos.

3.1.1 La dualidad de la Inseguridad Informática

El concepto de Seguridad de la Información tiene una faceta interesante, pues se hace necesario proteger la Información que se tiene y mantener un control en el acceso a la misma, por lo que se deberá hacer una buena clasificación, así como establecer estrategias para darle continuidad a la disponibilidad en caso de situaciones de falla.

En múltiples investigaciones realizadas, se considera el tema de la Seguridad Informática como una disciplina del conocimiento donde se busca cerrar la brecha de los eventos inesperados que puedan comprometer los activos de una organización y así, contar con estrategias para avanzar ante cualquier eventualidad.

Consideremos ahora el estudio de la Inseguridad Informática, como una disciplina dual donde los académicos y practicantes de la industria buscan las maneras detalladas para que ocurran eventos inesperados, establecer las condiciones extremas de funcionamiento de los dispositivos o estrategias, todo

con el fin de hacer caminar en condiciones límite la operación de la organización y sus negocios. La estrategia dual sugiere contextualizar en un escenario real la incertidumbre inherente de la seguridad informática para revisar entre otros aspectos (Schneier, 2003):

- ¿Cómo funciona el sistema?
- ¿Cómo no funciona el sistema?
- ¿Cómo reacciona ante una falla?
- ¿Cómo hacerlo fallar?

Por tanto, la inseguridad informática como disciplina dual en el estudio de la seguridad informática, establece un paradigma complementario (es decir dual a la seguridad informática) que comprende las propiedades emergentes de los sistemas (analizados) bajo condiciones y realidades extremas, las cuales no son viables en una estrategia de protección causal (dualismo) sugerida por la seguridad informática actual. En este sentido, se quiere plantear la necesidad de revisar nuestra manera de abordar el tema de la protección de los activos de una organización, no solamente establecer las causas y los efectos, sino comprender las relaciones entre los objetos revisados y considerar las reacciones entre éstas, que pueden sugerir efectos no predecibles en los modelos causales. Es decir, conociendo que tan inseguros somos, podemos comprender que tan seguros podríamos llegar a ser.

Cuando se plantean las condiciones de análisis de la seguridad y las pruebas de los elementos de los sistemas se consideran, entre otros, algunos elementos comunes desde el punto de vista de Whittaker (2003):

- Se requiere que el equipo de pruebas trabaje sobre la descripción del comportamiento del producto o sistema,

- Se requiere que el producto o sistema sea ejecutado en un ambiente real o simulado,

- Se requiere que la funcionalidad del producto o sistema sea explorada de una manera metódica y que los resultados de las pruebas bien sean positivos o negativos, puedan ser analizados en contexto y así, ofrecer un concepto formal del mismo.

En este contexto, las relaciones causales deben ser determinadas y concretadas de tal forma que sea posible detallar y sustentar los posibles estados exhibidos por el sistema, al ser sometido a las pruebas de comportamiento sugeridas dentro del dominio de la definición del producto mismo. Esta estrategia si bien aporta elementos detallados sobre el sistema y su funcionamiento futuro, ofrece pocas luces sobre comportamientos inesperados y condiciones extremas de operación, dado que no se abre la posibilidad a una lógica de la inseguridad informática como reflexión dual del ejercicio.

Al revisar la inseguridad informática como estrategia de pensamiento estratégico, se reconoce que un sistema es tan seguro como su falla de seguridad

más reciente; porque cuando ocurre o se manifiesta un problema de seguridad, las personas se vuelven más experimentadas y saben qué hacer, que los sistemas mal diseñados (pensamiento natural en Seguridad Informática) no están preparados para fallar (pensamiento dual en Inseguridad Informática). En pocas palabras, comprender la inseguridad informática del sistema en evaluación para hacer el sistema dinámico y flexible ante nuevos ataques, atacantes o fallas de Seguridad (Schneier, 2003).

La inseguridad informática como pensamiento dual en Seguridad Informática descubre que las relaciones entre los elementos del sistema son capaces de producir efectos positivos y negativos, los cuales son capaces de comprometer su supervivencia. En este sentido, comprender la inseguridad informática como el dual de la Seguridad Informática, en el contexto organizacional, representada esta última en sus participantes, sus procesos y tecnología (Cano, 2005), permite revisar las propiedades emergentes de la seguridad informática en un escenario con múltiples variables, repensar la Seguridad misma mas allá de una directriz de la corporación, como una mente pensante que aprende y evoluciona en su hacer.

En razón de lo antes mencionado, y esculcando a fondo el concepto de Seguridad Informática, este proyecto busca acercar dicho concepto a la realidad organizacional y sus procesos, la tecnología informática que los soporta y el contexto particular que hace realidad la dinámica de la Seguridad Informática en cada una de las situaciones empresariales, como una iniciativa para establecer una integración del concepto en el entorno organizacional, y llevarlo más allá de la seguridad informática, involucrando la seguridad de la información como un tema multidisciplinario inmerso en la evolución misma de los procesos de negocio de las organizaciones.

3.1.2 Explorando la dualidad de la Seguridad: La mente segura

El concepto de la organización como una mente pensante y actuante, con un pensamiento complementario (dual) nos sugiere que la seguridad informática, como una distinción más de la organización, representa una dinámica de acción que podríamos recrear considerando los elementos de la mente segura sugeridos por Day (2003). Para este autor, una mente segura consiste en la revisión y práctica de virtudes y reglas de seguridad[2] con el fin de tomar decisiones claras, consistentes y efectivas.

Complementario a esta propuesta, la existencia de la mente insegura, como realidad presente de la organización, es un punto de análisis adicional que se considera, no solo para dar sentido a la práctica de las virtudes y reglas de seguridad, sino para mantener la perspectiva de la incertidumbre inherente al proceso de la seguridad informática.

La mente insegura como dual de la mente segura, puede sugerir elementos de análisis de situaciones extremas en las organizaciones que lleven no solamente a considerar las vulnerabilidades y riesgos de las información de los procesos de la empresa, sino repensar los procesos mismos para hacerlos más confiables, en la medida que se consideren las perspectivas diferentes de la seguridad implícitas en cada uno de los participantes de los mismos. La mente insegura es una posibilidad de caminar y repensar el análisis de riesgos como un modelo de hacking (Horton, 2003), consistente de

[2] Las virtudes de la seguridad son: La seguridad deber ser una consideración diaria, la seguridad debe ser un esfuerzo comunitario, las prácticas de seguridad deben mantener un foco generalizado, las prácticas de seguridad deben incluir medidas de entrenamiento para todo el personal de la organización.
Las reglas de seguridad son: Regla del menor privilegio, Regla de los cambios, Regla de la confianza, Regla del eslabón más débil, Regla de separación, Regla de los tres procesos, Regla de la acción preventiva y Regla de la respuesta apropiada e inmediata

reconocimiento del sistema objetivo, manipulación y compromiso del objetivo, apalancamiento del ataque y conquista de nuevos objetivos.

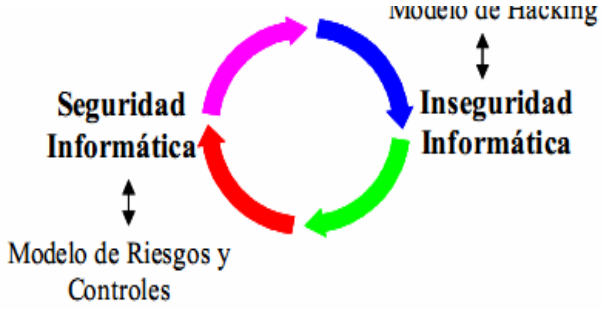

Figura 3.2: Concepto Dual de la Inseguridad Informática, **Fuente:** Cano, 2004.

En razón a lo anterior, la mente insegura, al igual que la inseguridad informática son parte de un mismo continuo que busca entender que la seguridad informática como necesidad organizacional, no es más que el resultado de una propiedad emergente de un sistema que conoce sus condiciones extremas, su operación límite, así como sus recursos y posibilidades para darle sentido a la razón de su misión. Es decir, reconocer que los ataques y fallas de seguridad informática son una constante y por tanto, se requiere conocer y validar los niveles de siniestralidad o falla que la organización puede manejar en la operación de su negocio.

