Universidad Latinoamericana de Ciencia y Tecnología

Escuela de Administración

Licenciatura en Administración de Empresas

Tutor: MBA Carlos Soto

"La administración del riesgo informático-tecnológico en las empresas costarricenses"

Gustavo A. Núñez Carballo
1-779-737

Mayo, 2003

TABLA DE CONTENIDOS

TABLA DE GRAFICOS

AGRADECIMIENTOS

A Dios por brindarme todo lo necesario para poder dar este paso.

A mi esposa y mis hijas por su sacrificio y amor.

A los profesores por su ayuda y colaboración.

Al recuerdo de mi Madre, quien en vida me dio todo.

INTRODUCCIÓN

La información es poder, reza una frase. Y sin embargo podemos hacerla más fuerte aun: la información bien resguardada no sólo es poderosa sino también muy valiosa. Estamos en una etapa de la era mundial en donde tener acceso a la información es algo tan sencillo como navegar en Internet y buscar lo que queramos, así de simple, pero también, por qué no, así de peligroso. Pero si nosotros, seres individuales nos preocupamos porque a una página de Internet le dimos algo de nuestra información personal, ¿cómo se sentirá una empresa al poner a disposición todo su ser empresarial a nosotros?. Por que así es. Las redes de computadoras se han convertido en herramientas del bien y del mal. ¿Exagerado? No cuando descubramos lo que sucede en el intrincado mundo de la tecnología y más aún cuando nos demos cuenta cuán preparadas están o no algunas de las empresas costarricenses. Y es que nos enteraremos que no sólo afuera hay peligro, sino que son en ocasiones, los de casa los malhechores más peligrosos. No compre cinco perros Bulldog si lo que necesita cuidar es un casa de ratones con sólo un acceso, pero tampoco compre un solo Pequinés si lo que espera cuidar es un castillo y sus múltiples puertas de entradas. Y aún si tiene un castillo y compra los Bulldog que necesite, pregúntese: ¿ya los entrenó?, ¿saben ellos lo que tienen que cuidar?, ¿distinguen ellos entre los de casa y los de afuera?, ¿contrató a los entrenadores correctos para que los administren?, ¿si un perro falla, puede otro tomar su lugar? Piense en todo esto y se dará cuenta que estamos hablando de algo muy serio.

CAPITULO I: JUSTIFICACIÓN, PROBLEMA, OBJETIVO E HIPÓTESIS

1.1 Justificación

Desde un usuario en su hogar, pasando por quien maneja su pequeño negocio, hasta llegar a las medianas y grandes empresas, todos utilizan la tecnología informática para ser mejores. Pero ¿cuán segura es esta herramienta?, ¿la última tecnología es infalible? Por supuesto que no. Pero la seguiremos utilizando, así que lo mejor será prevenir y minimizar la posibilidad ante cualquier tipo de pérdidas.

Los datos son reveladores y no podemos hacernos de la vista gorda solamente porque nuestro país es pequeño y no una potencia comercial como los Estados Unidos de Norteamérica. El informe "2002 Computer Crime and Security Survey" del Computer Security Institute (CSI) y de la Federal Bureau Investigation (FBI) confirman secretos a voces sobre la seguridad informática:

- El 90% de las empresas detectó violaciones en su seguridad.
- El 80% indicó pérdidas económicas debido a las violaciones de su seguridad.
- El 44% pudo cuantificar sus pérdidas económicas en $455,848,000.00
- Sólo el 34% reportó los incidentes a las autoridades.

Las empresas costarricenses en su mayoría se cuidan de la posibilidad de ingreso de un virus, pero nunca están al 100% a salvo, no aseguran sus sistemas informáticos contra las famosas y molestas "caídas". No guardan buen respaldo de sus negocios diarios. Somos casi por naturaleza seres reactivos y hoy en día la tecnología avanza a pasos agigantados, por lo que si apostamos a ella debemos movernos tan rápida y eficientemente como ella, o mejor aún anticipando sus jugadas.

La importancia de la seguridad de la tecnología informática en nuestras empresas proveerá herramientas para una mejor competencia a todo nivel, elevando productividad interna y confiabilidad en el usuario. De este modo nos evitaremos escuchar: "lo siento pero nuestro sistema se cayó".

1.2 Problema de Investigación

Actualmente el uso de la tecnología informática en las empresas costarricenses es indiscriminado y aumenta a pasos agigantados, sin que todas las empresas o usuarios estén conscientes de cuánto riesgo involucra esto. Los resultados de una encuesta nacional en los Estados Unidos de Norteamérica revelan datos importantes y la mayoría de ellos impresionantes. Este estudio confirma que la amenaza del crimen cibernético y otras violaciones de seguridad informática continúan sin tregua y que además la pérdida financiera continúa en ascenso vertiginoso. En Costa Rica no existen datos tan concretos como los norteamericanos porque en nuestro país el tema es relativamente nuevo en las empresas. Sin embargo ya varias empresas tanto privadas como públicas se han visto afectadas por la infección de diversos y famosos virus informáticos como el Nimda o el I LOVE YOU, sólo para citar un par. Ellos han visto cómo la operabilidad de sus sistemas se ve anulada por estas intromisiones y con lo cual su productividad también disminuye lo que nos permite sacar por conclusión simple que existe una pérdida financiera importante. Qué le parecería llegar a una compañía cualquiera, por ejemplo una agencia de viajes, en la cual usted necesita hacer una reservación en algún vuelo urgente, y sin embargo le comentan que en este momento “el sistema está caído”, ¿le suena conocido? ¡Claro! Esto le sucede a cientos de empresas diariamente, no importa si son públicas o privadas, y sin embargo para el usuario-cliente el problema es muy simple: “esta compañía no sirve” Fácil conclusión a la que usted y yo llegamos

cada vez que la respuesta es la anterior. Pero internamente ¿qué sucedió mal?, ¿cómo es posible que una empresa no pueda tener su sistema "arriba" todo el tiempo?

¿Cuán preparada estaba la empresa? Nadie está lo suficientemente preparado. Ahora bien, si una empresa decide entrar a competir utilizando la tecnología en todos sus términos, pero sobre todo la informática, ¿no será lo más lógico asegurarse de que esta herramienta no falle? Si bien hay empresas que lo hacen, la gran mayoría utiliza un pensamiento simplista para abstenerse de hacer mayores erogaciones, el cual es: "eso a mi no me va a pasar" y sin embargo siempre sucede lo inevitable, lo lógico que ocurre cuando ante un posible riesgo no nos preocupamos por prevenirlo: la desgracia.

Entonces podemos asignarle las causas del problema a varios aspectos elementales: la empresa tiende a no ponerle atención previo al aspecto de la seguridad tecnológica. Asumen, como mencionábamos anteriormente una posición de confort en donde, "mientras no me ocurra, no es conmigo". Normalmente los gerentes confían a plenitud en la tecnología y en quienes la administran. Ellos se encargan de comprar la tecnología que necesitan y la ceden a sus administradores de redes o de sistemas informáticos para que ellos la utilicen y controlen. Con esta administración la empresa espera prevenir algún evento futuro, lo cual bien sabemos que es casi imposible, sobre todo porque nunca sabremos en qué momento, cómo o quién nos puede atacar o qué tipo de

eventos nos pueden ocurrir. Aunado a todo lo anterior es importante mencionar que los equipos activos así como el software necesario para la implementación de un completo sistema de seguridad tecnológico representan una inversión financiera considerable que no todas las empresas parecieran estar aún muy convencidas de realizar.

Una correcta administración de la tecnología y los sistemas informáticos, ofrece a las empresas que apuestan por ellos, una amplia gama de opciones para competir fácil y flexiblemente a todo nivel, así que podemos afirmar que quien logra administrar mejor el riesgo que implica la tecnología podrá obtener una ventaja competitiva importantísima hoy en día en los negocios. Asimismo podemos argumentar, que aquellos que no inviertan correctamente en cuidar sus inversiones a nivel tecnológico, comenzarán perdiendo fe en sí mismos, credibilidad ante el cliente, perderán mercado y lógicamente obtendrán muchas pérdidas financieras importantes, lo que para muchas empresas podría significar el final de su carrera en los negocios.

Pero ante un panorama así de gris debemos buscar salidas apropiadas para cada problema, con el fin de salir gananciosos. Existen diversas formas de prevenir los ataques, caídas de sistemas y demás. Hablamos de una correcta y sencilla aplicación de políticas internas, de contratación de personal idóneo y hasta la compra de equipo sofisticado y programas especiales. Todo esto puede permitir a las empresas costarricenses trabajar en una era en donde la tecnología es cosa

diaria y en al cual debemos prevenirnos de los ataques y demás riesgos de la tecnología informática.

Definición del Problema

¿Cómo se puede disminuir el nivel de riesgo informático-tecnológico en las empresas costarricenses?

¿Cómo afecta directamente a las empresas la poca planificación en ésta área?

¿Cómo pueden atacar el problema?.

1.3 Objetivos

Objetivo General

- Evaluar los niveles de seguridad informática-tecnológica con respecto a la información administrativa y financiera en las empresas costarricenses.

Objetivos Específicos

- Analizar los modelos existentes de seguridad informática-tecnológica en las empresas costarricenses

- Estudiar los factores de riesgo informático-tecnológico a los que se ven sometidas las empresas costarricenses.

- Determinar los tipos de estrategias administrativas utilizadas por las empresas costarricenses y ver su incidencia en las políticas de seguridad informática-tecnológica.

- Analizar los perfiles de capacitación de las personas a cargo de velar por la seguridad tecnológica e informática de las empresas costarricenses.

- Estudiar la legislación informática-tecnológica costarricense existente que afecten el desarrollo de las operaciones en ésas áreas.

Objetivo de Propuesta

- Formular un procedimiento básico guía para la implementación de un sistema de seguridad informática-tecnológica para las empresas cuyo nivel de seguridad así lo requiera.

1.4 Variables

1- Seguridad Informática-Tecnológica

Definición Conceptual:

- Técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red y la información contenida en ellos frente a daños accidentales o intencionados.

Definición Operacional:

- Será todo aquello que le permite a las empresas evitar y/o defenderse de cualquier ataque, interno o externo, que pudiera causarle daños o pérdidas económicas, patrimoniales e intelectuales.

Definición Instrumental:

- La seguridad informática-tecnológica será analizada por medio entrevistas y encuestas a las empresas.

2- Modelos De Seguridad Informática-Tecnológica

Definición Conceptual:

- Un modelo representa algo digno de ser imitado

Definición Operacional:

- Serán aquellas estrategias, políticas e implementación de equipos y programas especiales que le han ayudado a las empresas que los utilizan seguridad en su entorno informático-tecnológico.

Definición Instrumental:

- Las entrevistas y los cuestionarios nos permitirán establecer junto con el conocimiento de la tecnología actual, los mejores modelos de seguridad informática-tecnológica implementados por empresas costarricenses.

3- Factores de Riesgo

Definición Conceptual:

- El riesgo es la opción de obtener un resultado negativo en alguna actividad. El factor de riesgo es aquella acción que nos provoca esa posibilidad de obtener el resultado negativo.

Definición Operacional:

- Serán todas aquellas acciones que le provocan a las empresas una posibilidad de riesgo o alguna pérdida económica, patrimonial e intelectual.

Definición Instrumental:

- Analizaremos las respuestas ofrecidas en las encuestas y en las entrevistas.

4- Estrategias Administrativas

Definición Conceptual:

- Es la planificación, organización y dirección que los gerentes han determinado para su empresa.

Definición Operacional:

- Serán todas aquellas prácticas y teorías que la dirección de la empresa ha desarrollado y que afectan directamente el desarrollo de la seguridad informática-tecnológica de la compañía.

Definición Instrumental:

- Las entrevistas, encuestas y consultas a la memoria de las empresas nos guiarán a la definición de ésta variable.

