ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Instituto de Ciencias Matemáticas

Auditoria y Control de Gestión

"Esquemas de Seguridad de Correo Electrónico"

TESIS DE GRADO

Previa a la obtención del Título de:

AUDITOR EN CONTROL DE GESTIÓN

Presentada por:

Betsabeth Gabriela Salazar Almeida

GUAYAQUIL – ECUADOR

Año

2007

AGRADECIMIENTO

A Dios por todas sus bendiciones, su ayuda, protección y dirección durante toda mi vida.

A mis padres con todo mi amor y admiración por darme su apoyo y fortaleza en todo momento a quienes debo y agradezco cada uno de mis logros.

A mis hermanos por ser mi ejemplo a seguir, mi espejo cada mañana y por brindarme su apoyo en los momentos más oportunos.

Agradezco a todos los profesores del ICM por impartirme sus sabios conocimientos y de manera especial a mí Directora la Ing. Alice Naranjo por su valiosa ayuda y dedicación en la realización de esta Tesis.

A mi enamorado, a mis amigos y a todas las personas que con su apoyo incondicional hicieron posible este trabajo.

DEDICATORIA

A DIOS

A MIS PADRES

A MIS HERMANOS

TRIBUNAL DE GRADUACIÓN

Ing. Washington Armas
DIRECTOR DEL ICM
PRESIDENTE

Ing. Alice Naranjo
DIRECTORA DE TESIS

Ing. Dalton Noboa
VOCAL

Ing. Soraya Solis
VOCAL

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesis de Grado, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL"

(Reglamento de Graduación de la ESPOL).

Betsabeth Gabriela Salazar Almeida

RESUMEN

El presente trabajo nos muestra, que debido al auge alcanzado por las comunicaciones electrónicas y consecuentemente por las transacciones económicas derivadas de ellas, se ha conseguido despertar un interés por dotar a las mismas de condiciones fundamentales de seguridad, que las haga confiables, aumentando así el número de negocios concretados por el correo electrónico, protegiendo de esta manera la información contra amenazas tales como la pérdida, la libre divulgación, la manipulación, etc. Es ahí donde se ve la necesidad de Seguridad de Correo Electrónico permitiendo así que la información transmitida sea confiable e íntegra. Para ello, disponemos de diversas herramientas que permiten maximizar la seguridad de nuestro correo electrónico de forma efectiva.

Nosotros como usuarios debemos conocer y estar preparados para hacer frente a los cambios tecnológicos y así salvaguardar la integridad de la información que viaja por correo electrónico

Como podremos observar, la idea principal de este trabajo es dar una visión clara de las medidas de seguridad de correo electrónico que podemos aplicar, para asi minimizar los riesgos.

ÍNDICE GENERAL

Pág.

III. FUNDAMENTACIÓN NORMATIVA Y/O ESTÁNDARES EN AUDITORIA DE SISTEMAS

IV. CASO PRÁCTICO: EVALUACIÓN DE SEGURIDAD DE CORREO ELECTRÓNICO

ANEXOS

GLOSARIO

BIBLIOGRAFÍA

ABREVIATURAS

ASCII	American Standard Code for Information Interchange
ISP	INTERNET SERVICE PROVIDER
TCP	Transport Control Protocol
IP	Internet Protocol
LAN	Local area network
ICANN	Internet Corporation For Assignet Names and Numbers
TLD	Top Level Domain
ccTLD	County Code Top Level Domain
NIC	Network Information Center
DNS	Servidores de Nombre de Dominio
NIST	National Institute of Standard and Technology

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

Introducción

El correo electrónico ha ido evolucionando con el pasar de los años tanto así, que en la actualidad decimos que es un recurso básico con un funcionamiento fácil y sencillo, es un servicio de mensajería electrónica que tiene por objeto la comunicación no interactiva de texto, datos, imágenes o mensajes de voz entre un "originador" y los destinatarios designados que se desarrollan en sistemas que utilizan equipos informáticos y enlaces de telecomunicaciones. El correo electrónico sobrepasa fronteras y soberanías de cada región, con una rapidez y facilidad asombrosa.

Con el progreso constante del correo electrónico nace el derecho a la privacidad y la protección de los mensajes electrónicos de los usuarios, ya que estos constantemente se ven vulnerados por personas inescrupulosas con los conocimientos necesarios en informática para poder hacerlo.

El presente trabajo centra su objetivo en la seguridad del correo electrónico, en el primer capítulo se hace un recorrido de las diferentes formas de comunicación hasta llegar al correo electrónico. Así mismo se da a conocer sus principales características, ventajas, desventajas en comparación con el correo tradicional.

En la segunda parte se indican algunos conceptos básicos relacionados con la seguridad de correo electrónico así como la importancia de la misma en la actualidad.

En el tercer capítulo se efectúa un análisis claro y resumido de ciertos estándares relacionados con la seguridad de correo electrónico como: COBIT, ISO 17799, COSO, SAC, LEY DE COMERCIO ELECTRÓNICO.

En el cuarto y último capítulo se realiza una Evaluación de Seguridad de Correo Electrónico en el cual se dan a conocer a la Gerencia de TecMotors S.A. las conclusiones y recomendaciones para la mejora del mismo.

CAPÍTULO 1

1. Antecedentes

En el presente capítulo se dará a conocer como la comunicación ha evolucionado desde las formas más primitivas de expresión hasta el uso de sofisticadas tecnologías que permiten una comunicación entre una o varias personas, cada vez más instantánea. De igual manera se dará a conocer algunas características del correo electrónico así como las ventajas, semejanzas y diferencias con el correo tradicional. También se mostrará un análisis de las vulnerabilidades que el mismo presenta.

1.1 Evolución Histórica del Correo Electrónico

Los seres humanos nos diferenciamos de los animales por nuestro razonamiento, lo cual en base a ciertos estudios y teorías psicológicas se manifiesta por medio del lenguaje; es decir, la habilidad que tenemos para comunicarnos entre nosotros, que nos permite exteriorizar nuestros pensamientos. Las formas más primitivas de comunicación implicaban la presencia física de ambas partes de la

comunicación; tanto emisor como receptor debían estar juntos al establecer la comunicación.

Con la aparición de la escritura 1.500 años A.C. esto cambió totalmente, tanto así que ya no era necesaria la presencia de ambas partes de la comunicación para poder tener una; pero en cambio se necesitó del transporte físico del mensaje, que generalmente era en papel, y así nació un primer concepto de portadora de un mensaje.

Los antiguos Incas implementaron un ingenioso sistema de transmisión de mensajes este consistía en utilizar personas que recorrían la extensión de su reino llevando consigo y pasando de boca en boca el mensaje hasta que éste llegara a su destinatario.

Dicho sistema de correo se parece bastante al que actualmente funciona, pero un poco más sofisticado, es decir, con una legislación que lo regula y protege; pero la idea fundamental sigue siendo la misma, 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.