Mientras la seguridad informática es un concepto subjetivo de acuerdo a Schneier, la inseguridad informática es objetiva, es decir propia al objeto. No es posible evitar la inseguridad informática pues es una propiedad inherente a los objetos. Por tal motivo, se hace necesario explorar en profundidad dicha

propiedad, pues mientras más se comprenda la realidad de la inseguridad, con mejor se podrá comprender la Seguridad Informática de las organizaciones.

Considerar la inseguridad informática como parte del ejercicio de Seguridad Informática de las organizaciones, sugiere la capacidad de las organizaciones para cuestionarse sobre la situación real del balance entre seguridad, facilidad de uso y funcionalidad no para lograr mayores niveles de confiabilidad y aseguramiento de sus arquitecturas, sino para evaluar el nivel de dificultad requerido por los atacantes para ingresar y vulnerar los medios de protección (Cole, 2002). Con un pensamiento de este nivel, las organizaciones no buscarán solamente incrementar la confianza de sus clientes, sino comprender que la seguridad no es un problema de tecnología, sino un problema de riesgos y las diferentes maneras de comprenderlos y manejarlos: una mente segura.

3.2 Seguridad en la empresa

Mientras más se conoce la Inseguridad Informática, más se podrán comprender las acciones y resultados de la seguridad en las organizaciones. En este sentido, la detección de posibles problemas de seguridad no generaría valor sin una adecuada respuesta. Una respuesta que reconozca la Inseguridad Informática como insumo y el ataque de seguridad como una variante a considerar en la protección de los activos. En consecuencia, cuando somos capaces de reconocer y actuar en situaciones inesperadas, nuestra capacidad de análisis y control aumenta, pues nuevas perspectivas se abren a las relaciones que exhibe la Inseguridad Informática (Cano, 2004).

La evolución de la seguridad informática, no sería posible sin la equivalente evolución de la calidad y sofisticación de los ataques desarrollados por los intrusos. No se puede negar la importancia de las creativas maneras de confrontar y vulnerar las soluciones de seguridad planteadas durante estos años, pues sin ellas las mejoras planteadas a la fecha no tendrían la formalidad y dimensión que se plantea en los productos actuales de seguridad.

En estos momentos podría decirse que para muchos usuarios domésticos, y peor aún usuarios corporativos, pareciera que la cultura y visión con relación a la seguridad ha pasado desapercibida; No se evidencia ningún papel protagónico en el concepto de seguridad.

Después de los 80's y entrando a los 90's, las organizaciones se han basado en redes de comunicaciones que permiten un flujo más oportuno de información (Barnett, 1999). Esta dinámica de negocios multilateral, interconectada y basada en relaciones dinámicas e internacionales, inicia el camino de la reconciliación del tema de seguridad con el tema de negocio.

Se habla de reconciliación y no de incorporación del concepto de seguridad informática, pues el concepto siempre ha estado en las organizaciones desde hace mucho tiempo, sólo que disociado y especializado en los profesionales de tecnología. Esta reconciliación se promueve de manera natural dado que, al igual que los negocios, la seguridad informática es un conjunto de relaciones que cubren la tecnología, la organización y los individuos. Luego, mientras no se comprendan estas relaciones en el contexto de las relaciones de negocio, la seguridad informática no será parte del valor agregado de las relaciones con los

clientes y tendrá limitaciones para lograr una cultura de seguridad y control inherente a los procesos corporativos basados en las acciones individuales.

Cada vez que se mira a la seguridad informática en el milenio nuevo, se confunden los límites de la tecnología, la organización y los individuos, lo cual sugiere que la reconciliación debe avanzar en medio de un camino incierto para las organizaciones que buscan responder algunos interrogantes: *¿Cómo desarrollamos una cultura de seguridad de la información? ¿Cómo hacer para que las personas sean conscientes de su responsabilidad con la seguridad? ¿Cómo hacemos para que los empleados nos ayuden a detectar situaciones de posibles fallas de seguridad? ¿Cómo hacer para que los de tecnología de la información ayuden en la implementación de mejores condiciones de seguridad? ¿Cómo hacer para que la seguridad de la información sea un tema importante de la alta gerencia?*

En este contexto, las prácticas organizacionales relacionadas con la seguridad muestran las corrientes diferentes que llevan a las empresas de modelos formales de seguridad y control, con sanciones y estrictas directrices, a disposiciones medianamente formales y con controles mínimos para mantener el adecuado acceso y control de la información.

Esta realidad, generalmente responde a una perspectiva reactiva de situaciones que previamente se han presentado, que hace que una nueva forma de operar se plantee por la organización y que generalmente no responde a un modelo o reflexión concreta que oriente las directrices de seguridad y su relación con el proceso de negocio donde se encuentra el empleado.

Así, este documento pretende detallar algunas de las prácticas organizacionales relativas a la seguridad, donde se analizarán en el contexto los principios claves de la misma: confidencialidad, integridad y disponibilidad. Se tendrán en cuenta su utilidad y coherencia con las realidades de la dinámica de las organizaciones. Es importante destacar, que la experiencia del investigador y del autor del modelo, soporta estas prácticas en un campo laboral donde se valora el rol de la seguridad.

El tema de seguridad informática en sí, plantea la necesidad de comprender las situaciones a las que se está expuesto cuando no se tiene seguridad. Una clara contradicción que efectivamente sugiere que se están evaluando constantemente las expectativas y condiciones esperadas e inesperadas del contexto de los diferentes elementos y relaciones de la seguridad: tecnología (T), organización (O) e individuo (I); para el buen desarrollo de las operaciones y relaciones de la dinámica de los negocios.

La revisión de las prácticas organizacionales de la seguridad informática, basadas en esta trilogía de elementos –TOI-, establece una manera de revisar la concentración de esfuerzos de la organización para materializar y avanzar hacia una cultura de seguridad, más allá de las fronteras de las especificaciones técnicas y dominio de la disciplina de la ingeniería. Si bien esta propuesta no pretende ser la solución definitiva a las prácticas organizacionales en seguridad, es una manera de comprender los alcances de dichas prácticas en la realidad de las organizaciones.

Consiguientemente, se entenderán las prácticas como ejercicios permanentes que las corporaciones desarrollan como soporte a las directrices

formales e informales de seguridad establecidas por las directivas, para fortalecer las estrategias de seguridad y control que son inherentes a los procesos de negocio.

3.3 Glosario

- Activo: recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.

- Amenaza: es un evento que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

- Ataque: evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.

- Autenticidad: se interpreta en que el uso y/o modificación de la información por parte de un usuario debe ser irrefutable, es decir, que el usuario no puede negar dicha acción

- Confidencialidad: los componentes del sistema serán accesibles sólo por aquellos usuarios autorizados.

- Desastre: interrupción de la capacidad de acceso a información y procesamiento de la misma, a través de computadoras necesarias para la operación normal de un negocio.

- Disponibilidad: los usuarios deben tener disponibles todos los componentes del sistema cuando así lo deseen.

- Impacto: posibilidad de medir la consecuencia al materializarse una amenaza.

- Industria: una industria se define como un grupo de compañías oferentes de productos o servicios que son sustitutos cercanos entre sí.

- Innovación: puede definirse como algo nuevo o novedoso, con respecto a la forma como una empresa opera o sobre los productos que genera.

- Integridad: los componentes del sistema sólo pueden ser creados y modificados por los usuarios autorizados.

- Políticas de seguridad: una política de seguridad es una forma de comunicarse con los usuarios y los gerentes. Las políticas establecen el canal formal de actuación del personal, en relación con los recursos y servicios informáticos importantes de la organización.

- Riesgo: posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la organización.

- Seguridad física: puede asociarse a la protección del sistema ante las amenazas físicas, incendios, inundaciones, sismos, cables, control de accesos de personas, entre otros.

- Seguridad lógica: protección de la información en su propio medio, mediante el enmascaramiento de la misma usando técnicas de criptografía, equipos de contención, entre otros.

- Vulnerabilidad: posibilidad de ocurrencia de la materialización de una amenaza sobre un activo.

CAPÍTULO 4
LAS CUATRO ESTACIONES

4.1 Introducción

Mientras en la banca, el riesgo o motivador fundamental de la administración de riesgos es el fraude, es decir, *"esa conducta que busca engañar a un tercero, buscando un beneficio propio"*, en otras industrias, es la fuga de información, esa *"acción deliberada y consciente para liberar información de carácter estratégico o sensible, que debilita la posición estratégica de una organización"*. Los dos riesgos enumerados, demuestran ampliamente que cada sector requiere estrategias diferentes para hacer que sus negocios funcionen de la mejor forma y generen valor para sus accionistas.