5- Perfiles de Capacitación

Definición Conceptual:

- Son las capacidades académicas de los encargados de administrar el sistema de seguridad informático-tecnológico de la empresa.

Definición Operacional:

- Es el grado de capacidad tanto académico como práctico de las personas encargadas de administrar todo el sistema de seguridad informático-tecnológico de la empresa y de sus habilidades para prevenir los riesgos.

Definición Instrumental:

- Entrevistas con los jefes de éstas personas así como con el departamento de recursos humanos. Las encuestas nos permitirán conocer éste detalle también.

6- Legislación

Definición Conceptual:

- Normas de carácter general y abstracto que regulan una serie de supuestos o relaciones indefinidas, que contienen un efecto jurídico concreto para todos y cada uno de los supuestos a los que la propia ley se refiere.

Definición Operacional:

- Cualquier artículo de cualquier ley que afecte el desarrollo de la seguridad informático-tecnológico de las empresas.

Definición Instrumental:

- Consulta a la legislación pertinente costarricense, y entrevista con juristas con experiencia en el tema.

1.5 Hipótesis

Las empresas costarricenses que se preocupan de su seguridad informática-tecnológica pueden prevenir los ataques y posibles pérdidas económicas, intelectuales y patrimoniales que éstos pueden provocar.

CAPÍTULO II: MARCO TEÓRICO

2.1 Enfoque Situacional.

Costa Rica es hoy por hoy una nación sumida en la era tecnológica. El apoyo que los distintos gobiernos le han brindado a este tema con el paso de los años, ha permitido cierto tipo de madurez. Costa Rica posee un mercado en donde existen más de 600 empresas que se dedican a la comercialización de la tecnología. Tiendas que venden computadoras, distinto hardware y software para empresa y hogar; empresas de servicios, mantenimientos y consultorías en el área tecnológica se encuentran por doquier en el Valle Central de Costa Rica.

La producción de software "made in Costa Rica" y por los mismos ticos, crece a pasos agigantados. No podríamos hablar del efecto que el acceso a las tecnologías de información de punta ha tenido sobre nuestro desarrollo, sin olvidarnos de algunas características de nuestro pueblo como son:

1. Educación gratuita y obligatoria desde 1869.
2. Abolición del ejército en el año 1949
3. Garantías sociales de acceso a todos nuestros compatriotas desde 1943.
4. Manutención de un régimen de derecho y gobiernos democráticos, con una total estabilidad política.

5. Disminución de los impuestos de los Computadoras, a partir del año 1985.
6. Creación de la Fundación Omar Dengo e instauración de los laboratorios informáticos, en todas las escuelas y colegios públicos del país.
7. Clara decisión de nuestros gobernantes en la utilización de la tecnología y los sistemas de información para la mejora de los servicios.
8. Creación del Centro Nacional de alta tecnología en el año 1997.
9. Implementación del acuerdo de la Organización Mundial del Comercio, incluyendo el Acuerdo de los ADPIC (Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio).
10. Instauración del programa de mejoramiento del sector Software de Costa Rica.
11. Firma de la Declaración Ministerial sobre el Comercio de Productos de Tecnología de la Información (también conocido como el "Acuerdo ITA", según sus siglas en inglés).

Tales son las oportunidades e igualmente importante la calidad de los ticos en esta área donde localmente existen más de 130 empresas dedicadas al desarrollo de software, con una gran diversidad de aplicaciones disponibles caracterizadas por su alta calidad y funcionalidad, que convierten al país en la nación con más desarrolladores de Software per cápita en el mundo.

Estas y otras características han posicionado al Software de Costa Rica como uno de los más cotizados del mercado internacional, tanto por su calidad y costo, como por el respaldo que ofrece. Según información recabada de la Promotora de

Comercio Exterior, actualmente, más de un 70% de las empresas locales exportan a diversos mercados, distribuidos en los cinco continentes del mundo, con un crecimiento acelerado en todas las áreas.

2.2 Enfoque Conceptual.

"La seguridad no es un producto, es un proceso. Usted no puede solo añadirla a un sistema después de un incidente. Es vital entender los riesgos y amenazas reales, diseñar políticas de seguridad para llevar esos riesgos y amenazas a niveles aceptables, y trabajar con medidas apropiadas para su prevención." Bruce Schneier (2001)

La definición de este experto en seguridad es la precisa para el desarrollo de nuestra investigación. Existen además términos ligados al de seguridad y que están en contraposición pero que se derivan uno del otro. No se necesitaría de la seguridad si no se estuviera en algún riesgo de ataque por presentar una vulnerabilidad. El ataque o penetración es un evento transitorio en un momento específico, mientras que una vulnerabilidad existe independientemente del momento de observación. Un ataque es pues, un intento de aprovecharse de una o varias vulnerabilidades.

La Seguridad Informática incluye técnicas que se han desarrollado con el fin de proteger los equipos informáticos individuales (aquí hablamos de computadores

personales básicamente) y conectados a la red de una empresa, frente a daños accidentales o intencionados. Los daños pueden mencionarse desde el daño físico al equipo, así como la pérdida de datos y hasta el acceso a bases de datos sin autorización.

Un modelo de Seguridad Informática vamos a considerarlo como aquel digno de ser imitado. Y en aspectos de seguridad informática nada es nuevo y todo lo es a la vez. Por esto debemos encontrar un modelo que pudiera ser perfecto y el cual podamos hacer propio. Así como en los negocios se copian diversos modelos de administración de las empresas tales como la reingeniería, el justo a tiempo, la calidad total y muchos otros que por eficientes y eficaces han sido bien acogidos por la gran mayoría de las empresas en el mundo entero.

Las mejores prácticas son un grupo de actividades que al incluirlas todas en un esquema proveen una forma de manejo del riesgo, evitando en sus posibilidades los ataques, pérdida de la información, y hasta la pérdida económica. Podemos citar por ejemplo, que con algunas políticas internas sencillas se puede lograr lo antes mencionado. Podemos bloquear el acceso a información confidencial destruyendo la información impresa, impidiendo que otras personas puedan observar la pantalla del computador, manteniendo la información y los computadores bajo llave o retirando de las mesas los documentos sensibles, solo para mencionar muy pocos.

Todas las empresa mantienen una meta en su diario quehacer y alrededor de esta meta giran sus acciones que le permitirán llegar hasta allá, lo que comprende a las estrategias administrativas. Como dice Alvaro Cedeño (1999) en su libro "Administración de Empresas", *"Es el entramado de objetivos o metas y de las principales políticas y planes de acción, conducentes al logro de esas metas formuladas de manera que quede definido el negocio en el cual va a estar la compañía y la clase de compañía que es en el presente y va a ser en el futuro".*

Para hacer que la empresa como un todo (cada uno de sus colaboradores) apliquen lo que la empresa quiere, es la dirección de la compañía la encargada de apuntar primero el norte y luego de avanzar hacia allá empujando a los rezagados y apoyando a los de adelante. Si la dirección no está comprometida será muy difícil que los colaboradores lo estén por ella. Por eso las estrategias administrativas que la compañía se haya trazado deben ser reales y deben contener la seguridad informática tecnológica incluida en alguno de sus puntos. Si la empresa logra apuntarse (dirección, mandos medios y operativos) en velar por la seguridad, debe asegurarse que las personas encargadas para esto cumplan un nivel de capacitación acorde con lo requerido. La empresa deberá ofrecer asimismo la capacitación necesaria en temas nuevos e importantes.

Esta capacitación para el personal a cargo de la administración de los recursos para asegurar la seguridad informática es, según Edwin Flippo (1988), *"...el proceso mediante el cual una persona adquiere las habilidades y conocimientos*

específicos para la ejecución de los deberes relativos a un trabajo en particular..." y aún mejor la definición de Mario Espinoza (1988), en cuanto a la capacitación es: *"...el proceso enseñanza-aprendizaje orientado a mejorar los conocimientos de una persona, sus habilidades y actitudes (cualquiera que sea su nivel jerárquico), con el propósito de que pueda alcanzar un desempeño óptimo en su puesto y de esta forma contribuir al logro de los objetivos organizacionales."*

Otro elemento importante en nuestro campo de estudio es el ajuste al sistema de derecho. El Derecho como ciencia social debe responder a los cambios en la sociedad, lo cual incluye una posición específica de frente a las nuevas formas de delincuencia ligadas a los avances tecnológicos. La legislación deberá responder esencialmente a tres aspectos básicos, a saber:

1- Privacidad de las comunicaciones electrónicas.

2- Integridad, confidencialidad y disponibilidad de la información y finalmente

3- La esfera patrimonial.

Los juristas apenas empiezan a establecer algunas bases regulatorias sobre el tráfico de información a través de la Internet así como de los ataques, ya sean estos malintencionados o no, a las empresas y sus propiedades.

En materia de seguridad informática, uno de los elmentos más comunes son los llamados virus. Según Microsoft en su Enciclopedia Interactiva Encarta (2001), los virus informáticos son *"programas, generalmente destructivos, que se*

introducen en el computador (al leer un disco o acceder a una red informática) y pueden provocar pérdida de la información (programas y datos) almacenada en el disco duro".

Para detectar la presencia de un virus pueden emplearse varios tipos de programas antivíricos. Los programas de rastreo pueden reconocer las características del código informático de un virus y buscar estas características en los ficheros del computador. Como los nuevos virus tienen que ser analizados cuando aparecen, los programas de rastreo deben ser actualizados periódicamente para resultar eficaces. Algunos programas de rastreo buscan características habituales de los programas virales; suelen ser menos fiables.

En 1949, el matemático estadounidense de origen húngaro John von Neumann, en el Instituto de Estudios Avanzados de Princeton (Nueva Jersey), planteó la posibilidad teórica de que un programa informático se reprodujera. Esta teoría se comprobó experimentalmente en la década de 1950 en los Laboratorios Bell, donde se desarrolló un juego llamado Core Wars en el que los jugadores creaban minúsculos programas informáticos que atacaban y borraban el sistema del oponente e intentaban propagarse a través de él. En 1983, el ingeniero eléctrico estadounidense Fred Cohen, que entonces era estudiante universitario, acuñó el término de "virus" para describir un programa informático que se reproduce a sí mismo. En 1985 aparecieron los primeros caballos de Troya, disfrazados como un programa de mejora de gráficos llamado EGABTR y un juego llamado NUKE-LA. Pronto les siguió un sinnúmero de virus cada vez más complejos. El virus llamado

Brain apareció en 1986, y en 1987 se había extendido por todo el mundo. En 1988 aparecieron dos nuevos virus: Stone, el primer virus de sector de arranque inicial, y el gusano de Internet, que cruzó Estados Unidos de un día para otro a través de una red informática. El virus Dark Avenger, el primer infector rápido, apareció en 1989, seguido por el primer virus polimórfico en 1990.

Otro problema de seguridad lo constituyen los cortes de fluidos eléctrico. Para evitar problemas en caso de apagón eléctrico existen las denominadas UPS (acrónimo de *Uninterrupted Power Supply*), y que son baterías que permiten mantener el sistema informático en funcionamiento, por lo menos el tiempo necesario para apagarlo sin pérdida de datos. Sin embargo, la única forma de garantizar la integridad física de los datos es mediante copias de seguridad.

El acceso es otros enfoque del campo de la seguridad informática. Es posible que las claves y las tarjetas de acceso a los diferentes sistemas de las empresas se vean reforzadas por mecanismos biométricos basados en características personales únicas como las huellas dactilares, los capilares de la retina, las secreciones de la piel, el ácido desoxirribonucleico (ADN), las variaciones de la voz o los ritmos de tecleado.