Cuenta una historia que mientras Samuel Morse viajaba alrededor de Europa, su madre, en Estados Unidos, cayó gravemente enferma, inmediatamente su familia intentó contactarlo por medio de una carta pero para cuando ésta llegó a él su madre ya había muerto. Este hecho condujo a Morse llevar a cabo una profunda investigación sobre las propiedades de la transmisión de la corriente eléctrica a través de un cable, la cual finalizó con la invención del telégrafo en el año de 1835. Y éste fue el primer medio de transmisión eléctrico del que se tiene registro. Pronto las líneas telegráficas se extendieron por todo el mundo y cuando estas líneas no podían establecerse se recurrió a la radio transmisión; ahora se contaba con un medio de transporte rápido y, relativamente, barato. El telégrafo fue casi totalmente reemplazado 40 años después por el revolucionario invento de Graham Bell, el teléfono, tan revolucionario que actualmente sigue vigente. Este sistema tiene una escala global y conecta una colosal jerarquía de conmutadores, multiplexores y conversores de señales que permiten una comunicación a cualquier lugar del mundo.

Este sistema se acopla perfectamente para la transmisión de voz de un extremo al otro o casi perfectamente, pero para la transmisión de datos resultaba poco satisfactorio por lo que se construyó paralelamente a la red telefónica la red de telex, que a mediados de

los años 20 nació 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, también se proporcionaba una inherente seguridad ya que éstas máquinas para establecer una comunicación tenían una especie de protocolo de acuerdo (handshaking). A medida que pasaron los años la información fue ganando mayor importancia en la vida empresarial y en los años 60 las grandes compañías iniciaron la instalación de grandes computadoras y a conectar terminales “bobas” a ellas; teniendo así acceso a su información y a sus otros recursos, memoria, procesador, dispositivos de E/S, etc.

Figura 1.1 Funcionamiento del servidor hacia las terminales.

Esta gran computadora o Mainframe hacía las veces de servidor hacia las terminales que servía, de ahí que se la llamaría Server (**Servidor**) y dependiendo de sus servicios se la denominaría File-Server (**servidor de archivos**), Print-Server (**servidor de impresión**). Posteriormente a los usuarios se les hizo evidente la posibilidad y necesidad de intercambiar datos y hacer así la interacción más

dinámica y eficiente, sin la necesidad de que los usuarios tuvieran que estar físicamente juntos, así surgió la implementación de un Mail-Server (**servidor de correo**) como el que se muestra en la Figura 1.1.

A su vez, y simultáneamente 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 sus estudiantes se puso en marcha la ARPANET, la predecesora en cierta manera de la INTERNET.

Posteriormente la historia registra que en Octubre de 1969 Leonard Kleinrock profesor de informática manda el primer mensaje de e–mail a un colega de Stanford.

Más tarde en Marzo del año 1972 Ray Tomlinson, autor del primer software para correo electrónico, elige el símbolo @ para direcciones. Él pertenecía a la BBN (Bolt Beranek & Newman), una empresa que constituía uno de los 15 nodos existentes en aquel entonces.

La novedad consistía en que se podían enviar y recibir mensajes en un sistema de red distribuida (varias redes interconectadas), el cual se basó en un programa ya existente para el envío de correo electrónico

entre ordenadores de una misma red (llamado SNDMSG) y en otro programa experimental de envío de archivos (llamado CPYNET).

En 1975 tuvo amplia repercusión un e-mail enviado por la reina Isabel II del Reino Unido, y al año siguiente se creó la primera empresa de servicios de mensajería electrónica, OnTyme, aunque ésta no tuvo mucho éxito, debido al poco número de usuarios de redes distribuidas.

En 1982 se creó el primer enlace exitoso entre 25 ciudades.

En 1983 El Collage de Colby en Waterville una institución de educación superior asigna cuentas de correo a todos sus usuarios y posteriormente en 1994 el New Yorker publica una entrevista sobre correo electrónico con Bill Gates, quién describe: “nuestro correo es totalmente seguro”.

Consecuentemente, con la llegada de la oferta en los precios de las computadoras personales, la idea de red cambió totalmente tanto así que hoy no hablamos más de procesamiento centralizado, sino de procesamiento distribuido, cada día más empresas instalan LANs de computadoras personales, y con la posibilidad de conectar varias LAN surge inevitablemente una gran red mundial, la INTERNET.

El correo electrónico se creo con la finalidad de permitir a distantes colegas que trabajan para una empresa que tiene una LAN, trabajar juntos, es decir, compartir experiencias, intercambiar ideas y proyectos. Luego se vio la posibilidad de hacer que un usuario pudiera acceder a este mismo servicio en forma remota, es decir sin estar conectado a la red, en realidad conectado por medio de una línea telefónica y un MODEM, como se muestra en la figura 1.2.

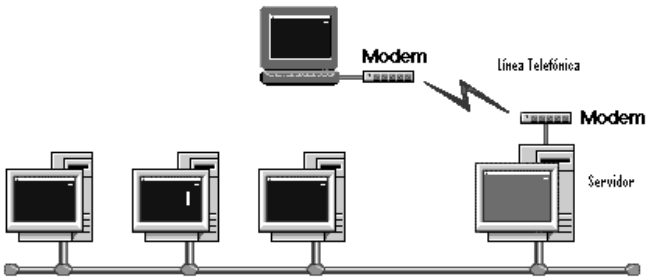


FIGURA 1.2 Conexión mediante vía telefónica y MODEM.

El siguiente paso en la expansión era conectar varias LAN para que intercambiaran los mensajes dirigidos a sus usuarios. Figura 1.3**.** Dicha implementación incluye una dificultad adicional, cada servidor de correo debe conocer sus usuarios locales (conectados a su red) y los remotos (de la otra red), así se introducen las direcciones de correo y los dominios.

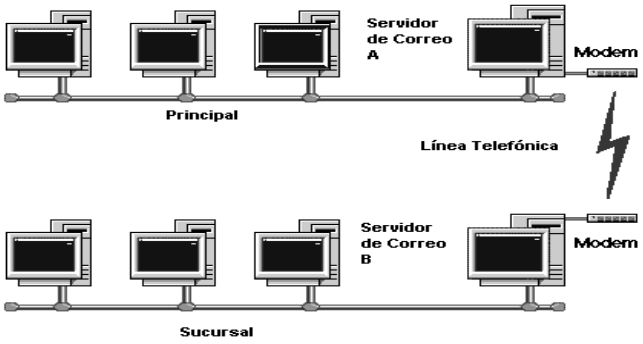


FIGURA 1.3 Conexión de varias LANs

En un principio, enviar un mensaje de correo electrónico consistía en un usuario escribiendo el mensaje en un programa específico de aplicación, en contraposición con el servidor de correo, que era de un editor de texto, posiblemente un corrector ortográfico, una base de datos de la forma de una libreta de direcciones, un administrador de archivos (los mensajes recibidos o no enviados) y un módulo de comunicaciones para poder transferirlos.