Dentro de este marco, las TIC's juegan un papel fundamental, bien para apalancar una estrategia de seguridad y control que limite la materialización de un fraude o la fuga de la información, o bien para ser herramienta facilitadora de los mismos. Sin embargo, es de clarificar, que para el tratamiento de cualquiera de los dos riesgos identificados, las TICS únicamente no son suficientes, por lo cual se requiere una visión holística que permita integrar las múltiples variables que explican las interrelaciones de las personas, la tecnología y los procesos, para así visualizar acciones que permitan confrontar dichos riesgos.

Tanto el fraude como la fuga de información, son realidades que están apalancadas en aplicación sistemática de malas prácticas, que llevan indefectiblemente a las organizaciones al escenario de los incidentes, los cuales

deben ser identificados, clasificados, valorados e investigados (cuando la situación lo amerite y valoración lo establezca) de cara a reconocer que debemos continuar aprendiendo de lo que ocurre y claro está, evitar que la misma conducta o condición se haga evidente (Cano, 2009c).

Por lo tanto, se pensó en concienciar al recurso humano, como estrategia para fortalecer el eslabón más débil de la cadena. Y basados en la experiencia del investigador y la línea conceptual del ***Dr. Cano***, se pensó en la siguiente metodología llamada “Las cuatro estaciones”:

4.2 Fase 1: Preparación

Al iniciar la primavera, es momento de preparar la tierra y sembrar la mayoría de los cultivos básicos para aprovechar la llegada próxima de las lluvias; al igual en este método. La primera etapa es la de reconocimiento del terreno, de identificar con quien se va a trabajar, y cómo podría hacerse.

La estación de inventariar los recursos disponibles, la de entrevistarse con los presuntos implicados y conocer sus apreciaciones y expectativas. Es la etapa de conocer el negocio y a las personas que hacen parte de él, para saber así, qué es lo que les interesa y cómo se llegará a eso.

4.3 Fase 2: Planificación

El verano está caracterizado por tener los días más largos y los rayos solares con menor inclinación, por lo que las temperaturas son las más altas del año. La segunda etapa es la de mayor trabajo, es necesario reunir un equipo bueno de trabajo que planee y le dé forma al programa de sensibilización.

Entonces, adoptar un enfoque de gestión del cambio en las iniciativas de sensibilización reviste una importancia crucial, dado que contribuye a reducir las diferencias existentes entre un problema determinado, y las respuestas humanas a las necesidades de cambio, incluso si se trata de un cambio cultural.

El uso de los principios clave de la gestión de cambios (por ejemplo, la aplicación de un criterio selectivo a las comunicaciones, la participación, la formación y la aplicación) contribuirá a alcanzar los objetivos de las iniciativas de sensibilización, y ayudará a establecer las bases para programas futuros o de seguimiento.

Los cambios deben gestionarse desde una perspectiva integral, a fin de incluir los esfuerzos y obtener beneficios reales y duraderos. Para apoyar un programa de concienciación es importante llegar a un acuerdo sobre los principales factores:

- Identificar a las partes interesadas, en la toma de decisiones, la planificación, la aplicación y la evaluación.

- Establecer una meta clara para los criterios de valoración del cambio.

- Definir con claridad funciones y responsabilidades.

- Vincular e integrar los principales elementos de cambio.

- Gestionar los riesgos.

- Establecer una comunicación abierta, clara y oportuna.

- Adoptar enfoques flexibles, que permitan adaptarse a las necesidades de las diferentes partes interesadas.

- Facilitar los recursos para el cambio.

Obtener el apoyo de la dirección, y el patrocinio del programa de concienciación, es probablemente el aspecto más crucial de la iniciativa. Es necesario lograr un consenso entre los responsables de la toma de decisiones sobre la importancia y la oportunidad de financiar el programa (ENISA, 2006).

No se ahondará mucho en el tema, pero justificar la inversión en seguridad de la información, nunca ha sido nada fácil. El Retorno Sobre la Inversión en Seguridad (ROSI), es la herramienta adecuada para justificar tal inversión. El ROSI se deriva del indicador financiero ROI (Retorno sobre la inversión, que mide

la relación entre el retorno sobre una inversión, y la inversión, determinando los ingresos de la misma) y ayuda a identificar cuando dejaría de perder la empresa gracias a un proyecto de seguridad que mitigue incidentes (Ormella, 2006).

Algo que sustenta lo anterior, y que también hace parte de la planeación, es determinar cuáles son las ventajas del programa.

Otros aspectos claves de esta etapa son:

- Seleccionar el personal y los materiales necesarios para el programa.
- Preparar el plan de trabajo.
- Definir las metas y los objetivos.
- Definir los grupos destinatarios.
- Desarrollar una lista de tareas y asignar responsables.
- Definir indicadores cuantificables para medir la efectividad del programa.

4.4 Fase 3: Aplicación

El otoño es la estación donde los días reducen su duración; en este programa, una buena organización y programación garantizan la mayor parte del éxito. En esta etapa, cada uno de los miembros debe desempeñar su rol en la ejecución de la iniciativa.

La labor desempeñada en las estaciones anteriores, puede parecer larga y burocrática hasta este punto, donde se verá recompensado el tiempo dedicado a determinar los requisitos, diseñar la solución y mejorar los resultados, porque si las anteriores se llevan a cabo correctamente, la ejecución del programa transcurrirá sin problemas, y con mayor eficacia.

4.5 Fase 4: Evaluación

Con el invierno se cierra el ciclo, pero cuando esta estación llegue, se debe estar listo, y muy bien preparado. El invierno es la estación de los días más cortos, y las bajas temperaturas. El invierno torna al ambiente tenso.

Un punto de partida determinado antes de la puesta en escena, ofrece una instantánea dentro de los grupos destinatarios. El cumplimiento de los objetivos debe revisarse a la vista de los resultados obtenidos, y de la eficacia de los mismos. Si el plan no garantiza los resultados deseados, se debe modificar e iniciar nuevamente (ENISA, 2006).

Finalmente, se enumeran ciertos factores a tener en cuenta para lograr una evaluación satisfactoria:

- Se debe tener cuidado con la implementación de tecnologías nuevas. La tecnología normalmente avanza más rápido que cualquier programa de concienciación.

- La correcta segmentación del auditorio es un factor decisivo. Hay que olvidar la expresión ***"Todos por igual"***, porque en la organización, los destinatarios nunca van a ser iguales.

- Un error muy común, es el ***"exceso de información"***.

- La falta de organización y seguimiento, pueden tirar todos los esfuerzos por la borda.

- El mensaje debe llegar donde debe llegar, y para esto hay que explicar los motivos del programa.

- La ingeniería será la piedra en el zapato, por lo cual se debe prevenir a los destinatarios.

CAPÍTULO 5

LO QUE CREEMOS SABER Y EN REALIDAD DESCONOCEMOS

5.1 Introducción

Lo que creemos saber y en realidad desconocemos, es un programa que busca generar cultura organizacional con respecto a la seguridad de la información de la compañía, que se soporta en la definición de políticas, normas, procedimientos y en la implementación de herramientas de control definidas por la organización.

Por medio de este programa, se quiere que los lectores conozcan algunos aspectos fundamentales de la seguridad de la información, así como las conductas esperadas y responsabilidades que sobre el tema deben asumir los funcionarios de la compañía.

Cabe destacar, que este programa asume los temas base que toda compañía sin importar la industria ni el tamaño, debería socializar con sus empleados.

El programa se compone de una sección primera en la que se describen varios aspectos importantes de la seguridad de la información, seguidos de una evaluación que busca afianzar los conceptos explicados.

5.2 Objetivos

- Proteger la Información crítica de la empresa, generando consciencia sobre la importancia de la seguridad de la información de la compañía, basados en el hecho de que todos somos responsables de su cuidado.

- Explicar a los funcionarios de la compañía, los principios fundamentales para el cuidado de la información, dejando claro no solamente cómo proteger los sistemas, sino la razón por la cual es importante su protección y la forma en que los usuarios se convierten en la primera barrera de seguridad.

