Universidad Latinoamericana de Ciencia y Tecnología

Escuela de Ingeniería Informática

Propuesta de un Modelo para la Adquisición e Implementación de Firmas Digitales en la Transmisión de Datos a través del Correo Electrónico en el Banco Centroamericano

Baltodano Madrigal Yesenia, 2-0536-0510

Proyecto de Graduación Presentado ante el Programa de Ingeniería en Informática, como parte de los Requisitos para optar por el Grado de Licenciatura.

San José, Costa Rica

Agosto, 2003

ÍNDICE

ÍNDICE DE GRÁFICOS

ÍNDICE DE TABLAS

1. INTRODUCCIÓN

1.1 Antecedentes de la Banca en Costa Rica

La siguiente es una reseña histórica de los antecedentes de la Banca en Costa Rica, tomada de los libros Ciento Cinco Años de Vida Bancaria en Costa Rica de Rufino Gil Pacheco (1974) y del libro escrito por Tomas Soley Güell, Compendio de Historia Económica y Hacendaria de Costa Rica (1940).

La historia bancaria en Costa Rica inició alrededor de 1850, cuando diferentes causas de distinta índole, principalmente económica y fiscal, dieron pie a la proposición de la fundación de un Banco Nacional de Costa Rica. Sin embargo, este primer intento fue rechazado. El presidente de esa época, el Dr. José María Castro Madríz, consciente de que la fundación de un Banco Nacional era necesaria y útil para la economía que se estaba viviendo en esos años, siguió intentando la materialización de su proyecto, pero nuevamente fracasó su intento.

En 1857, se firmó un contrato llamado Medina-Escalante. Este contrato indica la fundación del Banco Nacional de Costa Rica, como primera institución bancaria, el cual, posteriormente sería modificado y se agregaron nuevas cláusulas, lo que dio como resultado, la firma de un nuevo contrato para 1858, llamado Cañas-Escalante. No obstante, no fue hasta el 15 de junio de 1858 cuando el Banco Nacional de Costa Rica se constituyó como primera institución bancaria, no solo con cobertura nacional, sino también en Centro América.

Posteriormente, el 25 de junio de 1863, se fundó el Banco Anglo Costarricense. Una de sus principales obras fue el establecimiento del cheque como medio de pago; fue el primero en dar el servicio de cuenta corriente en el país.

Catorce años más tarde, se crea el Banco de la Unión, el 15 de abril de 1877. Este Banco cambió su nombre a Banco Centroamericano, en un acuerdo tomado por la Junta Directiva de ese entonces, el 17 de noviembre de 1890.

A partir de 1900 se fundaron en Costa Rica 5 entidades financieras más que brindaban los servicios de crédito a los clientes. Estas instituciones fueron: el Banco Comercial de Costa Rica, Banco Mercantil de Costa Rica, Banco Internacional de Costa Rica, Sucursal del Royal Bank of Canadá, el Crédito Agrícola de Cartago. Luego vino la fundación del Banco Central de Costa Rica, entre muchos otros de los que existen actualmente en el país.

Posterior a la creación de estas instituciones bancarias, se dan reformas bancarias, estructuraciones y evoluciones del sistema financiero nacional con el fin de constituir un estado banquero, nacionalización de la banca, competencia entre los bancos nacionales, leyes, entre otros, que dieron como resultado la reforma bancaria con la que contamos actualmente conformada por bancos nacionales e internacionales, públicos y privados. Una de las reformas bancarias que se da es la creación de la Ley Orgánica del Sistema Bancario Nacional, en 1953. El objetivo de la creación de esta Ley era luchar contra la inviolabilidad de las cuentas corrientes en la fijación del concepto de que los Bancos no fueran dependencias gubernamentales. Además, se acordó una nueva campaña para las cuentas corrientes, el ahorro y la presentación de los presupuestos en una fórmula igual para todos los Bancos. En 1954 se aprobó la redacción del contrato para la apertura de cuentas corrientes, y se acordó hacer publicidad o una campaña a favor de la dignificación de la cuenta corriente, con el fin de atraer más capital y evitar los cheques sin fondos. También se creó un comité interbancario para el manejo de las cuentas corrientes. Se formuló una nueva campaña publicitaria, se cambiaron impresiones sobre el cobro de intereses, su tipo y clase de operaciones. En los años posteriores a la creación de la Ley Orgánica, se notó una extensión de los servicios bancarios a través del país por medio de sucursales y agencias, debido a la necesidad de incrementar el ahorro y las cuentas corrientes.(1974, págs. 19-400; 1940, págs. 5-200.)

1.2 Tema

Propuesta de un modelo para la adquisición e implementación de Firmas Digitales en la transmisión de datos a través del correo electrónico en el Banco Centroamericano.

1.3 Problema

¿Cómo se puede diseñar un modelo de firmas digitales para los datos que se transmiten por medio la red en el Banco Centroamericano que reduzca el riesgo provocado por la ausencia de controles y mecanismos de autenticación y confidencialidad?

1.4 Justificación

En los últimos años se ha podido observar cómo las instituciones, cualquiera que sea su índole, han incursionado ampliamente en la informática como herramienta de gran apoyo para la toma de decisiones. Las constantes innovaciones en materia de hardware con capacidades cada vez más grandes en almacenamiento, velocidades, manejo simultáneo de tareas, entre muchos otros, son perseguidos por los empresarios que desean brindar el mejor y más rápido servicio a los clientes.

En lo que respecta al software, las empresas también tienen un apoyo muy grande, ya que en el mercado se puede encontrar una variedad de aplicaciones que permiten realizar las actividades diarias de las instituciones. Lo último relacionado con software en las empresas, que antes solían desarrollar sus propios sistemas. Sin embargo, ahora la tendencia es contratar otras empresas externas para el desarrollo, implantación y mantenimiento de las aplicaciones, las cuales a su vez, por su naturaleza de origen, se amoldan a las necesidades y requerimientos de la empresa que los solicite. Con la contratación externa para el desarrollo de sistemas, las empresas obtienen grandes beneficios como lo son: los proyectos son terminados en tiempos más cortos que si fueran desarrollados por funcionarios de la institución, se pueden reutilizar las labores que realizan las personas encargadas de dar mantenimiento a los sistemas en actividades más útiles, entre otras.

Para nadie es un secreto que actualmente vivimos en un mundo basado en comunicaciones a través de redes de datos y principalmente por medio del correo electrónico como medio fácil, rápido, certero, cómodo, entre otros, para la transmisión de información. No obstante, las empresas por lo general se encargan de asegurar la información que se transmite fuera de las fronteras de la red de datos interna de la institución, y mantienen desprotegida la red interna. Las estadísticas lo confirman. Sólo en el 2000 los fraudes en Estados Unidos eran de un 82% a los "Web Sites", un 12% a los servicios de correo electrónico y un 4% a los grupos de noticias. Sin embargo, para el 2001 los ataques a los "Web Sites" disminuyeron a un 78%, al igual que a los grupos noticiosos, y solamente los ataques del correo electrónico aumentaron a un 18%[1]. De igual forma, se ha comentado que los principales ataques a las instituciones provienen de sus propios empleados, por lo que no se debe restar importancia a la información que se transmite internamente por medio del correo electrónico de la empresa.

Casi todas las actividades financieras que se realizan habitualmente en el mundo requieren de algún tipo de identificación que haga responsables a las personas de las consecuencias de las operaciones. En la vida diaria, basta tomar la pluma y firmar un talonario para reconocer la existencia de un pago o deuda, autorizar a que el banco lo abone y cargue después el débito en una cuenta y hacer responsable de toda la operación a quien hizo el trámite, incluidas las consecuencias legales que puedan derivarse de una hipotética falta de liquidez. Como se puede ver, la firma es en sí un acto sencillo, pero que desencadena variadas e importantes consecuencias. Parece bastante lógico que el sistema de dinero digital intente basarse en un mecanismo similar.

No obstante, conceder a una serie de combinaciones de bits tal carga de implicaciones no es tarea sencilla, ya que los bits pueden copiarse, manipularse y duplicarse con mucha facilidad en un papel por intrusos, más conocidos como "hackers", "phrackers" o "crakers", los cuales al final van a terminar utilizando esa información confidencial para modificarla, destruirla, y en el peor de los casos, alterarla a conveniencia ajena (principalmente para

[1] Tomado de www.fraud.org, Estadísticas de fraudes en internet del 2001

beneficio propio del "hacker"), y sin importar el motivo, causando grandes pérdidas financieras tanto a la institución bancaria como al cliente. Lo anterior refleja una gran brecha de seguridad por solucionar en especial, hoy en día, donde muchas empresas bancarias necesitan certificarse a sí mismas, a sus clientes individuales y corporativos para que los datos que envían a través del correo electrónico viajen de manera segura.

A raíz de la necesidad planteada en los párrafos anteriores, es que surge la incógnita de cómo asegurar los datos que se envían a través del correo electrónico. En este caso, la orientación del tema es hacia el mecanismo de autenticación y confidencialidad que se puede implantar en el correo electrónico relacionada con la información que se maneja tanto a nivel interno como externo de una empresa bancaria, debido a que Costa Rica está innovando en la tecnología del manejo de datos electrónicos por ser un método más cómodo, fácil y ágil de hacer comunicación entre dos personas o entes. Al viajar la información a través del correo electrónico de forma legible, se ve expuesta a que algún intruso capture el paquete de información y manipule de manera inadecuada los datos que se están transfiriendo.

Es importante mencionar que en la Asamblea Legislativa se está tramitando un proyecto de ley de Firma Digital y Certificados Digitales con el fin de que respalden toda aquella información que es transmitida por medio electrónico. Este proyecto pretende "mantener la armonía con los elementos principales de la regulación internacional sobre el tema, brindando el marco jurídico adecuado y viable para la contratación electrónica, y en general, las regulaciones jurídicas basadas en la comunicación mediante medios informáticos o telemáticos, sean o no de índole comercial". Además, en setiembre del 2000, la ONU creó la "UNCITRAL Model Law" y la "EU Directive", la cual es una ley que regula el manejo de firmas digitales en varios países unidos, entre los que se encuentra Costa Rica.

Muchas instituciones bancarias aún no toman conciencia de que el activo más importante para una empresa, así como para un cliente, es la información. A menudo, envían por medio del correo electrónico información confidencial sin ninguna protección o

encriptación, por lo que cualquier persona malintencionada puede ver claramente el contenido del correo enviado y manipularlo inadecuadamente, ya sea alterando el mensaje original, capturando la información y facilitándola a la competencia para hacer un daño o porque pertenece a la misma, borrándola, entre otros.

Innovan en el mundo de las transferencias de datos sin tener conocimiento de lo delicado que es esta transmisión de información por medio del correo electrónico. A raíz de este gran problema es que nace la idea de realizar una investigación basada en firmas digitales, con el fin de determinar si es o no, una solución para asegurar que los datos enviados a través del correo electrónico puedan autenticar y asegurar la confidencialidad de los mensajes a un usuario o empresa.

1.5 Objetivos Generales

Diagnóstico

a) Estudiar los mecanismos de autenticación y confidencialidad utilizados en la trasmisión de información a través del correo electrónico en el Banco Centroamericano.

Propuesta

b) Proponer un modelo para la adquisición e implementación de firmas digitales en el Banco Centroamericano.

1.6 Objetivos Específicos

Diagnóstico

a) Determinar los mecanismos de autenticación y confidencialidad para la información que es enviada por medio del correo electrónico, utilizados actualmente en el Banco Centroamericano.

b) Identificar las necesidades de autenticación y confidencialidad de los datos trasmitidos a través del correo electrónico que utiliza el Banco Centroamericano.

c) Determinar las regulaciones o leyes de Costa Rica y tratados internacionales relacionados con el uso de firmas digitales.

d) Identificar las empresas que brindan servicios de firmas digitales para autenticar y asegurar la confidencialidad de la información enviada por el correo electrónico.

e) Analizar las ventajas y desventajas que poseen las empresas que ofrecen los servicios de firmas digitales utilizadas para autenticar y asegurar la confidencialidad de los datos transmitidos por el correo electrónico.

f) Identificar los requerimientos de hardware y software que son necesarios para implementar un modelo de firmas digitales.

Propuesta

g) Definir un modelo de adquisición e implementación de firmas digitales para el uso del correo electrónico en el Banco Centroamericano.

h) Definir las implicaciones administrativas en la implementación de firmas digitales en el Banco Centroamericano, de acuerdo con la importancia relativa de la información que se desea resguardar.

1.7 Variables

Según Santiago Zorrilla y Miguel Torres (1992) las variables son definidas como "todo aquello que se puede medir, controlar o estudiar en una investigación". p. 62

Para efectos del presente estudio, se definieron las siguientes variables de investigación:

Variable: Mecanismos de autenticación y confidencialidad

Definición conceptual: son mecanismos que permiten autenticar y asegurar la confidencialidad de la información que es enviada por medio del correo electrónico a una o varias personas internas o externas a la institución en que labora.

Definición operacional: los criterios de evaluación por utilizar son la descripción de los mecanismos de autenticación y confidencialidad de los mensajes por medio del correo electrónico, las desventajas que presenta la utilización de estos mecanismos y la fortaleza que ofrecen ante posibles ataques.

Variable: Necesidades de autenticación y confidencialidad

Definición conceptual: dentro del entorno de la información enviada por medio del correo electrónico, son los requerimientos que tiene una persona, empresa u otro para autenticar y asegurar la confidencialidad de sus activos.

Definición operacional: los criterios de evaluación son los requerimientos de las personas por autenticar y asegurar la confidencialidad de los datos, las herramientas que ofrece el mercado actual, y la selección de la mejor opción para la empresa.

Variable: Regulaciones

Definición conceptual: son las leyes que emite el Estado de Costa Rica por medio de la Asamblea Legislativa y aquellos que nos regulan por medio de Tratados Internacionales

con el fin de hacer cumplir las directrices establecidas en las mismas, imponiendo multas y castigos penales a quienes las incumplan.

Definición operacional: se determinarán las leyes que actualmente existen tanto a nivel nacional como internacional, que tengan relación con el uso de las firmas digitales para el envío de información a través del correo electrónico.

Variable: Empresas

Definición conceptual: son las instituciones consolidadas en el mercado de la seguridad de los datos que ofrecen servicios para autenticar y asegurar la confidencialidad de la información enviada por medio del correo electrónico.

Definición operacional: se identificarán las empresas que ofrecen mecanismos para autenticar y asegurar la confidencialidad de la información que viaja por el correo electrónico.

Variable: Ventajas y desventajas

Definición conceptual: beneficios y desventajas que ofrece una solución de firmas digitales a una empresa.

Definición operacional: se describirán las ventajas y desventajas que ofrece la herramienta de firmas digitales a una empresa.

Variable: Hardware y Software

Definición conceptual: son todos aquellos dispositivos periféricos de los que está compuesto por ejemplo un computador, una red, a través de los cuales se logra la

interconexión entre varios equipos; y las aplicaciones por medio de las cuales se puede administrar los dispositivos periféricos.

Definición operacional: se determinarán las características de hardware y software necesarias para implantar un proyecto de firmas digitales en una empresa.

Variable: Implicaciones administrativas

Definición conceptual: actividades costo–beneficio, técnicas, operacionales de control interno, y de capacitación en que debe incurrir una empresa a raíz de la adquisición e implantación de un proyecto de firmas digitales. Estas actividades incluyen capacitaciones, remodelaciones de los departamentos, compras de nuevos equipos, reestructuración o solicitud de nuevos recursos humanos, entre otros.

Definición operacional: la variable implicaciones administrativas estará regida por el recurso humano que se vaya a disponer para dar marcha y mantenimiento al proyecto, las capacitaciones que deberán impartir para capacitar al recurso humano en el uso y manejo adecuado del hardware y software, en las políticas del negocio que se deberán definir para el uso y administración correcta del hardware y software involucrado en el proceso, entre otros.

2. MARCO TEÓRICO

Indiferentemente del tipo de actividad a la que se dedica la empresa, hoy en día, gran parte de las instituciones bancarias en el ámbito nacional pertenecientes al sector público, buscan ampliar sus mercados financieros por medio del concepto de comercio electrónico, haciendo banca virtual. Instituciones bancarias que hasta el momento han logrado ingresar en ese mercado meta de los clientes por medio de Internet, e incluso los que tienen como objetivo llegar y establecerse en él, deben utilizar una serie de mecanismos especializados que les permitan asegurar los datos que se transmiten por medio de la red con el fin de asegurar que las transacciones se realicen, los datos formen parte de las transacciones y el

dinero que involucra la realización de las mismas, logren mantener la integridad, autenticidad, confiabilidad, confidencialidad y calidad de los datos. Sin embargo, el resultado de todas estas transacciones financieras debe ser reportado a los usuarios de dichos servicios bancarios virtuales. El medio más utilizado para brindar al cliente lo que en persona se puede llamar el comprobante de la transacción realizada por medio de la banca virtual o bien, envío de la información personal de los negocios del cliente[2] es el correo electrónico, pero esta información al enviarla no es encriptada, por lo que cualquier persona ajena a la información puede verla claramente y manipularla de manera inadecuada.

Actualmente, se pueden encontrar muchos mecanismos que contribuyen con la búsqueda de la seguridad de los datos, algunos de ellos son los muros de fuego, configuración de enrutadores y "switches", red privada virtual ("VPN"), criptografía, firmas digitales por correo electrónico, entre otros. Todos juntos conforman un paquete de seguridad muy importante para asegurar los datos que diariamente se transmiten por medio de la red.

A la mayoría de los funcionarios que poseen niveles gerenciales en las instituciones bancarias públicas del ámbito nacional, les falta tener conocimiento y conciencia de las vulnerabilidades de los medios electrónicos y de los datos que son transmitidos por medio de red, y en este caso por el correo electrónico para la institución y clientes; los controles, las herramientas o técnicas que ofrece el mercado con el fin de contribuir con su seguridad; los mecanismos y la supervisión necesaria para asegurar que ellos pueden autenticar la identidad de todos los individuos involucrados en el proceso o la comunicación de la información y proteger el tráfico de datos de la modificación, destrucción, interferencia o contaminación.

En los últimos años se ha podido observar cómo las instituciones, cualquiera que sea su índole, ha incursionado ampliamente en la informática como herramienta de gran apoyo para la toma de decisiones. Las constantes innovaciones en materia de hardware con

[2] Negocios del cliente: estados de cuentas corrientes, tarjetas de crédito, movimientos de cuentas de ahorros, tarjetas de débito.

capacidades cada vez más grandes en almacenamiento, velocidades, manejo simultáneo de tareas, entre muchas otras, son perseguidas por los empresarios que desean brindar el mejor y más rápido servicio a los clientes.

En lo que respecta al software, las empresas también tienen un apoyo muy grande, ya que en el mercado se puede encontrar una variedad de aplicaciones que permiten realizar las actividades diarias de las instituciones. Lo último relacionado con software en las empresas, es que estas antes solían desarrollar sus propios sistemas. Sin embargo, ahora la tendencia es contratar otras empresas externas para el desarrollo, implantación y mantenimiento de las aplicaciones, las cuales a su vez, por su naturaleza de origen, se amoldan a las necesidades y requerimientos de la empresa que los solicite. Con la contratación externa para el desarrollo de sistemas, las empresas obtienen grandes beneficios como son que los proyectos son terminados en tiempos más cortos que si fueran desarrollados por funcionarios de la institución, se pueden reutilizar las labores que realizan las personas encargadas de dar mantenimiento a los sistemas en actividades más útiles, entre otras.