El mensaje se quedaba guardado en el mail-server hasta que el usuario destinatario se conectara con él y solicitara los mensaje que le tuviera pendientes, el proceso inverso de envío de mensajes era muy similar cuando el usuario terminara de escribir su mensaje y especificara la dirección del destinatario, se conectaba con el servidor a fin de almacenar el archivo hasta que el destinatario lo solicitara. Cuando el servidor está conectado a sólo una red, la única limitación

de la dirección de destino, además de no permitir espacios en blanco, era que cada dirección debía identificar de forma unívoca a cada usuario. Con una LAN esta restricción es fácil de aplicar pero con más de una la situación es más compleja; así se introducen los dominios de los usuarios que representan a qué servidor pertenecen y que tienen la forma de una dirección válida, es decir sin espacios en blanco ni caracteres prohibidos; para diferenciar el nombre del usuario de su dominio se adoptó el carácter "@" que significa "en" (“at” en ingles) entonces la dirección Felix@Servidor.A se puede leer como "Felix en Servidor.A"

El problema se dió cuando se intentaron conectar servidores de correo que utilizaban productos comerciales distintos, que aunque conceptualmente hacían lo mismo eran totalmente diferentes. El hecho era que hasta ese momento no existía un estándar que reglamentara cómo debían implementar los productos este servicio. La necesidad de una norma se hizo más evidente cuando redes totalmente distintas comenzaron a conectarse mediante la INTERNET.

Por ejemplo, una compañía multinacional, que tuviera sucursales en varios países del mundo y quisiera intercambiar e-mail tenía que contratar a un ISP (INTERNET SERVICE PROVIDER) y así tener

acceso ilimitado a la INTERNET. Este arreglo podría tener la forma de la figura 1.4.

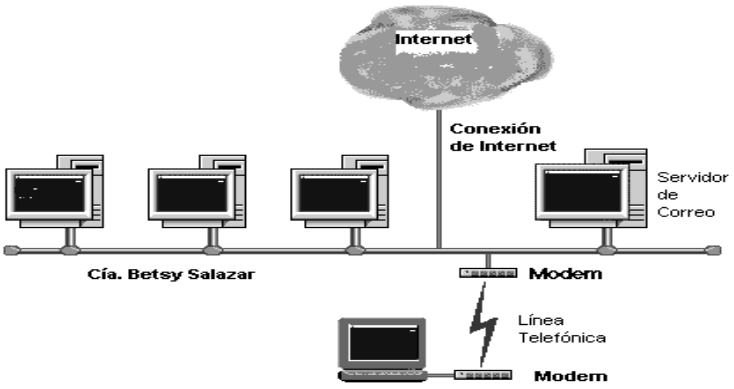


FIGURA 1.4 Acceso a Internet

Desde entonces el correo electrónico se ha convertido en el servicio más utilizado por los usuarios de Internet y por lo tanto uno de los más populares.

El correo electrónico es un recurso básico compitiendo o integrando a otros medios como el teléfono y hasta el fax, ya que su funcionamiento es simple; con un programa informático semejante a un procesador de textos se escribe un mensaje y se indica la dirección electrónica donde desea enviarse. De allí queda depositado el mensaje en otro ordenador o buzón hasta que el destinatario lo lea.

En la siguiente tabla se resumen datos históricos interesantes del correo electrónico.

TABLA I

HITOS EN LA HISTORIA DEL CORREO ELECTRÓNICO

Octubre, 1969	Leonard Kleinrock, un profesor de informática de la Universidad UCLA manda el primer mensaje de e-mail a un compañero en Stanford.
Marzo, 1972	Ray Tomlinson, autor del primer software para correo electrónico, elige el símbolo @ para direcciones.
Febrero, 1975	Reina Isabel II del Reino Unido es la primera jefa de estado en enviar un mensaje de e-mail
Otoño, 1976	Se creó la primera empresa de servicios de mensajería electrónica OnTyme.
1982	Se creó el primer enlace exitoso entre 25 ciudades.
Septiembre, 1983	El College de Colby en Waterville, Maine es una de las primeras instituciones de educación superior en asignar cuentas de correo a todos sus estudiantes.
Enero, 1994	El New Yorker publica una entrevista en la que Bill Gates dice: "nuestro correo es totalmente seguro".
1996	Lanzamiento de Hotmail.
1997	Aparición del SPAM (publicidad masiva no solicitada vía correo electrónico)
2002	Aparición del correo electrónico vía celular.

Con la aparición de la INTERNET se hace realidad el sueño de desaparecer las fronteras físicas, crear un espacio donde el tiempo es un concepto muy flexible, introducir las ideas de tiempo y distancia cero; aunque todavía estamos lejos de la implementación de semejante empresa, estamos en camino y el correo electrónico es una de las herramientas que nos llevará a conseguir tan anhelado sueño.

A esta transformación que ha sufrido la comunicación en la sociedad de la información, se refiere Fernández Esteban cuando dice:

> **"***Los nuevos medios de comunicación electrónicos modifican radicalmente el intercambio de información que deja de ser dependiente del tipo de transporte para ser un proceso en el que la información se mueve a la velocidad de la luz. Las redes telemáticas permiten que mucha información que era previamente inaccesible y sin valor debido a que estaba en un lugar remoto, se convierta en útil y valiosa a través de la Red. Así, el acceso a bases de datos remotas y la transmisión de datos, sonidos e imágenes en tiempo real a cualquier parte del planeta, son ya hechos consumados. Del mismo modo, personas con las cuales se podía mantener una relación a distancia pueden ser ahora compañeros de trabajo que interactúan de un modo eficaz."* [Fernández Esteban]

1.2 Correo Electrónico y su importancia

El correo electrónico es un servicio de red que permite a los usuarios recibir y enviar mensajes. Se lo conoce también como e-mail, dicho

término se deriva de Electronic Mail, “correo electrónico”; “mensajería electrónica” es un significado más restrictivo, que suele referirse a mensajes enviados desde dispositivos de comunicaciones, como teléfonos celulares [(1)] .

Un mensaje de correo electrónico puede estar compuesto tanto de texto como de imágenes, archivos de datos o mensajes de voz, así como de otros elementos multimedia digitalizados, animaciones o hasta vídeos. Para su composición, envío y lectura sólo se usan dispositivos electrónicos y programas (software), sin precisar, en ningún momento, de elementos físicos ajenos a los dispositivos electrónicos, como puede ser la impresión en papel, ni de la manipulación física del contenido, como ocurre en el envío o la entrega del correo tradicional.

Los mensajes de correo electrónico se codifican por lo general en formato de texto ASCII (American Standard Code for Information Interchange) que mapea caracteres alfabéticos y simbólicos a código numérico y viceversa.

[(1)] Mc Graw – Hill de Informática. Internet Manual de Referencia

Cuando se escribe un mensaje en el correo, por defecto, éste se envía en código ASCII, y ya que es un estándar universal, no tiene ningún tipo de seguridad.

El correo electrónico representa una de las primeras aplicaciones de Internet y sigue siendo la de mayor uso. Un alto porcentaje del tráfico total en el Internet se debe al correo electrónico. A continuación mostramos el número aproximado de mensajes enviados diariamente en todo el mundo.