- Divulgar las definiciones hechas por la gerencia general, a través de las políticas de Seguridad de la Información.

5.3 Equipo de trabajo, sus roles y responsabilidades

- Comité de Seguridad de la Información: define las Políticas de Seguridad de la Información, y los mecanismos de divulgación y control.

- Oficial de Seguridad de la Información: garantiza que los funcionarios de la compañía reciban capacitación en seguridad, por medio del programa de sensibilización y además, vela por el cumplimiento de las políticas definidas.

- Funcionarios de nivel directivo, profesional y medio: cursan el programa de concienciación en Seguridad de la Información, y cumplen con las definiciones hechas a través de las políticas de Seguridad de la Información.

5.4 Etapas de la implementación

- Realizar una campaña previa de expectativa.

- Identificar los funcionarios de nivel directivo, profesional y medio de la compañía, para programar con la anticipación debida las sesiones de capacitación para cada una de las áreas.

- Realizar las sesiones de capacitación, efectuar la evaluación del programa y asegurar la firma del contrato de Seguridad de la Información.

- Hacer entrega del programa a la gestión del componente humano, para garantizar la continuidad del mismo.

- Comenzar el monitoreo de los activos de información clasificados y el reporte de los eventos identificados.

5.5 Descripción general

El programa está compuesto de nueve secciones cortas que describen conceptos fundamentales sobre Seguridad de la Información, seguidas de una evaluación con 15 preguntas, la cual se aprueba con un 75% de respuestas correctas. A continuación, se detallan las secciones y lo explicado en cada una:

Clasificación de la Información

La información es uno de los activos más importantes para la compañía, y por lo tanto, se le debe dar un tratamiento seguro. No importa cuál es su cargo en la empresa, usted maneja información que es esencial para los intereses de la compañía

Las políticas de seguridad de la información están definidas para todos los funcionarios de la compañía. Usted debe conocerlas y cumplirlas.

Para preservar la confidencialidad, integridad y disponibilidad de la información de la compañía, ésta debe ser clasificada en términos de su valor, de los requisitos legales, de su sensibilidad e importancia.

La información se debe clasificar en las categorías siguientes:

- Pública: es la información disponible para todos los empleados y terceros. Ejemplo: Información colocada en el sitio web de la compañía.

- Interna: corresponde a la información disponible para todos los empleados que la necesiten, a la cual sólo se le puede dar un uso interno. Ejemplo: Procedimientos publicados en la intranet.

- Privilegiada: es la información de uso exclusivo de un grupo de personas, a la cual sólo pueden tener acceso funcionarios con una clara necesidad de conocerla, y aquellos terceros que hayan firmado un acuerdo de confidencialidad. Ejemplo: Metodologías e instructivos propios de cada área.

- Confidencial: información secreta a la que pueden tener acceso exclusivamente personas seleccionadas cuidadosamente y con necesidades empresariales evidentes. La revelación no autorizada de esta información, puede causar daños significativos a los intereses de la empresa. Ejemplo: nuevos lanzamientos, fórmulas de productos, estrategias clave de negocio.

Atienda las siguientes recomendaciones para mantener la seguridad de la Información:

- La información que sea clasificada como “Confidencial” deberá ser etiquetada como tal, tanto en formato físico como electrónico: informes impresos, presentaciones en pantalla, archivos digitales (Microsoft Word,

Microsoft Excel, Microsoft PowerPoint, Microsoft Project), mensajes electrónicos y medios de almacenamiento (cintas, CD, DVD).

- No se debe compartir la información con todos los usuarios de la red sin antes establecer restricciones. Verifique que al compartir información, únicamente lo haga con los usuarios que están autorizados a tener acceso a ésta.

- Cada usuario es responsable de que su equipo de cómputo permanezca bloqueado cada vez que se retire de su puesto de trabajo.

- No se deben crear accesos directos a información privilegiada o confidencial en el fondo de escritorio de su equipo de cómputo.

- En su ausencia, no deje expuesto ningún tipo de información, datos o documentos en su escritorio. Los documentos en papel y los medios de almacenamiento externos (USB, CD, DVD) deben ser almacenados bajo llave, en archivadores u otro medio seguro.

- Tenga cuidado con la información en impresoras, fax, fotocopiadoras y sobre su escritorio: la información confidencial o privilegiada, deberá ser enviada a la impresora protegida por contraseña. Una vez impresa, debe ser retirada de la impresora inmediatamente. En caso de que no se requiera, debe destruirse utilizando trituradores de papel.

- Igualmente, sea cuidadoso con la información que envía y recibe por fax, así como aquella a la que le toma copias. No deje documentos abandonados en las máquinas de fax o fotocopiadoras.

- La eliminación apropiada de la información que ya no se necesita (incluyendo borradores, copias u hojas que salieron mal) es indispensable. Esto se aplica tanto a documentos en papel como a medios de almacenamiento tales como: discos, DVD, CD, cintas, entre otros.

- No deje información olvidada en salas de reuniones (papeles sobre las mesas, en papeleras, escrita sobre tableros, en memorias USB, entre otros).

- Sea precavido al discutir asuntos relacionados con el trabajo en zonas públicas, dentro y fuera de los edificios de la empresa.

- Lo anterior, también se aplica a la lectura o actualización de documentos confidenciales (verifique siempre quien lo observa).

- La información revelada en foros confidenciales, no debe ser discutida en otros escenarios. En reuniones e interacciones profesionales exprese apenas lo necesario.

- Recuerde, toda la información obtenida durante su trabajo es apenas para uso interno, debe ser compartida exclusivamente con las personas autorizadas a tener acceso a ella, y en los escenarios apropiados.

Manejo de contraseñas

No divulgue sus contraseñas a nadie: son secretas. Los usuarios que le han sido asignados para acceder a la información son personales e intransferibles. Cada usuario es responsable de todo uso que se le dé a sus cuentas en los sistemas. Incluso si otra persona las utiliza con o sin su permiso.

En caso de vacaciones o ausencias prolongadas, solicite al departamento de Informática la inactivación temporal de sus cuentas de usuario de los sistemas.

Toda desvinculación de funcionarios de la compañía, o cambio de funciones que implique revisar los privilegios sobre los sistemas, deben ser comunicados oportunamente al departamento de informática.

Tenga una clave segura: aplique las más estrictas normas cuando genere sus contraseñas. Las claves sólo protegen los sistemas de información si se siguen los procedimientos correctos de seguridad.

Si sospecha que alguien más conoce su contraseña, cámbiela de inmediato.

Use claves con calidad:

- Combinación de letras, números y caracteres especiales.

- No use apellidos, nombres o iniciales de sus hijos, o cualquier cosa que pueda ser fácilmente relacionada con usted.

- Nunca escriba su clave. Apréndasela de memoria.

- Cambie su clave periódicamente y no reutilice claves antiguas.

Dispositivos móviles

Cada vez se guardan más datos en aparatos móviles, incluyendo portátiles, pockets, teléfonos celulares, memorias USB, CD's o DVD's, cámaras digitales y reproductores de música.

Los dispositivos portátiles son cada vez más ligeros, pequeños y fáciles de llevar consigo. Pero también, es cada vez más fácil que se pierdan o sean robados.

Recuerde que está prohibido copiar información de propiedad de la empresa en equipos personales. Esto incluye todo tipo de equipos móviles, así como los ordenadores de su casa.

La información confidencial de la compañía ***NO*** debe ser copiada en medios de almacenamiento removibles (USB, CD, DVD). En caso de ser estrictamente necesario, copiar este tipo de información, sólo se puede hacer esta copia con la previa aprobación del dueño de la información, y en medios aprobados por la dirección de informática.

Por otro lado, la información deberá ser grabada de forma segura: bajo técnicas de cifrado de datos, como mínimo estableciendo una contraseña fuerte y compresión en ZIP. Siga las recomendaciones ya dadas para construir sus contraseñas.

En caso de viaje, los equipos portátiles deberán ser llevados como equipaje de mano. Al transportar un equipo portátil en un vehículo, éste deberá ser guardado en un lugar seguro. Nunca coloque estos equipos en lugares visibles o al alcance de extraños.

Riesgos con terceros

Muchos de los incidentes de seguridad, no se deben a ataques técnicos, sino al aprovechamiento de la falta de conciencia sobre la seguridad de la información o por el descuido de los empleados.