2.1 Redes de Telecomunicaciones de Datos

Para tener un panorama más claro de todo aquello que está en torno del correo electrónico, la seguridad de esta herramienta y los mecanismos existentes que contribuyan a asegurar los datos que se envían y reciben por este medio, se comenzará explicando de manera básica algunos conceptos de red.

Según Tom Sheldon (1995), el término red se define como un conjunto de computadoras y periféricos (impresoras, módem, escáner, entre muchos otros) que se interconectan por algún medio, el cual puede ser un cable (conexión directa), a través de un módem (conexión indirecta) o por medio de redes públicas o privadas. Cualquiera que sea el medio, a través de él, viajarán los datos. Por otra parte, los dispositivos pueden estar en un mismo lugar o dispersos en uno o varios edificios. Pueden estar separados por muchos kilómetros y conectados mediante el uso de líneas telefónicas dedicadas, microondas, fibras ópticas o

sistemas similares. Incluso pueden estar dispersos por el mundo y conectados a través de medios de comunicación a larga distancia, como son los enlaces por satélite.

2.2 Gamas de Red

Existen diferentes gamas de tipos de redes. Entre las más conocidas y utilizadas a nivel mundial se encuentran las LAN, MAN y WAN.

Las redes de área local son más conocidas por sus siglas en inglés LAN. Una red LAN es un segmento de red con estaciones de trabajo (computadoras personales) con dirección propia y servidores enlazados que se encuentran funcionando dentro de la misma área. Ejemplo de ello, sería una serie de computadoras y servidores interconectados entre sí dentro de un edificio.

Otro tipo es la red de área metropolitana o MAN. Al igual que la anterior posee computadoras y servidores enlazados a lo largo del área de ciudades o municipios. Para interconectarse utiliza las facilidades que proporciona la compañía de telecomunicaciones local.

Estos dos tipos de redes son las que frecuentemente más se utilizan por las distintas empresas a nivel nacional e internacional. No obstante, también existe otro tipo de red conocida como WAN (red de área extensa), la cual cruza las fronteras interurbanas, interestatales o internacionales. Las interconexiones se realizan por medio de los servicios públicos y privados de telecomunicaciones. En otras ocasiones, también se suele hacer utilizando los satélites y microondas.

La red corporativa por su parte, interconecta todos los sistemas de computadoras de una organización, independientemente del sistema operativo, de los protocolos de comunicación, de las diferentes aplicaciones o de la ubicación geográfica; por lo tanto, puede ser una LAN, MAN o WAN. La red se ve a sí misma como un plataforma sobre la cual, se conectan muchos tipos de dispositivos distintos. Se emplean diversas técnicas para

ocultar las diferencias entre sistemas y así los usuarios pueden acceder a cualquier recurso de forma transparente.

2.3 Tipos de Redes

Además de las gamas de red anteriormente citadas, encontramos otros tipos de redes como lo son: Internet, Intranet y Extranet.

La Internet, por ejemplo, es una red que permite la transmisión de datos a través de un grupo de recursos de información mundial. Internet ha crecido tanto que conecta a millones de usuarios de computadoras alrededor del mundo. Esta red de redes global está constituida por redes pertenecientes a universidades, gobiernos, corporaciones y particulares, conectadas a través de redes públicas y privadas. Para efectos del presente estudio, el término de Internet se entenderá como la conexión de distintas redes externas con la red corporativa, las cuales por su naturaleza no están bajo el control de la organización y son consideradas redes hostiles. La esencia de este concepto se deriva de la factibilidad de conectar dos redes a través de los servicios en que se basa la red mundial Internet. Algunos de estos servicios técnicos son: correo electrónico, telnet, ftp, world wide web (www), http, html, entre otros. (para un mejor entendimiento del significado de estos servicios, ver glosario).

Con respecto a Intranet, es una red corporativa privada que usa productos y tecnologías de Internet. Las compañías comúnmente, establecen las Intranets para sus empleados, sin embargo, algunas de ellas ofrecen accesos a usuarios externos. Adicionalmente, las intranets comparten todas la virtudes de la WWW, incluyendo la habilidad de publicar documentos que contiene gráficos, sonido, video y enlaces de hipertexto. Dado que los documentos son creados usando el mismo protocolo HTML, cualquier usuario de la red con un “web browser” (es decir, un buscador de páginas en Internet) puede accesarlos.

Por su parte, la Extranet se refiere, básicamente, al acceso de una red pública como Internet, a una red privada o Intranet. Esta red utiliza la tecnología TCP/IP propia de

Internet para permitir un acceso controlado, impidiendo el paso a zonas privadas. Normalmente, una Extranet forma parte de una Intranet.

2.4 Seguridad en Redes de Datos

En el contexto de redes de datos, la seguridad se refiere al establecimiento de un conjunto adecuado de controles que permiten minimizar los riesgos a los que están expuestos los recursos computacionales.

En la actualidad, la seguridad de redes se ha convertido en un asunto cada vez más importante en la mayoría de los ambientes corporativos alrededor del mundo, debido a que en las últimas décadas han ocurrido grandes avances tecnológicos, tanto en el campo de la computación como en el área de las telecomunicaciones. A pesar de los grandes beneficios que ha traído esta evolución tecnológica, el hecho de compartir recursos con terceras personas, ha creado riesgos asociados, los cuales amenazan diariamente la seguridad e integridad de los datos de las empresas. Algunas de estas amenazas o riesgos son:

- ***Uso o acceso no autorizado a recursos informáticos:*** el cual involucra el uso de cualquier recurso de red sin el permiso previo, por tal motivo, se considera se considera como acceso no autorizado. Su gravedad depende del sitio y la naturaleza de la pérdida potencial.

- ***Vandalismo y sabotaje:*** cuando se analiza esta amenaza, es necesario conocer cuáles son las medidas y los medios con los que se recuperará la información dañada o destruida. La destrucción de los datos causada por actividad de Internet no autorizada requiere una cantidad considerable de tiempo y recursos para investigar y reparar el daño.

- ***Robo de datos:*** cualquier información almacenada en equipos de computación es susceptible al robo, y más aún, cuando su trasiego es a través de Internet, ya que incrementa considerablemente la amenaza de ser robada.

- ***Repudiación:*** cuando uno o más usuarios involucrados en una comunicación, niegan su participación. Ésta es una amenaza crítica en las transacciones financieras y en los acuerdos electrónicos contractuales.

- ***Negación del servicio:*** se presenta cuando el acceso a sistemas o aplicaciones es interrumpido, retrasado o abortado en un momento dado.

- ***Pérdida de la integridad de los datos:*** los "hackers" o cualquier otro intruso, pueden utilizar Internet y tomar los archivos bases de las organizaciones para modificarlos o destruirlos sin importar el motivo. Estos actos pueden causar impactos financieros altamente costosos en las empresas que se vean afectadas por un ataque de este tipo.

- ***Interceptación de la información:*** se refiere a la observación de la información mientras se transmite a través de las redes. Los "sniffers" de red pueden robar los códigos de usuarios y claves de acceso no encriptados que son enviados en texto puro.

- ***Enmascaramiento:*** es cuando un usuario se hace pasar por otro usuario dentro de una red empresarial.

- ***Caballos de troya:*** son sistemas o programas de aplicación que son alterados por otros y contienen instrucciones alteradas u otra instrucción adicional que le permite al intruso realizar algún tipo de actividad maliciosa y no ser detectado.

- ***Virus y bombas lógicas:*** los virus de computadora son códigos de programa que se adhieren a un software de aplicación o a un componente ejecutable de un sistema; con ellos se puede alterar y/o eliminar archivos, cambiar datos o negar la disponibilidad de los recursos.

Además de los riesgos y amenazas mencionadas anteriormente, se debe tener presente que existe una amenaza más y que suele ser la que más se presenta en las instituciones, ésta es el sabotaje e inadecuado manejo de los datos y servicio que ofrece la red corporativa por parte de personal interno de la empresa. Estos pueden ser empleados disgustados con la compañía, personas sobornadas por diferentes medios para cometer el delito, o simplemente son delincuentes.

Como es conocido, la información es uno de los activos más importantes de una empresa, sea cual sea su naturaleza, y debido a que cada día existen más y nuevas brechas de seguridad en las redes, sobre todo las conectadas a Internet, el grado de exposición al riesgo se incrementa paralelamente. Debido a lo anterior, es de suma importancia que las organizaciones piensen en proteger la información.

No obstante, la inversión en que se debe incurrir para implementar seguridad en los recursos informáticos es muy costosa, aunque de mucho bien, si se consideran las pérdidas a las que se expone una empresa al haber visto violada la seguridad de los datos.

Por otra parte, existen varias organizaciones que llevan un adecuado control y administración de la seguridad de forma continua. Para ello, han designado a un grupo especializado de personas, el cual cuenta con herramientas y procedimientos de aplicación continua que les permite mantenerse a la vanguardia con la seguridad tecnológica. Esta actualización ha sido obligada, porque precisamente se han dado cuenta de que los acelerados avances de la tecnología, generan nuevos hoyos en la seguridad de sus recursos evidenciando nuevas vulnerabilidades o enfrentándolos a amenazas más complicadas.

A pesar de lo anterior, también existen empresas que no toman conciencia clara de la importancia de la seguridad, exponiendo sus activos a un alto nivel de riesgos que pueden llevarlos a serios impactos, tanto financieros como de imagen.

Muchas de las amenazas actuales combinadas con las vulnerabilidades que presentan algunas redes corporativas pueden llegar a convertirse en incidentes en cualquier momento,

y por consiguiente, producir efectos negativos en las empresas e incluso nefastos para empresas cuya razón de ser, es la confianza y credibilidad de los clientes, como es el caso de las entidades financieras.

2.5 Técnicas de Seguridad

Con el fin de minimizar los riesgos relativos con los ataques que pueden recibir las redes en una empresa, se deben utilizar una serie de técnicas básicas, cuya finalidad es proveer seguridad tanto en las comunicaciones entre los equipos como en los datos que en ellos se almacenan. Estas técnicas se refieren principalmente a:

- ***Autenticación:*** cuando existe una comunicación entre dos entidades, sean estas personas, instituciones o computadoras, generalmente existe un método en el que una entidad conoce realmente quién se está comunicando. Para esto se pueden utilizar algunas aplicaciones o métodos que proveen servicios de autenticación. Si se habla de comunicaciones a través de Internet, la necesidad de contar un grado de confianza y certeza en las comunicaciones es mayor.

- ***Autorización:*** una vez que el usuario es identificado dentro del sistema, la autorización se encarga de permitirle acceder a los recursos. La autorización consiste en una serie de listas de control de acceso definidas por los supervisores y administradores de la red. A través de estas listas, al usuario se le permite acceso a directorios, archivo, objetos o recursos disponibles.

- ***Confidencialidad o privacidad:*** consiste en ocultar los datos que por su naturaleza sensitiva deben protegerse de accesos no autorizados, asegurando que la información transmitida entre el emisor y el receptor no ha sido interceptada o divulgada a terceros. Actualmente, las tecnologías más usadas para asegurar la privacidad y la seguridad transaccional incluyen la criptografía, firmas digitales y tarjetas inteligentes entre otras, cuya efectividad depende de que las tecnologías

utilizadas sean capaces de proveer el nivel deseado, anonimato y que sean instaladas correctamente.

- ***Integridad:*** garantiza que la información es auténtica y no ha sido alterada o borrada de forma no autorizada. Al igual que para la confidencialidad, existen herramientas utilizadas para chequear la integridad por cuanto aún los computadores mejor protegidos ocasionalmente podrían tener intromisiones. El propósito de estas herramientas es examinar los archivos del sistema con el fin de determinar si se ha realizado algún cambio no esperado o no autorizado.

- ***Auditoría:*** consiste en registrar todas las acciones efectuadas por los usuarios y procesos, de tal manera que se puedan seguir las actividades maliciosas o involuntarias. Algunos de los eventos que deben registrarse son la creación y borrado de directorios, creación, apertura, cierre, borrado, renombrado, escritura y almacenamiento de archivos, modificaciones de entradas de directorios, eventos del servidor, eventos del usuario, entre otros.

- ***No repudiación:*** radica en negar el origen, retención, envío o integridad del contenido de un documento. Este técnica es utilizada , principalmente, cuando el recurso tecnológico está siendo atacado o saboteado en línea.

2.6 Niveles de Seguridad

De acuerdo con los estándares de seguridad en computadoras desarrollado por el Departamento de Defensa de los Estados Unidos, se define el criterio estándar para la evaluación de computadoras confiables. Para ello se usan varios niveles de seguridad para proteger los recursos informáticos de un ataque al hardware, software y a la información guardada. Los niveles de seguridad que se describen en el libro naranja son los siguientes:

- ***Nivel D1:*** es la forma más elemental de seguridad disponible basada en que todo el sistema no es confiable y en la afirmación de que no hay protección disponible para

el hardware y el sistema operativo. La autenticación se compromete con facilidad y no existe para los usuarios.

- ***Nivel C:*** está conformado por dos subniveles de seguridad denominados C1 y C2:

  - *Nivel C1:* sistema de protección de seguridad discrecional: este estándar posee algún tipo de protección para el hardware. Los usuarios deben identificarse en el sistema por medio de una cuenta de usuario y una palabra clave. La combinación de estos dos ingredientes permite determinar los derechos de acceso a los programas e información que tiene cada usuario.

  - *Nivel C2:* junto con las características de C1, el nivel C2 incorpora características de seguridad adicionales, las cuales crean un ambiente de acceso controlado y aseguran la capacidad de reforzar las restricciones a los usuarios, no solo considerando los permisos asociados que poseen, sino por medio de niveles de autorización. Por otra parte, este nivel requiere auditoría de sistema, incluyendo la creación de un registro de auditoría para cada evento que ocurre.

- ***Nivel B:*** está conformado por tres subniveles:

  - *Nivel B1:* protección de seguridad etiquetada: este nivel parte del principio de que un objeto bajo control de acceso obligatorio, no puede aceptar cambios en los permisos hechos por el dueño del archivo.

  - *Nivel B2:* protección estructurada: requiere que se etiquete cada objeto. Los dispositivos como discos duros, cintas o terminales podrán tener asignado un nivel sencillo o múltiple de seguridad. Este es el primer nivel que empieza a referirse al problema de un objeto a un nivel más elevado de seguridad en comunicación con otro objeto a un nivel inferior.

- *Nivel B3:* nivel de dominios de seguridad: refuerza los dominios con la instalación de hardware. Este nivel requiere que la terminal del usuario se conecte al sistema por medio de una ruta de acceso segura.

- ***Nivel A:*** o nivel de diseño verificado es el nivel más elevado de seguridad considerado por el Departamento de Defensa de los Estados Unidos. Incorpora un exhaustivo proceso de diseño de control y verificación. Este nivel se alcanza cuando se incluye a todos los componentes de los niveles inferiores; además, el modelo debe ser verificado matemáticamente y es necesario realizar un análisis de los canales encubiertos, y que el hardware y software han sido protegidos para evitar violaciones a los sistemas de seguridad.

2.7 Mecanismos de Seguridad

El mercado actual ofrece muchos mecanismos, técnicas y herramientas para brindar una mayor seguridad a los datos que son transmitidos por medio de la red. Entre los que se pueden encontrar están:

- ***SSL(Secure Socket Layer):*** se utiliza en relaciones empresa-cliente. Proporciona un canal seguro entre clientes y servidores de Internet. Este protocolo se invoca de manera automática.

- ***Criptografía:*** mantiene la seguridad de la ola de información mediante la aplicación de algoritmos o funciones matemáticas. Su operación es independiente del medio de almacenamiento o la protección de seguridad física. Utiliza elementos de cifrado , llave y descifrado.

- ***Certificados y firmas digitales:*** el certificado es una credencial emitida por una autoridad certificadora que valida que el usuario o emisor es quien dice ser. Los certificados pueden representar a un individuo, empresa u organización. Por su parte

la firma digital es la encriptación de un texto plano en una secuencia de caracteres ilegibles.

- ***Protección perimetral:*** localizado entre la red interna (privada) e Internet (pública). Defiende de usuarios maliciosos o redes poco confiables, aísla la red interna, divide redes internas corporativas, entre otros. Uno de los diversos tipos de protección perimetral son los muros de fuego que pueden bloquear tráfico no deseado, direccionar tráfico interno a sistemas más seguros, ocultar vulnerabilidades de los sistemas internos, registrar el tráfico desde y hacia la Intranet, ocultar información, proveer robusta autenticación, entre otros. También se encuentran los sistemas de detección y prevención de intrusos; análisis de vulnerabilidades, entre otros.

- ***Redes privadas virtuales (VPN):*** es básicamente un medio de comunicación para proteger la información enviada a través de una red.

- ***Protección antivirus:*** escaneo y revisión de virus, software malicioso o programas que afecten la seguridad de la información. Es importante recalcar que los virus son un problema de seguridad y no de disponibilidad o afectación de archivos.

- ***Monitoreo del tráfico:*** es el monitoreo y registro de eventos de seguridad en la red, establecimiento de políticas y procedimientos para escalar incidentes.

- ***Políticas y procedimientos de la organización:*** las políticas y procedimientos son los requisitos mínimos definidos por la organización para la administración y uso adecuado de los recursos tecnológicos.

2.8 Métodos de ataque

A pesar de que en cuanto a la seguridad de computadoras, las empresas deberían mantenerse al día, esta tarea es una de las más frustrantes, ya que es difícil encontrar profesionales en informática con amplio conocimiento en el área de seguridad, sobre todo,

con una noción extensa de cómo contrarrestar todas las técnicas utilizadas para entrar forzadamente en las máquinas.

Debido a lo anterior, es importante que para la contratación de un profesional informático en seguridad, se tome en cuenta la premisa que dice que "la práctica hace al maestro", y considerar dentro de los criterios de evaluación, aquella persona con mayor experiencia y conocimientos teóricos y prácticos de los métodos de ataques a los que se puede enfrentar la organización.

Cuando una persona ha atendido un ataque en un ambiente informático, a menudo esta experiencia le permite identificar problemas similares en sistemas con los que se está familiarizado. Muchos de los ataques que ocurren, por lo general guían hacia otros descubrimientos que mejoran la seguridad general de los sistemas.

En la actualidad se puede encontrar una serie de métodos de ataque, entre algunos de los más conocidos están:

- ***Ataques basados en la palabra clave:*** se lleva a cabo adivinando la combinación del código de usuario y la palabra clave de una forma lógica; utilizando la "fuerza bruta" mediante la mezcla de una gran cantidad de palabras posibles para obtener ingreso a los sistemas o por medio de pequeños programas que se pueden bajar de Internet y que realizan una serie de combinaciones lógicas internas hasta descifrar la clave. Este tipo de ataque requiere de una cantidad considerable de tiempo y esfuerzo por parte del intruso, por lo que muchos han cambiado los ataques de "fuerza bruta" por otros más efectivos, como lo son la ingeniería social y el "sniffing".