TABLA II

TRÁFICO DE E-MAILS DEL AÑO 2003 AL 2007

Año	Billones de e-mails por día
2003	56,40
2004	71,40
2005	92,40
2006	121,00
2007	164,30

Se estima que para el año 2010 será de 200,32 billones de e-mails por día.

x	y		
año	billones de e-mail por día	x2	x*y
2003	56,4	4012009	112969,2
2004	71,4	4016016	143085,6
2005	92,4	4020025	185262
2006	121	4024036	242726
2007	164,3	4028049	329750,1

Siendo:

	x	y
media	2004,999501	94,14872525
varianza	2,5	
covarianza	53,08	

$$b1 = \frac{Co\,\mathrm{var}\,ianzaX}{VarianzaX}$$

$$bo = MediaY - b1 * MediaX$$

b1	bo
21,232	-42476,0007

Entonces, para calcular el estimado para el año 2010 sería:

bo +(b1*2010)

Siendo igual a 200,32

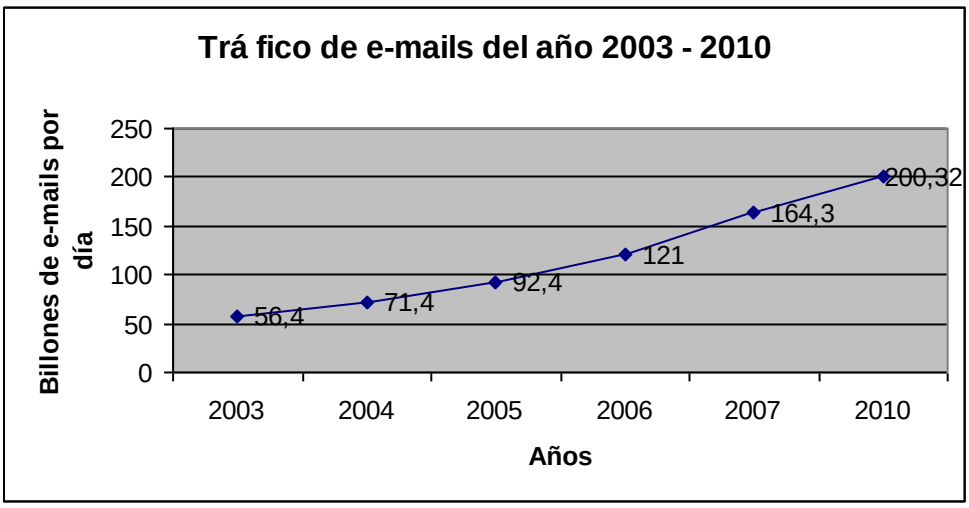


FIGURA 1.5 Tráfico de e-mails del año 2003 al 2010 del mundo
Fuente: Asociación de Usuarios de Internet – www.aui.es

El correo electrónico o servicio de mensajería interpersonal, se ha convertido en una herramienta de comunicación eficaz para los usuarios ya que ofrece una rapidez en el envío de mensajes, sin necesidad de que el emisor y el receptor estén conectados simultáneamente. Así también ha impulsado el comercio internacional facilitando el acceso a productos e información puestos a disposición de quien lo desee.

El correo electrónico es un medio de comunicación que evoluciona constantemente; esto ha permitido ofrecer un medio servicio eficiente, instantáneo, ágil y cada vez más seguro. Debido a estos muchos usuarios de Internet acceden a la Red exclusivamente atraídos por este servicio y su uso se extiende paulatinamente en el mundo. El correo electrónico y las llamadas telefónicas son los servicios más utilizado por los internautas en Ecuador, con el 97.8%. Le siguen la navegación web 85.6%, diálogos directos 58.4%, juegos 23.7%, foros o noticias con el 3.1%.

Uso de los servicios de Internet en Ecuador

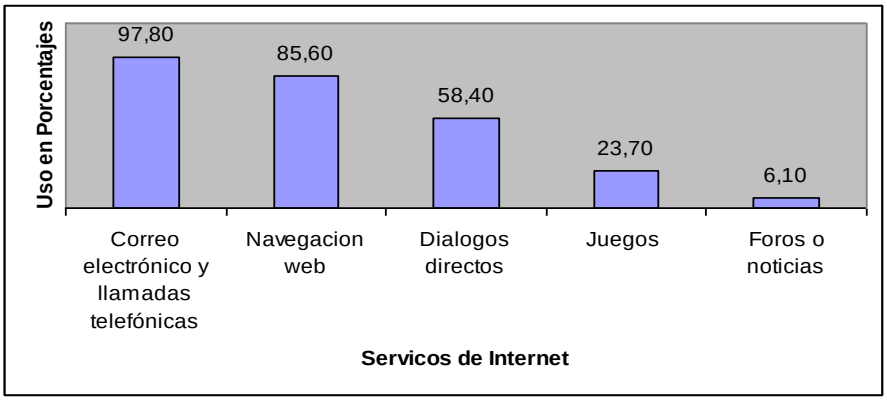


Figura 1.6 Uso en porcentajes de los servicios de Internet en Ecuador
Fuente: http://www.supertel.gov.ec/, 2007

Como podemos observar los dos primeros servicios son usados en forma creciente entre ellos el correo electrónico.

La siguiente tabla muestra a continuación el número de mensajes aproximados que se envían diariamente.

TABLA III

NUMERO DIARIO DE MENSAJES ENVIADOS

Mensajes	Personas
Ninguno	2
Uno	11
Dos	12
Tres	9
Cuatro	2
Cinco	5
De seis a nueve	1
De diez a quince	1
Más de quince	3

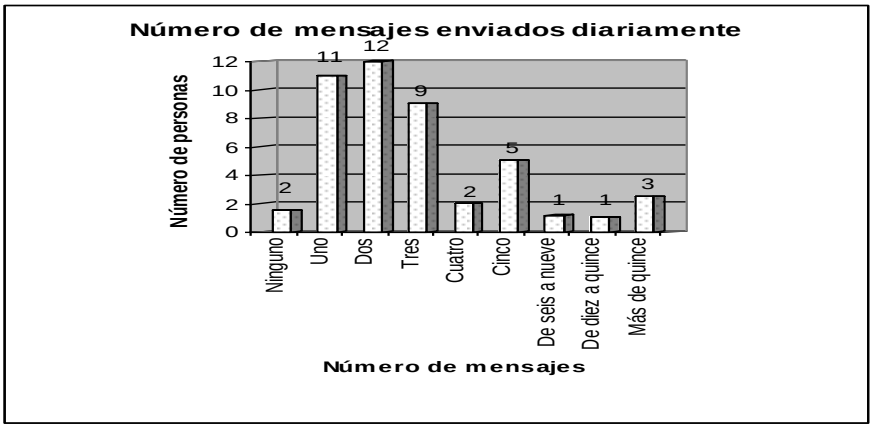


FIGURA 1.7 Número diario de mensajes enviados
Fuente: Asociación de Usuarios de Internet – www.aui.es, 2007

Podemos observar que uno, dos y tres son las cantidades más frecuentes de mensajes enviados diariamente.

Otro de los usos que se le ha adjudicado a este medio es la educación a distancia, pues ha posibilitado el contacto entre estudiantes y profesores independientemente del sitio geográfico en el que se encuentren.

El correo electrónico es como un servicio de transmisión y conducción de señales por las redes y se incentiva el uso de este medio de comunicación en las nuevas relaciones humanas y laborales [(2)] .