Los *hackers* son usuarios muy avanzados que por su elevado nivel de conocimientos técnicos son capaces de superar determinadas medidas de protección. Su motivación abarca desde el espionaje industrial hasta el mero desafío personal. Internet, con sus grandes facilidades de conectividad, permite a

un usuario experto intentar el acceso remoto a cualquier máquina conectada, de forma anónima. Los *crackers* por su parte, son personas sin escrúpulos que se especializan en violar medidas de seguridad de una computadora, servidor, sistema o red para obtener información que cree valiosa. Las redes corporativas o computadores con datos confidenciales no suelen estar conectadas a Internet; en el caso de que sea imprescindible esta conexión se utilizan los llamados cortafuegos (firewall), que sonsiste en un computador situado entre las computadoras de una red corporativa e Internet. El cortafuegos (firewall) impide a los usuarios no autorizados acceder a los computadores de una red, y garantiza que la información recibida de una fuente externa no contenga virus.

Unos computadores especiales, denominados servidores de seguridad, proporcionan conexiones seguras entre las computadoras conectadas en red y los sistemas externos como instalaciones de almacenamiento de datos o de impresión. Estos computadores de seguridad emplean el cifrado en el proceso de diálogo inicial, al comienzo del intercambio electrónico, lo que evita una conexión entre dos computadores a no ser que cada uno de ellos reciba confirmación de la identidad del otro.

La Criptografía es la ciencia que trata del enmascaramiento de la comunicación de modo que sólo resulte inteligible para la persona que posee la clave, o método para averiguar el significado oculto, mediante el criptoanálisis de un texto aparentemente incoherente. En su sentido más amplio, la criptografía abarca el uso de mensajes encubiertos, códigos y cifras.

En la actualidad, los organismos oficiales, los bancos y muchas empresas transmiten gran cantidad de información confidencial, en forma de comunicación de datos, de una computadora a otra. La comunicación se efectúa por línea telefónica u otros canales no privados.

Se han propuesto diferentes alternativas, como el criptosistema de clave pública (PKC), que utiliza una clave pública y otra secreta. El PKC, basado en un enfoque matemático, elimina el problema de la distribución de claves pero no resulta tan eficaz, desde el punto de vista informático, como el DES. En 1978 apareció el denominado algoritmo RSA, que utiliza dos números primos de 100 cifras, p y q, para formar su producto $n = pq$, desarrollando la dificultad inherente a la factorización de los números primos. Desde entonces se han estudiado muchas variantes de este tipo de claves, aunque parece ser que RSA continúa siendo el sistema más eficaz y seguro.

Normalmente quienes hablan de seguridad tecnológica e informática son los fabricantes y desarrolladores del hardware y software especializado. Para todos los demás aquello no es importante sólo hasta el momento en que les ocurre la desgracia. En Costa Rica no existen trabajos especializados y exclusivos del tema. Se han escrito varios artículos, los proveedores de seguridad tecnológica han realizado pequeños seminarios, pero no es suficiente. A nivel internacional el tema sí ha sido tocado más profundamente y se han escrito varios libros sobre el tema. Utilizaremos algunos, mencionaremos otros, pero realizaremos un escrito propio capaz de ofrecer opción en nuestro mercado nacional. El Internet será

una fuente de especial apoyo debido a su inmediatez de entrega de datos y acceso a ellos en un tema tan nuevo en nuestro medio.

CAPÍTULO III: METODOLOGÍA

Cualquier proceso investigativo, desde el mas sencillo hasta el más complejo es siempre originado por una situación problemática, la cual debemos descubrir. Es así que la investigación se convierte en un medio para conocer la realidad por medio de la búsqueda y explicación de hechos. Ezequiel Ander-Egg (1986), menciona que investigar *"es una forma de plantear problemas y buscar soluciones mediante una indagación".*

Existen diversos métodos de investigación, cada cual con sus características específicas, y el experto G.L. Dankhe los divide en exploratorios, descriptivos, correlacionales y experimentales (o explicativos).

Ante el método exploratorio de investigación, Ronald Weis (1986) define que este tipo de métodos *"...tienen por objeto ayudar a que el investigador se familiarice con la situación del problema, identifique las variables mas importantes, reconozca otros cursos de acción, proponga puntos idóneos para trabajos ulteriores y puntualice cuál de esas posibilidades tienen la máxima prioridad en la asignación de los escasos recursos presupuestarios de la empresa".*

Jaime Arellano (1981) define la investigación descriptiva como la que "propone describir, retratar en aspectos relevantes una realidad particular una realidad particular que sirve para obtener diagnósticos o pronósticos de la realidad dada".

Básicamente se centran en la medición de los conceptos o variables de una manera independiente.

Medir el grado de relación existente entre dos o más conceptos de variables es la tarea de la investigación por el método correlacional. Mientras que el método explicativo pretende ir un poco más allá de la mera descripción de los conceptos o de las relaciones entre ellos, y "deberá responder a las causas de los eventos físicos o sociales", según nos explica Jaime Arellano (1981).

Los alcances de la presente investigación son para todo aquel que desee conocer el ambiente de seguridad de la tecnología informática con la que se trabaja en buena parte de las empresas costarricenses y la forma en que podrían evitarse muchas de las pérdidas que sufren las empresas por esta causa.

Las limitaciones han sido de acceso a información que de una u otra forma las empresas han calificado como secreta y de confianza en las respuestas obtenidas al aplicar las encuestas y realizar las entrevistas.

Para cumplir con los objetivos de la presente investigación y lograr medir tanto las variables como los diversos indicadores, fue necesaria la utilización de los siguientes sujetos y fuentes.

3.1 Sujetos

Lo primero que definiremos serán las empresas a investigar. Se ha tomado como base para delimitar el campo de acción, la información brindada por una empresa productora de software con amplio conocimiento del mercado tecnológico, que ha definido el mercado de la siguiente manera:

- Las empresas pequeñas son las que posean de 100 a 499 computadores.
- Las empresas medianas son las que tengan entre 500 y 999 computadores.
- Las empresas grandes son las que posean más de 1000 computadores.

Para el alcance de los objetivos el mercado a investigar es el mediano, en donde al momento de la investigación existían 600 empresas que cumplen con nuestro perfil el cual se especifica a continuación:

1- Ser costarricenses ubicadas dentro de nuestro territorio, independientemente de si son publicas o privadas y ser reconocidas en nuestro mercado.
2- Poseer como mínimo la cantidad de 50 computadores interconectadas dentro una red local.
3- Poseer acceso a Internet.
4- Tener una ubicación URL. (página en Internet)
5- Preferiblemente con sucursales u oficinas fuera de su edifico central.

6- Debe manejar una operación considerada crítica.

7- No podrán ser organismos internacionales.

8- No podrán ser multinacionales.

Los sujetos de investigación serán los profesionales en quienes confían las empresas para asignarles la administración de la seguridad informática. Asimismo se entrevistará a por lo menos un especialista en las áreas de legislación informática y seguridad tecnológica. Véanse en anexos las guías de entrevistas y las encuestas.

3.2 Fuentes

Hay varios métodos que se pueden utilizar para obtener la información que se requiere. Básicamente hablamos de tres medios que son la búsqueda de datos ya publicados por otras fuentes, la segunda es la realización de un experimento y la tercera por medio de entrevistas o encuestas.

En el caso particular de esta investigación se han utilizado dos de los anteriores; el primero, que es la recopilación de información ya publicada, para la realización de la primera parte de la investigación. Mientras que para obtener la información para el cumplimiento de nuestros objetivos se practicaron las entrevistas uno-a-uno y las encuestas generales.

Como menciona Hernández, Fernández y Baptista (1991), *"...el instrumento es la herramienta del método y responde a la pregunta con que se hace..."*.

3.4 La muestra

La muestra de las empresas encuestadas, fue obtenida gracias a un listado proveído por una empresa fabricante de software de última tecnología, conforme al perfil determinado para la clasificación de las empresas, dentro de la cual se escogieron compañías situadas en un rango de medianas y de medianas a grandes. Para ubicar mejor al lector se informa que las empresas son medidas por la cantidad de computadoras que posean conectadas a su red informática, siendo así que el grupo llamado "medianas" son empresas con una base instalada de 101 hasta 500 computadoras, con alrededor de 350 empresas, y las "de medianas a grandes" son compañías con una plataforma que va desde las 501 hasta las 1000 computadoras y que actualmente son un total de 250 empresas.

Las empresas de interés son 600, resultado de la suma de las "empresas medianas" y las "de medianas a grandes", de las cuales – al azar - se les envió a 200 de ellas los cuestionarios y respondieron 50 empresas entre el mes de octubre del 2002 y enero del 2003.

Por razones obvias se les garantizó a los informantes de las encuestas y a los entrevistados la total confidencialidad, asi como reservarse el nombre de la empresa en el momento de presentar los datos.

CAPÍTULO IV: ANÁLISIS DE RESULTADOS

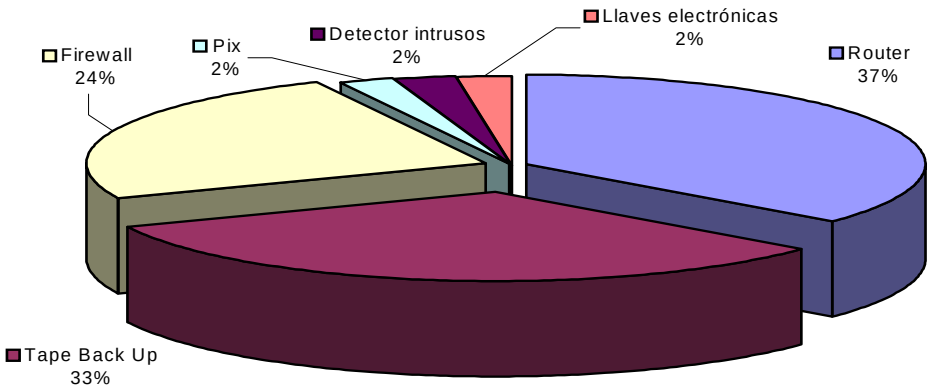
Luego de nuestra investigación, se han logrado obtener los resultados que ofrecen un panorama general pero muy cierto sobre el tema en cuestión.

Las empresas costarricenses no operan bajo la mejor seguridad tecnológica ni tampoco están comprometidas como deberían, con lo que es evidente puesto que no existe una correcta administración del riesgo.

4.1 Seguridad

Tomando en cuenta las variables ofrecidas al inicio del presente trabajo, comenzaremos mencionando que la seguridad informática-tecnológica de las empresas en Costa Rica el hardware y software no son utilizados de tal manera

GRAFICO #1
HARDWARE DE SEGURIDAD UTILIZADO POR LAS EMPRESAS
COSTARRICENSES, PERIODO OCT. 02 - ENE. 03

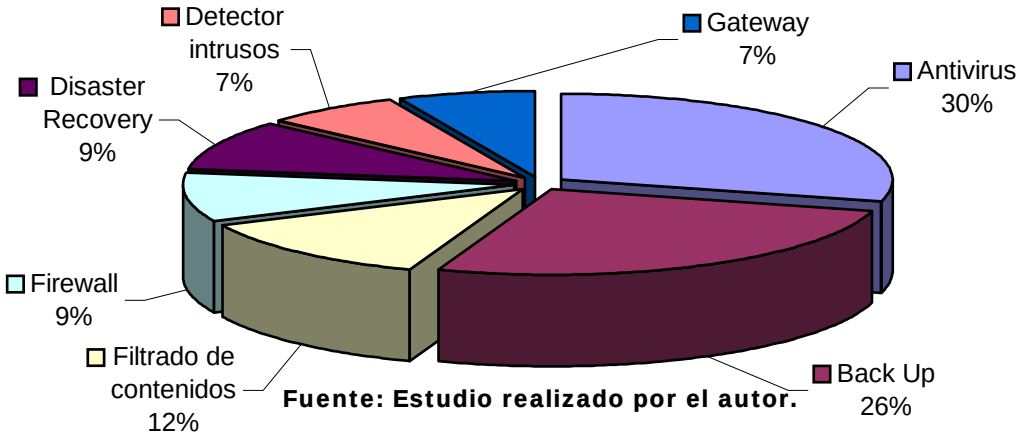


Fuente: Estudio realizado por el autor.

que les permita ya sea prevenir los ataques, o de alguna forma, "curar la herida" causada por ese ataque. Como observaremos en el gráfico #1 (Hardware) y en el gráfico #2 (Software), todas las empresas encuestadas poseen Router, para una efectiva conexión a Internet y antivirus para la prevención de ataques. El segundo equipo que por mayoría (33%) utilizan las empresas es el "tape back-up" por medio del cual se permite hacer copias de seguridad de distintos archivos que para la empresa sean indispensables, hablamos de bases de datos, información financiera y hasta correos electrónicos de claves. Ya mencionamos que el Router es el equipo que todos mencionaron, sin embargo para una conexión más segura con el mundo y para evitar indeseables ataques o intrusos un 24% de las empresas mencionaron que utilizan el Firewall. Sin embargo y a pesar que todas las empresas consideran su negocio de suma importancia, solo el 2% de ellas posee "detectores de intrusos" y "llaves electrónicas". Si bien estas dos herramientas son más especializadas, deberían ser tomadas en cuenta para aquellas empresas que mantienen colaboradores móviles y que manejan información muy importante en sus portátiles, aspecto que hoy en día tienen la mayoría de las corporaciones en nuestro país.