- ***Ingeniería social:*** están basados en los actos cotidianos de las empresas, sobre todo en los aspectos que por su rutina pasan por alto mecanismos de autenticación personal. Generalmente, este método involucra al "hacker" de un extremo de una línea telefónica y al usuario ingenuo al otro lado. Un ejemplo de este tipo de ataque

es el siguiente, en donde el intruso se va a hacer pasar como el administrador del sistema y llama a un usuario X:

Intruso: *Hola, mi nombre es Mario, soy el administrador del sistema. Alguien de su oficina me llamó para que le arreglara el problema que tienen ustedes con el comando "/s".*

Usuario X: *Ok. Dígame, ¿qué tengo que hacer?*

Intruso: *Solo permítame su código de usuario y la palabra clave para arreglarlo desde aquí, espere unos minutos antes de usar el sistema.*

Usuario X: *El código es **XXXXX** y el password es **12345**. Muchas gracias.*

- ***"IP Spoofing":*** involucra la entrega de información falsa acerca de una persona o la identidad de un host para obtener acceso no autorizado a los sistemas o a los servicios que estos proveen. Esto se logra cuando un host le permite a otros comunicarse a través de relaciones de confianza sin requerir autenticación, utilizando los archivos "rhost" en el directorio raíz de los sistemas UNIX, en el cual se almacenan los nombres de los equipos a través de los cuales los usuarios pueden tener acceso, sin necesidad de ingresar un código de usuario, a través del comando "rlogin" u otro similar con los argumentos apropiados. El primer paso de un ataque spoofing es identificar dos máquinas objetivo, las cuales serán llamadas X y Y. Una vez que los "host" han sido identificados, el intruso va a establecer una conexión con el equipo Z, de tal manera que Y crea que ésta ha sido hecha por X, cuando en realidad se inició desde la máquina del atacante (llamada Z). Esta conexión es acompañada de un mensaje falso, el cual contiene la dirección IP de X solicitando la conexión con Y. Una vez recibido este mensaje, Y va a responder con un mensaje similar reconociendo la solicitud y estableciendo un número de secuencia con el cual X debe verificar la autenticidad. Mientras sucede lo anterior, Z está enviando una gran cantidad de paquetes al equipo X para sobrecargar su capacidad de respuesta y evitar que responda al mensaje enviado por Y. Cuando X está

sobrecargado, Z utiliza una serie de herramientas para adivinar el número de secuencia que debe responder a Y, y así establecer la comunicación. Cuando esta comunicación se establece, Y cree que está comunicado con X. Sin embargo, Z ha recibido un acceso no autorizado al equipo Y.

- ***Robo de sesión (sesión "hijacking"):*** en este método un intruso busca conexiones entre dos equipos para intentar hacerse pasar por uno de ellos. Una vez que ha obtenido el control de un equipo a través del cual se ejecuta esta conexión, monitorea la forma en que procede la conexión, de esta manera es capaz de determinar los números de secuencia usados por ambas partes, sin realizar el complicado proceso descrito para el método de ataque "spoofing". Como resultado de lo anterior, el usuario es literalmente botado de la conexión y el intruso puede continuar como si fuera el usuario original.

- ***Olfateo de paquetes ("sniffing") o husmeo en la red ("snooping"):*** el "snooping" también conocido como "sniffing", consiste en interceptar los paquetes que viajan en cualquier parte entre un punto de origen y un punto de destino. La manera de actuar es instalando un dispositivo llamado "sniffer" en cualquier sitio a lo largo de la ruta de conexión entre dos equipos. La información que los intrusos gustan de examinar son los "host", los nombres de usuario y las claves de acceso, los cuales son los más utilizados para atacar a las compañías. Además, por medio de este método, es fácil obtener de manera ilegal, los datos y los mensajes electrónicos que viajan a través de las redes de las corporaciones.

- ***Ataques que explotan las vulnerabilidades de la tecnología:*** esto se refiere a las brechas de seguridad que presentan los sistemas. La solución para combatir esta debilidad es creando e instalando parches que solucionen estas vulnerabilidades; sin embargo, por cada vulnerabilidad que es corregida aparecen nuevas debilidades lo que implica que en cualquier momento un intruso podrían aprovecharse de una debilidad del sistema, que aún no es ampliamente conocida e ingresar a los sistemas de la compañía de manera no autorizada.

2.9 Correo electrónico

El ser humano por su naturaleza social y capacidad de razonamiento ha ido en la búsqueda de nuevas formas para comunicarse y expresar sus pensamientos. Las formas más primitivas de comunicación requerían que tanto el emisor como el receptor estuvieran físicamente uno frente al otro para establecer la comunicación. Con el nacimiento de la escritura, esto cambió radicalmente, ya que no era necesario la presencia física de ambas partes, sino que lo requerido fue el transporte físico del mensaje, principalmente papel. De esta forma nació el primer concepto de portador de un mensaje. A raíz de esta nueva forma de comunicación, también se idearon nuevas maneras de enviar o transmitir los mensajes, utilizando personas que recorrían grandes extensiones e incluso intermediarios que transmitían de boca en boca el contenido del mensaje, hasta que este llegara a su destinatario.

Este primer intento de un sistema de correo se acerca bastante al que funciona actualmente a nivel mundial. Un poco más refinado, con jerarquías de distribución, legislación que lo regula y protege, pero el concepto fundamental es el mismo, el transporte físico de un mensaje. El problema con este sistema es que hace uso de medios de transporte que por lo general son caros y lentos.

Posteriormente, Samuel Morse luego de una profunda investigación sobre las propiedades de la transmisión de la corriente eléctrica a través de un cable, finalizó con la invención del telégrafo, el cual, luego con la inclusión de la radio trasmisión, logró desarrollar un medio de transporte rápido y relativamente barato.

Casi 40 años después, Graham Bell inventó el teléfono. Este sistema tiene una escala global y conecta una inmensa jerarquía de conmutadores, multiplexores y conversores de señales que permiten una comunicación a cualquier lugar del mundo, siendo perfecto para la transmisión de voz de un extremo a otro. Paralelamente a la red telefónica, se construyó el telex, como la manera más rápida de tener información bursátil actualizada. Una máquina

telex podía comunicarse con cualquier otra máquina por medio de una línea telex, la cual proporcionaba una relativa seguridad, ya que para establecer una comunicación se hacía por medio de una especie de protocolo. A medida que pasaron los años la información fue ganando mayor importancia en la vida empresarial y en los sesentas, las grandes compañías comenzaron a instalar computadoras y a conectar terminales "bobas" a ellas, teniendo así acceso a su información y a sus otros recursos, memoria, procesador, dispositivos de entrada y salida(E/S), entre otros.

A su vez, y paralelamente con la expansión de las redes de computadoras en la industria y el comercio, el Departamento de Defensa de los EE.UU. comenzó su incursión en este mundo y con la ayuda de Universidades y de estudiantes puso en marcha la Arpanet, la predecesora en cierta manera de la Internet. En este contexto, se tiene como registro de la primera transmisión de un e-mail el año 1971.

Con la llegada de las computadoras personales, la idea de red cambió radicalmente. Hoy no hablamos más de procesamiento centralizado, en su lugar tenemos procesamiento distribuido. Cada día más empresas instalan redes de área local (LAN), redes de área metropolitana (MAN) y redes de área extensa (WAN), y con la posibilidad de conectar este tipo de redes surge inevitablemente una gran red mundial, la Internet.

Con la aparición de la Internet nace en los profesionales de la informática la idea de liberar al mundo de las fronteras físicas, crear un espacio donde el tiempo es un concepto muy flexible, introducir las ideas de tiempo y distancia cero, entre otros; y aunque todavía estamos lejos de la implementación de semejante empresa seguimos en la búsqueda, y el correo electrónico es una de las herramientas que nos llevará a conseguir tan anhelado sueño.

Hoy en día, el correo electrónico es una herramienta de suma importancia en el entorno empresarial a nivel mundial. La finalidad del correo electrónico es el intercambio de ideas, opiniones, comentarios, documentos de trabajo de baja, mediana y/o alta importancia, confidencialidad y riesgo; documentos de estudio y de entretenimiento; entre otros, con

personas de diversos puntos de la empresa, provincia, país e incluso del mundo a través de redes LAN, WAN, MAN y su combinación.

El proceso de envío de un mensaje por medio del correo electrónico consiste en un usuario origen escribe el mensaje en un programa de aplicación llamado cliente de correo, el cual a la vez está enlazado al servidor de correo electrónico a través de este mismo programa de aplicación. Por lo general, el servidor de correo consiste en un editor de texto, con corrector ortográfico, una base de datos en forma de una libreta de direcciones, un administrador de archivos (mensajes recibidos o no enviados) y un módulo de comunicaciones para poder transferirlos. El mensaje creado por el usuario origen después de seleccionar el nombre del usuario destinatario envía el correo, el cual queda almacenado en el servidor de correo hasta que el usuario destinatario utilizando su aplicación de cliente de correo se conecte con el servidor y solicite los mensajes reservados para él (usuario destinatario).

2.10 Tipos de Ataques

El correo electrónico constantemente está expuesto a una serie de ataques provocados por personas sin escrúpulos.

Algunos de estos ataques son:

- ***Terrorismo:*** envío de correos electrónicos con contenido ilegal por naturaleza, es decir, todo aquel que constituya complicidad con hechos delictivos, ejemplo: programas piratas, amenazas de terrorismo, pornografía, estafas, virus, y otros.

- ***Envío de mensajes a través del correo electrónico de otra persona sin previa autorización:*** esto significa el uso de la cuenta de correo de una persona sin su consentimiento para el envío de mensajes. Esta abuso aplica, aun y cuando el contenido del mensaje sea válido, es decir, no contenga información terrorista u otro tipo.

- ***Envío de correos masivos con información no solicitada:*** estos correos suelen ser los enviados de forma masiva a distintas direcciones de correo electrónico con información de publicidad o cualquier otro tipo de información no solicitada por el destinatario.

- ***Ataques con el objeto de dificultar o negar el servicio:*** dirigido tanto al usuario del correo electrónico como para el propio servidor de correo. Este ataque consiste en el envío de un alto número de mensajes por segundo o cualquier variante que tenga el objetivo de paralizar el servicio por saturación de los canales a través de los cuales se envían los mensajes, la capacidad de CPU del servidor de correo o del espacio en disco del servidor o de la computadora del usuario.

- ***Olfateo o husmeo de los paquetes:*** consiste en interceptar los paquetes o tramas que componen un correo y capturar, borrar o modificar la información contenida con el fin de provocar un daño a la integridad de la información, o para obtener información confidencial para ser utilizada en beneficio propio (del atacante) o para beneficio de otros (vendiendo el contenido del mensaje).

Entre las ventajas que ofrece el correo electrónico se encuentra que es un excelente medio de comunicación, ya que permite el intercambio de ideas, opiniones, comentarios, documentos de trabajo de baja, mediana y/o alta importancia, confidencialidad y riesgo, entre otros, con personas de diversos puntos de la empresa, provincia, país e incluso del mundo a través de redes LAN, WAN, MAN y su combinación; es fácil de usar, ágil, eficaz, con grandes cantidades de almacenamiento que pueden ser controladas, entre muchas otras.

Como parte de las desventajas, algunas de ellas son: exposición a los distintos tipos de ataques, pérdida de la integridad de la información, pérdida completa de la información, pérdidas financieras para la empresa, pérdidas sociales, como son de imagen y credibilidad de la persona, de la empresa, negación del servicio, entre los más comunes.

Todavía existen muchas instituciones a nivel nacional que no tienen conciencia o cultura de seguridad, principalmente de las debilidades que existen alrededor de los mensajes que son enviados por correo electrónico y lo sensible o clasificada que es la información que remiten por este mismo medio.

El delito informático parece ser un "buen negocio". Es un objeto pequeño en el que la información está almacenada en "contenedores pequeños" (no es necesario un camión para robar el banco, joyas, dinero); el contacto físico no existe en la mayoría de los casos y es posible asegurar el anonimato y la integridad física del delincuente; el objeto codiciado (la información) tiene un alto valor, ya que el contenido (los datos) vale mucho más que el soporte que los almacena (disquete, disco compacto, entre otros). La mejor solución para la protección de los datos es el uso de técnicas criptográficas.

2.11 Concepto de Criptografía

Según Manuel Aceves y Arthur Andersen, Firmas Digitales y PKIs (2000), la criptografía se define como el "arte de escribir mensajes secretos. Es el estudio sistemático de técnicas y métodos que permiten transformar la información en aparente ininteligibilidad, de una manera reversible y secreta" (sesión 312). Esta técnica mantiene la seguridad de la información mediante la aplicación de algoritmos o funciones matemáticas. Su operación es independiente del medio de almacenamiento o la protección de seguridad física.

En la actualidad, más y más datos están siendo almacenados y comunicados en forma automática. Esta característica hace que los datos sean más fáciles y rápidos de utilizar. Sin embargo, ello además significa que las técnicas físicas de seguridad, principalmente para el envío de información a través del correo electrónico, sean capaces de proveer una seguridad efectiva a los datos almacenados y enviado de forma digital. La criptografía ofrece una alternativa para proveer de seguridad a los datos manejados digitalmente.

Los esquemas de seguridad propician la confidencialidad de los datos por medio de la transformación de la información de manera legible a ilegible. Así, los esquemas de

seguridad son más versátiles que los tradicionales mecanismos de seguridad, ya que la operación es independiente del medio por el cual es almacenada la información, independientemente de la protección física con que cuente el equipo que guarda los datos.

La criptografía asegura la seguridad de los datos almacenados en forma digital. Los esquemas de firmas digitales son ejemplos de esquemas criptográficos.

Los sistemas criptográficos se componen de algoritmos y llaves (públicas y privadas). Un algoritmo es una conversión matemática que se realiza a los datos, tanto para encriptarlos como para desencriptarlos. Los tipos de algoritmos o criptosistemas que existen son: llave o clave secreta (también conocida como sistema simétrico o criptosistema simétrico); llave o clave pública (conocida como sistema asimétrico o criptosistema asimétrico); y cifrado con criptosistemas de clave secreta.

Los algoritmos simétricos (llave secreta) son operaciones de cifrado y descifrado que utilizan una misma llave, es decir, con la misma clave se cifra y se descifra el texto, por lo que la seguridad reside en mantener dicha clave en secreto. Los sistemas de clave secreta son muy rápidos pero no tienen firma digital. Este sistema da al usuario integridad pero no confidencialidad.

Los algoritmos asimétricos (llave pública) son aquellos que utilizan llaves distintas, pero matemáticamente relacionadas para el cifrado y descifrado por medio de las llaves privadas y públicas. En otras palabras, cada usuario crea un par de claves, una privada y otra pública, inversas dentro de un cuerpo finito. Lo que se cifra en emisión con una clave (privada), se descifra en recepción con la clave inversa (pública). La seguridad del sistema reside en la dificultad computacional de descubrir la clave privada a partir de la pública. Para ello usan funciones matemáticas de un solo sentido con trampa. Los sistemas de clave pública son muy lentos, pero tienen firma digital. Este sistema da confidencialidad pero no integridad.

Por su parte, los criptosistemas de clave secreta son una combinación de ambos esquemas, sistema simétrico y sistema asimétrico que brinda ambas ventajas, confidencialidad e

integridad, las cuales se logran si se protegen las claves en el cifrado y en el descifrado; es decir, se obtienen simultáneamente si se protege la clave secreta.

La llave es un valor secreto que permite encriptar un mensaje de una manera distintiva. La administración de las llaves debe ser muy cuidadosa y segura, ya que de ello dependerá la integridad y confiabilidad de los datos, por lo que no deberán ser divulgadas. Deberán ser secretas, difíciles de adivinar, instaladas en los dispositivos receptores de manera confiable y todas las entidades (personas/dispositivos) autorizadas para intercambiar datos deben contar con una llave.

2.12 Firmas Digitales

La impresión de una firma en un pagaré, talonario, contrato, cheque u otro documento de similar relevancia, permite establecer un compromiso entre dos partes; a través de este documento, una de las partes puede reclamar derechos sobre el activo que está de por medio y respaldado por una firma. Este concepto de certificación por medio de una firma, envuelve el concepto de firmas digitales, como autenticación del proceso utilizado para confirmar la identidad de una persona, prueba de que la persona que firmó se responsabiliza de los hechos, para proveer integridad de una información en específico, y otros. Por lo tanto, y tal como lo menciona PriceWaterHouseCoopers, Internet Actual (2000), firma digital son “datos expresados en formato digital, utilizadas como método de identificación de un firmante y de verificación de la integridad del contenido de un documento digital, que cumpla con los siguientes requisitos: pertenecer únicamente a su titular; encontrarse bajo su absoluto y exclusivo control; ser susceptible de verificación; y estar vinculada a los datos del documentos digitales de modo tal que cualquier modificación de los mismos ponga en evidencia su alteración.” (sesión 232), es decir, es una transformación o cifrado que hace el emisor de un mensaje utilizando un sistema simétrico o asimétrico (llave privada) al receptor que descifrará el mensaje por medio del mismo sistema a través de una clave o llave pública que el firmante con anterioridad le ha enviado al receptor para que pueda leer el mensaje.

Amador Rodríguez (1985) define firma digital como "aquel procedimiento de seguridad que permite al autor de un mensaje representado en forma digital binaria, firmarlo con las mismas propiedades que tiene la firma de un documento escrito sobre papel, a la manera convencional" (p. 205). Como Amador lo menciona en su definición anterior, la idea de la firma digital es que solamente una persona pueda producirla, y cualquiera pueda reconocerla, del mismo modo que ocurre en la práctica comercial corriente; por ejemplo, la inclusión en el mercado laboral de aplicaciones como el correo electrónico, que tratan de reemplazar al documento soportado en papel, obliguen a buscar métodos de firma de mensajes electrónicos.

Precisamente de la técnica de criptografía nace el concepto de firmas digitales como mecanismo para garantizar que los datos o el mensaje recibido proviene realmente de la persona que lo firma, en especial si se trata de contratos electrónicos, que este sea firmado de alguna manera, que la firma digital genere la misma obligatoriedad que su homóloga autógrafa; la imposibilidad de ser negada por su autor, por supuesto evitar que sea alterada en su camino del emisor al receptor, entre muchos otros detalles. La firma digital se constituye como el mecanismo más nuevo provisto por la tecnología criptográfica contemporánea. El valor de la firma digital es el testimonio de que el mensaje firmado pudo haber provenido únicamente de la persona que mantiene la llave privada.

Como ya se mencionó anteriormente, los esquemas de firmas digitales son derivados de los esquemas de criptográficos. Los esquemas de firmas digitales fueron propuestos en 1976 por Whitfield Diffie y Martín Hellman, estos además introdujeron los conceptos relacionados con la encriptación por medio de llaves públicas. Las firmas digitales son diseñadas para proveer autenticación en los datos originales, integridad de los datos y la no repudiación. Los esquemas de firmas digitales son conocidos como mecanismos de firmas digitales.

El principio básico de un esquema de firma digital, como se mencionó anteriormente, es que un usuario tiene una llave secreta y otra pública. El valor de estas llaves será generado por el usuario dueño de la clave. La llave secreta será utilizada por el emisor para encriptar

el texto. La llave pública es la que el dueño de la llave privada (emisor) entregará a todas las personas (receptores) con las que necesita comunicarse. El receptor utilizará la llave pública para desencriptar el texto y confirmar que el mensaje fue enviado por el emisor dueño de la llave privada.

La especificación técnica de un esquema de firma digital, involucra la descripción de tres procedimientos computacionales, matemáticos o algoritmos:

- ***Procedimientos para la generación de la llave:*** permiten generar las llaves que serán utilizadas por el procedimiento de firmado y por el procedimiento de verificación. Cada vez que es utilizada, el procedimiento genera un par de llaves que consisten en la llave de firmado y la correspondiente llave de verificación. Es importante mencionar que el procedimiento para la generación de la llave utiliza un generador de números aleatorios y un par diferente cada vez que es utilizado. Para las aplicaciones, la llave de firmado se debe mantener en secreto, por eso se le conoce con el nombre de llave secreta. Similarmente, en la mayoría de las aplicaciones, la llave de verificación es distribuida a todos los destinatarios con quienes el dueño de la llave secreta desee compartir para que verifique la procedencia del correo, por eso es conocida como llave pública.