[(2)] Libro Verde de la Convergencia de los Sectores de Telecomunicaciones, los Medios de Comunicación y las Tecnologías de la Información (Unión Europea)

1.3 Características del correo electrónico.

Entre las principales características del correo electrónico podemos señalar las siguientes:

- **Rápido**

  A diferencia de un mensaje enviado por correo normal que puede tardar varios días en llegar a su destino, uno enviado por correo electrónico tardará regularmente solamente algunos minutos. Es decir, en un sistema de red de computadoras es indiferente para cada usuario el recibir correo ya sea de lugares físicos cercanos o lejanos.

- **Costo**

  Enviar un mensaje vía correo electrónico a un destinatario en cualquier parte del mundo tiene un costo mínimo es decir sólo el costo de acceder al servicio de Internet.

- **Asíncrono**

  No requiere la intervención del emisor y receptor al mismo tiempo. El sistema de correo electrónico no exige del emisor, una conexión en línea con el destinatario, mientras elabora su mensaje, puesto que puede utilizar un editor de texto.

- **Buzón o cuenta de correo**

  El usuario debe registrar un buzón o cuenta, en un sistema de correo electrónico que esté disponible para lo cual le asignan una dirección, la misma que debe difundirse en la correspondencia física o electrónica que envíe.

1.4 Ventajas del correo electrónico frente a otros tipos de comunicación.

El correo electrónico presenta una serie de ventajas frente a otros medios de comunicación (Teléfono, correo tradicional, personal) entre las cuales podemos mencionar:

- **Aparición de "comunidades virtuales"**

  Grupo de individuos separados geográficamente, que comparten intereses comunes.

- **Veloz.**

  Esta es la ventaja más clara. Una carta por correo ordinario puede tardar muchos días en llegar a su destino, mientras que un mensaje enviado por correo electrónico a cualquier parte del mundo, podrá ser leído en cuestión de horas, minutos e incluso

segundos (dependiendo de las conexiones existentes en el momento de enviar el correo).

- **Carece de fronteras.**

  Es posible la colaboración en un mismo proyecto de personas que se encuentran entre sí a varios kilómetros de distancia. Las fronteras y distancias desaparecen con el uso del correo electrónico. Ya que sólo es cuestión de segundos o minutos el envió de mensajes.

- **No hace falta la presencia del receptor y emisor al mismo tiempo para enviar un mensaje.**

  E-mail presenta también ventajas respecto a la comunicación telefónica. Enviaremos nuestros mensajes cuando sea conveniente para nosotros sin necesidad de tener que estar pendientes de que exista un interlocutor en el otro extremo de la conexión.

- **Servicio 24 horas.**

  Disponible las 24 horas del día, los 7 días de la semana y los 365 días del año.

- **Es económico.**

  Respecto al precio de la conexión, cabe destacar que mientras una llamada telefónica a nivel nacional o internacional puede resultar de elevado costo, el e-mail permite el intercambio de mensajes a bajo precio, aún si la otra persona con la que estemos comunicándonos esté en el otro extremo del mundo.

- **Funcionamiento sencillo.**

  Puede ser utilizado por estudiantes, amas de casa, profesionales, comerciantes, es decir, puede ser usado por cualquier persona que lo desee y necesite ya que su funcionamiento es fácil.

- **Cómodo y dinámico.**

  Cómodo porque se puede hacer uso de este servicio en cualquier parte (oficina, casa, cyber, centro comercial, etc).

  Dinámico, ya que permite la posibilidad de recibir el correo aunque no esté en el lugar donde lo usa habitualmente.

1.5 Semejanzas del correo electrónico con el correo tradicional

Entre las semejanzas con el correo tradicional encontramos las siguientes:

- **Transporte Físico del mensaje.**

  Sea cual sea el medio por el que viaje la información, el mensaje siempre requerirá un medio físico.

- **Existe emisor y receptor.**

  Debe existir un emisor y un receptor. Emisor será la persona/empresa que está enviando el mensaje mientras que receptor será la persona / empresa para quien va dirigido.

- **No se necesita de la presencia física de ambas partes.**

  Para enviar o recibir un mensaje no se requiere la presencia de ambas personas ya que los mensajes enviados se almacenarán en el buzón de entrada de cada usuario.

1.6 Diferencias con el Correo tradicional

Entre las principales diferencias podemos mencionar las siguientes:

- **Ahorra tiempo.**

  Un correo tradicional puede tardar desde 1 día o más en llegar a su destino dependiendo de la distancia mientras que un e–mail tardará segundos o minutos.

- **Fácil acceso.**

  Para acceder cada usuario a su cuenta sólo debe digitar su nombre de usuario con que esté registrado y su contraseña. Pudiendo hacer uso del mismo desde cualquier parte del mundo y a cualquier hora.

- **Confiable.**

  Si se tiene ciertas precauciones, la información que viaja por correo electrónico es confiable. Como por ejemplo; cambiar cada cierto tiempo las contraseñas y que éstas no sean fáciles de deducir, son los primeros puntos que se deben tener en cuenta para evitar que personas ajenas, accedan a nuestra cuenta de correo.

- **La dirección del remitente tiene que ser la correcta.**

  Podemos decir que en el correo tradicional para enviar una carta no es necesaria la dirección del remitente mientras que en el

correo electrónico si es necesario. Además nosotros debemos poseer una cuenta de correo para poder enviar un e-mail de lo contrario no se lo podrá hacer.

1.7 Vulnerabilidades

Una vulnerabilidad de correo es un exploit lanzado mediante correo electrónico. Un “exploit” de correo es básicamente una debilidad que puede estar incrustada en un correo, y que puede ser ejecutada sobre el equipo del destinatario una vez que reciba el correo. Esto permite al hacker eludir los cortafuegos o firewall y los productos anti-virus teniendo acceso a toda la información y contaminando nuestro equipo.

- **Falta de seguridad del canal de comunicación.**

  Los medios de comunicación rara vez se consideran seguros debido a que en la mayoría de los casos escapan a nuestro control; ya que pertenecen a terceros, resulta prácticamente imposible asegurarse totalmente de que no están siendo intervenidos. Basta con imaginar el correo tradicional al enviar una carta. ¿Quién nos asegura que en el proceso de envío ésta no haya sido leído por terceras personas o qué no se pierda en el camino?, pero no por esto debemos dejar de usar este servicio.

- **No hay garantía de que los mensajes lleguen íntegramente.**

  Sobre la integridad del mensaje desde el momento que se envía hasta cuando llegue a su destino, vale indicar la definición ofrecida por Corripio que al efecto señala:

  > *"La integridad se entiende como la fiabilidad del contenido del mensaje o documento, de forma que la información transmitida sea un fiel reflejo del dato que representa en realidad. La definición de integridad debe comprender los términos de exacta, autorizada y completa y se dirige a asegurar que los datos recibidos se corresponden exactamente con los enviados por un emisor autorizado***."** [Corripio]

  Ciertamente, la integridad se exige como un principio de seguridad del envío de la comunicación y comprende tanto la identidad entre el contenido emitido y el recibido, como la identidad de quien aparece como titular de la cuenta y quien la utiliza efectivamente.

  Es necesario que las partes tengan esa garantía de quien ofrezca el servicio de mensajería electrónica, del mismo modo que en el correo tradicional se exigía la certeza de que los envíos llegasen a su destino tal y como fueron remitidos.