Uno de los principales riesgos con terceros, es la técnica conocida como Ingeniería Social, considerada como el método más efectivo de ataque por parte de un hacker.

La ingeniería social es un intento de manipular a una persona, para que facilite información que no debería revelar. Por ejemplo, alguien haciéndose pasar por un alto directivo en tono amenazante, o por un proveedor o cliente que exige recibir información por teléfono, o que la información se le envíe a una dirección de correo electrónico que no esté registrada.

Una forma habitual y frecuente de ataque por parte de terceros, es el método conocido como “Phishing”. El “Phishing” generalmente se realiza mediante mensajes de correo electrónico, que contienen enlaces a sitios Web que parecen ser el sitio original. Usualmente, se busca obtener información bancaria de personas o empresas, suplantando un remitente legítimo y de confianza, por ejemplo, un banco. El atacante puede solicitar contraseñas o datos bancarios, por ejemplo, números de tarjetas de crédito, que serán utilizados para adquirir ilegalmente bienes y servicios.

Para protegerse de este tipo de ataques, atienda las siguientes recomendaciones:

- Revele información solamente si está autorizado a hacerlo.
- No diga más de lo necesario.
- Notifique siempre los intentos por obtener información que le parezcan sospechosos.

- No conteste los correos electrónicos “phishing”, simplemente repórtelos y bórrelos.

Riesgos del correo electrónico

El correo de la empresa, debe ser empleado para fines laborales.

Nunca envíe información de la empresa a través de correos personales (hotmail, yahoo, gmail) o servicios de mensajería instantánea (MSN Messenger, Yahoo Messenger, ICQ).

Los correos de origen desconocido deben ser eliminados sin abrirse, dado el riesgo de que contengan virus o cualquier otro mecanismo peligroso.

No utilice firmas “escaneadas” en correos electrónicos y documentos anexos.

No participe en cadenas de mensajes.

Asegúrese siempre de haber especificado los destinatarios correctos antes de enviar el mensaje.

Virus y programas maliciosos

Los virus y otros programas maliciosos pueden causar el mal funcionamiento de su computador, pérdida de datos e incluso el envío de información confidencial para personas externas.

Informe al departamento de informática inmediatamente, si su computador tiene algún comportamiento extraño, o si sospecha que tiene algún tipo de virus o software malicioso.

Cuando su equipo de cómputo permanezca desconectado de la red interna por períodos prolongados (en caso de viajes, licencias, vacaciones), ejecute una actualización manual de los sistemas de protección, tan pronto el equipo sea conectado a la red nuevamente.

Hardware y Software

No se permite la instalación de ningún software adicional al aprobado por la Compañía.

Nunca descargue software de Internet para ser instalado en su equipo de cómputo. Este puede contener virus u otro tipo de software malicioso.

Nunca realice intervenciones directas sobre el software o el hardware de los equipos de cómputo de la compañía. Es una responsabilidad que pertenece al departamento de informática.

Los equipos que no pertenezcan a la empresa (personales), no deben ser conectados a la red interna de la compañía. Por ejemplo, en el caso de un proveedor que requiera conectarse a la red, sólo lo podrá hacer obteniendo la previa autorización del departamento de Informática, luego de validar que su equipo no representa un riesgo para la información interna información.

Navegación segura en Internet

Internet ofrece una gran oportunidad para el intercambio de información y negocios electrónicos.

Sus beneficios vienen creciendo para nuestro negocio con el pasar del tiempo. Sin embargo, el uso inadecuado de Internet puede causar severos daños a la compañía.

Ingrese a Internet sólo a través de herramientas aprobadas por la Dirección de Informática (navegador instalado en su equipo).

Navegue por Internet dentro de los horarios laborales, exclusivamente en sitios que tengan relación con las funciones que usted desempeña en la empresa.

Absténgase de ingresar a sitios con contenidos que pueden poner en riesgo la seguridad de la red interna, porque pueden contener elementos como virus u otro tipo de software malicioso (páginas de sexo, entretenimiento, hacking, entre otros).

Seguridad en casa

Recuerde que sus familiares o amigos no están autorizados a utilizar equipos de cómputo de la empresa, ni tampoco deben tener acceso a la información de la compañía.

En caso de llevar información de la compañía a su casa, debe almacenarla en forma segura, evitando el acceso de terceros. No está permitido conservar información de la empresa fuera de la compañía, devuélvala inmediatamente después de usarla.

Como se ha podido apreciar en los temas tratados hasta el momento, el acceso y uso de información de la compañía requiere de ciertas precauciones en cualquier lugar en que usted se encuentre: en la oficina, en su casa y en sitios públicos.

Recuerde que es su responsabilidad garantizar la protección adecuada de la información que le ha sido confiada por la empresa.

Para evaluar si los mensajes transmitidos en este programa han sido comprendidos y han llegado a todos los empleados de la empresa, se exigirá la realización del examen siguiente.

Al finalizarlo, obtendrá su puntaje estableciendo el porcentaje de respuestas correctas. El examen será aprobado con un setenta por ciento o más de aciertos.

Entonces, esta información deberá ser utilizada exclusivamente para generar estadísticas sobre la cantidad de personas que han completado con éxito el programa (sin indicar los puntajes), datos que serán presentados a la Gerencia General, clasificados por área y funcionario.

Una vez comenzada la evaluación, ésta no deberá ser interrumpida.

Afirmación	Verdadero	Falso
1. Si mi jefe me solicita mi contraseña de acceso a los sistemas de la compañía debo revelársela.		
2. Sólo la información impresa debe ser etiquetada como “Confidencial”.		
3. Los borradores dañados de documentos clasificados como “Confidenciales” o “Privilegiados” pueden botarse sin problema a la papelera.		
4. En caso de vacaciones o ausencias prolongadas debo solicitar al Departamento de Informática		

	inactivación temporal de todas mis cuentas de usuario.		
	5. Está prohibido copiar información “Confidencial” o “Privilegiada” de la empresa en equipos de cómputo personales (PC, USB, IPOD, MP4, portátiles, pockets) u otros medios de almacenamiento que no pertenezcan a la compañía.		
	6. Estoy autorizado a facilitar cualquier información de la Compañía a una persona que trabaje para la misma.		
	7. No está permitido enviar información de la empresa a través de correos personales (hotmail, yahoo, gmail) o servicios de mensajería instantánea (MSN Messenger, Yahoo Messenger).		
	8. Los correos de origen desconocido y cadenas de mensajes deben ser eliminados sin abrirse, dado el riesgo de que contengan virus o cualquier otro mecanismo peligroso.		
	9. Se pueden traer equipos personales a la empresa y conectarlos a la red interna para realizar funciones de mi trabajo.		
	10. No estoy autorizado a instalar software en mi equipo de cómputo, por ejemplo, para escuchar música o para realizar tareas que no tengan que ver con mis funciones en la		

compañía.		
11. La información propiedad de la empresa se clasifica en las siguientes tres categorías: abierta, común y secreta.		
12. Al abandonar mi puesto de trabajo, puedo confiar en que mi equipo de cómputo se bloqueará automáticamente, por lo tanto, no debo tomar ninguna medida de seguridad adicional.		
13. Una forma segura de compartir información con otros usuarios de la red interna, es a través de carpetas compartidas y estableciendo los permisos adecuados.		
14. Es seguro crear accesos directos a información “Confidencial” o “Privilegiada” en el escritorio de mi equipo de cómputo.		
15. Si los funcionarios de soporte a usuarios del Departamento de Informática piden mi contraseña de usuario para atender un requerimiento, debo revelársela.		

Tabla 5.1: Examen sobre seguridad de la información.

A continuación, se relacionan las respuestas correctas a cada una de las afirmaciones anteriores.