El software de seguridad especializado, por otra parte, es más utilizado por las empresas ya que es más accesible y posible tenerlo que el hardware. Mencionábamos que todas las empresas poseen un software antivirus. Como segundo programa, utilizado por las empresas para protegerse de eventuales pérdidas de información y datos indispensables, en un 26% de ellas poseen un software de respaldos o "back up". Normalmente este se utiliza en combinación

GRAFICO #2
SOFTWARE DE SEGURIDAD UTILIZADO POR LAS EMPRESAS COSTARRICENSES, PERIODO OCT. 02 - ENE. 03

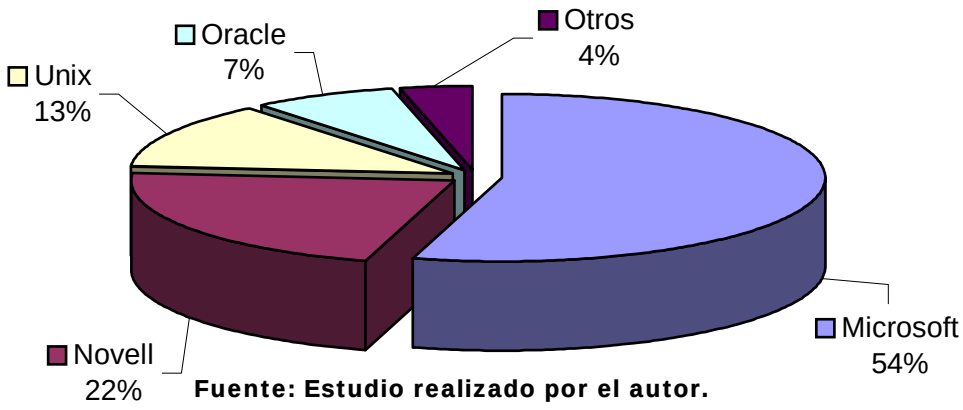


Fuente: Estudio realizado por el autor.

con el hardware para realizar los back-up. Un 12% de las empresas utilizan el "filtrado de contenidos" tanto para Internet como para el correo electrónico. Con ésta herramienta la empresa puede prevenir tanto la incorrecta utilización de éstos instrumentos por parte de sus colaboradores como la mala intención de otros por ingresar a la empresa virus que puedan ser dañinos.

Otros programas utilizados pero en menor porcentaje por nuestras empresas son el "Firewall" y el "Disaster Recovery" ambas con un 9% del total de las muestras. De ambas el Disaster Recovery debería definitivamente ser parte de todas las empresas pues significa mantener su empresa en funcionamiento aún después de algún grave desastre ocurrido con la información de su empresa. En menor porcentaje se utilizan el Detector de Intrusos y un Gateway para proteger la salida y/o entrada a Internet. Pero no sirven de nada el software ni el hardware si la empresa no posee una plataforma tecnológica de trabajo segura. El 54% de las empresas encuestadas tienen los sistemas operativos de Microsoft como su

GRAFICO #3
PLATAFORMA DE SOFTWARE UTILIZADA POR LAS EMPRESAS COSTARRICENSES, PERIODO OCT. 02 - ENE. 03



Fuente: Estudio realizado por el autor.

plataforma básica, a pesar del concepto generalizado sobre la inseguridad de ésta plataforma. (Grafico #3)

Quizá esto refleje la importancia y el esfuerzo que la citada empresa desarrolladora ha empleado para borrar esa imagen, pues a partir de su sistema operativo Windows 2000 Server se presentan mejores herramientas para trabajar en comunicación y colaboración constante bajo un esquema de seguridad casi infranqueable. Y decimos “casi” porque la seguridad del sistema operativo de Microsoft (y cualquier otro, en realidad) será tan fuerte o débil como sus administradores así lo implementen.

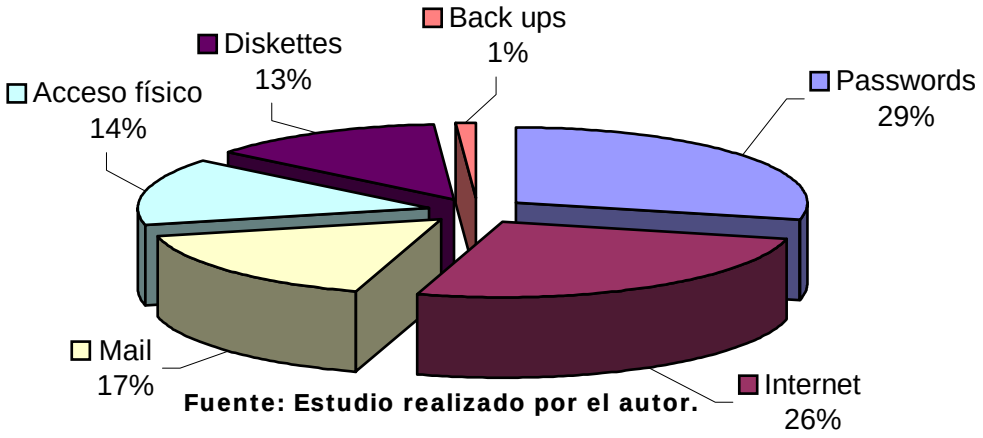
Otras sistemas operativos utilizados por las diferentes empresas encuestadas son la Novell con un 22%, Unix con un 13%, Oracle con un 7% y otros con un 4%. Normalmente las empresas utilizan una plataforma cruzada en donde incluyen uno o más de los sistemas anteriormente citados.

4.2 Modelos de Seguridad

La siguiente variable a analizar habla sobre los modelos utilizados de seguridad informática-tecnológica (Gráfico #4). En éste ámbito nuestras empresas pareciera que no poseen un modelo definido en cuanto a políticas de seguridad ni estrategias administrativas propiamente dicho y más que utilizar un modelo predefinido las empresas prefieren dar mano a las mejores prácticas tal y como las definimos dentro de nuestras variables.

Y es que aspectos como manejo de contraseñas, restricción de accesos físicos y

GRAFICO #4
POLITICAS DE SEGURIDAD UTILIZADAS POR LAS EMPRESAS COSTARRICENSES, PERIODO OCT. 02 - ENE. 03



Fuente: Estudio realizado por el autor.

virtuales, así como la eliminación de utilización de dispositivos grabables y otros detalles que han venido a utilizarse como regla y que poco a poco las empresas desarrolladoras comienzan a implementar dentro de sus sistemas operativos. En nuestra investigación, el 29% de las empresas encuestadas utilizan políticas internas sobre las contraseñas (passwords) de acceso a la red corporativa. Sin

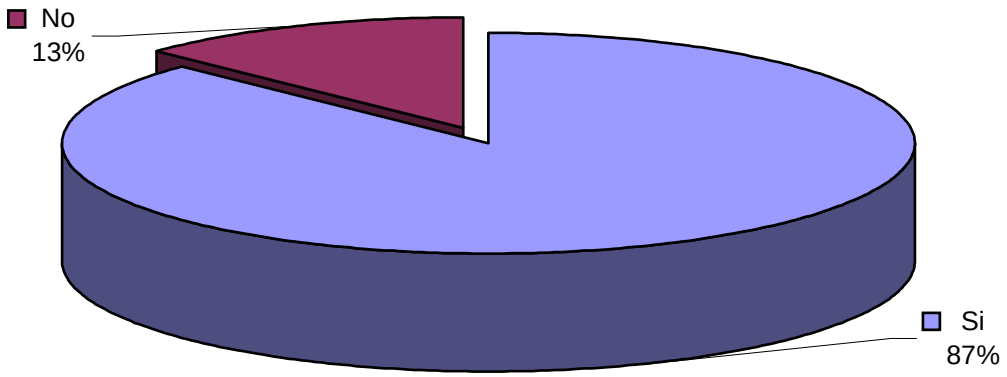
embargo y como lo mencionan diferentes expertos en el tema de la seguridad informática, las empresas poco pueden hacer ante la forma en que el usuario "archiva" sus contraseñas, ya que en algunos de los casos conocidos, escriben su contraseña "privada" en un papel y éste lo pegan bajo el teclado o inclusive en el monitor. En el siguiente punto de la investigación, el 26% de las empresas regulan el acceso o utilización a la Internet. Luego tenemos que tan solo el 17% de las empresas regulan en alguna forma la utilización del correo electrónico. Por más amenazas que se le indiquen a los usuarios para que no utilicen el correo para enviar y recibir mensajes que de alguna forma puedan atentar con la seguridad, los usuarios nunca llegan a comprender el por qué de éstas amenazas (y en muchos casos tampoco el área de informática).

4.3 Factores de Riesgo

Los factores de riesgo han sido determinados dentro de las variables como aquellas acciones que le provocan a las empresas una posibilidad de riesgo o alguna pérdida económica, patrimonial e intelectual y es que debido a los múltiples niveles de vulnerabilidad de las redes y la cantidad siempre creciente de técnicas de ataque, también aumentan los riesgos al bienestar corporativo.

El impacto de los ataques en las redes de las compañías puede variar desde consecuencias fáciles de cuantificar como las operaciones comerciales interrumpidas hasta pérdidas que son difíciles de calcular como los perjuicios al valor de las marcas. Las empresas costarricenses dicen que tan sólo el 48% de ellas poseen planes de contingencia para eventualidades relacionadas con la

GRAFICO #5
ATAQUES RECIBIDOSPOR LAS EMPRESAS COSTARRICENSES (SI/NO)
EN PORCENTAJES, OCT.2002 - ENE.2003

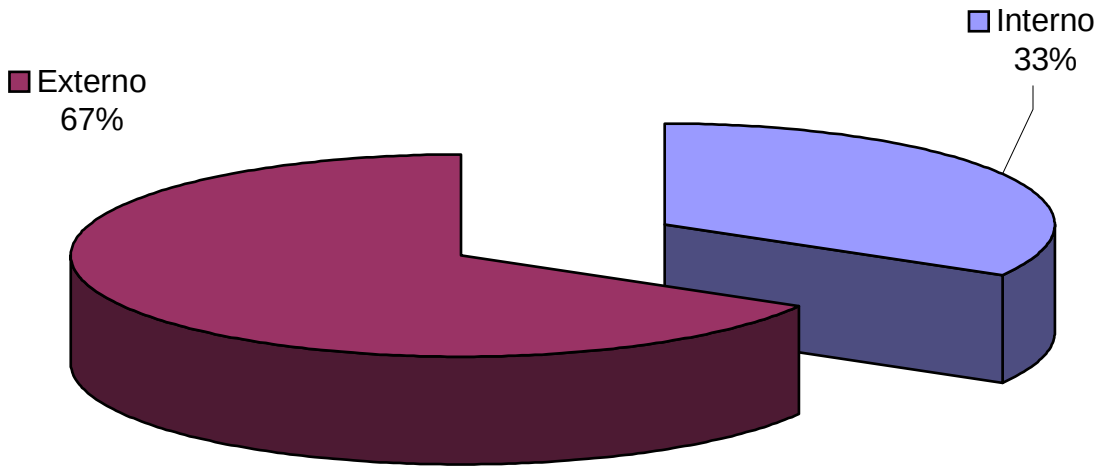


Fuente: Estudio realizado por el autor

posible violación de la seguridad en sus operaciones críticas, con lo cual queda al descubierto el hecho de que nuestras empresas actúan sólo cuando algo les ha ocurrido, o sea por reacción y no proactivamente, aún cuando la mayoría de ellas (87%) responde que si han sufrido algún tipo de ataque (Gráfico #5).