- ***Procedimiento de firmado:*** transforma los datos para producir una firma. Cada vez que es utilizada, el procedimiento toma como entrada la generación de la llave de firmado utilizando el procedimiento de la generación de la llave y los datos desde algún espacio de datos predeterminado. El procedimiento de firmado externo o de salida es una firma. Si el procedimiento de firmado de un esquema de firma digital es probabilístico, significa que cada mensaje puede tener una variedad de firmas válidas, lo que luego se llamará esquema de firmado probabilístico. Si el procedimiento de un esquema de firma digital es determinístico, significa que cada mensaje tiene solamente una firma válida, a la que se le conoce como esquema de firmado determinístico.

- ***Procedimiento de verificación:*** los usuarios que reciban mensajes firmados necesitan estar habilitados para comprobar que la firma adjunta al mensaje es correcta. El procedimiento de verificación se encarga de tomar el mensaje de entrada recibido y la firma junto con la llave pública perteneciente al origen, son verificadas. Si estas coinciden el mensaje es aceptado como válido.

2.13 Propiedades de un mecanismo de firma

Todo mecanismo de firmado debe cumplir con al menos tres requerimientos para asegurar la efectividad de los servicios de seguridad.

El primero y más obvio requerimiento es que los tres procedimientos anteriormente descritos deben involucrar en cada uno de sus procesos de eficiencia.

El segundo requerimiento es que el esquema de seguridad esté bien definido. Un esquema de firmado bien definido es uno en el cual la verificación de la transformación de la firma digital es verificada y aceptada como válida si concuerda.

El requerimiento final es que el mecanismo de protección sea seguro.

2.14 Características de una Firma Digital

Entre los aspectos de aseguramiento o servicios que ofrecen las firmas digitales encontramos los siguientes:

- ***Confidencialidad:*** es la habilidad de enviar información entre participantes de una manera que previene que otros puedan leerla.

- ***Autenticación:*** verificar la identidad de alguien o algo.

- ***Integridad de datos:*** asegurar al receptor de un mensaje que éste no ha sido alterado desde que fue generado por una fuente legítima, proveyendo credenciales de difícil falsificación.

- ***No repudiación:*** negar el origen, retención, envío o integridad del contenido de un documento.

Además, para que las firmas digitales tengan mayor validez y legalidad, se recomienda que estén respaldadas a través de una autoridad certificadora, la cual se encarga de emitir, a quien lo solicite, un certificado rotulado con una firma digital que otorga fe de que las atribuciones de claves de firmas digitales son originales. Según la empresa PriceWaterHouseCoopers, Internet Actual (2000), los certificados digitales se encuentran amparados a leyes que en caso de ser incumplidos, pueden generar:

- Responsabilidad civil o comercial por incumplimiento de contratos, daños y perjuicios, mora en la entrega o pago, entre otros.

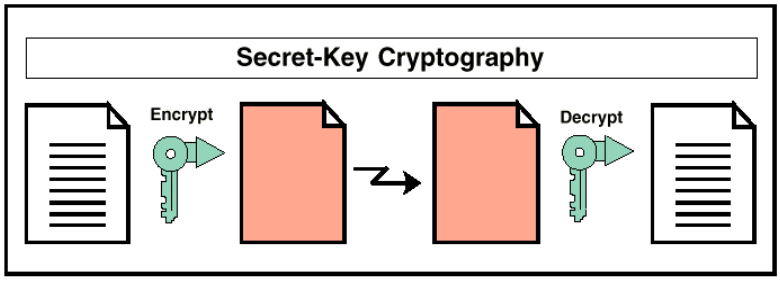
- Responsabilidad administrativa tanto al incumplimiento de normativa como a posibles sanciones que puedan ser aplicadas.

- Responsabilidad penal por fraude, daño, apología del crimen, calumnias e injurias, propiedad intelectual, y otros.

2.15 Tipos de Mecanismos de Firmas Digitales

En la actualidad, se puede encontrar dos tipos de mecanismos o sistemas de cifrado utilizados en los diferentes programas de firmas digitales que ofrece el mercado al público en general; estos son los mecanismos o sistemas simétricos, y mecanismos o sistemas asimétricos.

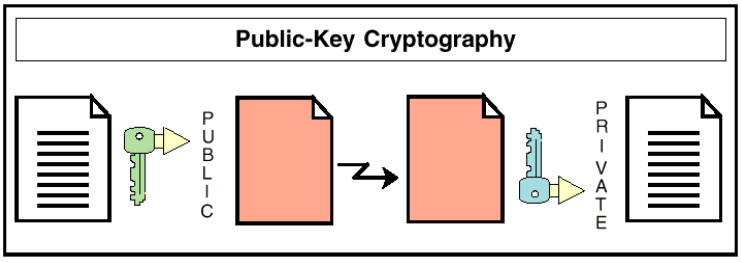
La clave que utilizan los sistemas simétricos para descifrar es la misma que la de cifrar (o es una variación directa de ella).



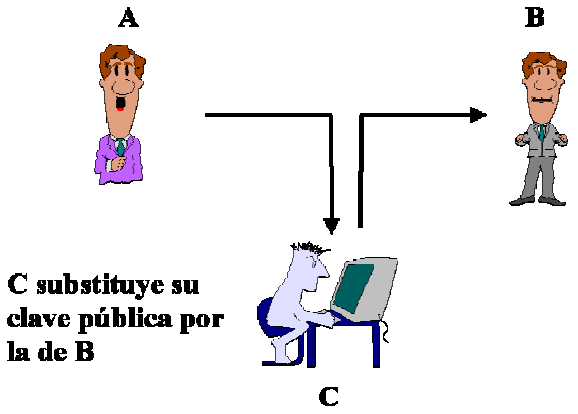
De esta forma, si se quiere encriptar un mensaje, se debe poseer el algoritmo de encriptación (programa) y la clave personal, y esa clave personal debe distribuirla a todas aquellas personas a las que se pretende enviar mensajes encriptados, ya que ellos deben utilizarla para desencriptar la información cifrada.

Este mecanismo de encriptación tiene el problema de que ambas partes deben ponerse de acuerdo en la clave, razón por la cual, se hace inseguro el envío de la clave, ya que de cualquier forma que ésta se envíe, es posible que alguien la intercepte, ya sea instalando micrófonos (si es una comunicación oral), o capturando el envío electrónicamente. En definitiva, si algún indeseable consigue la clave, podrá leer todos los mensajes, lo que se considera un gran agujero en la seguridad.

Debido a la anterior debilidad, aparecieron los sistemas asimétricos. En estos sistemas, cada usuario dispone de dos claves, una privada y otra pública, de tal forma que lo que una cifra la otra descifra y viceversa. Lo importante en este proceso es que la clave privada sólo la conoce el usuario propietario de ella, y es la pública la que distribuye para que el resto del mundo la utilice para enviarnos mensajes, si alguien capta el mensaje no podrá descifrarlo ya que sólo se descifra con la clave privada y está en nuestra posesión. De esta forma la clave pública se utiliza para encriptar y la privada para desencriptar.



Como se puede observar, este mecanismo soluciona los problemas del sistema simétrico, ya que no es necesario comunicar ninguna clave privada, sólo las claves públicas, por lo que aumenta de manera notoria la seguridad del sistema. Sin embargo, surge un nuevo problema que es el de "Usurpación de Personalidad"; es decir, que alguien que no es realmente a quien se desea enviar el mensaje, se haga pasar por él, entregando su clave pública, y capturando todos los mensajes dirigidos al destinatario original; es más, este intruso podría reenviar el mensaje al destinatario original, haciéndolo creer que no ha pasado nada, lo que provocaría que este individuo no sea descubierto.



Para corregir este problema, surgen las Autoridades de Certificación (CA)[3], las cuales brindan a su empresa o persona física, un certificado digital con el que se puede comprobar la identidad real de la empresa o persona de quien estamos recibiendo el mensaje.

Las mejores prácticas indican que las firmas digitales deben cumplir con al menos los siguientes requisitos:

[3] De las Autoridades Certificadoras y Certificados Digitales, se hablará en el siguiente tema.

- Cumplir con reglas de seguridad del algoritmo utilizado.

- Deben indicar la identidad del titular, el número de serie del certificado, la fecha de expiración del certificado, una copia de la llave pública, firma de la autoridad certificadora, entre otras.

- Utilizar una llave pública lo suficientemente larga es un factor importante que le ayuda al usuario a proteger de una forma más segura la información que luego encriptará, ya que cuanto más larga es la contraseña, más difícil será de descifrar para un intruso.

- Deben estar certificadas por una autoridad certificadora.

2.16 Certificados Digitales

Certificado digital es un paquete encriptado emitido por una autoridad certificadora (CA, en sus siglas en inglés) confiable, que contiene una llave pública que identifica al dueño de la llave, especifica la vigencia del certificado e incluye la firma digital de la autoridad certificadora. El propósito fundamental de un certificado digital es mostrar que una llave pública pertenece en verdad a una persona.

Los certificados digitales, por lo general, constan de las siguientes partes: número de serie del certificado, nombre distinguible de la autoridad certificadora, identificador del algoritmo hash (para la firma de la autoridad certificadora), período de validez del certificado, nombre distinguible del titular de la llave, llave pública del titular y firma digital de la autoridad certificadora.

Las Autoridades de Certificación cumplen con una función notarial en donde verifican la identidad y solvencia de usuarios y entidades proporcionando un certificado digital o "Digital ID". La certificación en redes abiertas utiliza certificados que se basan en permitir:

- Firmar digitalmente los mensajes de tal forma que el receptor pueda descifrarlos y tener acceso a su contenido, garantizando la autenticidad y el no repudio.

- Cifrar la información (encriptación) de tal forma que sólo el receptor pueda descifrarlos y tener acceso a su contenido, garantizando su integridad y confidencialidad.

- Asegurar y autentificar la identidad de acceso de los usuarios de Intranets/Extranets. De forma muy simple, podemos decir que un certificado digital contiene la clave pública de la persona o entidad para la que se emite, junto con información propia, y todo ello firmado electrónicamente por la CA.

Una de las principales autoridades de certificadoras que existen actualmente es "VeriSign" (www.verisign.com), la cual extiende certificados tanto para empresas como para personas, además de ofrecer servicios de seguridad completos, para Intranets, Extranets y Comercio Electrónico.

La autoridad certificadora, entre otros aspectos debe ser una autoridad que goza de la confianza de los usuarios de un sistema de encriptación de llave pública; proveer una declaración (certificado digital) que testifica que la llave pública pertenece a la persona cuyo nombre está indicado; puede ser cualquier autoridad central que avala las identidades de aquellos a los que ha emitido certificados y garantiza que cada identidad esté asociada con una llave específica; una compañía puede emitir certificados a sus empleados o una universidad a sus estudiantes, maestros y empleados; una corporación puede establecerse como una autoridad certificadora pública, verificando las identidades de sus clientes y expidiendo certificados a su favor.

La institución que lo desee puede escoger mantener una certificación interna o contratar un “outsourcing” de este servicio con un tercero, como lo es la empresa Verisign. En un esquema de “outsourcing”, la autoridad certificadora es reemplazada por una autoridad

registradora, la cual se encargará de la inscripción, autenticación y generación de los pares de llaves. La entidad certificadora externa recibirá solicitudes de certificados de la autoridad registradora y expide, distribuye y almacena certificados, y mantiene la lista de revocación de certificados actualizada.

Algunos aspectos de seguridad que se deben considerar son el uso de un sistema establecido de firmas digitales; la implantación efectiva de la firma digital; una estación de trabajo de la autoridad certificadora dedicada y fuera de línea; una distribución segura de la llave pública de la autoridad certificadora y del dueño de la llave; la generación de la llave privada de la autoridad certificadora; una protección de la llave privada de la autoridad certificadora; un respaldo protegido de llaves; y un soporte para la revocación de llaves.

3. METODOLOGÍA DE LA INVESTIGACIÓN

3.1 Métodos de Investigación

Existen diversos métodos para efectuar una investigación, entre los que se encuentran:

- ***Método exploratorio:*** según Roberto Hernández (1991), el método exploratorio se realiza sobre un tema de investigación del que se tiene poco conocimiento, o bien, que en un pasado no ha sido sometido a estudio. Es una técnica que permite adecuarse a fenómenos relativamente desconocidos o entregarse a una investigación más profunda de un tema específico de interés. El método exploratorio es el más apto para recabar la información básica, de desarrollo y análisis para la realización del presente proyecto, ya que facilita de sobremanera la obtención de los datos específicos que se hallan estrechamente ligados con el tema en desarrollo. La recolección de datos se basó en la búsqueda de temas similares al tema de investigación tanto en libros, en revistas tecnológicas, conferencias, Internet, artículos científicos, entre otros; como en la aplicación de cuestionarios a los usuarios directos del correo electrónico, observancia y análisis de los correos leídos por los usuarios.

- ***Método descriptivo:*** para John Best (1992), el método descriptivo ayuda a analizar e interpretar los datos recabados con el fin de la comprensión y probable solución de problemas. El método descriptivo fue de provecho en la presente investigación, debido a que existe una serie de variables unidas al objeto en estudio, para las cuales se planteó como objetivo evaluar e identificar los métodos y necesidades de seguridad en el Banco Centroamericano. Para un mejor resultado, se utilizó un software de análisis de datos, el cual contribuyó a la obtención de las conclusiones y recomendaciones de esta investigación.

- ***Método tecnológico aplicado:*** según Ezequiel Ander Egg (1992), el método tecnológico aplicado está orientado a la realización de investigaciones, cuyas características despiertan el interés en la aplicación, utilización y consecuencias prácticas de los conocimientos Este método resultó necesario para un estudio más profundo de las variables derivadas de los objetivos de la investigación y la esquematización del documento. Por medio del método tecnológico, se logró identificar las fortalezas y debilidades del esquema de seguridad actualmente implantado en el Banco Centroamericano para el uso del correo electrónico, envío y protección de los datos, así como de las ventajas y desventajas de las soluciones que se ofrecerán al final de esta investigación. Es importante mencionar que este método se alimenta de los dos anteriormente citados.

3.2 Fuentes de Información

La información recopilada para esta investigación se obtuvo mediante la recolección de datos primarios (información obtenida de la aplicación de cuestionarios a la muestra total de los sujetos de la investigación y por medio de la observación participativa) y fuentes secundarias (consulta de material bibliográfico, conferencias, charlas o seminarios, sitios de Internet referentes al tema en estudio, y otros).

El material bibliográfico se refiere a todo aquel material impreso que permite la elaboración del marco teórico de la investigación, y la definición de cada uno de los diferentes conceptos tratados en este estudio.

Las conferencias, charlas o seminarios son cursos que se imparten a todas aquellas personas que desean asistir, en los cuales se tratan diversos temas que contribuyen a ampliar el conocimiento de todos los que participan. El lugar de ubicación varía según sea la actividad, ya que esta puede ser congresos que se realizan anualmente, a nivel nacional o internacional, o seminarios que se programan sin período definido.

3.3 Origen de los datos

El origen de los datos fue recolectado por medio de una muestra de la población total. Para extraer la muestra se utilizó la siguiente fórmula estadística:

El origen de los datos fue recolectado por medio de una muestra de la población total. Para extraer la muestra, se utilizó la siguiente fórmula estadística:

Población total: N=89

1) Población Infinita: $N0 = P*G*[Z/e]^2$

Donde:

N0= tamaño de la muestra para la población infinita

P= probabilidad de éxito, P= 50%

G= probabilidad de fracaso, G= 50%

Z= nivel de confianza deseado, Z= 95%

e= error de estimación, e= 5%

$N0= 0.5*0.5*(1,96/0,05)^2$

N0= 0.25 * 1537

N0= 385

2) Población Finita: N= N0 /{[N0+(N-1)]/N}

Donde:

N0= tamaño de la muestra para la población infinita, N0= 385

N= tamaño de la muestra de población finita

N= tamaño de la población, N= 89

N= 385 /{[385+(89-1)] /89}

N= 385/(473/89)

N= 73

El resultado que se obtuvo de la aplicación de la fórmula es el siguiente:

Población total: 89

Muestra: 73

El cuestionario desarrollado para recolectar información fue enviado a toda la población en investigación, debido a que es muy pequeña. Sin embargo, por la probabilidad de respuesta, se aplicó la muestra para obtener el margen de error.

La metodología para seleccionar muestras indica que debe definirse el tamaño de la población, nivel de confianza, la precisión y la tasa de error esperados:

- ***Tamaño de la población:*** consiste en el número total de elementos del que se obtendrá la muestra.

- ***Nivel de confianza:*** es la probabilidad de que el valor obtenido por una muestra no difiera del valor verdadero del universo en una cantidad establecida, conocida como precisión. Generalmente el nivel de confianza se expresa como porcentaje, de forma que por ejemplo, un nivel de confianza de 95% significa que hay 95 oportunidades de cada 100 de que la muestra sea representativa.

- ***Precisión:*** es la cantidad o porcentaje que el investigador acepta que se desvíe el valor obtenido en su examen, del verdadero promedio del universo. En otras palabras, es la amplitud con que se realiza una estimación. Esa amplitud puede ser expresada con más o menos un porcentaje dado, dentro del cual se encuentra el verdadero valor de las características de la población en estudio, con un nivel de confianza dado. De esta manera, si con base en su prueba el investigador afirma que la tasa de error proyectada en una población dada es 5%, ± 2%, ello significa que la tasa de error puede ser tan pequeña como 3% o tan grande como 7%.

- ***Tasa de error esperada:*** es el porcentaje de error que el investigador cree que encontrará como resultado de una prueba. Para estimar la tasa de error el investigador podrá guiarse por los resultados de una auditoría anterior, por una conversación con los administradores, por un estudio preliminar, o por una pequeña prueba piloto.

3.4 Sujetos

La población total está conformada por todos los directores, gerentes locales y regionales del Banco Centroamericano.

Los datos provienen de una muestra de 73 personas seleccionada de una población total de 89 individuos. Para efectos de este trabajo fue necesario obtener una muestra con el fin de cumplir con la confiabilidad de la información recopilada, ya que los sujetos de la investigación son personas con puestos gerenciales que tienen su tiempo muy comprometido.

3.5 Instrumentos

Dentro de los diferentes instrumentos que existen para recopilar información durante una investigación, se encuentran las siguientes:

- ***Observación:*** según James A. Senn (1993), la observación permite tener una relación más estrecha a través de los sentidos, donde se observan los elementos investigados por medio de un proceso planificado sistemáticamente y con una serie de fases previstas. Existen diversos tipos de observación entre los que se pueden citar, la observación estructurada que es controlada, y que cuenta con una serie de instrumentos de recolección, y la no estructurada que es simple y no planificada. Para efectos de esta investigación se utilizó la observación no estructurada, con el fin de obtener una visión amplia de la utilización del correo electrónico entre los individuos de la investigación. Este método fue utilizado con el objetivo de determinar el uso y la importancia que le dan los usuarios al correo electrónico como medio de transferencia de información. Este aspecto se midió por medio del porcentaje de lectura y respuesta del cuestionario remitido a cada uno de los individuos de la muestra.

- **Cuestionario:** para Julie y Kenneth Kendall (1997), el cuestionario se halla conformado por una serie de preguntas que se dirigen a uno o varios encuestados. Dichas preguntas deben ser claras, bien estructuradas, con extensión y temática limitada, y que representen una clara validez. Esta técnica se empleó en la investigación, con el fin de determinar la utilidad que le dan los sujetos en estudio al correo electrónico (p. 107-147); además, de que era la forma más práctica de recolectar los datos, tomando en cuenta las características de los individuos que conforman la población total, es decir, los funcionarios de la alta gerencia.