Respuestas
1. FALSO: las contraseñas no se comparten con nadie. Estas son personales e intransferibles. Toda transacción que se realice en los sistemas a través de los usuarios que le han sido asignados es su responsabilidad, sin excepciones.
2. FALSO: toda la información clasificada como “Confidencial” generada en medios físicos (papel), o electrónicos: informes, presentaciones en pantalla, archivos digitales (word, excel, power point, project), mensajes electrónicos y medios de almacenamiento (cintas, CD, DVD); debe ser etiquetada como tal.
3. FALSO: los borradores y copias malas contienen la misma información valiosa que el documento final. Deben recibir el mismo tratamiento seguro de la versión definitiva. Nunca recicle papel con información “Confidencial” o “Privilegiada”. Esta información debe ser destruida si no va a ser utilizada.
4. VERDADERO: cuando un funcionario sale a vacaciones, o se va a ausentar por un periodo largo de tiempo (por ejemplo licencias o incapacidades), se debe comunicar al Departamento de Informática esta novedad, solicitando la inactivación temporal de las cuentas de usuario de los sistemas. Recuerde que toda transacción que se realice en los sistemas a través de los usuarios que le han sido asignados es su responsabilidad.
5. VERDADERO: las políticas de seguridad de la información de cualquier empresa, deben prohibir copiar información “Confidencial” o “Privilegiada” propiedad de la compañía en equipos personales.
6. FALSO: antes de revelar información, debo asegurarme de que la persona esté autorizada. La información que ha sido clasificada como “Confidencial” o “Privilegiada” sólo puede ser conocida por un determinado grupo de personas.
7. VERDADERO: el único medio autorizado para enviar información de la empresa, es el servicio de correo electrónico que provee la misma a sus empleados.
8. VERDADERO: el correo electrónico es una fuente importante de infección de virus y otros tipos de software malicioso. Siempre que reciba correos de origen desconocido, o reenvío de cadenas de mensajes, elimínelos sin

abrirlos.
9. FALSO: sólo los equipos asignados por la compañía pueden ser conectados a la red interna. Incluso si un proveedor requiere conectarse a la red, se debe obtener la autorización previa del departamento de informática.
10. VERDADERO: los únicos funcionarios autorizados para realizar cualquier intervención sobre los equipos de cómputo de la compañía, son los del área de soporte a usuarios del Departamento de Informática.
11. FALSO: La información propiedad de QUALA se clasifica en cuatro categorías: Pública, Interna, Privilegiada y Confidencial.
12. FALSO: siempre que abandone su puesto de trabajo, debe asegurar que su equipo de cómputo permanezca bloqueado, oprimiendo las teclas CTRL+ALT+SUPR y ENTER. El bloqueo automático solo se activa después de un periodo de inactividad, tiempo en el cual alguien puede suplantar su identidad en la red, e incluso robar información de la compañía.
13. VERDADERO: windows permite compartir información a usuarios o grupos de usuarios a través de la red de forma segura, siempre y cuando nos aseguremos de asignar correctamente estos permisos. Esta práctica es más segura que la copia de información en medios externos como USB's, CD's, DVD's los cuales se pueden llegar a perder fácilmente.
14. FALSO: nunca debe crear accesos directos a información clasificada como "Confidencial" o "Privilegiada". Esto facilita en gran medida las acciones indebidas de alguien que quiera robar información de la Compañía.
15. FALSO: las contraseñas de usuario son estrictamente personales. En caso de requerir ingresar con su cuenta de usuario a su información, esto debe hacerse bajo su estricta supervisión.

Tabla 5.2: Respuestas al examen en seguridad de la información

CAPÍTULO 6

PROTEJAMOS NUESTRA INFORMACIÓN

6.1 Introducción

La información es uno de los activos más importantes para la compañía, y por lo tanto, se le debe dar un tratamiento seguro. Independiente del cargo que se ocupe en la empresa, se maneja información que es esencial para los intereses de la compañía.

En consecuencia, la información corporativa únicamente debe ser revelada a las personas autorizadas a tener acceso a ella. Por otra parte, no debe ser manipulada afectando los objetivos de la compañía, y debe estar siempre disponible cuando el negocio lo requiera.

Gracias a la rápida evolución de las Tecnologías de Información y Comunicación TIC's, las compañías a nivel mundial han identificado problemáticas que no se pueden subsanar solamente con la implementación de controles en los sistemas de información o adquiriendo nuevos componentes de infraestructura (firewall, detector de intrusos). Los riesgos han evolucionado, por lo que ya no se habla únicamente de Seguridad Informática, sino que se ha avanzado hacia un marco más conceptual de Seguridad de la Información.

Últimamente, se viene dando el cambio a seguridad de la información como traducción más adecuada de *information security*. Pero pese a ello, todavía existen muchos especialistas que siguen llamando así al puro enfoque técnico comentado previamente.

En realidad, la seguridad de la información es bastante más amplia, porque no es simplemente una cuestión técnica, sino una responsabilidad de la alta gerencia y de los cuadros directivos de una organización. En tal sentido, hay que tener en cuenta que el ambiente TIC's tiende a estar orientado al servicio y a actuar como función habilitante de los procesos de negocios. En esto difiere de los procesos centrales mismos de una organización, que constituyen el núcleo de los negocios de una empresa.

De hecho, sin involucrar activamente las unidades y líderes de negocio, ejecutivos y directivos, no puede existir un plan sustentable de seguridad de la información a partir de los riesgos determinados. Y todo esto dentro del sistema de dirección y control propio de un adecuado gobierno corporativo, como define la OECD (Organización para la Cooperación y Desarrollo Económico, OCDE en español) al ***corporate governance***. Ahora se trata, entre otras cosas, de considerar también a la gente, los procesos y funciones de negocio, la protección de todos los activos/recursos de una organización; en donde toda la empresa es la impulsora, propietaria y beneficiaria de la seguridad de la información, en un marco de responsabilidades compartidas.

La extensión del concepto usual de seguridad informática al de seguridad de la información, implica un corrimiento y visión más amplia de un marco de riesgos de negocios respecto de la perspectiva tradicional de seguridad técnica,

basada principalmente en vulnerabilidades. Según lo visto anteriormente, tal extensión se da de dos maneras. Por un lado, en el contexto de la seguridad de la información los riesgos de negocios incluyen no sólo las vulnerabilidades y un aspecto de las amenazas, sino el conjunto de los factores que determinan tales riesgos: activos, vulnerabilidades y amenazas. Por otra parte, los riesgos de negocios que se consideran incluyen los riesgos organizacionales, operacionales, físicos y de sistemas TIC's.

En todo este escenario, especialmente de riesgos organizacionales y operacionales, aparece un factor generalmente descuidado y aún desconocido en la implementación de medidas de seguridad. Se trata del factor gente, porque tales medidas requieren cambios de comportamiento y actitudes, lo que puede entrar en conflicto con los esquemas de la mayoría de las personas, por su resistencia natural a los cambios y los mecanismos de defensa que se disparan para el caso (Ormella, 2006). Una visión ilustrativa de tales conceptos puede visualizarse en la figura 6.1.

Figura 6.1: Seguridad informática vs. Seguridad de la información, **Fuente:** Ormella, 2006.

Con el fin de proteger la información crítica y crear consciencia sobre la importancia de la Seguridad de la Información, se ha diseñado el programa ***"LO QUE CREEMOS SABER Y EN REALIDAD DESCONOCEMOS"***.

6.2 ¿Por qué desarrollar el programa?

Debido al rápido crecimiento de las compañías, estas son cada día más visibles, y se ven expuestas a que otras personas quieran obtener su información. Por lo tanto, el conocimiento se convierte en el diferencial mayor frente a los competidores, lo que redunda en un tratamiento seguro de la información.

En este orden de ideas, el acceso y uso de la información requiere de ciertos cuidados. Todos los funcionarios de la organización, deben ser responsables de su protección. Los funcionarios requieren de una capacitación formal en Seguridad de la Información, de modo que sean la primera línea de defensa de este activo valioso.

6.3 Mecanismos y herramientas esenciales para garantizar el éxito del programa

Todos los funcionarios de nivel directivo, profesional y medio de la compañía deben completar satisfactoriamente el programa, a través de una sesión de capacitación en la intranet. Al final del programa, el funcionario deberá aprobar la evaluación del mismo con un 75% o más de respuestas correctas.

Todos los funcionarios que completen el programa deberán firmar un contrato de Seguridad de la Información, ratificando su compromiso con el cumplimiento de las políticas de Seguridad de la Información de la compañía. Este documento deberá se anexado a la hoja de vida.

6.4 Beneficios

Los beneficios más significativos que tiene el programa son:

- Fomentar la disciplina de los funcionarios en el cuidado de la información que manejan.

- Salvaguardar el conocimiento de la compañía para lograr ser exitosos.