Es evidente que los riesgos informático tecnológicos aumentan considerablemente si no se mantienen planes de contingencia, con más razón antes de haber recibido un ataque. En la mayoría de éstos ataques, el 67% exactamente, los encargados del área de tecnología e informática creyeron determinar que fueron por violaciones externas mientras que el restante por usuarios de la red empresarial (Gráfico #6).

GRAFICO #6
PROCEDENCIA DE LOS ATAQUES SUFRIDOS POR LAS EMPRESAS COSTARRICENSES, PERIODO OCT. 02 - ENE. 03



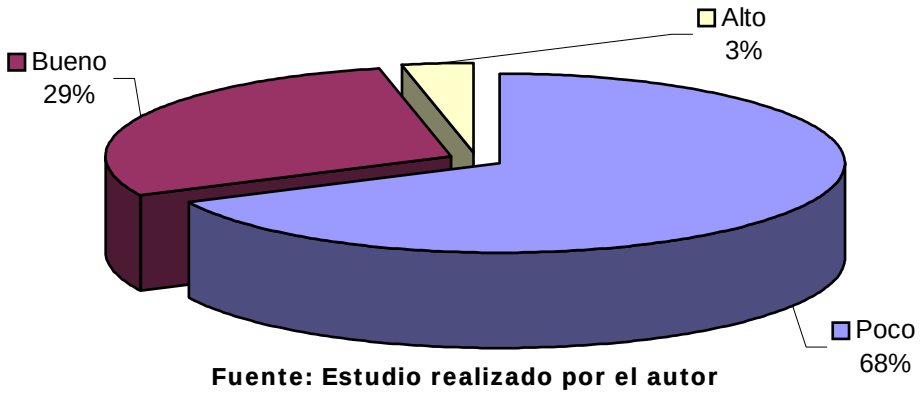
Fuente: Estudio realizado por el autor

Sin embargo este dato no concuerda con los datos que se manejan a nivel mundial en donde se tienen estudios en donde cerca del 80% de los delitos informáticos son cometidos por empleados de la empresa. Los empleados por ejemplo, pueden enviar por correo electrónico información confidencial a fuentes externas. Según la Sociedad norteamericana para la seguridad industrial, este robo de "propiedad intelectual" cuesta a las corporaciones de los EE.UU. 24 millones de dólares al año. En el 74% de los casos, el problema tiene su origen en las propias corporaciones.

Para evitar de alguna forma los riesgos ante estos ataques el área gerencial de las empresas deben buscar que las estrategias administrativas sean las prácticas y teorías que la dirección de la empresa desarrolle y que afectan directamente el diario accionar de la seguridad de la compañía. El estudio determinó que el nivel

gerencial en nuestras empresas demuestra muy poco compromiso con la seguridad en sus estrategias ya que tan sólo el 3% de ellas demuestran un nivel de alto compromiso, mientras que un 29% demuestran un buen compromiso y un 68% denota un bajo interés por la seguridad informática tecnológica de la empresa (Grafico #7).

GAFICO #7
COMPROMISO DE LA GERENCIA CON LA SEGURIDAD TECNOLÓGICA EN LAS EMPRESAS COSTARRICENSES, PERIODO OCT. 02 - ENE. 03



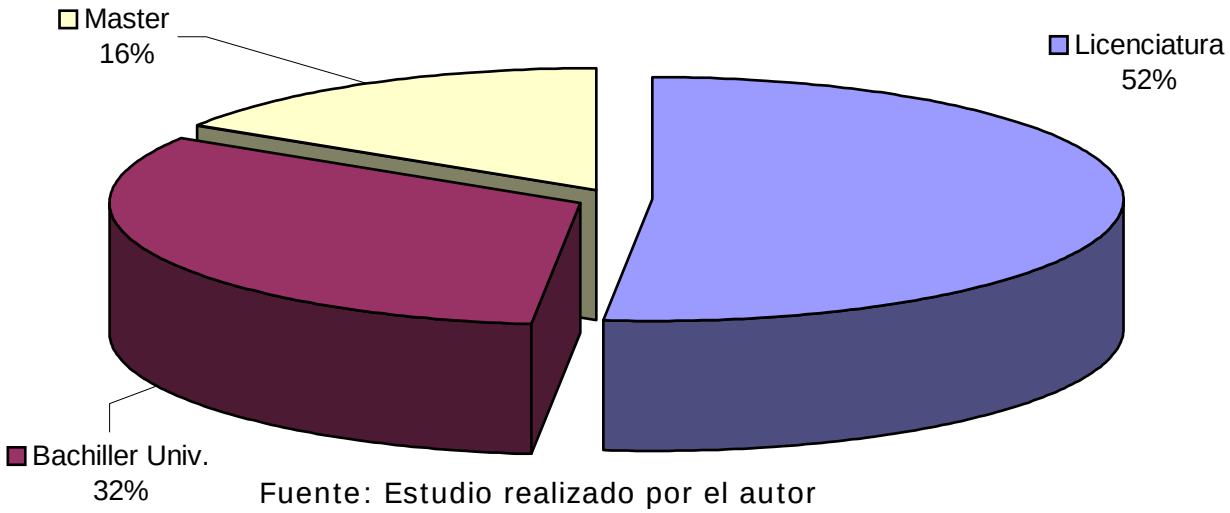
Fuente: Estudio realizado por el autor

El compromiso fue determinado por el apoyo o no en proyectos de seguridad, incluyendo antivirus, filtrados de contenido y cualquier hardware o software necesario para esas funciones, así como por el apoyo y facilidades en brindar capacitación en el tema a sus administradores de la red o área encargada de la seguridad.

4.4 Capacitación del personal en seguridad informática

El estudio revela que todas las empresas encuestadas poseen personal con estudios y títulos en áreas de su campo. Poseen bachilleres (32%), licenciados (52%) y maestrías (16%). (Grafico #8) sin embargo, ninguna empresa se ha interesado en enviar o brindar capacitación a sus encargados del área tecnológica en el tema de seguridad informática.

GRAFICO #8
GRADO ACADEMICO DE LOS ADMINISTRADORES DE LA SEGURIDAD TECNOLÓGICA EN LAS EMPRESAS COSTARRICENSES, PERIODO OCT. 02 - ENE. 03

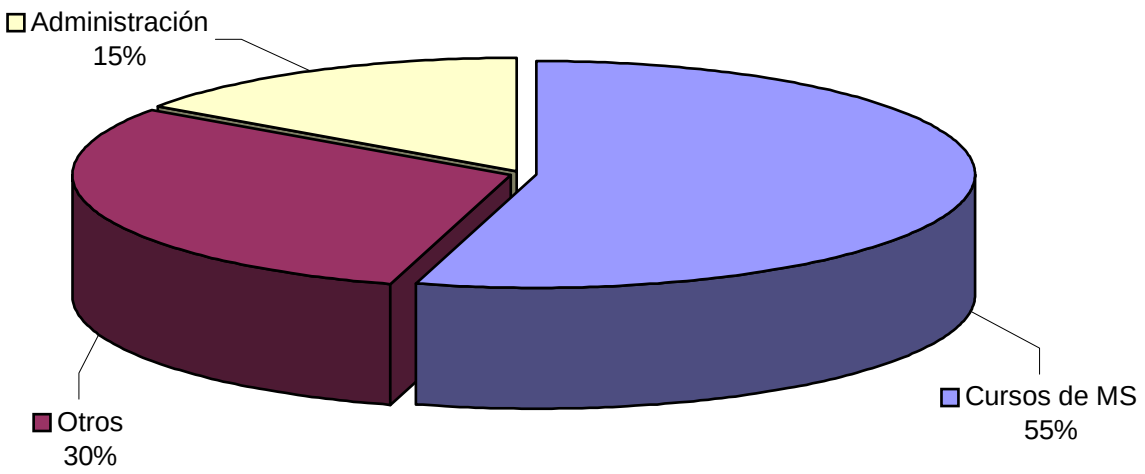


Fuente: Estudio realizado por el autor

La mayoría de los encuestados, han recibido cursos o seminarios sobre temas de tecnología más ninguno sobre el tema específico de seguridad. (Grafico #9) La variable "perfiles de capacitación" en su definición operacional es el grado de

capacidad tanto académico como práctico de las personas encargadas de administrar todo el sistema de seguridad informático-tecnológico de la empresa y de sus habilidades para prevenir los riesgos dentro de la empresa. Con estos resultados se revela que las personas encargadas de administrar los recursos tecnológicos a favor de la seguridad no se especializan como deberían ni tampoco reciben el suficiente apoyo de parte de la empresa para, por lo menos, tomar algunos cursos o seminarios sobre seguridad informático tecnológico.