Un instrumento debe ser tanto confiable como válido para proveer seguridad en el estudio de un proyecto específico. Para Jaime Arellano (1990), la confiabilidad de un instrumento se mide en relación con su capacidad de entregar datos certeros, en tanto que la validez se refiere a la facultad de medir con eficiencia y efectividad lo que se quiere evaluar a través de la confiabilidad.

De lo anterior, se desprende que para que exista validez, el instrumento debe ser confiable. No obstante, la confiabilidad de un instrumento no es necesariamente ratificación de su validez.

En lo que respecta a la validez, Jaime Arellano menciona tres tipos:

- ***Validez de contenido:*** a través de un análisis de los ítemes se analiza el contenido de los datos obtenidos por medio del estudio del instrumento, y confronta estos resultados, con la variable que se desea medir.

- ***Validez empírica:*** se deben poner a prueba los sujetos resultantes del estudio del instrumento, comparándolos con los otros sujetos de otra medición acerca de la misma variable u otra similar.

- ***Validez por hipótesis:*** busca confrontar los resultados obtenidos de los sujetos con los de las hipótesis planteadas sobre los mismos sujetos. Si los resultados obtenidos de esta comparación concuerdan, se puede decir que el instrumento es válido.

Con el fin de dar validez a los instrumentos utilizados en esta investigación, en el caso de la entrevista se definieron los objetivos previos para dar una estructura más sólida a las preguntas.

3.6 Análisis de Resultados

Por medio de la aplicación de un cuestionario fue posible recopilar la información primaria para el desarrollo de la presente investigación.

Este cuestionario se aplicó por medio del correo electrónico, y fue enviado a un total de 89 personas quienes conforman la gerencia del Banco Centroamericano, debido a la limitación de tiempo con la que cuentan los sujetos de la investigación. Por lo anterior, fue necesario aplicar la técnica de muestreo, por lo que al final, se muestreó 85 usuarios en total, quienes fueron los que contestaron el cuestionario.

De las 85 personas que contestaron el correo, 77 son usuarios administrativos y 8 son usuarios de tecnología.

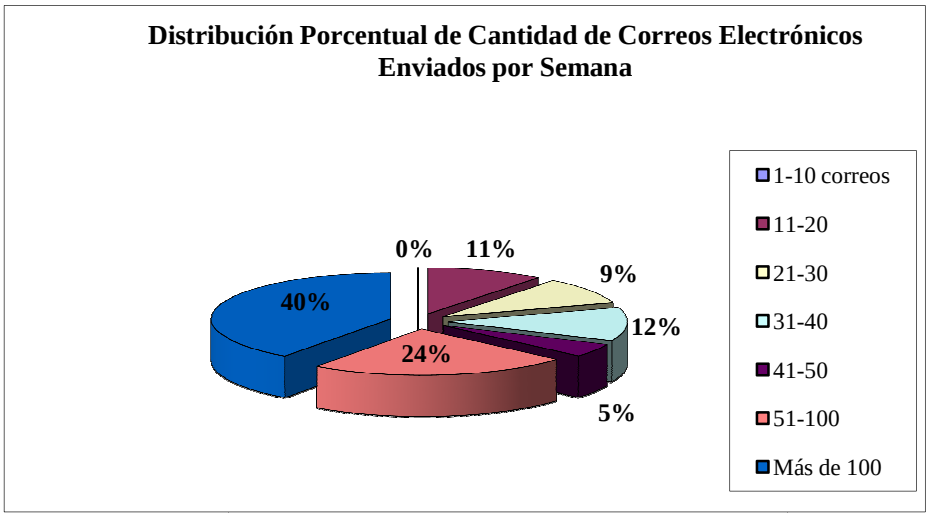
A continuación, se detalla los resultados del análisis de las respuestas de los sujetos de la investigación.

La totalidad de los usuarios consultados poseen cuenta y clave de acceso para ingresar a la red interna del Banco Centroamericano, así como una cuenta de correo electrónico.

De los 85 sujetos encuestados, el 40% envía más de 100 correos por semana; el 24% por lo general envía de 51 a 100 correos por semana. En menor cantidad, el 12% de los usuarios

envía de 31 a 40 correos semanales; 11% de 11 a 20 correos y solamente un 5% envía de 41 a 50 correos por semana. Estos datos se grafican en la siguiente imagen:

Gráfico N° 1

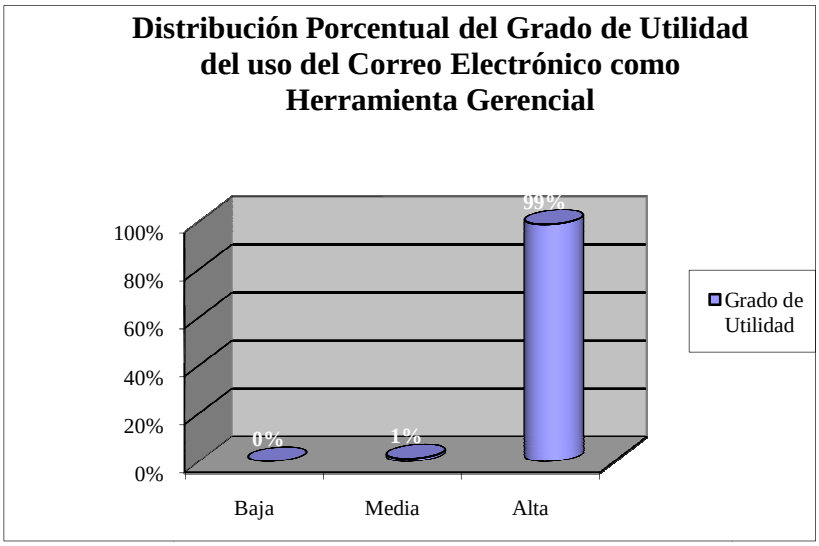


Fuente: Cuestionarios aplicados a los usuarios gerenciales del BC

Del análisis anterior se puede deducir en forma general, y tomando como referencia quienes envían más o menos de 50 correos por semana, que el 64% de los usuarios envían más de 50 mensajes, mientras que el 36%, menos de 50.

Es importante tomar en cuenta esta proporción de correos enviados por persona y por semana, ya que en el mundo actual, muchas instituciones de países desarrollados y subdesarrollados están utilizando el correo electrónico como herramienta gerencial para enviar y recibir mensajes de todo tipo, incluyendo correos con información confidencial que sirve para la toma de decisiones, por lo que quisimos conocer el grado de utilidad que representa para los usuarios encuestados su uso como medio de comunicación y herramienta gerencial, con el fin de determinar si la tendencia de la empresa va acorde con los países desarrollados y subdesarrollados. El resultado fue el siguiente: el 99% de los consultados contestó que el uso del correo es alto, mientras que solamente el 1% mencionó que no lo es, tal y como se muestra en el siguiente gráfico:

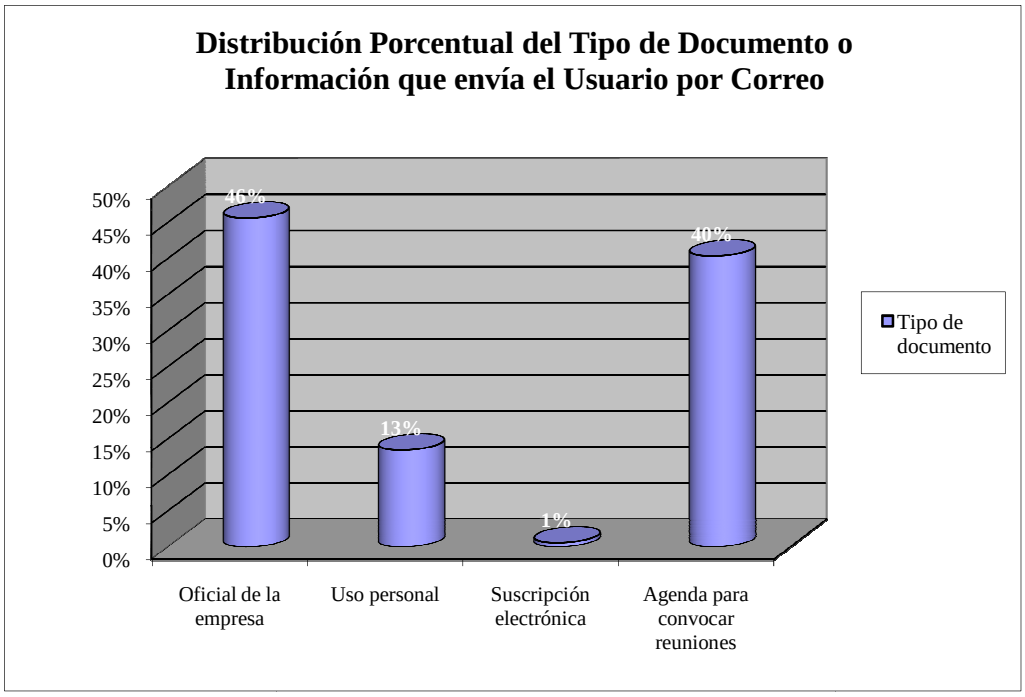
Gráfico N° 2



Fuente: Cuestionarios aplicados a los usuarios gerenciales del BC

Aunado a lo anterior, se quiso conocer qué tipo de información suelen enviar los gerentes encuestados, con base en cuatro opciones que les dimos a escoger. El resultado fue que el 46% de los sujetos que contestaron el cuestionario, utilizan el correo para enviar documentos oficiales de la empresa y el 40% convocatorias a reuniones por medio de esta herramienta. En menor porcentaje, un 13% de las personas utilizan el correo para enviar mensajes de tipo personal, y solamente el 1% lo usa para enviar suscripciones electrónicas de la institución. En la figura adjunta, se grafican estos datos:

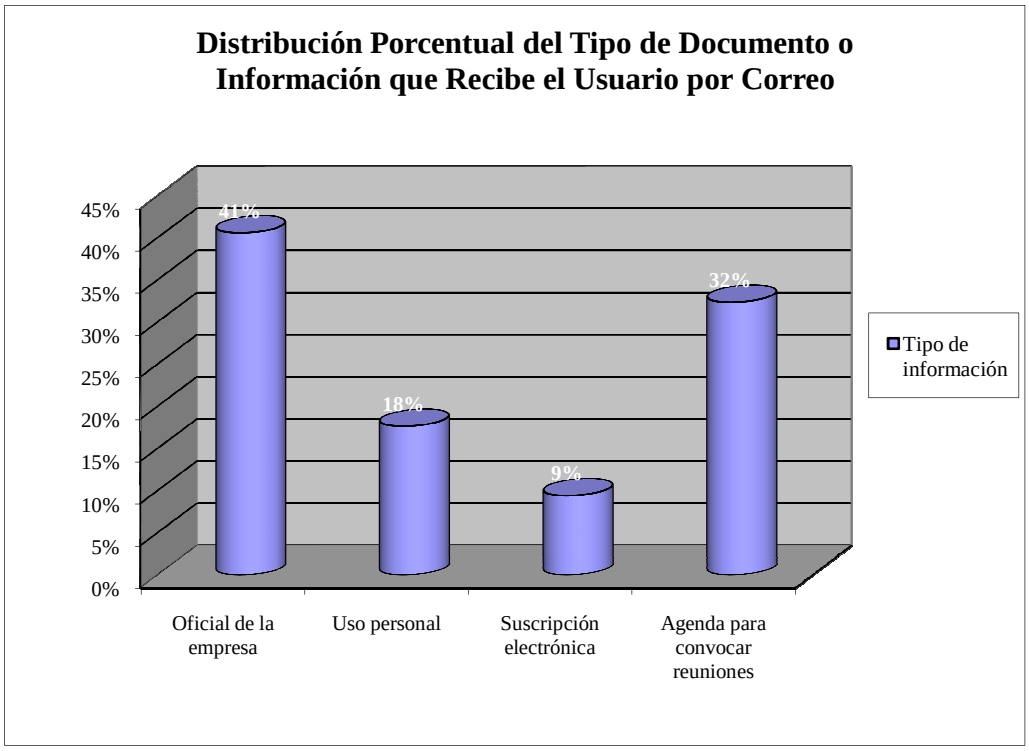
Gráfico N° 3



Fuente: Cuestionarios aplicados a los usuarios gerenciales del BC

Respecto a los mensajes que acostumbran recibir, los usuarios mencionaron que el 41% de estos son comunicaciones oficiales de la empresa; el 32% son convocatorias a reuniones por medio de la agenda del correo; 18% reciben documentos de tipo personal y un 9% que son suscripciones electrónicas, tal y como se muestra en el siguiente gráfico:

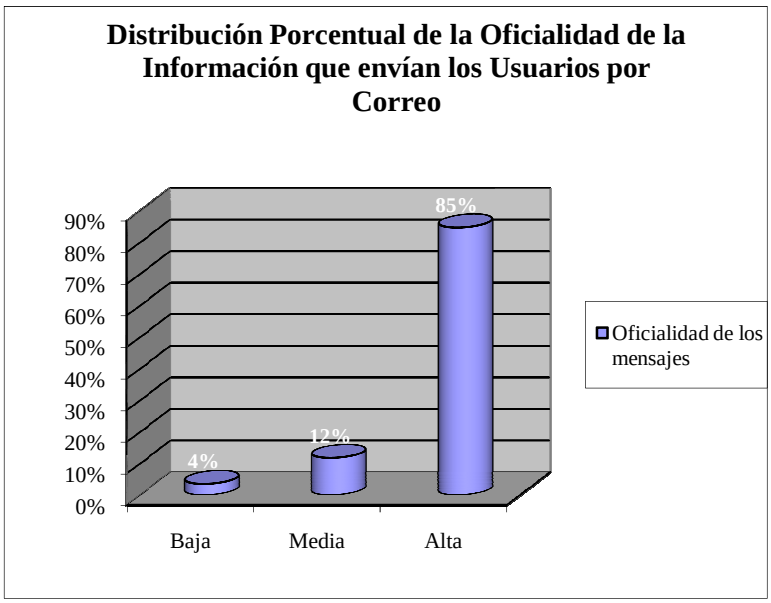
Gráfico N° 4



Fuente: Cuestionarios aplicados a los usuarios gerenciales del BC

Como se puede observar, los usuarios acostumbran enviar y recibir documentos de tipo oficial para la institución. Pero, ¿qué tan oficiales son estos documentos? A esta consulta los usuarios respondieron que un 85% de los mensajes son de alta oficialidad o importancia, un 12% de mediana importancia y un 4% son de baja oficialidad. (Ver el gráfico N° 5)

Gráfico N° 5



Fuente: Cuestionarios aplicados a los usuarios gerenciales del BC

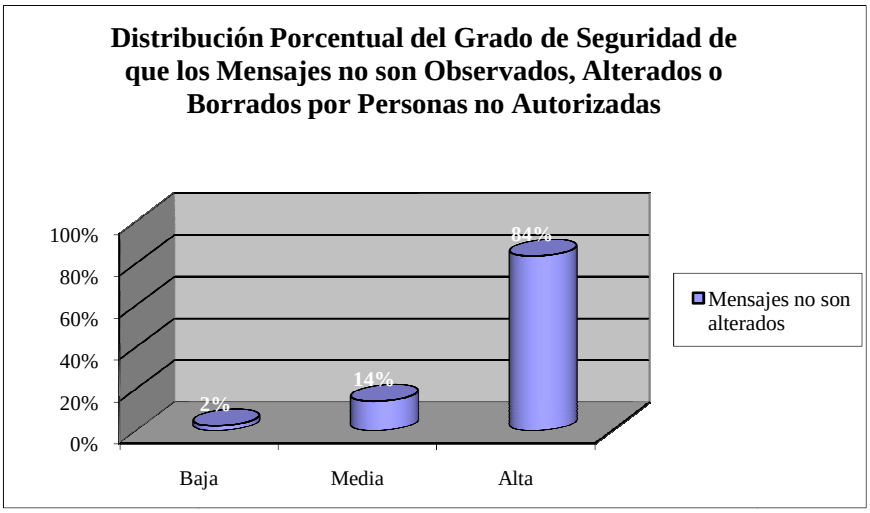
Estos últimos tres gráficos, representan el alto porcentaje de información de la empresa que se transmite por medio del correo, el tipo de información que se acostumbra transmitir y la oficialidad de estos mensajes, por lo que, a raíz de ello, se puede asegurar que el correo electrónico está siendo utilizado como herramienta gerencial entre los funcionarios de la institución, lo que a la vez implica un mayor grado de exposición a que los datos sean alterados o borrados por personas no autorizadas, sino se cuenta con mecanismos que ayuden a proteger la información. Debido a esto, se le consultó a los sujetos de la investigación si poseen alguna herramienta instalada en el correo electrónico que les permita mantener un cierto grado de seguridad, confidencialidad, confiabilidad e integridad de la información que transmiten por medio de esta herramienta; el 79% indicó que no tenían ningún mecanismo, técnica o herramienta que les ayudará a asegurar lo anterior, y el 21% respondió que sí poseía alguna. En el caso de estas respuestas, es importante mencionar que el Banco a la fecha, no posee ninguna herramienta que ayude a asegurar los datos que se transmiten por el correo, por lo que quienes contestaron afirmativamente, son personas que consiguieron alguna herramienta de este tipo de libre acceso en Internet.

Quisimos saber si la herramienta que han utilizado es una firma digital, y por tanto les consultamos si han utilizado alguna técnica de este tipo para el envío y recepción de mensajes electrónicos, y el 91% de los sujetos respondieron que no, y un 9% de ellos dijo que sí.

Esto quiere decir que de los usuarios que dijeron haber utilizado una herramienta que permita mantener un cierto grado de seguridad, confidencialidad, confiabilidad e integridad de la información que transmiten por medio de correo, solamente de un 9% a un 21% han utilizado un software de firma digital. No obstante, quienes respondieron que han utilizado un programa de firma digital fueron los usuarios de tecnología, mientras que los gerentes administrativos no lo han utilizado.

Además, pretendimos conocer qué tanto grado de seguridad tienen los usuarios de que la información que se transmite por correo puede ser observada, alterada o borrada por personas no autorizadas. El 84% de ellos dicen tener un grado de seguridad alto de que su información no es vista, ni alterada por intrusos; el 14% indicó tener un grado de seguridad medio y solamente el 2% de los usuarios considera que sus correos pueden ser vistos por intrusos. Estos resultados se encuentran en el siguiente gráfico:

Gráfico N° 6



Fuente: Cuestionarios aplicados a los usuarios gerenciales del BC

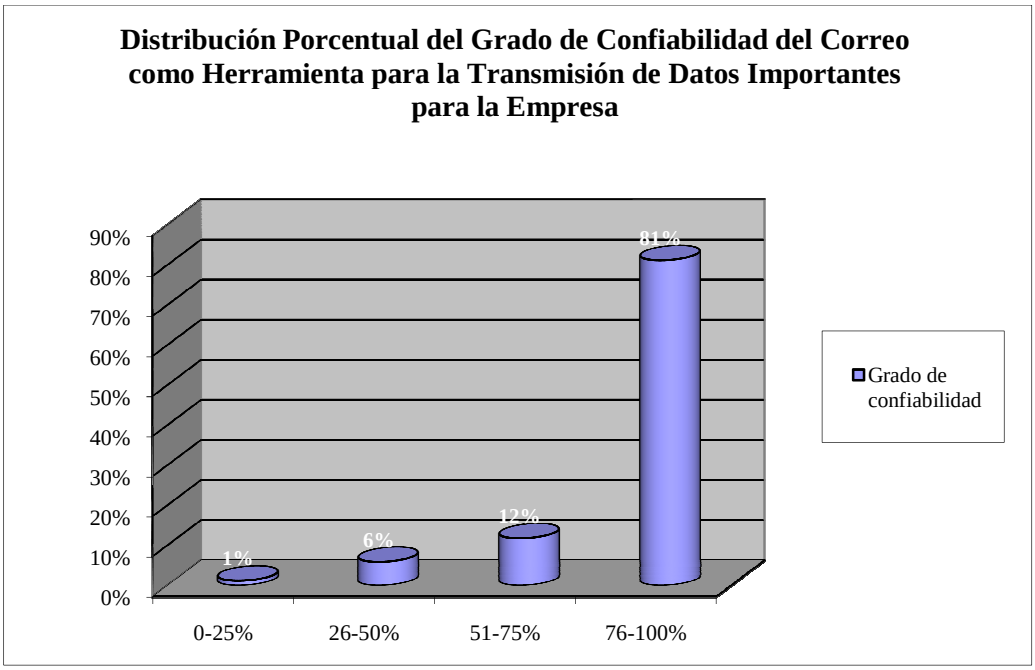
Es importante notar que la mayoría de los sujetos investigados consideran que sus correos no pueden ser observados, alterados o borrados por personas no autorizadas.