Por ejemplo, es posible que al enviar una cotización a un cliente, un competidor intercepte su mensaje y modifique la oferta original antes de que llegue a manos del cliente (alteración de la información).

- **No se garantiza al remitente que el mensaje llegó a su destino**

  Cuando nosotros enviamos un correo electrónico no tenemos la seguridad de que éste llegó o va a llegar a su destino. En la actualidad no existe un medio seguro que determine si el mensaje llegó al destinatario, pero en caso que exista algún problema de comunicación o que la dirección haya sido mal digitada, el administrador de correo de forma automática enviará un mensaje al usuario indicando lo sucedido.

  Sin embargo, actualmente se parte de la hipótesis de que todo mensaje enviado fue recibido por el destinatario, pese a que es difícil de certificar con plena certeza. Aunque no hay que olvidar: ¿cuántas veces en el correo tradicional una carta se desvió de su destino ó se perdió? Internet no es una herramienta infalible pero tampoco es desechable. Por el contrario, pese a ésta y otras desventajas que poco a poco se están perfeccionando, es hoy en día el medio de comunicación más económico y eficaz.

- **Falta de privacidad de las comunicaciones.**

  El correo es protegido en su carácter de comunicación personal o privada por el secreto de las comunicaciones, por lo que en principio, su contenido es inviolable y no puede ser incautado o abierto sin intervención judicial, tal como se aplica al correo tradicional y con las excepciones indicadas para el correo laboral y administrativo.

  Como veremos más adelante, la LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRONICAS Y MENSAJES DE DATOS garantiza el secreto de las comunicaciones y sanciona a quienes no cumplan con sus disposiciones. El e-mail es fácil de usar, copiar el contenido, usurpar e intervenir por lo que su protección resulta necesaria ante el auge tecnológico.

  Al no haber garantía total de la identidad del emisor y del receptor, ni garantía de confidencialidad en el intercambio de la información, hay riesgos de que la información pueda ser interceptada por un tercero; que exista suplantación de la identidad del emisor o receptor y por ende violación de la comunicación.

La libertad y el secreto de las comunicaciones afectan a cualquier procedimiento de intercomunicación privada. El secreto de las comunicaciones protege la reserva o carácter privado de la comunicación, sea cual sea el contenido de la misma.

El correo electrónico es de acceso libre salvo en lo que respecta a medidas de seguridad que resguarden su contenido y eviten su alteración. Debe entenderse, entonces, que el ciudadano no puede solicitar intervenir un correo pero sí puede solicitar visualizar su contenido u obtener una copia del mismo si demuestra poseer un interés legítimo en la información que conste en el correo respectivo.

Por ejemplo, es posible que al enviar una lista de los próximos precios de venta al público a un distribuidor, un competidor intercepte el mensaje y mejore oferta (espionaje).

- **Suplantación de Identidad.**

  Suplantar la identidad de otra persona vía correo electrónico es sencillo, basta con conocer el usuario y contraseña de una persona para poder ingresar, acceder y hacer uso de su cuenta de correo.

Nosotros como usuarios debemos tener en cuenta ciertas precauciones al momento de digitar nuestro usuario y contraseña de correo, ya que cualquier persona podría estar pendiente y anotar o memorizarlas para posteriormente usarlas, accediendo a toda la información que tengamos almacenada y hacer uso del correo.

Por ejemplo, en el caso de enviar una cotización a un cliente, una persona inescrupulosa podría enviar un mensaje haciéndose pasar por el usuario de esa cuenta y lograr indisponerlo con el cliente (suplantación de identidad o impersonificación).

- **Difusión de contenido inadecuado.**

  Es evidente que la difusión de contenido y/o información de la organización de forma inadecuada o ilegítima a través del correo electrónico, puede afectar sensiblemente los derechos de los receptores así como los de terceros, poniendo en riesgo a la empresa.

- **Falta de confiabilidad de la información.**

  Confiabilidad es saber que la información que estamos recibiendo proviene de la fuente original, que no ha sufrido ninguna clase de manipulación.

  En la actualidad contamos con firma electrónica, certificación de firma electrónica, entre otros medios de seguridad que hasta cierto punto pueden garantizar que la información llegue a su destino, minimizando así los riesgos a la seguridad de correo electrónico.

  Debemos tener en claro que a medida que la tecnología avanza, las medidas de seguridad deben avanzar conjuntamente o paralelamente ya que al igual que hay peritos desarrollando software de seguridad existen otras personas que trabajan para burlar todas estas seguridades.

- **Acceso a las cuentas de correo.**

  Sobre la seguridad del correo podemos decir que cualquier persona que conozca nuestra clave de acceso puede hacer uso de él libremente. . En este caso la seguridad depende del usuario ya que se debe tener medidas preventivas minimizando asi estos riesgos.

Por ejemplo, darse cuenta de que nadie esté observando al momento que digitamos nuestra clave, no asignar claves tan sencillas, no anotarlas, entre otras. Todos estos puntos nos ayudarán a preservar la seguridad de nuestro correo.

Así mismo cualquier persona con los conocimientos necesarios en informática puede ingresar a nuestro correo y manipular toda la información que tengamos.

- **Correo No Deseado.**

  Al igual que en el correo tradicional, en el correo electrónico llegan constantemente propagandas de diferentes tiendas comerciales a nuestros buzones de entrada ofreciendo sus diferente productos o servicios.

  En la actualidad existen varios tipos de correo no deseados los cuales los presentamos en la siguiente tabla.

TABLA IV
TIPOS DE SPAM

Porcentaje	Tipo	Descripción
10%	Salud	Estos ofrecen o aconsejan productos y/o servicios relacionados con la salud. Ejemplo; tratamientos médicos, cirugías, etc.

9%	Internet	Son los servicios que ofrecen ciertos proveedores de Internet. Ejemplo; diseño Web, programas de filtrado de SPAN.
6%	Otros	Son correos que obviamente no pertenecen a ninguna de las anteriores características mencionada.
5%	Ocio	Son aquellos que ofrecen premios, juegos, descuentos en actividades de ocio. Ejemplo; Cruceros, casinos online, juegos.
5%	Fraude	Son aquellos mail que aparentan ser de importante empresas, pero que en realidad no lo son. Esto se conoce con el nombre de "Phising". Estos mensajes suelen usar trucos para que los usuarios revelemos información personal. Como dirección de correo, contraseñas, etc. Por ejemplo; verificación de tarjetas de crédito, actualizaciones de facturas.
3%	Políticos	Por lo general estos mensajes piden donaciones de dinero al partido o a una causa específica a cambio de productos relacionados con la campaña. Ejemplo; elecciones.
2%	Religiosos	Son aquellos que contienen información o servicios religiosos. Ejemplo; astrología, religión organizada.