GRAFICO #9
ESTUDIOS AFINES ADMINISTRADORES DE LA SEGURIDAD EN LAS EMPRESAS COSTARRICENSES, PERIODO OCT. 02 - ENE. 03



Fuente: Estudio realizado por el autor

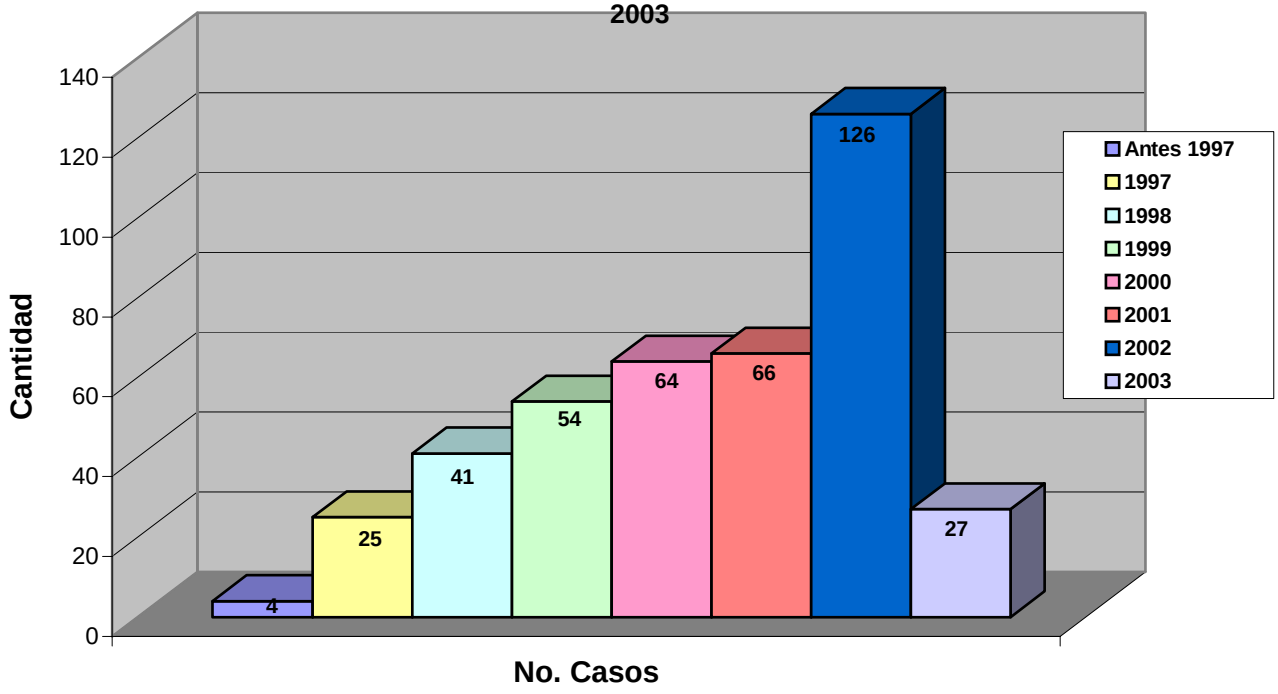
4.5 Legislación

La legislación de los delitos informáticos es un aspecto que en nuestras variables hemos definidos como cualquier artículo de cualquier ley nacional que afecte el desarrollo de la seguridad informático tecnológico de las empresas en Costa Rica. Ante este aspecto el 39% de las empresas indican que no conocen ninguna legislación al respecto mientras que el otro 61% apunta que si. Yendo más hacia delante se les preguntó qué era lo que conocían y confesaron que lo único que conocen es lo relacionado con la protección de los derechos de autor esencialmente pues la piratería de software en nuestro país es un tema que ocupa un lugar importante a pesar de lo esfuerzos realizados por las empresas productoras de software, el gobierno y la Business Software Alliance, empresa que defiende los intereses de los asociados productores de software. Para la investigación de esta variable se entrevistó al señor Erick Lewis, Encargado de la Sección de Delitos Informáticos perteneciente al Departamento de Investigaciones Criminales del Organismo de Investigación Judicial de Costa Rica, y efectivamente la mayoría de casos que son investigados por su departamento son aquellos que tienen que ver con la violación de los derechos de propiedad intelectual. La generalidad de los casos que se atienden tienen que ver con el fraude, la comunicación y la privacidad. Generalmente quienes presentan los casos son las entidades gubernamentales pues deben hacerlo por orden administrativo. Según la experiencia del señor Lewis la mayoría de los casos

presentan un delito perpetrado desde el interior de la misma empresa o por empleados, o desempleados de las empresas afectadas. Su consideración es de un 90% a 95% casos de este tipo y apenas un 5% o 10% de los casos tienen como acusado a una persona totalmente externa a la empresa perjudicada.

Los casos presentados desde 1997, año de su creación, son los siguientes:

GRAFICO #10
CASOS INGRESADOS POR AÑO PARA INVESTIGACIÓN POR DELITOS INFORMÁTICOS EN LAS EMPRESAS COSTARRICENSES, PERIODO DE 1997 AL 2003



Fuente: Sección de Delitos Informáticos, OIJ

Según vemos en el gráfico #10, los casos presentados ante la sección de Delitos Informáticos han venido creciendo año a año. En el primer año de creación (1997) se presentaron 25 casos y para el segundo un total de 41 para una variación del 39%. El mayor aumento se registra en el 2002 con un total de 126

casos para una variación total del 49% con respecto al año anterior. A febrero del 2003 se han presentado 27 casos y se espera que, si el ritmo continúa igual, se termine el año con 162 casos registrados y una variación del 22%.

Para concluir, se acota que la seguridad tecnológica en las empresas costarricenses, según Róger Mora del Grupo Nación, uno de los expertos en el tema entrevistado para esta investigación, llega hasta donde el presupuesto alcance. Confirma que la preocupación principal de los clientes es que no les "roben" información confidencial pero que no van más allá de un nivel que podríamos llamar básico o nivel 1 que es el de control de los virus.

Los niveles de seguridad que nuestro experto menciona son 4:

1- Control (eliminación y prevención) de los virus informáticos.
2- Políticas y normas en la red privada, para que los empleados no puedan fácilmente acceder o dañar información importante.
3- Firewall, para el bloqueo de puertos desde Internet.
4- Detección de intrusos.

Quien no tenga al menos los tres primeros niveles no puede sentirse seguro.

CAPÍTULO V: CONCLUSIONES Y PROPUESTA

5.1 Conclusiones

Las empresas costarricenses presentan la intención de avanzar hacia una seguridad tecnológica que les provea una mayor eficiencia en sus negociaciones y que les permita competir de una mejor manera en el mundo globalizado de hoy. Sin embargo esa intención queda desplazada al enfrentarse a un presupuesto el cual no presenta grandes reservas para el área tecnológica. Según lo obtenido en esta investigación quienes no escatiman en asignar recursos a esta área, son las empresas del sector financiero, específicamente bancos. Las demás empresas solo actúan según las circunstancias.

Las siguientes son las conclusiones a las variables presentadas al inicio del trabajo.

Seguridad Informática Tecnológica.

Definitivamente todas las empresas se preocupan por mantener algún tipo de seguridad que les permita laborar y generar sus ingresos y mantener su negocio de forma más segura. Todas ellas han implementado las técnicas que les permitan estar en un mejor nivel de seguridad. Lo que se recomienda es que las empresas se profesionalicen en este tema, implementando las capacitaciones, cursos y seminarios que se ofrecen, así como la asociación con una empresa experta en el tema para que les asesore.

Modelos de Seguridad Informática Tecnológica.

Es claro que nuestras empresas no utilizan un modelo predefinido sino que han tenido que ir implementando pedazos de soluciones conforme les van apareciendo las necesidades. No se puede pretender que las empresas adopten un modelo único como si fuera una receta, pero sí es importante que ellas puedan aplicar algún formato que les ayude a mejorar su nivel de seguridad. Sentarse a planificar y poder pensar en el futuro inmediato, de mediano y de largo plazo y con base en esto adoptar un modelo de seguridad acorde con lo proyectado.

Factores de riesgo

Los datos ofrecidos por el Organismo de Investigación Judicial sobre los casos ingresados por año a la Sección de Delitos Informáticos, reflejan que año con año las empresas se enfrentan a mayores riesgos reales que afectarán en algún momento su seguridad. Asimismo en las respuestas obtenidas de las empresas se refleja que los ataques son una realidad y que no podemos hacernos de la vista gorda y esperar que “a mí no me suceda”.

Estrategias Administrativas

Las Gerencias Generales o Juntas Directivas usualmente no ofrecen una misión ni visón de seguridad a sus clientes y empleados. Ya lo mencionó nuestro experto entrevistado, que el nivel de la seguridad en las empresas llega hasta donde lo permita el presupuesto, y que generalmente, este no es mucho. Su personal en general no está culturizado para prevenir y no se respetan las políticas y normas

que pudiesen colaborar con la seguridad. Se recomienda una reingeniería del pensamiento en donde una nueva prioridad para todos los altos mandos, sea la de la seguridad.

Perfiles de Capacitación

Las empresas no "invierten" en su personal de tecnología de información lo necesario como para tener dentro de su organización a alguien que les pueda ayudar con nuevas ideas en el tema de la seguridad. No los envían a cursos que les aprovechen en el tema. No se entrenan en nuevas tecnologías. Son más utilizados como apaga fuegos que como asesores de TI. Las empresas costarricenses deberán comprender que las capacidades académicas de quienes están al mando de su seguridad deben ser calificadas.

Legislación

Se comprobó que no existe una legislación clara sobre el tema a nivel nacional. Está claro que las empresas no pueden ampararse en las leyes para evitar un riesgo. La sección de Delitos Informáticos del Organismo de Investigación Judicial hace grandes esfuerzos para resolver los casos que se van presentando, sin embargo no siempre es posible pues es comprensible que las empresas afectadas no quieran verse envueltos en algún escándalo mayor que pudiera afectarles aún peor que lo afectado por el ataque. Se recomienda que las empresas se cuestionen sobre sus políticas y normas internas a fin de no verse envuelto en tanto embrollo por algo que se puede prevenir fácilmente.

5.2 Propuesta

Luego de presentar el análisis de los resultados de nuestra investigación se presenta la propuesta para que las empresas costarricenses puedan comparar el nivel de riesgo actual de su seguridad informático tecnológico.

La propuesta girará en torno a las necesidades que presentan las empresas y que se desarrollará por medio de los siguientes seis puntos:

1- Cuatro Principios del Ciclo Vital de la Seguridad de la Información.
2- Seguridad Integrada
3- Políticas y Normas Internas
4- Guía para Planes de Contingencia
5- Medidas de Seguridad
6- Planes de contingencia específicos.

5.2.1 Cuatro principios del ciclo vital de la seguridad de la información.

1. Evaluación de riesgos

Evaluar los riesgos de seguridad de la información y determinar niveles de riesgos aceptables.

2. Diseño e implementación de la seguridad

Incorporar las políticas, normas, procedimientos y la tecnología de la seguridad como elementos esenciales en el diseño e implementación de todos los sistemas y redes de información.

3. Manejo de la seguridad

Adoptar un enfoque completo para el manejo de la seguridad en todo el ciclo de vida de los sistemas y redes de información.

4. Reevaluación

Estudiar y reevaluar la seguridad de los sistemas y redes de información y si es pertinente, modificar las políticas, normas, procedimientos y tecnología.

Los cuatro principios anteriores apuntan la dirección que debe tomar la planeación si se quiere que la protección sea rentable. Se le recomienda a la organización que esté considerando implementar estos principios que tenga en cuenta utilizar un sistema de administración de la seguridad de la información.

Ha sido una práctica generalizada el hecho que la seguridad de la red en las empresas está formada por una variedad de productos puntuales de diferentes distribuidores, lo cual plantea los siguientes problemas:

- ***Uso ineficiente del personal de TI:*** Al comprar productos múltiples, el personal de TI debe implantar, administrar y monitorear datos similares de manera repetitiva. Los productos puntuales muestran una perspectiva limitada de la postura de seguridad y cuando surge un virus, las "soluciones" que ofrecen los distribuidores deben ser probadas y verificadas con varias tecnologías.

- ***Menor protección de la esperada:*** Cuando los clientes compran productos a múltiples distribuidores, no se puede asumir que estos productos funcionan perfectamente o se comuniquen unos con otros. La realidad es que los productos de múltiples distribuidores rara vez operan entre sí y casi no se comunican entre ellos NINGUNA información, lo que puede generar enormes vacíos que aprovechan los hackers para hacer ataques de amenazas combinadas.

- ***Mayores costos:*** El personal de TI está gastando más en dólares y costos indirectos para implementar, administrar y actualizar múltiples productos puntuales que lo que gastaría con una solución integrada. El resultado es pagar más y recibir una menor protección.

5.2.2 Seguridad Integrada

Las tecnologías de seguridad importantes que se pueden integrar en las empresas de nuestro estudio son las siguientes:

1. **Firewalls:** Controlan el tráfico de las redes al seleccionar la información que entra y sale de la red para garantizar que no ocurran accesos no autorizados.

2. **Detección de intrusos:** Detecta el acceso no autorizado y proporciona alertas e informes que se pueden analizar en cuanto a la identificación de la configuración y el programa de trabajo de la máquina.

3. **Filtrado de contenidos:** Identifica y elimina el tráfico no deseado.

4. **Redes Privadas Virtuales (VPN):** Protege las conexiones fuera del perímetro lo que le permite a las organizaciones comunicarse en Internet de manera segura.

5. **Manejo de la vulnerabilidad:** Descubre fisuras en la seguridad y sugiere mejoras.

6. **Protección antivirus:** Protege contra los virus, gusanos y caballos de Troya.

5.2.3 Políticas y Normas Internas

Las normas corporativas de uso de Internet deben ser todo lo claras y accesibles para los empleados que sea posible. Asegúrese de que comprenden quién tiene acceso a la Web y en qué momentos. También deben comprender las normas de la compañía en cuanto a correo electrónico personal y examinación de Internet. Algunas compañías piden a sus empleados que firmen un formulario en el que confirman que conocen las normas.

Se recomienda filtrar el contenido del correo electrónico. La combinación de esta posibilidad con el filtrado de Internet y una protección antivirus adecuada constituye el punto de partida para que el departamento de sistemas pueda proteger la seguridad de la red.