Asociada a la pregunta anterior, se les consultó a los gerentes si conocían algún método o herramienta que le permita a un intruso alterar la información que ellos envían por medio del correo. El 76% contestó que no conocían ningún método, y el 24% respondió afirmativamente a la pregunta; es decir, la mayoría de los sujetos de la investigación desconocen la existencia de métodos, técnicas o herramientas para alterar la información. Como se puede observar, esta pregunta se encuentra muy relacionada con la anterior, y a pesar de que los usuarios en cierta forma se contradicen en sus respuestas en un 8% entre los encuestados que consideran que sus datos no pueden ser alterados y los que desconocen la existencia de herramientas o técnicas para alterar los mensajes electrónicos, queda claro que existe poca conciencia por parte de los usuarios en materia de cultura de seguridad y de las amenazas a las que se encuentran expuestos los mensajes que son enviados y recibidos por medio del correo electrónico, ya que las probabilidades de alterar un mensaje son muy altas y ellos las desconocen; se debe recordar que en el mercado existen muchas herramientas que se consiguen fácilmente y de forma gratuita en la Internet, que permiten burlar y sabotear las redes de datos y los distintos programas de correo electrónico. Esta afirmación se refuerza con el siguiente análisis: se consultó a los sujetos de la investigación si conocían algún método de encriptación para la información que es enviada por medio del correo electrónico, y las respuestas fueron que un 88% de los usuarios no conocen los métodos de encriptación y solamente un 12% respondió que sí conocían alguno. Sin embargo, de los que contestaron afirmativamente, el 80% son informáticos, y un 20% son administrativos, por lo que se demuestra una vez más, los pocos conocimientos que poseen los usuarios finales acerca de herramientas que permitan asegurar la información que es enviada y recibida a través del correo electrónico. Este mismo resultado se obtuvo al consultar a los usuarios si conocían alguna técnica de firmas digitales para el uso del correo electrónico.

De acuerdo con el grado de confiabilidad que debería tener el correo electrónico como herramienta para el envío y recepción de mensajes, el 81% de los sujetos dijeron que debía

estar entre el 76% y 100%. El doce por ciento de los encuestados considera que el grado de confiabilidad debe ser de 51% al 75%; el 6% mencionó que la necesidad de confiabilidad en el correo debía era de 26% al 50% y solamente un 1% indicó que debía ser de 0% al 25%. Este análisis se muestra en el siguiente gráfico:

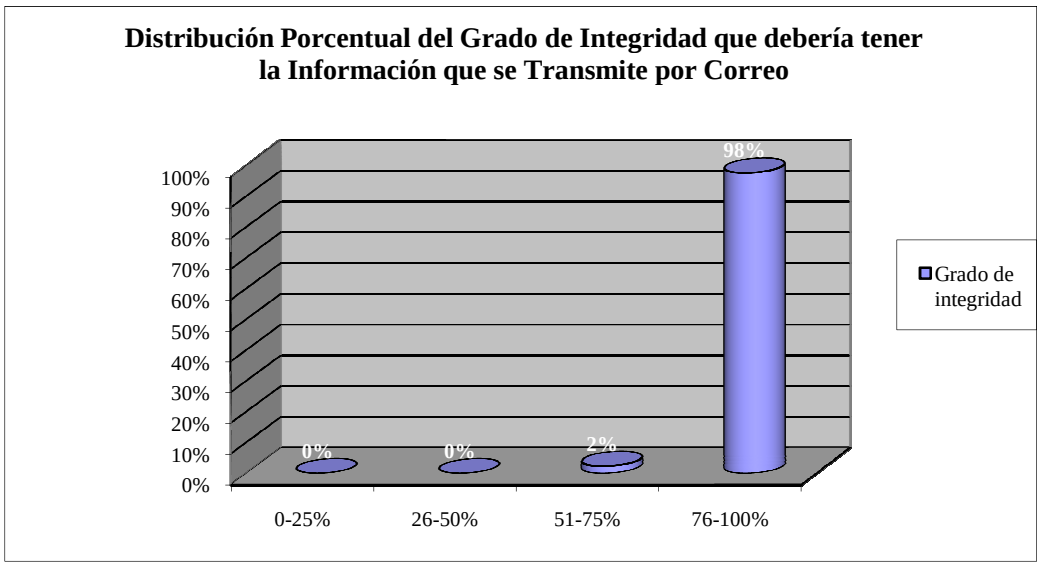
Gráfico N° 7



Fuente: Cuestionarios aplicados a los usuarios gerenciales del BC

Respecto al grado de integridad de los datos que se transmiten por medio del correo, el 98% de los usuarios considera que la necesidad de integridad debe ser del 76% al 100% y solamente el 2% respondió que debe ser del 51% al 75%, tal y como se muestra en el siguiente gráfico:

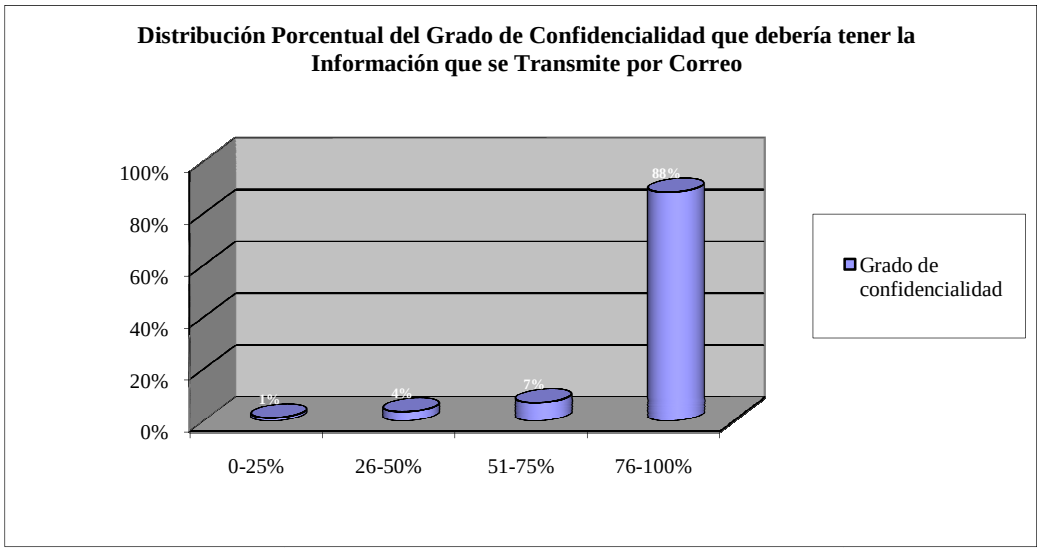
Gráfico N° 8



Fuente: Cuestionarios aplicados a los usuarios gerenciales del BC

También se consultó acerca del grado de confidencialidad. El 88% de los encuestados indicó que el correo electrónico debe tener de un 76% a un 100% de confidencialidad en la transmisión de datos. El 7% respondió que debe ser del 51% al 75% y un 1% dijo que debe ser 0% al 25%. En el siguiente gráfico se ilustra esta situación:

Gráfico N° 9



Fuente: Cuestionarios aplicados a los usuarios gerenciales del BC

Sin embargo, para tener un conocimiento más amplio de la necesidad, que tienen los usuarios, de proteger la información que se transmite por correo electrónico, no es suficiente conocer cuáles son sus requerimientos respecto a la confiabilidad, integridad y confidencialidad de la información que se transmite por medio de la red. Además de esto, es preciso conocer qué tipo de información es la que desean proteger. El 88% de los sujetos de la investigación respondió que los mensajes que envían y reciben son de carácter privado y el 12% indicó que era público. El análisis final indica que sí es necesario e importante asegurar los datos que se transmiten por medio del correo.

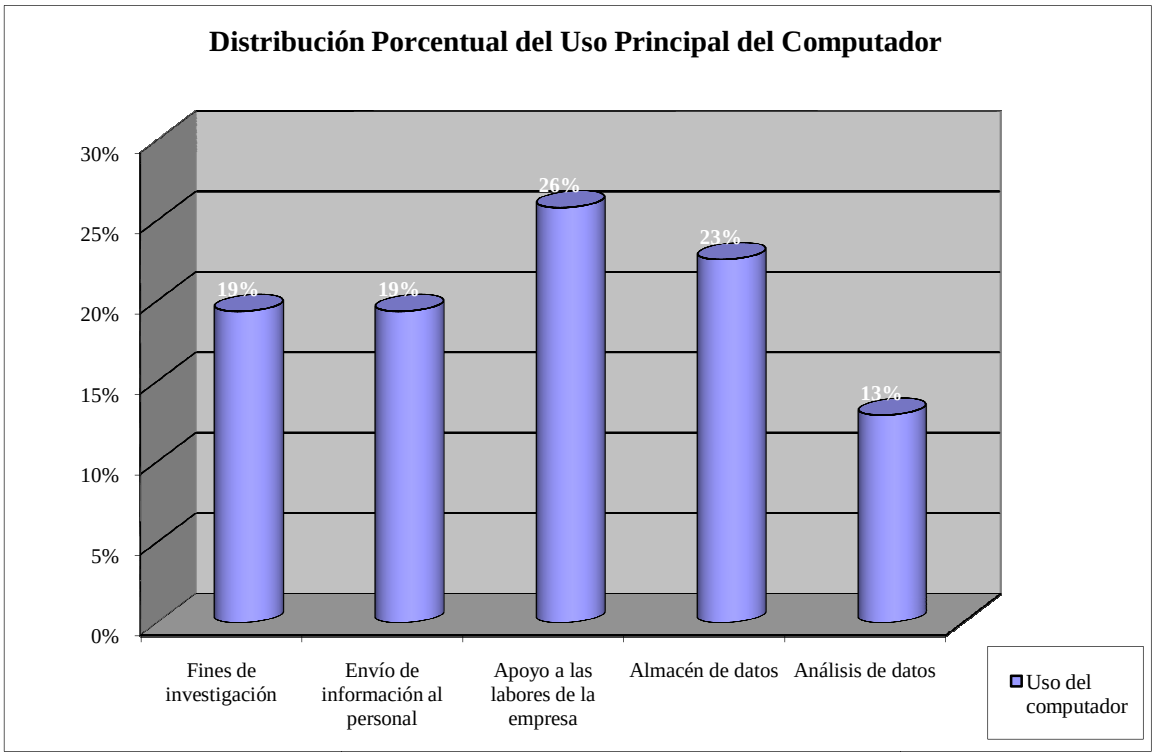
De los 85 sujetos que componen la muestra, 77 son usuarios administrativos. Específicamente a ellos, les consultamos acerca de la necesidad que tienen de asegurar la información que diariamente transmiten por medio del correo electrónico. El 96% indicó que sí tenían necesidades de proteger la información, y el 4% dijo que no era necesario. Sin embargo, el 99% de los gerentes administrativos está de acuerdo en implementar una solución de firma digital con todo y las implicaciones administrativas que ello puede conllevar, con el fin de asegurar un poco los mensajes electrónicos que transmiten por medio del correo.

Además, a los gerentes administrativos se les consultó si tienen instalados programas de encriptación para los mensajes enviados y recibidos por correo electrónico. El 95% respondió que no. Sin embargo, el 5% de los 77 usuarios administrativos dijo que sí. Es conveniente mencionar que el Banco no posee ninguna técnica o herramienta de este tipo. Por su parte Internet ofrece herramientas de encriptación libres para quien desee obtenerlas. Algunos de estos paquetes tienen a la vez, mecanismos de firmas digitales para el correo electrónico, por lo que quienes respondieron afirmativamente, adquirieron el software bajado de la web en forma gratuita.

Por otra parte, de los 85 sujetos de la investigación, 8 son gerentes del área de tecnología de información. A ellos se les consultó cuál era el uso principal que le dan al computador. El 26% de los encuestados respondió que lo utilizan para actividades que apoyen la labor de la empresa, el 23% dijo que lo utiliza como almacén de datos, el 19% para fines de

investigación y para el envío y recepción de información, y el 13% como herramienta de análisis de datos, tal y como se muestra en el siguiente gráfico:

Gráfico N° 10



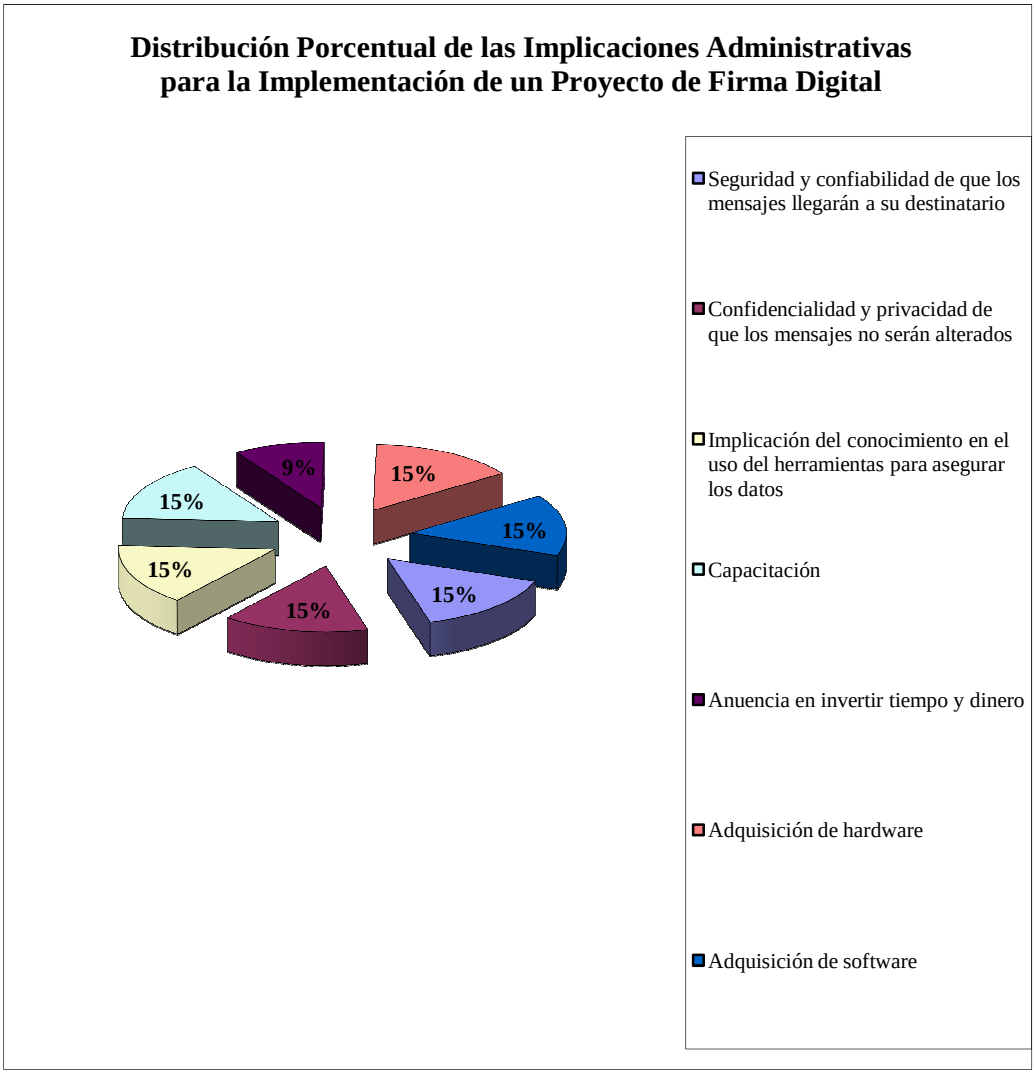
Fuente: Cuestionarios aplicados a los usuarios gerenciales del BC

Se quiso conocer qué tanto conocimiento tienen los usuarios tecnológicos de mecanismos o herramientas que le ayuden a garantizar la confiabilidad y confidencialidad de los datos; el 75% de los gerentes tecnológicos respondió que no conocían ninguna técnica, y el 25% mencionó conocer algún mecanismo. Si revisamos una de las anteriores respuestas dadas por la totalidad de los encuestados acerca del conocimiento de alguna técnica de encriptación, 10 sujetos contestaron afirmativamente, de los cuales, el 80% son usuarios informáticos y solamente el 20% son administrativos. Como resultado, se puede deducir que aunque la totalidad de los usuarios informáticos conocen o tienen un pequeño conocimiento en materia de técnicas o mecanismos de encriptación, la mayoría desconoce las ventajas o beneficios que ofrecen en el aseguramiento de la información, tal y como lo es que ayudan a garantizar la confiabilidad y confidencialidad de los datos. Relacionado

con el tema, el 100% de los gerentes de tecnología entrevistados, consideran que es necesario e importante asegurar la privacidad y confidencialidad de los datos que se transmiten por medio del correo electrónico.

Por último, se les preguntó a los usuarios de tecnología qué implicaciones positivas o negativas consideraban ellos que tendría al adquirir una solución de firmas digitales, entendiendo positiva como que estarían dispuestos a invertir en ella y negativa como que no invertirían en ella. El resultado de la consulta fue la siguiente: el 15% de los usuarios considera que con la implementación de una solución de firma digital, reforzarán en gran medida la seguridad y confiabilidad de que la información llegará a su destinatario y obtendrán un mayor grado de confidencialidad y privacidad de que la información no será alterada, ni robada por algún intruso; además, consideran que la adquisición de un paquete de firma digital ampliará el conocimiento en el uso de herramientas para asegurar los datos que se envían por correo electrónico. De igual forma, el 15% de los usuarios considera que aceptarían adquirir el hardware y software necesario, así como recibir una adecuada capacitación, con el objetivo de implementar adecuadamente la solución de firma digital. Referente a la implicación de carácter monetario y de tiempo, el 9% de los gerentes de tecnología consideran que la adquisición de un software de firma digital para el correo electrónico sería una buena inversión tanto de tiempo como de dinero. Estos resultados se grafican en la siguiente figura:

Gráfico N° 11



Fuente: Cuestionarios aplicados a los usuarios gerenciales del BC

Como se puede notar, la mayoría de los usuarios gerenciales están anuentes en adquirir e implementar una solución de firmas digitales para proteger la información que se transmite por medio del correo electrónico.