Fuente: Asociación de Usuarios de Internet - www.aui.es, 2007

- **No hay forma de garantizar que el mensaje ha sido leído por su destinatario.**

  En general, no hay forma de saber si un mensaje ha sido leído por el destinatario. Sin embargo, hay una orden que puede dar esta información. Esta se llama finger y presenta información pública sobre cualquier usuario en la Internet (Existen lugares que

prohíben a finger acceder a sus sistemas. Esto se debe a razones de seguridad o simplemente para disminuir las peticiones de red que llegan al sistema)

Ciertas versiones de finger informan si el usuario tiene correo sin leer. Por ejemplo, supongamos que se ha enviado un correo a un amigo cuya dirección es silver@fuzzball.ucsb.edu se puede obtener información de éste utilizando: finger silver@fuzzball.ucsb.edu. Si el sistema finger en su computadora presenta información de correo, la salida contendrá algo como esto:

New mail received Thu Apr 1 12:39:22 1994;
Unread since Thu Apr 1 08:16:11 1994.

Actualmente esta utilidad viene incorporada en algunos sistemas de correos y permiten la confidencialidad de lectura de un mensaje.

1.8 Impacto en las empresas

El correo electrónico se ha convertido en una herramienta empresarial fundamental debido a que los empleados utilizan el correo electrónico para fines laborales, ente las que se incluye:

- Informes generales de la empresa.

- Comprobación de información sobre reuniones.
- Delegación de tareas.
- Intercambio de información.
- Desarrollo de proyectos.
- Envio de informes, entre otras.

Pero así también tiene sus desventajas debido a que los trabajadores además de emplearlo como medio de comunicación laboral también lo utilizan para realizar otras actividades como, por ejemplo:

- Leer y contestar correos no deseados.
- Almacenamiento de información innecesaria.
- Envio de mensajes cadenas.
- Envio de mensajes personales.
- Entre otros.

Ocasionando:

- Saturación del servidor de correo debido a la cantidad de mensajes enviados y recibidos imposibilitando asi el abrir un mensaje y la acción posterior correspondiente.
- Incremento en los costos de la empresa (perdida de dinero).
- Perdida de tiempo.
- Cometer errores debido a la falta de concentración.

- Desarrollar adicción al correo electrónico.
- Entre otros.

Por estos y otros motivos las empresas necesitan comenzar a desarrollar e implementar políticas de seguridad de correo electrónico para asi optimizar este medio de comunicación.

Entre algunos de las agresiones que ha sufrido el correo electrónico podemos mencionar la que tuvo Hotmail el 30 de agosto de 1999, después de recibir informaciones sobre ataques de hackers a algunos de sus servidores, la empresa Microsoft desconecta su sistema durante aproximadamente 2 horas. Los hackers habían entrado en cuentas Hotmail a través de proveedores ajenos sin usar ninguna contraseña. Las cuentas de correo electrónico gestionadas por el Hotmail fueron vulnerables durante varias horas, y cualquiera podía ver los mensajes de otro, introduciendo tan sólo el nombre del usuario.

CAPÍTULO 2

2. MARCO TEORICO

En el presente capítulo se dará a conocer algunos conceptos básicos sobre correo electrónico los mismos que ayudarán a comprender los esquemas de seguridad, mostrando así la importancia de preservar la seguridad del correo electrónico. Así también se dará a conocer los diferentes programas utilizados por las empresas para salvaguardar su información vía e-mail. La mayor parte de los programas para empresas incluye diversos niveles de seguridad y opciones de privacidad, servidores de seguridad, filtros de correo electrónico no deseado y otras funciones. De igual manera se mostrará un análisis de la metodología Delphi. Todos estos temas son los que se exponen a continuación.

2.1 Dominios

Es el nombre, patente o razón social en la Web. Es algo así como la dirección única mediante la cual alguien o alguna empresa será ubicada.

Esta dirección es asignada por varios organismos o empresas y todos ellos están regulados por el ICANN (Internet Corporation For Assignet Names and Numbers) el cual como un ente regulador.

Ejemplo: www.tecmotors.com.ec, que se descompone en:

- www: World Wide Web;
- tecmotors: Dominio;
- com: Comercial;
- ec: Ecuador.

Cada dominio esta regulado por un NIC (Network Information Center) que muchas veces trabaja localmente como enrutador y normador de dominios en cada país. En el Ecuador se llama nic.ec. El más conocido es: www.networksolutions.com sitio en el que se puede averiguar no sólo si un dominio está libre para registrar sino también quién ha tomado el nombre que nos interesa.

Cada dominio tiene un sufijo denominado TLD (TOP LEVEL DOMAIN). Los más comunes son:

TABLA V
TLD MÁS COMUNES

Extensión	Corresponde a:
.com	Actividad comercial
.net	Actividad de Internet, sistemas o redes

.org	Organizaciones (Usualmente sin fines de lucro)
.edu	Instituciones educativas
.fin	Instituciones financieras
.mil	Dependencias militares de los estados
.gov	Organizaciones gubernamentales
.biz	Organizaciones de negocios
.tv	Empresas y cadenas televisas o relacionadas
.info	Sitios de apertura libre de dominio TLD o de primer nivel
.name	para sitios personales

Fuente: http://dominios.cinfonet.com/?web=info, 2003

Adicionalmente a los TLD, existen los ccTLD (Country Code) código de país, que se refiere a 2 caracteres que identifican al código del país. Ejemplo, ec, cl, ar, us, es, entre otros.

En Ecuador se puede tramitar cualquier dominio con un ISP (proveedor de Internet, ejemplo; SATNET, ecuanet), pero lo aconsejable es acudir al NIC.EC.

También existen DNS (Servidores de nombre de dominio) que permiten que en el navegador podamos poner la dirección URL o IP es decir; www.dominio.com o 200.31.6.54 respectivamente. Cada DNS mantiene una lista con la equivalencia IP de los computadores de un determinado número de dominios.

Cuando se registra un dominio sin derecho a su propiedad se denomina “Caber Squatting” y cuando mediante acciones de programación cambiamos la información de un dominio direccionándolo a otro servidor o dejando que funcione bajo la entidad correcta se denomina “Domain Hijacking” o Secuestro de Dominio. Por ejemplo, es como cuando una empresa no tiene RUC es decir, es fantasma pero aún así sigue funcionando.

2.2 Buzón o cuenta de correo electrónico

Es nuestra dirección de correo en Internet. Para explicarlo de forma sencilla, es como si tuviésemos una casilla de correo tradicional con la compañía Z y que nuestro número o nombre de apartado es felixsalazar. En este caso, nuestra dirección sería: el apartado de correos felixsalazar en la compañía Z. Para simplificar la notación, podríamos poner juntas las dos partes de la dirección separadas el signo @ (arroba). Entonces la dirección del apartado de correos sería felixsalazar@compañíaZ, y ya podríamos empezar a utilizarlo.

Pues bien, de forma parecida funciona el correo electrónico. Por ejemplo; tomemos la dirección felixsalazar@yahoo.es. Las direcciones de correo tienen dos partes separadas por el símbolo @ (arroba). La

primera parte indica nuestro nombre (nombre de usuario) o login con el que el propietario de la cuenta accede a su buzón de correo electrónico, en este caso felixsalazar y la segunda parte es el dominio (yahoo.es), que indica la dirección de Internet en la que está el servidor de correo, la cual es otorgada y administrada por un proveedor de correo electrónico. En este caso la dirección felixsalazar@yahoo.es hace referencia a la dirección de correo de un usuario llamado felixsalazar y que se encuentra en yahoo.es. Cabe indicar que el usuario felixsalazar sólo puede tener una cuenta de correo con ese nombre en yahoo.es, pero puede tener otras cuentas de correo en otros servidores: felixsalazar@espol.edu.ec. Un usuario puede tener tantas cuentas como desee.