El correo electrónico de los empleados puede causar varios tipos de violaciones a la seguridad. Si los empleados abren archivos adjuntos no solicitados del correo electrónico o no analizan los documentos adjuntos en busca de virus antes de abrirlos, entonces la empresa es vulnerable a los ataques de virus.

Para evitar violaciones a la seguridad por factores humanos se recomienda a las empresas seguir los siguientes pasos:

1. Establecer una política para el uso de Internet. Infórmeles a los empleados el reglamento de la compañía acerca del uso personal del correo electrónico e Internet. El desarrollo de políticas para el uso de Internet también le ayuda a los gerentes de la tecnología de la información a

configurar y monitorear las soluciones de seguridad para la red con más eficiencia.

2. Utilizar la tecnología que analiza el correo electrónico en busca de contenidos inadecuados y registra la actividad en Internet que no sigue los parámetros establecidos por la gerencia.

3. Los expertos jurídicos dicen que monitorear el correo electrónico de los empleados y el uso de Internet puede ayudar a proteger la compañía en caso de una demanda. Tenga una política y solución adecuadas para monitorear el contenido con el fin de demostrarles a los empleados que se está haciendo esfuerzos por protegerlos del acoso de la siguiente forma:

    a. Capacitar a los usuarios para que sepan cuándo y cómo descargar las últimas actualizaciones de antivirus y cómo detectar un virus potencial. Enséñales a los empleados cómo analizar documentos antes de abrirlos.
    b. Reparar los agujeros conocidos en el software para reducir las posibilidades de que un virus entre por las páginas web o el correo electrónico.
    c. Desarrollar una política para las contraseñas, requiriendo cambios frecuentes de contraseñas y capacitando a los usuarios en las tácticas de ingeniería social y refuerce la posición de que nunca deben revelar una contraseña. El software para descifrar las

contraseñas está disponible para ayudar a encontrar contraseñas débiles de usuarios en su red. Sin embargo, el software no protegerá a la compañía contra la negligencia de los empleados. Con frecuencia basta con capacitarlos.

d. Determinar las necesidades del empleado para acceder a la información importante y restrinja el acceso sólo cuando sea estrictamente necesario para su desempeño en la compañía.
e. Avisar a los empleados sobre los peligros de descargar software, protectores de pantalla y otros programas similares gratuitos.

Políticas para el uso adecuado de Internet

Establecer una política de capacitación constante y consistente al usuario con énfasis en los objetivos de la seguridad para la compañía. Comenzar por determinar sus necesidades en relación con la política y el nivel de capacitación que requiere cada departamento. Por ejemplo, el personal de seguridad de la tecnología de la información necesita tener un conocimiento profundo de los productos y sistemas de seguridad que utiliza la compañía mientras que el personal diferente al técnico y de administración debe tener una comprensión general de las políticas adoptadas.

Existen varias opciones de capacitación, como aprendizaje práctico, capacitación basada en la Web, capacitación en el aula de clase o por medio de seminarios. Se debe tomar en cuenta lo que los empleados necesitan aprender y luego

determinar los métodos de capacitación que serán más efectivos. Según los expertos, para enfatizar el sentido de cultura empresarial y reforzar la importancia de mantener la confidencialidad, quizás es más efectivo una capacitación en el aula de clase o por medio de seminarios presenciales. Si necesita instruir a los empleados sobre el uso del nuevo software de seguridad, sería mejor un método práctico. Capacitar a los profesionales puede ayudar a determinar el método más efectivo que se debe adoptar.

5.2.4 Guía para planes de contingencia

Se recomienda crear y contar con un plan de contingencia que abarque lo tangible e intangible:

1. Reducción de los costos por perjuicios si ocurre un siniestro.
2. Las primas de seguro de bajo costo.
3. Mayor comunicación y mejores relaciones entre los departamentos.
4. Una mayor conciencia entre el personal de seguridad sobre la importancia de la seguridad y el valor de la propiedad que se está protegiendo.

Etapas clave en la elaboración de planes de contingencia

Las partes involucradas en el desarrollo de un plan de contingencia deben saber escuchar y comunicarse. Aunque existen algunas etapas importantes de

desarrollo, mantener un buen plan significa repetir continuamente estas etapas, volver a evaluar el plan y revisarlo.

1. **Determinación del objetivo:** El punto de partida para el desarrollo de un plan de contingencia es determinar un objetivo claro. El departamento de TI y los funcionarios de nivel ejecutivo deben identificar el objetivo operativo en caso de una emergencia en materia de seguridad. Por ejemplo, determinar si el objetivo es proteger cierta información y bienes, es mantener operaciones comerciales o brindar un excelente servicio al cliente. El objetivo ayudará al departamento de TI a definir un plan estratégico de acción y determinar los recursos que se deben proteger primero.
2. **Realización de un inventario completo:** Se deben identificar las principales herramientas de TI, los recursos y las tareas necesarias para realizar negocios y atender las funciones críticas establecidas en el objetivo de la elaboración de planes de contingencia. El inventario debe incluir recursos auxiliares como suministros de energía y recursos de respaldo.
3. **Análisis de riesgos:** Evalúe los perjuicios financieros, técnicos jurídicos y operativos totales que pudieran ocurrir como resultado de una brecha del sistema de seguridad. El riesgo abarcaría perjuicios potenciales a los clientes y compañías. También analice amenazas a la seguridad y los perjuicios que potencialmente podrían ocasionar a varios departamentos y operaciones. El software de administración de riesgos a la seguridad puede ayudar al personal de TI a evaluar el impacto de las amenazas a la seguridad de la compañía.

4. **Desarrollo de un plan de acción:** Repase los escenarios detallados de "qué pasaría si..." que implican diferentes amenazas a la seguridad y los efectos posibles en las operaciones. Para cada escenario potencial de disminución de riesgos, tenga en cuenta a las personas involucradas, sus responsabilidades, las consideraciones presupuestales, etc.
5. **Prevea un "Plan B":** Aunque los mejores planes de contingencia encuentran problemas técnicos, trate de anticiparse a estos problemas y crear soluciones alternas.
6. **Planeación de las comunicaciones y compras:** Los mejores planes son efectivos solo si los empleados tienen en cuenta su importancia y entienden sus mensajes y procesos. Los departamentos de recursos humanos, de aspectos jurídicos y finanzas deben revisar y responder a los planes de contingencia de seguridad en cada etapa de desarrollo.

Especificaciones del plan de acción

Los planes de contingencia variarán dependiendo del tipo específico de brechas del sistema de seguridad, como el ataque de virus que podría afectar las operaciones de la compañía de manera diferente a como lo haría una negación de servicio.

Debido al rango de amenazas a la seguridad, los planes de contingencia deben ser adaptables. Sin embargo, todos los planes efectivos deben responder por lo siguiente:

1. **Pérdida de la información:** Eventualmente las fallas en el fluido eléctrico, los virus, los hackers u otras fuerzas perjudicarán la información

importante de una compañía o la hará inaccesible. Prepárese para lo inevitable haciendo copias de seguridad del sistema y de la información. A fin de garantizar que se realicen copias de seguridad periódicamente, desarrolle una política de seguridad que establezca claramente lo siguiente:

a. Los medios que utilizará el personal de TI para hacer las copias de seguridad.
b. Quién realizará las copias de seguridad.
c. Con qué frecuencia se realizarán las copias de seguridad.
d. Los sitios de almacenamiento dentro y fuera del local destinados para las copias de seguridad de la información.

Los servicios de copia de seguridad en línea se están volviendo más comunes, sin embargo, el personal de TI debe investigar exhaustivamente las herramientas de seguridad de la compañía para el almacenamiento y la confiabilidad de las computadoras.

2. **Respaldo del hardware:** A las compañías con computadoras y servidores propios les gustaría contar con equipos de respaldo "rápido", que estén disponibles en caso que el servidor principal se dañe. Si el servicio al cliente es la prioridad de la compañía, es sensato tener equipos de respaldo. Las compañías con diferentes objetivos e intereses podrían redistribuir los fondos para destinarlos a equipos de respaldo del hardware a fin de proteger otras prioridades operativas.

3. **Suministros de energía de reserva:** Una falla en la energía puede dañar la información y afectar la capacidad de la compañía para prestar los servicios. Una fuente de energía ininterrumpida o UPS es un componente indispensable de todo plan de contingencia. Algunos modelos de UPS pueden suministrar protección contra los picos y fluctuaciones de corriente y la capacidad para calcular automáticamente las necesidades de energía del personal de TI. Los costos de las UPS varían dependiendo del "tiempo de ejecución" del modelo o del tiempo de energía disponible.
4. **Proveedores del servicio y socios comerciales:** La seguridad debe ser un aspecto clave que debe ser considerado por todo proveedor de servicio o estar estipulado en el contrato del socio comercial, especialmente cuando las partes involucradas son parte de una VPN o una cadena de suministros en red. El personal de TI debe estipular que todos los socios tienen las mismas herramientas de seguridad. El control de la seguridad debe ser un componente de las negociaciones de un contrato. Como parte de un plan de contingencia, el personal de TI debe evaluar las formas en que la red es vulnerable a las brechas de seguridad de la red de un socio.
5. **Recursos de TI:** En el caso de detectar una brecha de seguridad, el personal de TI podría necesitar personal adicional. Establezca relaciones con una agencia temporal de personal antes que ocurra una emergencia. El personal de TI también debe identificar a los consultores expertos de cuya experiencia se puedan beneficiar. También puede ser sensato negociar contratos de asistencia con los distribuidores antes que ocurra una crisis en la seguridad.

6. **Prensa:** El personal de TI debe trabajar con el departamento de relaciones públicas a fin de desarrollar una estrategia que solucione las brechas de seguridad. Debe especificarse detalladamente en un plan de contingencia la cantidad de información que debe revelarse (en caso de que se deba revelar) y quién debe comunicar esta información. Los planes también deben hacer asignaciones presupuestales para los costos adicionales del departamento de relaciones públicas. Evalúe si es necesario establecer relaciones con una agencia de relaciones públicas que tenga experiencia en comunicar información relacionada con alta tecnología.
7. **Aprobación de fondos:** Las situaciones de emergencia requieren gastos que no están contemplados en el presupuesto. Las partes responsables de elaborar un plan de contingencia deben revisar los estatutos de constitución y el reglamento de la compañía para determinar quien puede declarar cuando una situación es una emergencia y quien tiene autoridad para asignar los recursos de emergencias. En situaciones de emergencia se debe establecer un proceso de rápida asignación de fondos para las emergencias con el fin de evitar procesos demorados de solicitud y aprobación.

5.2.5 Creación de un documento y equipo de respuestas a incidentes

Redactar un documento de respuesta a incidentes explica de manera resumida el "imperio de la ley" para los procedimientos de emergencia y trata los siguientes aspectos:

- ¿Quién reporta a quién?

- ¿Quién es responsable de qué?
- ¿En qué circunstancias debería suspenderse un servicio de correo electrónico o un servidor de Internet?
- ¿Cuáles son los procedimientos para la comunicación y alerta de emergencias?

Un equipo de respuesta a incidentes realiza muchas de las acciones explicadas en el documento de respuesta a incidentes. Este equipo tiene papeles asignados previamente. En caso de identificar una brecha de seguridad, los integrantes del equipo están familiarizados con sus responsabilidades.

5.2.6 Medidas de seguridad

Los planes de contingencia no son únicamente estratégicos. Mientras que los planes solucionan principalmente escenarios hipotéticos, también necesitan que el personal de TI tome algunas medidas en tiempo real. Se recomiendan las siguientes:

- **Seguro:** En caso de una brecha de seguridad, el seguro cibernético puede ayudar a cubrir los costos debido a la pérdida de información, interrupción de las empresas, gastos en relaciones públicas, demandas de terceros como consecuencia de la negligencia en seguridad, etc. Las primas de seguro varían dependiendo del tamaño y naturaleza de los negocios en línea de la compañía. Las compañías de seguros casi siempre realizan auditorias de seguridad antes de dar cubrimiento a los solicitantes. Los

planes de contingencia pueden ayudar a disminuir los costos de las primas de seguro.