Por otra parte, las políticas y demás reglamentos para el uso de los recursos computacionales en las instituciones son necesarias para poder regular el uso adecuado de estos equipos, por parte de los usuarios finales. El Banco Centroamericano cuenta con políticas de este tipo. Sin embargo, por medio de la información recopilada a través del

cuestionario, el 20% de los sujetos investigados desconoce la existencia de estas políticas y el restante 80% las conoce y aplica.

Actualmente, en la Asamblea Legislativa se está tramitando un proyecto de ley, el cual pretende regular el uso de firmas digitales y certificados digitales para la protección de la información que se transmite a través del correo electrónico. Así que se consultó a los encuestados si tenían conocimiento de alguna ley o proyecto de ley existente en el país relacionada con firmas digitales. Al respecto el 87% de los individuos respondió que no conocían nada por el estilo, y solamente un 13% contestó afirmativamente. Es importante tener capacitado al usuario en este tipo de regulaciones, con el fin de evitar futuros problemas o sanciones por mal uso del equipo o programa por causa de no leerlas, que aunque si bien es cierto son de carácter obligatorio, siempre es bueno recordárselo a los usuarios.

3.7 Alcances y limitaciones

El alcance de esta investigación estaba orientado hacia los usuarios del correo electrónico del sistema bancario público nacional, específicamente los directores de divisiones, gerentes locales y regionales, que lo utilizan con mayor frecuencia para el envío de información de alta importancia y confidencialidad para la institución, como una de las principales herramientas de comunicación gerencial.

Como es conocido, antes de implementar un proyecto, es necesario “vender” la idea al área gerencial de la institución en estudio. Esta investigación requería obtener información de los usuarios administrativos de la gerencia de al menos 3 instituciones bancarias nacionales (Banco Popular, Banco Nacional y Banco Centroamericano), mediante la aplicación de los instrumentos seleccionados. Sin embargo, no fue posible aplicar los cuestionarios ni en el Banco Popular, ni el Banco Nacional, debido a que el primero no contestó a la solicitud de permiso en esa institución y en el Banco Nacional, no la aceptaron del todo. De los tres bancos que conformaban la muestra, solamente el Banco Centroamericano permitió

desarrollar los cuestionarios. Estas limitaciones, obligaron a la reducción del alcance original de este trabajo y reorientarlo a una sola institución, el Banco Centroamericano.

Otra de las limitaciones que se presentó durante el desarrollo de la investigación fue el tiempo limitado con el que cuentan los gerentes del Banco, ya que por sus continuas reuniones y responsabilidades gerenciales, o simplemente porque no consideraron la importancia que tiene un trabajo de este tipo, algunos no leyeron el correo enviado con el cuestionario, o los que lo leyeron, no contestaron.

Además, otra limitante de importancia en esta investigación fue la de no contar con una infraestructura tecnológica mínima para probar los distintos paquetes de software que existen en el mercado y de esta manera haber propuesto, más certeramente, una herramienta que se adecue a las necesidades de la institución con base en el análisis de costo – beneficio de adquirirla e implementarla.

Aunado a lo anterior, se presentó la restricción de que las empresas que ofrecen este tipo de software, fueron contactadas por medio de los servicios que ofrecen por Internet. No obstante la información que brindan a través de sus páginas web de los productos de firma digital, es escasa. Se intentó contactarlos por medio de las direcciones de correo que publican a disposición de los clientes para solicitar más información, pero nunca los contestaron, por lo que no fue posible añadir más datos de los productos en la propuesta.

4. CONCLUSIONES

Esta investigación se llevó a cabo con el fin de identificar en la población investigada el conocimiento que tienen en el tema de seguridad informática, específicamente en el uso de una herramienta tan común en el mundo actual para la transmisión de datos como es el correo electrónico.

Con base en la recopilación de la información primaria y secundaria, se procedió a hacer un análisis de los datos con el fin de obtener las conclusiones de la investigación, las cuales se presentan a continuación:

- Los usuarios finales consideran que el correo electrónico es una herramienta y medio de comunicación muy útil. El principal uso que le dan es como medio de comunicación para la transferencia de conocimientos, comentarios, sugerencias, toma de decisiones, consultas acerca del estado y composición de los productos y/o servicios actuales que tienen en el mercado, incluso de proyectos futuros, configuración de sistemas, redes, equipos, balances de comprobación, estados de resultados, fraudes que se hayan presentado en la empresa, debilidades en los sistemas actuales de atención y servicio al cliente, productos y/o servicios en el mercado e incluso de sistemas de alta importancia para la institución. Por lo general, la información o documentos que los usuarios envían y reciben a través del correo electrónico, son de carácter oficial y privado para la empresa.

- Los usuarios desconocen la existencia de métodos o herramientas que puedan alterar, borrar o capturar la información que se transmite por correo para fines ilícitos. De lo anterior se desprende la falta de cultura en seguridad y conocimiento de herramientas utilizadas para cometer delitos informáticos por parte de los usuarios finales. Por lo general, son personas que consideran que las herramientas que utilizan son seguras e invulnerables, sin tener conciencia de lo frágil y débiles que son los sistemas informáticos que sirven de apoyo a la administración para la manipulación de datos, almacén de datos, toma de decisiones, creaciones de nuevos productos y servicios, comunicaciones de alta confidencialidad y privacidad entre los gerentes de la institución a través de medios electrónicos, y otros. A menudo, suelen enviar información con estados de resultados, balances de comprobación, tácticas de mercadeo para la introducción de un nuevo servicio al mercado, diseños o bocetos de proyectos, servicios o productos nuevos, configuraciones de equipos principales tales como servidores, esquemas de seguridad de sistemas con alto número de transacciones de grandes volúmenes de dinero, diagramas de seguridad

de la composición de la red, problemas de vulnerabilidades internas en el servicio al cliente, funcionalidad de sistemas claves para la atención de público, para procesar alto número de transacciones, entre muchos otros, y en fin, mucha información delicada, de tipo privado, vulnerable a ser alterada, eliminada, utilizada de forma inadecuada, entre otros.

- La mayoría de los usuarios no tienen instalado en sus computadores personales, mecanismos de encriptación y firma digital que les ayuden a asegurar la integridad, confidencialidad, confiabilidad y privacidad de los datos que envían y reciben por correo electrónico y por ende, desconocen su existencia. Sin embargo, los usuarios finales consideran que el correo electrónico, utilizado como medio de comunicación para el envío y recepción de documentos importantes para la institución, debería tener un alto grado de integridad, confidencialidad, confiabilidad y privacidad.

- Para el uso del equipo de cómputo y el correo electrónico, se logró constatar que sí existen políticas y procedimientos que regulan su uso.

- Actualmente en el país, se está tramitando en la Asamblea Legislativa un proyecto de ley de Firma Digital y Certificados Digitales, sin embargo, la mayoría de los usuarios consultados desconocen la existencia de este proyecto. Además, a nivel mundial, la ONU creó un modelo de ley llamado UNCITRAL, el cual también regula el uso y manejo de firmas digitales en los países afiliados a la ONU entre los que se encuentra Costa Rica, pero también desconocían la existencia de esta ley.

- La administración de la empresa está dispuesta a "correr" con los gastos necesarios y demás implicaciones administrativas de adquisición de hardware, software, capacitación, inversión de tiempo y dinero, con el fin de obtener un poco más de seguridad, integridad, confidencialidad y confiabilidad en la información que suelen enviar y recibir a través del correo electrónico.

5. RECOMENDACIONES

Al finalizar la presente investigación, se logró comprobar el poco conocimiento e interés que tienen los usuarios por proteger los datos que transmiten a través del correo electrónico. Es por la anterior afirmación que a continuación se describen las siguientes recomendaciones:

- Capacitar a los usuarios en materia de seguridad, de manera que conozcan más acerca de las vulnerabilidades y amenazas a las que se encuentran expuestas los datos que se transmiten por medio de la red, entre los cuales se encuentran, el envío y recepción de datos a través del correo electrónico, con el fin crear cultura informática en los usuarios finales.

- Capacitar a los usuarios en materia de regulaciones tanto nacionales como internacionales y políticas y procedimientos de la institución, con el objetivo de crear conciencia en el uso de los recursos computacionales y conocimiento en las regulaciones que los amparan y protegen de los intrusos que acostumbran robar información confidencial.

- Realizar un estudio de las implicaciones operacionales, es decir, las necesidades que tienen los usuarios de la empresa en materia de protección de los datos y determinar los requerimientos necesarios para ayudar a proteger la información que se transmite por medio del correo electrónico, tanto en hardware como en software para adquirir un modelo o paquete de firma digital.

- Hacer un estudio en el mercado de los diferentes mecanismos y técnicas de encriptación y firma digital que permitan autenticar y asegurar la confidencialidad de la información enviada y recibida por medio del correo electrónico y brindar al usuario la protección necesaria de sus datos, acorde con las necesidades de la institución, con el fin de identificar las ventajas y desventajas que ofrecen.

- Hacer un estudio de las implicaciones administrativas y económicas asociadas en el proyecto de adquisición e implementación de firma digital de la institución, de acuerdo con la importancia relativa de la información que se desea resguardar.

- Adquirir un modelo de firma digital para la información que diariamente envían y reciben los usuarios a través del correo electrónico, y esta manera asegurar en un mayor grado, la protección, integridad, confiabilidad y confidencialidad de la información.

6. PROPUESTA

6.1 Introducción

Alrededor del mundo, muchos estudios relacionados con el área de seguridad informática han sido desarrollados, todos en la búsqueda de la solución "perfecta" al problema de protección de los datos, que sabemos no existe. Sin embargo, estos estudios suelen realizarse de manera general; ya que una de las principales áreas de seguridad en una empresa son las redes a través de las cuales, diariamente, se envían millones de datos, algunos de tipo sensible (privado) y otros públicos; otra es la configuración de los equipos servidores de una red que deben ser programados con mucho recelo, con el fin de cerrar cualquier posible servicio o acceso al equipo al personal interno y externo de la institución, entre muchos más; otras de las grandes debilidades del ambiente de seguridad es el envío de datos por medio de la red, para lo cual existe variedad de métodos y técnicas de encriptación, entre otros.

No obstante, casi siempre se deja de lado un factor muy importante en toda organización, el cual se convierte en la base sobre la que se levantará toda la infraestructura de seguridad: la capacitación del usuario en esa materia.

Luego de concluir esta investigación, y tomando como referencia el análisis de la información recolectada por parte de los propios protagonistas de este problema, los

usuarios, se nota que existe un débil conocimiento en materia de seguridad que involucra el conocimiento en general de las leyes que amparan todas aquellas violaciones contra la empresa en materia de seguridad, y por supuesto en mecanismos o técnicas que ayuden a proteger los datos. Como se mencionó anteriormente, el mercado ofrece una serie de soluciones para asegurar la información, e incluso a través de la Internet se facilita mucho la búsqueda de este tipo de herramientas. Por este motivo, esta propuesta, la cual de ahora en adelante nos referiremos a ella como PROCAFI[4], se centrará más en el aspecto de capacitación que en presentar una herramienta para la protección de datos.

6.2 Descripción de la Propuesta

PROCAFI se desarrollará con el fin de brindar al lector una solución a los problemas planteados en esta investigación.

Su principal enfoque será dar una solución de capacitación a los usuarios, debido a que los resultados obtenidos del análisis de la información recopilada, mostró grandes debilidades en el conocimiento de los usuarios en materia de protección de los datos, debilidades y amenazas del correo electrónico, métodos de seguridad, técnicas de encriptación, legislaciones locales e internacionales que regulan y castigan el uso indebido o ataques al correo electrónico, entre otras áreas importantes que deben ser de conocimiento básico por parte del personal de una empresa. Lo más preocupante de lo anterior es que en la investigación, se nota que no solo los usuarios administrativos desconocían estos temas, sino que también las propias personas con formación y desarrollo "profesional" en el área informática, lo cual deja mucho que pensar.

Otro punto que se mencionará, aunque en menor detalle es la propuesta de adquisición e implementación de un mecanismo o técnica de firma digital para el uso del correo electrónico, con el fin de asegurar en un mayor grado la información que se envía y recibe por correo electrónico.

[4] PROCAFI: Propuesta de Capacitación y Firma Digital

6.3 Alcances y Limitaciones

Debido a que el tipo de problema desarrollado durante la investigación es muy general y común, ésta solución aplica para todas aquellas instituciones y empresas de cualquier tipo comercial, financiero, gubernamental, y otros, en donde los usuarios utilicen el correo electrónico como una de los principales medios de comunicación y transmisión de información pública y con más razón, privada.

La propuesta que en inicio se pensó desarrollar era dar un valor agregado, el cual consistía en presentar al lector un trío de las mejores soluciones que ofrece el mercado mundial para adquirir un mecanismo o técnica de firma digital en el correo electrónico e incluso los posibles pasos que debían seguirse para implementar la solución que más se ajustara con las características de la empresa y con las necesidades de protección de los datos. Sin embargo, no fue posible añadir este valor agregado a la propuesta debido a que fue difícil obtener la información detallada de cada uno de los productos por parte de las empresas vendedoras y/o distribuidoras de los productos y así presentar una solución completa, tal y como se pensó en un inicio. Además, para presentar solamente las mejores opciones de firma digital es necesario contar con una infraestructura informática de considerable tamaño para desarrollar las pruebas. Así que, PROCAFI se limitará a nombrar las empresas con más prestigio, por la experiencia y calidad de sus productos, las cuales en la mayoría de las ocasiones han sido premiados con menciones honoríficas. También, se nombrará las herramientas que estas empresas ofrecen y algunas de las características que poseen.

Aunado a lo anterior, se presentó la restricción de que las empresas que ofrecen este tipo de software, fueron contactadas por medio de los servicios que ofrecen por Internet. No obstante la información que brindan a través de sus páginas web de los productos de firma digital, es escasa. Se intentó contactarlos por medio de las direcciones de correo que publican a disposición de los clientes para solicitar más información, pero nunca los contestaron, por lo que no fue posible añadir más datos de los productos en la propuesta.

6.4 Factibilidad

A continuación se presenta un análisis de las factibilidades técnicas, operacionales y económicas que representa para una empresa, implementar PROCAFI.

- ***Técnica:*** la factibilidad técnica de esta solución se enfoca en la infraestructura tecnológica con que debe contar la institución para implementar una solución de firma digital. En relación con estos factores técnicos, no es necesario contar con una plataforma tecnológica sofisticada, ya que por lo general estas herramientas se acoplan a la infraestructura operativa que posea la empresa. En caso de requerir alguna actualización de la plataforma tecnológica de la institución, las necesidades serían mínimas así como los gastos.

  Referente al recurso técnico del software, sí es necesario invertir debido a que con base en ello es que funcionará el cifrado y descifrado de los correos enviados y recibidos.

- ***Operativa:*** la factibilidad operativa de PROCAFI se orienta a las necesidades de recurso humano y su capacitación en distintos temas relacionados con tecnologías de información y seguridad. Referente al recurso humano necesario para administrar la herramienta de firma digital, va a ser mínimo, ya que estas herramientas por lo general son de fácil administración. Además, el mantenimiento y soporte que vaya a necesitar el programa no va a demandar mucho tiempo, debido a que casi no será necesario.

  El factor que sí requerirá de tiempo es el entrenamiento del personal de la institución que vaya a utilizar firma digital para la transmisión de los correos por medio de la red. El concepto encriptar y desencriptar suele ser difícil de comprender. Además, es necesario que a la hora de impartir la capacitación, se dé en forma cronológica, siendo el entrenamiento en el uso y manejo de firmas

digitales, la última capacitación que se imparta, posterior de haber adquirido el software.

Debido al amplio desconocimiento de los usuarios en materia de seguridad, y para que estos utilicen adecuadamente un software de firma digital en el correo electrónico; el entrenamiento que se brinde a los usuarios debería contemplar, al menos, temas tales como: seguridad informática, amenazas y riesgos en la seguridad informática, vulnerabilidades en el uso del correo electrónico, mecanismos o técnicas para asegurar la integridad y confidencialidad de los datos, regulaciones en el uso del correo electrónico y del proyecto de ley de firmas digitales que actualmente se encuentra en la Asamblea Legislativa.

- ***Económica:*** en este caso, los costos de capacitación para la institución van a ser pocos, debido a que el BC cuenta con una infraestructura adecuada para brindar capacitación al personal de la empresa. Este centro de capacitación se llama Universidad Corporativa (UC) y está a cargo de la gerencia de Recursos Humanos. La UC posee 4 aulas acondicionadas adecuadamente, de las cuales una es un laboratorio de cómputo con 36 computadoras, por lo que si consideramos la factibilidad técnica, el único gasto en que deberá incurrir el BC es en la contratación de profesores que impartan las clases. Este costo será mínimo, debido a que la mayoría de las clases serán impartidas por personal de la institución. El desglose de los profesores por materia es el siguiente:

Tabla N° 1

Instructores por Curso Propuesto			
	Curso Propuesto	**Profesor**	**Duración Estimada del Curso**
1	Seguridad informática	Alejandro Sebianni (Funcionario del BC)	2h

2	Amenazas y riesgos en la seguridad informática	Alejandro Sebianni (Funcionario del BC)	4h
3	Vulnerabilidades en el uso del correo electrónico	UC	2h
4	Mecanismos o técnicas para asegurar la integridad y confidencialidad de los datos	UC	4h
5	Regulaciones internas de la empresa en el uso del correo electrónico	Recursos Humanos (BC)	2h
6	Proyecto de ley de Firmas Digitales y otras regulaciones externas que reglen el uso del correo electrónico	UC	1h

Como se puede notar en el cuadro anterior, hay tres cursos en los que se indica que el profesor es UC. Cuando se dice esto, es porque la UC tiene la política de que se deben presentar al menos 3 currículos de los posibles profesores que impartirán esa materia cuando no son funcionarios de la institución. Luego, con base en el costo, temario y facilidades adicionales que brinden los instructores, se escogerá a quien dará el curso. Como parte de esta solución, a continuación se adjuntan los requisitos mínimos o conocimientos básicos que deberán cumplir los postulantes para impartir los cursos propuestos en este trabajo:

- Para los cursos de *Seguridad informática* y *Amenazas y riesgos en la seguridad informática*: concepto de seguridad; aplicación de controles de seguridad en ambiente de tecnología de información; ventajas y desventajas de aplicar seguridad informática; mecanismos y tipos de seguridad informática; riesgos, vulnerabilidades, amenazas y tipos de ataque relacionados con la seguridad informática.

- Curso de *Vulnerabilidades en el uso del correo electrónico*: concepto y uso del correo electrónico; vulnerabilidades y amenazas a las que se expone el correo

electrónico; mecanismos, técnicas y herramientas existentes en el mercado para cometer delito informático; riesgos asociados con el delito informático.

- Curso *Mecanismos o técnicas para asegurar la integridad y confidencialidad de los datos*: herramientas y mecanismos de protección que brinda el mercado para ayudar a proteger la información en todo el ámbito informático; es decir, redes, sistemas, servicios, bases de datos, herramientas de comunicación dentro de las cuales por supuesto está el correo electrónico, entre otros.

- Curso *Regulaciones internas y externas de la empresa en el uso del correo electrónico*; *Proyecto de ley de Firmas Digitales*: se recomienda que este curso sea impartido por personal de la institución con conocimientos en los lineamientos internos que posee la empresa en relación con el uso del correo y otra persona externa experta con conocimiento en materia de delito informático, regulaciones y leyes, como el proyecto de ley relacionado con firmas digitales y otros que rigen para el Gobierno de Costa Rica, tanto a nivel nacional como internacional.