- Asegurar la continuidad del negocio, conservando la información que es propiedad de la compañía.

6.5 Punto de vista de la dirección

Si bien es difícil vender a la directivas de cualquier compañía la idea de crear planes de sensibilización que aseguren unas mejores prácticas de sus empleados en temas como la seguridad de la información, se siente satisfacción cuando estas ideas se materializan, se implementan programas como el aquí propuesto, se logran buenos resultados y se aprecian opiniones como la siguiente: *“El programa*

de concienciación LO QUE CREEMOS SABER Y EN REALIDAD DESCONOCEMOS, a mi modo de ver las cosas, es una estrategia excelente para asegurar nuestra información, puesto que en primer lugar tiene un efecto psicológico para las personas que están manejando información sensible, de tal manera que siempre se están acordando de lo importante que es para la compañía el manejo de la confidencialidad, además es muy positivo que se complemente con algún tipo de herramienta que permita monitorear el comportamiento de dicha información clasificada, de tal manera que el funcionario pueda darse cuenta, gracias a una serie de alertas o mensajes emergentes, que está manejando información crítica, y que por tal debe darle tratamiento seguro. Por otra parte, también es muy positivo que la actitud sea formadora, puesto que seguramente la mayoría de personas que pierden información o permiten la fuga de esta, no lo hacen de 'mala voluntad', sino que se les olvida o cometen errores inconscientes. Este programa ayuda a los empleados a tomar conciencia de las faltas contra la seguridad que puede estar cometiendo", Gerente General.

CAPÍTULO 7

BALANCE DEL PROYECTO FINAL DE ESPECIALIZACIÓN

7.1 Conclusiones

7.1.1 Conclusiones Generales

La información es uno de los activos más importantes para la compañía, y por lo tanto, se le debe dar un tratamiento seguro. Lo anterior, hace que la información se convierta en el eje central sobre el cual gira la seguridad, definiendo acciones de protección y mecanismos de control para garantizar al negocio, la confiabilidad de dicha información.

La confidencialidad de la información es una característica requerida para las organizaciones modernas, donde no satisfacerla adecuadamente, implica posibles fallas que pueden poner en riesgo los negocios. Por ende, comprender la inseguridad de la información, más que detectarla, exige una reflexión profunda de la organización para avanzar en la gestión de la seguridad de la información (Cano, 2007).

Una forma de garantizar el tratamiento seguro de la Información sensible y confidencial de la compañía, evitando que ésta se vuelva pública de forma no

autorizada, es el diseño e implementación de un programa de concienciación en Seguridad de la Información que pueda ser usado por las empresas para mostrar a los empleados, aquellos comportamientos que pueden provocar un problema de Seguridad para la protección de los activos de Información de cualquier empresa.

7.1.2 Conclusiones teóricas

La seguridad es subjetiva y será diferente para personas de todo tipo, porque cada una de ellas determina su nivel de riesgo y evalúa sus estrategias compensatorias frente a los controles (Schneier, 2003). Es por esto, que en este programa de concienciación, la empresa debe transmitir de forma clara y precisa los objetivos del mismo y paralelamente, el riesgo de desconocer las buenas prácticas para el uso seguro de la tecnología, pero sobretodo, debe sensibilizar a los funcionarios de la compañía acerca que la protección de la información es responsabilidad de todos.

La seguridad no es una función que pueda ser verificada, como una reacción química o un proceso de manufactura. Por el contrario, solamente es efectivamente verificada cuando algo no sale bien; el atacante debe ser parte del diseño de un sistema de seguridad, así, el sistema debe tomar en cuenta el atacante para mantenerse seguro (Schneier, 2003). Por lo anterior, es también importante, que la empresa se comprometa con la definición, publicación y socialización de políticas de seguridad de la información, sin restar importancia a ninguna de estas tres acciones, porque esto permitirá al menos tener una guía, para saber lo que se debe y lo que no se debe hacer en cuanto a seguridad de la información.

Por otro lado, los sistemas de mensajería instantánea, así como las redes de igual a igual o P2P (Las cuales reciben su nombre porque no existe un servidor definido, sino que todos los usuarios son clientes y servidores de forma simultánea), facilitan la colaboración entre las personas, permiten expresar opiniones, compartir y buscar información que les asista en su constante necesidad de estar informados sobre las temáticas que son de su interés. En este escenario, la inseguridad de la información se materializa en vulneración de la privacidad de la información, la fuga de información sensible, la porosidad de un perímetro extendido y el mal uso de los datos para efectos de inteligencia o actividades ilícitas, así como también pueden llegar a ser puertas de entrada para todo tipo de software malicioso como virus, troyanos o gusanos. En consecuencia, las organizaciones, de cara a estos retos nuevos que propone la inseguridad, requieren establecer acciones propias de la gestión de la seguridad que permitan enfrentar y asegurar los riesgos que un escenario interconectado, global, poco regulado, altamente consultado y vulnerable, establece para los responsables de la seguridad de la información corporativa (Wilbanks, 2008).

7.1.3 Conclusiones metodológicas

Es necesario comprender donde se origina y a quienes afecta la información dentro de la organización, y cómo a través de la seguridad de la información se puede generar valor para la compañía. Cuando se establece que la información es un activo estratégico tan importante como las utilidades o las instalaciones, la gerencia establece los recursos y atención necesario para avanzar en una estrategia conjunta que permita asegurar la operación de la firma y la información que en ella se crea, transmite, transporta, almacena, recupera y destruye.

Cuando se logra incorporar la seguridad de la información dentro de los procesos de negocio, como parte normal de diseño y operación del mismo, las inversiones en seguridad dejan de ser un costo, y se convierten en una parte inherente dentro de la operación del negocio. Lograr esta transformación, no sólo requiere de un entendimiento de la seguridad dentro de la cultura organizacional, sino la materialización del concepto de seguridad dentro de los comportamientos de los individuos (Cano, 2009).

Comenta Walter Riso en su libro ***"Cuestión de dignidad"***, que ***"la prudencia nos obliga a deliberar con nosotros mismos, es la que gobierna nuestros deseos y suaviza nuestros impulsos"***, si esto es correcto, nuestras actividades y acciones frente a un paseo por el mundo de Internet, debería tener la misma connotación. Es decir, nuestro criterio y atención activa debería ser la constante cada vez que navegamos por Internet (Cano, 2009).

7.2 Recomendaciones

Un primer elemento dentro de la organización, es la cultura de seguridad de la información. Siguiendo las consideraciones del Dr. Edgar Schein, sobre cultura organizacional, una cultura esta compuesta por tres componentes: los artefactos, (lo que se observa, se ve, se siente y escucha), símbolos y comportamientos, (los valores expuestos, es decir, lo que le dicen) y finalmente, los supuestos básicos, aquello que los participantes dan por hecho.

Con base en lo anterior, podríamos decir que la cultura es la base fundamental de la gestión de la seguridad, entendida ésta como la promoción

inherente y natural de ***comportamientos confiables*** de las personas que permitan interiorizar la distinción de prácticas de protección coherentes con las políticas internas, el fortalecimiento de una percepción y administración del riesgo, el convencimiento emocional de una actitud de autocuidado, los impactos financieros de acciones inseguras y sobre manera, el interés y entendimiento propio de las regulaciones que sobre el tema se tienen. La cultura de seguridad de la información debe ser el animador y custodio de variables tan importantes para las organizaciones como su reputación, los ingresos, el cumplimiento regulatorio, la percepción del cliente y los fujos de información en los procesos (Westney, 2008).

7.3 Limitaciones

"Si bien la inversión en tecnologías de seguridad de la información no producen claramente un retorno sobre la inversión, sobre todo cuando las directivas se basan en hechos y datos (Valor monetario), esta inversión, focaliza las energías en la generación de 'expectativas y contextos' en los clientes que directamente benefician las relaciones con los terceros. La seguridad de la información al ser parte de la construcción de confianza y valor con los clientes, se hace una aliada estratégica del negocio" (Cano, 2009). La seguridad de la Información nunca va a devolver dinero de forma tangible para la compañía como una venta o la prestación de servicio, y esto es lo que hace que la gerencia muchas veces no decida invertir en seguridad. Lo que hay que hacer, es aprender de la experiencia del investigador, y elaborar un plan donde se muestre a las directivas que el retorno es intangible, porque este se logra apreciar en el mejor comportamiento de los empleados, en un fortalecimiento de la cultura organizacional, en un mayor sentido de pertenencia sobre la misma y en el ahorro de recursos que la seguridad de la información puede ofrecer, en caso de materializarse una amenaza.