- **Aplicaciones de la seguridad:** Los antivirus, la detección de intrusos y el software para el filtrado de contenidos de Internet y del correo electrónico pueden ayudar a proteger la red contra una variedad de amenazas a la seguridad como las siguientes:
    - Ataques de piratas
    - Ataques de virus
    - Negación de servicio
    - Intrusión de códigos móviles maliciosos
    - Fugas de información confidencial
    - Correo electrónico y contenidos calumniosos de los sitios web

5.2.7 Planes de contingencia específicos

Todas las etapas de análisis e implementación de un plan de contingencia deben respaldar el objetivo del plan. Debido a la variedad de brechas de seguridad, los planes de contingencia deberán ser adaptados a los diferentes escenarios. Sin embargo, el personal de TI debe planear algunas constantes como el suministro de energía, los respaldos de la información, los recursos adicionales del personal de TI, etc. Los costos para el desarrollo e implementación de un plan de contingencia completo pueden ser significativos, aunque siempre serán mayores los costos de tiempo de inactividad de la compañía y detrimento a la reputación debido a las brechas de seguridad.

5.3 Viabilidad

Esta propuesta es viable implementarla en las empresas costarricenses analizadas, por cuanto tienen los recursos tecnológicos para hacerlo. Un costo inicial es el de capacitación, pero este debe ser tomado como una inversión en capacidades y como un medio de incrementar la seguridad y evitar mayores riesgos.

Las situaciones de emergencia requieren gastos que no están contemplados en el presupuesto. Las partes responsables de elaborar un plan de contingencia deben revisar los estatutos de constitución y el reglamento de la compañía para determinar quien puede declarar cuando una situación es una emergencia y quien tiene autoridad para asignar los recursos de emergencias. En situaciones de emergencia se debe establecer un proceso de rápida asignación de fondos para las emergencias con el fin de evitar procesos demorados de solicitud y aprobación.

La propuesta integra elementos de costos como los siguientes:

- Consultoría
- Capacitación
- Implementación de la solución
- Hardware y Software

Los costos, a precios actuales, por una empresa de 100 usuarios, son los siguientes:

Consultoría

Este rubro incluye la participación activa dentro de la empresa para determinar correctamente las necesidades específicas de la misma. Este valor se determina por costo unitario por hora de la o las personas asignadas para realizar el trabajo. El costo promedio por hora para una consultoría en seguridad es de US**$80.00**. El tiempo para realizar una consultoría es muy variado sin embargo hemos determinado dos semanas como un tiempo prudente para realizar el estudio necesario en las empresas de nuestra investigación, para un total de US**$6,400.00** utilizando solamente a un experto para ejecutarla.

Capacitación

La capacitación implica la transferencia del conocimiento a los usuarios y al administrador de la seguridad en la empresa. El costo es de US**$40.00** por hora y se estiman un total de 40 horas de capacitación, para un total de US**$1,600.00**

Implementación

Este rubro se refiere a la instalación, configuración e implementación de las soluciones que requiera el cliente. Separaremos este rubro en hardware y software, en donde la hora por lo primero será de US**$40.00** para un total de US**$1,600.00** mientras que por el software será de US**$60.00** la hora para un total de US**$4,800.00**.

Hardware

ROUTER CISCO 2620	$3,367.40
FIREWALL CISCO PIX 506	$8,475.00
TAPE BACK-UP	$3,680.00
DETECTOR DE INTRUSOS	$10,170.00
SERVIDOR DE SEGURIDAD	$9,550.00
TOTAL:	**$35,242.40**

Software

Veritas Back-up	$985.00
Antivirus Enterprise Symantec	$4,500.00
Internet Security Acceleration – ISA Server	$1,570.00
Windows 2000 Server y licencias usuarios	$4,960.00
TOTAL:	**$12,015.00**

El total de la inversión será de $64,857.40

Hemos incluido los precios de los equipos y programas que más se utilizan en la seguridad tecnológica, sin embargo una etapa inicial de inversión puede incluir diferentes mezclas interesantes, tanto en Hardware como en Software, según lo determine el experto y el presupuesto de la empresa. Lo que si se comprueba es que la propuesta en viable.

BIBLIOGRAFÍA CITADA

(1) SCHNEIER, BRUCE: **"Secrets and Lies: Security in a networked world",** 1a. Edición, Down Hill, USA, 2001

(2) CEDEÑO GOMEZ, ALVARO: **"Administración de Empresas"**, 2ª. Edición, Editorial de la Universidad Estatal a Distancia, Costa Rica, 1990

(3) FLIPPO B., EDWIN: **"Principios de Administración de Personal"**, McGraw hill, México D.F., 4ª. Edición, 1988

(4) ESPINOZA VERGARA, MARIO: **"La Capacitación"**, Seminario INCAE, Costa Rica, 1988

(5) MICROSOFT: Enciclopedia Interactiva **ENCARTA**, 2001

(6) ANDER-EGG, EZEQUIEL: **"Técnicas de Investigación Social"**, Editorial El Ateneo S.A., 1a. Edición, México, 1986

(7) WEIS, RONALD: **"Investigación de Mercado"**, Prentice Hall, México, 1a. Edición, 1986

(8) ARELLANO, JAIME: **"Elementos de Investigación: Investigación a Través de su Informe"**, EUNED, Costa Rica, 1a. Edición, 1981

(9) R. HERNÁNDEZ, A. FERNÁNDEZ y P. BAPTISTA: **"Metodología de la Investigación"**, McGraw Hill, México, 2a. Edición, 1991

(10) **OPCIT**, Arellano Jaime, 1981

BIBLIOGRAFÍA CONSULTADA

ANDER-EGG, EZEQUIEL: **"Técnicas de Investigación Social"**, Editorial El Ateneo S.A., 1a. Edición, México, 1986

ARELLANO, JAIME: **"Elementos de Investigación: Investigación a Través de su Informe",** EUNED, Costa Rica, 1a. Edición, 1981

BERENSONM.L., LEVINE, D.M., **"Estadística para Administración y Economía"**, McGraw Hill, México, 2ª. Edición, 1994

CEDEÑO GOMEZ, ALVARO: **"Administración de Empresas"**, 2ª. Edición, Editorial de la Universidad Estatal a Distancia, Costa Rica, 1990

DANKHE, G.L. **"La comunicación humana: ciencia social"**. México D.F.: McGraw Hill de México, 1976

FLIPPO B., EDWIN: **"Principios de Administración de Personal"**, McGraw Hill, México D.F., 4ª. Edición, 1988

KOONTZ, HAROLD y WEIHIRICH, HEINZ, **"Administración Una Perspectiva Global"**, McGraw Hill, México, 1994

MICROSOFT: Enciclopedia Interactiva **ENCARTA**, 2001

R. HERNÁNDEZ, A. FERNÁNDEZ y P. BAPTISTA: **"Metodología de la Investigación"**, McGraw Hill, México, 2a. Edición, 1991

SCHNEIER, BRUCE: **"Secrets and Lies: Security in a networked world",** 1a. Edición, Down Hill, USA, 2001

WEIS, RONALD: **"Investigación de Mercado"**, Prentice Hall, México, 1a. Edición, 1986

Páginas de Internet:

www.symantec.com

www.cisco.com

www.microsoft.com

www.elfinanciero.com

www.nacion.com

www.capitales.com

www.cert.org

www.sans.org

www.icsa.net

www.securityfocus.com

www.incidents.com

ANEXOS

ENTREVISTA 1

Realizada al experto en seguridad informática.

1- Cual es su experiencia en el tema de la seguridad?

2- Cuál es la preocupación más común de los clientes en torno al tema de seguridad?

3- Cuáles son los niveles (capas) de seguridad en la tecnología informática? Deberían utilizarlas todas nuestras empresas?

4- Cuáles son las herramientas más seguras que deberían utilizar las empresas?

5- Existe algún modelo predefinido o manejado por alguna empresa digno de ser copiado?

6- Cuáles son los factores de riesgo que toda empresa debe considerar?

7- Los gerentes de las compañías reflejan la suficiente preocupación o interés por el aspecto de seguridad?

8- Puede cualquier persona encargarse de la seguridad de una empresa? Qué niveles académicos cree necesarios para esta persona? Qué conocimientos debe tener?

9- Qué conoce sobre la legislación informática en nuestro país? Qué opina?

10- Cuál cree usted que es un modelo óptimo que deben utilizar las empresas?

ENTREVISTA 2

Realizada al experto en legislación informática

1- Cuál es su experiencia en el tema? Cuántos años en tema específico de la informática?

2- Cuál ha sido en pocas palabras el desarrollo de la legislación informática en Costa Rica? Hacia dónde vamos?

3- Es suficiente lo que existe hoy en día? Qué falta?

4- Cuántos casos al año son presentados a las autoridades? Por su experiencia, cuántos más cree que no se presenten?

5- De los que pueda referirse, conoce montos económicos de las pérdidas o cuál ha sido el impacto de lo sucedido?

6- Como experto, qué se debe legislar y qué debería quedar sin jurisdicción?

ENCUESTA 1

Realizada a los encargados y/o administradores del área de informática de las empresas

1- Cuál es su puesto: (marque con X -sólo uno-)

a. ____ Gerente de TI
b. ____ Jefe de TI
c. ____ Asistente de TI
d. ____ Encargado

e. ____ Otro - Cuál? _____

2- Grado académico: (marque con X -sólo uno- su último grado)

a. Bachiller Universitario ____ en _____
b. Licenciado Universitario ____ en _____
c. Master ____ en _____
d. Técnico ____ en _____
e. Bachiller Colegial ____ en _____
f. Otro ____ en _____

3- Qué otros certificados o estudios afines posee?

_____ _____
_____ _____
_____ _____
_____ _____
_____ _____

4- Cuál es el nivel de compromiso de su empresa con la seguridad informática?

a. ____ Ningún Compromiso
b. ____ Poco Compromiso -Solo por reacción-
c. ____ Buen Compromiso –Mantiene un plan de prevención y capacita al administrador o encargado de la seguridad-
d. ____ Total compromiso –Además del punto anterior poseen a un experto en seguridad o a una empresa experta en el tema como socio de negocios-

5- Cuál es la plataforma tecnológica de su empresa?

_____
_____
_____
_____
_____

6- Utiliza su empresa alguno de estos equipos:

a. ____ Router
b. ____ Pix
c. ____ Firewall
d. ____ Tape Back-up
e. ____ Detector de intrusos
f. ____ Llaves de seguridad electrónica

g. ____ Otro relacionado a seguridad – Cuál (es) _____
_____

7- Utiliza su empresa alguno de éstos productos:

a. ____ Antivirus
b. ____ Detector de intrusos
c. ____ Firewall personal
d. ____ Gateway
e. ____ Filtrado de contenido
f. ____ Disaster Recovery
g. ____ Back-up

8- Maneja su empresa políticas internas de seguridad?

a. ____ No b. ____ Si - Cuáles:

_____
_____
_____
_____
_____
_____
_____
_____
_____

9- Conoce la legislación informática existente en nuestro país?

a. ____ Si –*pase a la siguiente pregunta-*

b. ____ No –*pase a la pregunta 11-*

10- En pocas palabras qué opina?

_____

_____

_____

_____

11- Ha sido su empresa víctima de alguna forma de delito informático ya sea interno o externo?

a. ____ Si –*pase a la siguiente pregunta-*

b. ____ No –*pase a la pregunta 11-*

12- Que ocurrió y como lo solucionaron?

_____

_____

_____

_____

13- Qué sucede cuando su operación crítica se ve interrumpida por alguna falla en sus sistemas (error humano, ataque o problema mecánico)?

_____

_____

_____

_____

MAPA CONCEPTUAL