Con respecto a la definición de los días, horarios exactos, así como los gastos de alimentación de los recesos y clase donde se impartirán los cursos estos, serán asignados y coordinados por la UC, debido a que estas actividades forman parte de las funciones que ellos realizan. Además ya existen otros cursos por dar, por lo que deberán coordinar la disponibilidad de los días, aulas y del profesor para luego definir el cronograma de capacitación con base en estas variables. Al respecto, en la siguiente tabla se propone un esquema de capacitación para los usuarios gerenciales de la institución, con el fin de facilitar este trabajo. Una vez que la UC haya realizado lo anterior, se encargará de comunicar el cronograma de capacitación a cada una de las gerencias de la institución involucradas en el proceso de entrenamiento.

Tabla N° 2

Esquema Propuesto de Capacitación para los Usuarios						
Curso	**Tiempo Estimado**	**Horario**	**Lugar donde se impartirá**	**Dirigido a**	**Cupo máximo**	**Semanas**
Seguridad informática	2h	Sábados: 08:00 a.m. a 10:00 a.m. y de 10:00 a.m. a 12:00 m.d.	Universidad Corporativa	Usuarios gerenciales	30 personas por grupo. Se propone crear 3 grupos de usuarios. *	Semanas 1 y 2
Amenazas y riesgos en la seguridad informática	4h	Sábado: 08:00 a.m. a 12:00 a.m.	Universidad Corporativa	Usuarios gerenciales	30 personas por grupo. Se propone crear 3 grupos de usuarios. *	Semanas 3-4-5
Vulnerabilidades en el uso del correo electrónico	2h	Sábados: 08:00 a.m. a 10:00 a.m. y de 10:00 a.m. a 12:00 m.d.	Universidad Corporativa	Usuarios gerenciales	30 personas por grupo. Se propone crear 3 grupos de usuarios. *	Semanas 6 y 7

Mecanismos o técnicas para asegurar la integridad y confidencialidad de los datos	4h	Sábado: 08:00 a.m. a 12:00 a.m.	Universidad Corporativa	Usuarios gerenciales	30 personas por grupo. Se propone crear 3 grupos de usuarios. *	Semanas 8-9-10
Regulaciones internas de la empresa en el uso del correo electrónico	2h	Sábados: 08:00 a.m. a 10:00 a.m. y de 10:00 a.m. a 12:00 m.d.	Universidad Corporativa	Usuarios gerenciales	30 personas por grupo. Se propone crear 3 grupos de usuarios. *	Semanas 11-12-13

*** Los grupos de usuarios estarán compuestos por las siguientes divisiones organizacionales:**

- **Grupo 1: Banca de Personas**
- **Grupo 2: Banca de Inversión, Fondos de Pensión, BC Valores, Finanzas y Control Contable, Gestión de Riesgo Banca Corporativa**
- **Grupo 3: Tecnología de Información, Gerencia y Subgerencia General, Mercadeo, Recursos Humanos, Banca Institucional**

Inicialmente, esta capacitación va orientada a los funcionarios de la gerencia, ya que la información recopilada y los resultados obtenidos de su análisis, demostraron un débil conocimiento en aspectos de seguridad, amenazas y vulnerabilidades en la protección de los datos y en el manejo de leyes y regulaciones tanto internas como externas de la empresa. Además, como es de conocimiento general, primero hay que "vender el producto" al área gerencial de la institución, es decir, hacer conciencia en ellos de los riesgos y amenazas que acechan el correo electrónico y la información que se transmite a través de ella y de las ventajas que obtendría la institución al implementar un programa de firma digital; por esta razón es que inicialmente la capacitación se orientará a este sector de la población total de la organización. A futuro, cuando los gerentes hayan tomado conciencia de la importancia de tener conocimientos básicos en los temas propuestos para la capacitación, se programará un entrenamiento a los principales usuarios de tecnología de información y de los usuarios responsables de brindar apoyo a sus compañeros de cada área o departamento de la empresa. Por último, se le impartirá estos conocimientos al personal restante de la institución por departamento. Estas capacitaciones, al igual que las que se impartirán a los gerentes, serán coordinadas por la UC.

Por otra parte, los costos de adquisición de firmas digitales oscilan alrededor de los $300 y $1000. Sin embargo, el costo general de la adquisición de este producto para la institución, dependerá de la cantidad de licencias que deseen.

6.5 Desarrollo de la Propuesta

La solución que se ofrece para resolver el problema en este trabajo está basada en tres grandes aspectos que son los siguientes:

- ***Definir un plan de capacitación al usuario***: se deberá definir un plan de capacitación que incluya al menos los siguientes temas:

  - *Seguridad informática:* se propone impartir este curso con el fin de enseñar a los usuarios los conocimientos y principios básicos relacionados con el tema de seguridad, tales como: ¿qué es la seguridad informática?, ¿para qué sirve la seguridad en TI?, ¿cómo se puede implementar seguridad informática en un ambiente de TI?, ¿cuáles son los beneficios y desventajas de aplicar seguridad informática en un ambiente de TI?, ¿qué tipos o mecanismos de seguridad existen?, ¿qué herramientas de seguridad ofrece el mercado para los distintos tipos de seguridad?, entre otros.

  - *Amenazas y riesgos en la seguridad informática:* con este curso se instruirá al usuario en los riesgos, vulnerabilidades, amenazas y los diferentes tipos de ataques que existen en el mundo con el fin de comprometer la seguridad de las empresas, redes, sistemas, datos, y otros.

  - *Vulnerabilidades en el uso del correo electrónico:* mostrar a los usuarios las vulnerabilidades y amenazas a las que se expone el correo electrónico; los mecanismos, técnicas y herramientas que ofrece el mercado para cometer un delito informático; los riesgos asociados a estas debilidades y mostrar ejemplos de la vida real.

  - *Mecanismos o técnicas para asegurar la integridad y confidencialidad de los datos:* se mostrará al usuario las herramientas y mecanismos de protección que brinda el mercado para ayudar a proteger la información en todo el ámbito

informático, es decir, redes, sistemas, servicios, bases de datos, herramientas de comunicación dentro de las cuales por supuesto está el correo electrónico, entre otros.

- *Regulaciones internas de la empresa en el uso del correo electrónico:* dar a conocer a los usuarios los lineamientos internos que posee la institución en relación con el uso del correo.

- *Proyecto de ley de Firmas Digitales y otras regulaciones externas que reglen el uso del correo electrónico:* dar a conocer a los usuarios el contenido del proyecto de ley de firma digital y los beneficios que esta ofrece al ambiente tecnológico, así como otras regulaciones relacionadas con el correo electrónico. Además, se les instruirá en las leyes que actualmente rigen para el Gobierno de Costa Rica, tanto a nivel nacional como internacional relacionados con el uso del correo y protección de la información que almacena y envía por medio del correo electrónico, con el fin de que conozcan las leyes que los amparan ante una posible captura, alteración o borrado de los mensajes enviados o recibidos.

Para cumplir con lo anterior, es necesario definir un grupo de personas o comité de capacitación que se encargue entre otras cosas de:

- *Contratar los expertos en la materia que se encargarán de impartir los cursos o charlas:* como ya se mencionó anteriormente, este punto lo asumirá la UC, ya que es la encargada de coordinar todo tipo de capacitación en la institución.

- *Definir el cronograma de capacitación según el tema:* debido a las funciones que le competen a la UC, es su responsabilidad coordinar con los instructores y definir el cronograma de actividades, de acuerdo con la disponibilidad de las aulas de capacitación, cursos ya propuestos y confirmados por impartir, duración del curso propuesto y personal que participará.

- *Definir el número de personas que conformarán cada grupo:* será necesario conformar los grupos de capacitación según el área usuaria, la necesidad de atención por parte del instructor con los asistentes y la capacidad del aula. Esta tarea también es responsabilidad de la UC. Es importante aclarar que todo el personal de la institución debe ser capacitado en estos temas. No obstante, para esta primera etapa se propone capacitar primero a los gerentes de cada área usuaria con el fin de que sean los primeros en obtener los conocimientos generales acerca de estos temas y de esta forma tomen conciencia de las amenazas a las que se encuentran expuestos, y así se interesen y preocupen por los activos computacionales del BC; además, de transmitir estos conocimientos e inquietudes del ambiente computacional a sus subalternos, tales como la existencia de estas vulnerabilidades y posibles soluciones para evitar que se materialice el riesgo.

- *Comunicación oficial a los funcionarios de la institución que participarán de los cursos:* una vez contratados los instructores, definido el cronograma y conformados los grupos, será responsabilidad de la UC comunicar a los participantes el día, la fecha, la hora y el lugar donde se impartirán los cursos, con dos semanas de anticipación como mínimo.

Además, se propone definir un plan de capacitación a futuro, de refrescamiento y actualización de los conocimientos impartidos durante esta primera etapa de capacitación por lo menos cada 2 años con una duración de un día máximo, en todos los temas propuestos en PROCAFI, ya que la tecnología avanza rápidamente y con ella, los nuevos tipos de ataques al ambiente de tecnología de información.

- ***Adquirir una técnica o mecanismo de firma digital con autoridad certificadora***: PROCAFI estará compuesta por 3 opciones de firma digital. Cada una de las propuestas contendrá:

  - Descripción del software

- Características y ventajas del software

- Desventajas o debilidades que posea el programa

- Requerimientos de hardware y de software

- Si ofrece certificación o tiene convenio con alguna autoridad certificadora.

Las empresas de más renombre y experiencia, y que incluso premios y menciones honoríficas han recibido por la calidad de los productos que ofrecen son: RSA, Verisign y Kyberpass.

RSA ofrece al público dos herramientas que permiten encriptar la información que se transmite por medio del correo electrónico con distintos alcances de protección; entre ellos RSA Keon y E-Sign. Para más detalle del producto, visitar www.rsasecurity.com

Verisign por su parte, posee una herramienta llamada Digital Ids, que ofrece firmado de correos electrónicos y encriptación del contenido del mensaje. Este producto lo puede encontrar en la siguiente dirección: www.verisign.com

Kyberpass brinda una herramienta llamada Kyberpass Secure E-Mail, que incluye: validación de firmas digitales en tiempo real, mapeo automático de firmas digitales, facilidad para administrar las tareas y políticas de seguridad, así como soporte fácil y transparente al usuario, cambio de clave cuando el usuario lo desee, entre otros. Para mayor información, acceder la página web: www.kyberpass.com

A continuación se presenta un cuadro con las características que posee cada uno de los productos mencionados anteriormente, con el fin de que la empresa compare y analice que opción se ajusta más a sus necesidades:

Tabla N° 3

Resumen Comparativo de Productos de Firma Digital				
Nombre y Descripción del Software	**Características y Beneficios**	**Desventajas del Programa**	**Requerimientos Mínimos de Hardware y Software**	**Autoridad Certificadora**
RSA Keon Es una solución para la seguridad del correo electrónico.	Administra identidades o cuentas de correo. Permite firmar digitalmente los mensajes. Permite la encriptación de mensajes. Fácil y rápido de usar. Posee una fuerte interoperabilidad con Microsoft 98 y 2000, además de Exchange Server 5,5.	Solamente funciona para el correo electrónico de Microsoft Outlook.	No se especifican requerimientos de hardware. Se requiere software Microsoft Outlook 98 o 2000 y servidor Exchange Server versión 5,5.	No indica.

RSA E-Sign Es una solución de firma digital que encierra las transacciones electrónicas, habilitando entre las organizaciones la rapidez y eficiencia en sus procesos de negocio.	Soporta certificados públicos por medio de Autoridades Certificadoras. Se ampara a la variedad de leyes y de firma digital. Provee eficiencia mejorada.	No indica.	No se especifican requerimientos de hardware Requiere sistema operativo Win 98/2000/NT 2da edición; Win NT 4.0 con SP6a; Win 2000 Professional con SP2; Win XP Profesional. Además, Internet Explorer 5.01, 5.5 y 6.0; Netscape 4.7.x y 6.x.	Sí.
Digital IDs for Secure E-Mail Protege los correos de las amenazas del mundo por medio de firma digital.	Permite autenticar los mensajes que envía por medio de una firma digital personal. Encripta el mensaje enviado por medio de una clave personal.	No indica.	No indica.	No indica.

Kyberpass Secure E-Mail Software para validar el correo electrónico por medio de firmas digitales.	Permite la validación de firmas digitales en tiempo real. Hace mapeo automáticos de firmas digitales. Facilidad para administrar las tareas y políticas de seguridad. Brinda un soporte fácil y transparente al usuario. Permite un cambio de clave cuando el usuario lo desee.	No indica.	No indica.	No indica.

- ***Capacitar al usuario en la herramienta adquirida***: una vez adquirida la herramienta de firma digital, es necesario capacitar a todo el personal que vaya a usarla para que sea utilizada de la mejor manera y se aprovechen los beneficios que ofrece.

6.6 Conclusiones

Para finalizar, se espera que al menos algunas de las soluciones presentadas en PROCAFI sean implementadas en la empresa, con el fin de brindar mayor seguridad, confiabilidad, confidencialidad y autenticación de los datos que acostumbra transmitir por medio del correo electrónico.

Se debe tener en cuenta que cada día tenemos más obligación de garantizar la integridad y confidencialidad de la información, ya que vivimos en una sociedad corrupta, y lo peor es que esta corrupción cada vez va en aumento. Continuamente aparecen nuevas debilidades en el área de seguridad de sistemas, que a la vez se convierten en riesgos potenciales para todas aquellas empresas que manejan sus operaciones y toma de decisiones por medios electrónicos.

Debemos estar preparados en todo momento en caso de que nos ataquen. El peor pensamiento que lleva al fracaso a toda persona y con mucho más razón a una institución, es aquel que dice: "...aquí nunca ha pasado nada, así que mientras no pase, yo no pienso actuar...". A esas personas les diría: ¡Aténgase al santo y no le rece! No debemos esperar a que nos pase algo para actuar, sino que debemos estar siempre prevenidos, ya que los beneficios de actuar en forma preventiva son mayores que los de actuar cuando los problemas se hayan presentado, ya que a la postre, el dinero que uno invierte en la prevención de los posibles daños de algún activo, en este caso de la información, es mucho menor que el que se invierte en la corrección de un desastre, debido a que las consecuencias no sólo radican en aspectos monetarios, sino que también afectan aspectos de imagen de la

empresa, pérdida de confianza de los clientes, negación del servicio al cliente (el cual, dependiendo de la orientación comercial de la empresa, puede ser catastrófico), entre otros.

El que arriesga gana, el que persevera triunfa, el que tiene un pensamiento futurista y preventivo, siempre irá a la vanguardia. Por eso, no descuidemos nuestro patrimonio, cuidémoslo ahora que lo tenemos, porque cuando decidamos actuar, puede ser muy tarde.

BIBLIOGRAFÍA

Bibliografía Consultada

ACEVES, Juan Manuel. Criptografía 102: PKIs y Firmas Digitales. San José, Costa Rica, 5a. Conferencia Anual Latin America CACS 2000. San José, Costa Rica, del 16 al 19 de octubre de 2000.

ANDER, Egg, Ezequiel. Metodología de Investigación. San José, Costa Rica, Publicación Interna de la ULACIT, 1992.

ARELLANO, Jaime. Elementos de la Investigación. San José, Costa Rica, EUNED, 1990.

BEST, John. Metodología de Investigación. San José, Costa Rica, Publicación Interna de la ULACIT, 1992.

Book Review Digital Signatures Security and Controls. 3 de octubre, 2002. Disponible en: http://www.isaca.org/bkr_dig.htm

Cryptographic Standards and Validation Programs at NIST). 6 de noviembre, 2002. Disponible en: http://csrc.nist.gov/cryptval/

Digital IDs. 10 de abril, 2003. Disponible en: http://www.verisign.com

DIGITAL SIGNATURES Global Knowledge Network Net Centric (Intranet-Extranet-Internet) Control & Security. 3 de octubre, 2002. Disponible en: http://www.isaca.org/gir/catDspl.cfm?catID=5&catName=Net%20Centric%20%28Intranet%2FExtranet%2FInternet%29%20Control%20%26%20Security

Digital Signature Trust Guaranteeing Identity in Digital Transactions. 6 de octubre, 2002. Disponible en: http://www.digsigtrust.com/home.html

DSA, RSA, ECDSA (FIPS 186-2); SHA-1 (FIPS 180-1). 6 de noviembre, 2002. Disponible en: http://csrc.nist.gov/cryptval/dss.htm

Ejemplo de fraude por correo electrónico en Nigeria. 21 de abril, 2003. Disponible en: http://www.zone-h.org/nigerianfraud

GARZA Roche, Regina. Auditoría, Control y Seguridad de eCommerce. 5a. Conferencia Anual Latin America CACS 2000. San José, Costa Rica, del 16 al 19 de Octubre de 2000.

GIL, Pacheco Rufino. 105 Años de Vida Bancaria en Costa Rica. Costa Rica, Editorial Costa Rica, 1974. 410 p.

HERNÁNDEZ, Roberto et al. Metodología de la Investigación. México, Mc Graw Hill, 1999.

KENDALL, Julie y Kenneth. Análisis y Diseño de Sistemas. México, Prentice Hall-Hispanoamericana S.A., Tercera Edición, 1997.

Kyberpass Secure E-Mail. 10 de abril, 2003. Disponible en: http://www.kyberpass.com

Lista de Seguridad Informática - SEGURINFO [segurinfo@acis.org.co]. Documentos en Español - Seguridad Informática. En SEGURINFO. 2 de abril, 2003; 8:54. Disponible también en: http://www.criptored.upm.es/paginas/docencia.htm#gteoria

news@sandfordtechnology.com. Security and Technology Newswire - July 2002. 10 de julio, 2002; 19:24. Disponible también en: http://www.sandfordtechnology.com

noticias@hispasec.com. una-al-dia (01/12/2002) Nuevo resumen trimestral del CERT. En Hispasec. 1 de diciembre, 2002; 14:25. Disponible también en: http://www.cert.org/summaries/CS-2002-04.html

PARKER, Timothy. Aprendiendo TCT/IP en 14 días. México, Prentice Hall Hispanoamericana, S.A., 1995. 414 p.

PRICEWATERHOUSECOOPERS. Internet Actual. 5a. Conferencia Anual Latin America CACS 2000. San José, Costa Rica, del 16 al 19 de Octubre de 2000.

RODRÍGUEZ Prieto, Amador. Protección de la Información Diseño de Criptosistemas Informáticos. Madrid, España, Editorial Paraninfo S.A., 1985. 251 p.

RSA E-Sign. 10 de abril, 2003. Disponible en: http://www.rsasecurity.com

RSA Keon. 10 de abril, 2003. Disponible en: http://www.rsasecurity.com

Seguridad en Internet. 27 de octubre, 2002. Disponible en: http://www2.ing.puc.cl/~jnavon/IIC3582/AVillal.html

SENN, James A. Análisis y Diseño de Sistemas. México, McGraw-Hill, Segunda Edición, 1993.

SHELDON, Tom, y otros. LAN Times, Enciclopedia de Redes Networking. Madrid, España, McGraw-Hill/Interamericana de España, S.A., 1994. 1117 p.

SHELDON, Tom et al. LAN Times, Guía de Interoperabilidad. Madrid, España, McGraw-Hill/Interamericana de España, S.A., 1995. 404 p.

SOLEY Güell, Tomás. Compendio de Historia Económica y Hacendaria de Costa Rica. San José, Costa Rica, Editorial Soley y Valverde, 1940. 199 p.

ZORRILLA Arena, Santigo y TORRES Xamar, Miguel. Guía para Elaborar la Tesis. México, McGraw-Hil Interamericana de México S.A de C.V., 1992. 109.