7.4 Investigaciones futuras

La inseguridad vive un proceso evolutivo de nunca acabar por lo que la empresa siempre debe estar a la expectativa de lo que la inseguridad pueda ofrecer. Por tal motivo, el equipo de seguridad debe estar siempre preparado para enfrentar los retos que se presenten. El equipo de seguridad debe ser un estratega dispuesto a sugerir planes que administren los riesgos y garanticen la continuidad del negocio. Afirma James E. Lukaszewski, "*Ser un estratega significa tener un compromiso con una aproximación mental que piensa más allá de la competencia, la oposición o la crítica y produce un modelo distintivo o único, una serie de pasos, opciones de solución u opciones de dirección*". Así mismo, continúa, "*la estrategia es el atrayente o la motivación que convoca a la gente y la ayuda a tener foco para moverse en la misma dirección*".

Con base en lo anterior, se considera que un área clave para investigaciones futuras, puede ser la informática forense, donde se podrán realizar estudios de huellas digitales que quedarían en cualquier sistema si llegasen a fallar nuestros aportes a la cultura de seguridad. Es decir, la informática forense permite identificar o detectar si un funcionario viola las políticas de seguridad de la información.

BIBLIOGRAFÍA

ALDEGANI, G. (1997). Seguridad informática. Mp Ediciones.

ANDREWS, K. (1977). El concepto de estrategia en la empresa. Universidad de Navarra.

ANSOFF, H. (1976). La estrategia de la empresa. Universidad de Navarra.

ARIAS, J. A. (2009). "Los ocho pecados mortales de la dirección", [en línea], disponible en: http://www.gestiopolis.com/administracion-estrategia/los-siete-pecados-mortales-de-la-direccion.htm, recuperado: 30 de enero de 2010.

ARDITA, J. (2001). Director de Cybsec S. A. Security System y ex-hacker, [En línea], disponible en: http://www.cybsec.com, recuperado: 30 de enero de 2010.

BARNETT, S. (1999). Computer Security Training and Education: A Needs Analysis. IEEE Symposium on Security and Privacy 1980 – 1999.

CANO, J. (2004). Administrando la Inseguridad Informática. Hackin9 – El registro de Windows. Abril.

CANO, J. (2004). Inseguridad Informática: Un concepto dual en seguridad informática. Universidad de los Andes, Facultad de Ingeniería, Mayo.

CANO, J. (2005). Concepto Extendido de la Mente Segura: Pensamiento Sistémico en Seguridad Informática. Universidad de los Andes, Facultad de Ingeniería Septiembre.

CANO, J. (2007). Administrando la confidencialidad de la información: Algunas consideraciones sobre el saneamiento de medios de almacenamiento. AR: Revista de Derecho Informático.

CANO, J. (2009). Los engaños en Internet: De las cadenas, del correo no deseado, de la mensajería basura y otros demonios.

CANO, J. (2009). Focalícese en la articulación de valor más que en el retorno de la inversión. IT-Insecurity, Agosto.

CANO, J. (2009). Fraude y Fuga de Información: Inseguridad en dos sectores críticos. IT-Insecurity, Noviembre.

COLE, E. (2002). Hackers beware. Defending your network from the wiley hacker. New Riders.

DAVENPORT, T.O. (1998). Capital humano. Ediciones Gestión 2000.

DAY, K. (2003). Inside the security mind. Making the tough decisions. Prentice Hall.

EDVINSSON, L. y MALONE, M.S. (1999). El capital intelectual (cómo identificar y calcular el valor de los recursos intangibles de su empresa). Ediciones Gestión 2000.

EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY, ENISA. (2006). Guía del usuario: Elaborar programas de sensibilización sobre la seguridad de la información. Junio.

FUNIBER (2007). Modulo de Administración y Dirección de Empresas. Fundación Universitaria Iberoamericana.

GATES, B (1999). Los negocios en la era digital. Ediciones Plaza & Janes.

HANCOCK, W. y RITTINGHOUSE, J. (2003). Cybersecurity Operations Handbook. Elsevier Digital Press.

HARPER, S. y LYNCH, J. (1992). Manuales de recursos humanos. Ediciones La Gaceta de los Negocios.

HORTON, M. y MUGGE, C. (2003). Network Security Portable Reference. McGraw Hill.

International Organization for Standardization. ISO / IEC 27001:2005ICOVE, D., SEGER, K. y VONSTORCH, W. (1995). Computer Crime. A Crimefighter's handbook. O'Reilly & Associates.

KRAUSE, M. y TIPTON, H. (1999). Handbook of Information Security Management. Auerbach.

LAPRIE, J. C. (1991). Dependability: Basic concepts and terminology. Springer-Verlag.

LLANES, W. (2004). La dirección estratégica en la empresa. Ediciones Centro de Estudios de Técnicas de Dirección (CETDIR).

MELZNER, S. (2009). "La diferencia entre datos e Información", [en línea], disponible en: http://sergiomelzner.com/negocios/la-diferencia-entre-datos-e-informacion/, recuperado: 30 de enero de 2010

MENGUZZATO, M (1991). La dirección estratégica de la empresa. Editorial Ariel.

MEYER, G. R. (1989). The Social Organization of the Computer Underground. PhD thesis, Northern Illinois University,

"Manual de Seguridad en Redes", [en línea], disponible en: http://www.arcert.gov.ar/webs/manual/manual_de_Seguridad.pdf, recuperado: 10 de enero de 2010.

NORTON, D.P. (2001). Medir a criação de valor, uma tarefa possível, em revista HSM Management, Ano 4, No.24, pp.88-94. Ed. Savana, São Paulo.

OLOVSSON, T. (1992). A structured approach to computer security. Technical Report 122. Chalmers University of Technology.

ORMELLA, C. (Sin fecha). “Seguridad informática vs. Seguridad de la información”, [En línea]. Disponible en: http://www.cai.org.ar/dep_tecnico/comisiones/CETI/trabajos/200905_informatica_vs_informacion.pdf, recuperado: 10 de enero de 2010.

ORMELLA, C. (2006). ROSI, Retoro sobre la inversión en seguridad.

PARKER, D. (1998). Fighting Computer Crime. A new framework for protection information. John Wiley & Sons.

PFLEEGER, C.P. (1997). Security in computing. Prentice Hall.

PROCTOR, P. y BYRNES, F. C. (2002). The secured enterprise. Protecting your information assets. Prentice Hall.

SANDOVAL, F. (2005). “Seguridad de la Información”, [en línea], disponible en: http://www.denegocio.com.mx/051012Seguridad.htm, recuperado: 10 de enero de 2010.

SCHETINA, E., GREEN, K. y CARLSON, J. (2002). Internet Site Security. Addison Wesley.

SCHNEIER, B. (2003). Beyond Fear: Thinking Sensibly about security in an uncertain world. Copernicus Books.

SEGU-INFO. “Políticas de Seguridad de la Información”, [en línea], disponible en: http://www.segu-info.com.ar/politicas/polseginf.htm, recuperado: 10 de enero de 2010.

VILLALÓN, A. (2002). “Seguridad de Unix y Redes Versión 2.1”, [en línea], disponible en: www.rediris.es/cert/doc/unixsec.pdf, recuperado: 10 de enero de 2010.

SMITH, A. (1937). Wealth of Nations. Ed. P.F. Collier & Son. New Cork.

THUROW, L. (1992). La guerra del siglo XXI. Editorial. Vergara.

VALDÉS, C. (2008). “Estrategia y Dirección Estratégica”, [en línea], disponible en: http://www.gestiopolis.com/administracion-estrategia/direccion-estrategica-concepto-de-estrategia.htm, recuperado: 10 de enero de 2010.

WESTNEY, E. (2008) Three perspectives on organizational change. Leading Change in Complex Organization. MIT Sloan School of Management. Executive Program. June

WHITTAKER, J. (2003). How to break software. A practical guide to testing. Addison Wesley.

WILBANKS, L. (2008). Need to share vs. need to assure. IEEE IT Professional. May/June.