Cabe señalar que cada buzón esta configurado con datos personales del propietario (nombre de usuario y pasword (contraseña)).

2.3 Formas de acceder a los mensajes de correo electrónico

Entre algunas de las formas para poder acceder a los mensajes de correo electrónico tenemos por la Web y Pop. Cada una de ellas con sus ventajas y desventajas.

2.3.1 Web

En ocasiones podemos estar interesados en leer el correo electrónico desde una página Web, sin necesidad de configurar nuestra computadora. Esto se conoce con el nombre de Web mail. Dicho servicio es muy útil ya que podemos leer, enviar y organizar nuestros correos desde cualquier parte del mundo, con conexión a Internet.

La privacidad de los usuarios de webmail se lleva a cabo mediante la utilización de nombres de usuario y contraseña única.

Algunos proveedores de servicios webmail son:

- Hotmail
- Gmail
- Yahoo

A continuación presentamos algunas ventajas y desventajas que presentan:

Ventajas:

- No necesita ser configurarlo.

- Los mensajes no tienen que descargarse al ordenador.
- Se puede acceder desde cualquier ordenador. Los mensajes pueden leerse, escribirse y enviarse desde cualquier lugar con un explorador y conexión a Internet.
- Las cuentas de correo se crean fácilmente, lo que permite su uso anónimo fácilmente.
- Nos brinda facilidad al momento de cambiar claves de acceso.
- Facilidad al exportar libreta de direcciones.
- Se puede configurar para todo tipo de idioma.
- Es más difícil que se infecte por un virus ya que los mensajes no se almacenan en nuestro ordenador a excepción que bajemos algún archivo adjunto a dicho mensaje.

Desventajas:

- El usuario tiene que estar conectado a Internet mientras lee y escribe los mensajes.
- Los servidores de webmail comerciales ofrecen espacio limitado para el almacenamiento de los mensajes. Ofrece poca capacidad de almacenamiento ya que ésta

dependerá de las que nos proporcione la compañía donde esté alojado.

- Muestran propaganda en los mensajes.
- Algunos mensajes no se pueden guardar en el disco duro.
- Cuando la conexión a Internet es lenta, puede ser difícil enviar los mensajes.
- Poca capacidad para proceso. Es para mensajes ligeros. Los mensajes enviados utilizando webmail son veinte veces más grandes, ya que el mensaje se envuelve en código html, por lo que se hace más lento su uso.

2.3.2 POP

En la actualidad todos los proveedores de Internet nos facilitan el acceso al correo electrónico y nos dan, junto con nuestra conexión, una cuenta (o varias) del tipo POP. Este tipo de correo se almacena en el servidor de correo de nuestro proveedor. Para poder leerlo es necesaria una aplicación que se conoce con el nombre de cliente de correo, que se pone en contacto con el servidor y descarga los mensajes a nuestro

ordenador. Por ejemplo; en Windows el correo más extendido es el Outlook (o el Outlook Express). A continuación mostramos algunas ventajas y desventajas:

Ventajas:

- Es rápido
- Es simple.
- No se necesita estar conectado para redactar los mensajes; sólo hay que conectarse en el momento que deseemos enviarlos.
- Los mensajes se descargan a nuestro ordenador desde el servidor, es decir, la capacidad de nuestro correo nos la marca el ordenador.
- Podemos leerlos luego, desconectados de Internet.
- No se necesita una dirección IP fija.

Desventajas:

- Depende de los recursos de la computadora.
- Es más fácil que se infecte por un virus. Esto dependerá del cliente de correo que usemos.
- Es necesario configurarlo y tener el software instalado antes de usarlo.

- No podrá revisar su correo desde cualquier computadora a menos que ésta se la configure.

2.4 Agente de Transporte del correo electrónico

El correo electrónico es el más importante de los servicios de Internet, cada día se envían incontables mensajes de una parte a otra. Muchos de estos mensajes son notas personales de un usuario a otro, reportes, ventas, videos, etc. El sistema de correo es un servicio general que puede transportar cualquier tipo de información.

La entrega de los mensajes está estandarizada por un sistema llamado SMTP (Simple Mail Transfer Protocol) Protocolo de Transferencia Simple de Correo, es parte de la familia TCP/IP. Describe el formato de los mensajes de correo electrónico y cómo deben manipularse para realizar su entrega. No importa cuál sea el agente de transporte que utilice una PC, siempre que sepa como enviar y recibir correo utilizando SMTP.

2.5 Seguridad de Correo Electrónico y sus componentes

El correo electrónico se ha convertido en una herramienta fundamental de las actividades cotidianas de ejecutivos, profesores, estudiantes e inclusive de amas de casa ya que para enviar un mensaje electrónico a otro usuario sólo necesitamos conocer su dirección electrónica. Pero también sabemos que una vez enviado el mensaje de correo electrónico perdemos el control sobre el mismo ya que es el servicio de correo el que se encarga de que el mensaje llegue a su destino; aún conociendo que el mismo puede pasar por diferentes etapas hasta llegar a su destino.

El uso del e-mail es tan común que cuando escribimos, enviamos y recibimos un mensaje ya sea de negocios o de tipo personal damos por sentado los siguientes puntos:

- Suponemos que el remitente del mensaje es quien dice ser.
- Suponemos que ninguna otra persona ha leído el e–mail.
- También suponemos que el mensaje recibido no ha sufrido ninguna alteración en el camino, es decir, que su contenido esta intacto.

Con el pasar del tiempo todas estas suposiciones van perdiendo validez. Constantemente escuchamos casos de acceso a las cuentas de correo por parte de personas no autorizadas, pérdida de información, entre otras. Debemos recordar que toda información que viaje por Internet es insegura, en otras palabras es fácil de que sea interceptada ya que la información viaja insegura por la Red. Por estas y otras razones debemos proveer a nuestro correo electrónico de medidas de seguridad que minimicen estos riesgos y así no privarnos de todas las ventajas que presenta el correo al dejar de usarlo. Por ejemplo, todos sabemos que, en el correo tradicional una carta puede ser leída o puede perderse y no por eso dejamos de usar este servicio.

2.5.1 Seguridad de Información de correo electrónico.

Debido a que la información que viaja por correo electrónico puede ser de fácil acceso por personas con los conocimientos necesarios en Informática debemos dotar al mismo de medidas de seguridad que reduzcan dichos riesgos.

La seguridad de correo electrónico implica que el mismo este libre de cualquier peligro, daño o riesgo y que mantiene altos porcentajes de fiabilidad.

ISO 17799 (del que luego se dará más detalle) define la información como un recurso de igual valor al resto de los activos de una organización y por consiguiente debe ser debidamente protegida.

Para que una información sea segura debe poseer las siguientes características:

- Confidencialidad: garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a ella.

- Integridad: salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

- Disponibilidad: garantiza el respaldo y acceso de los usuarios autorizados a toda la información y a los recursos relacionados con ella cada a vez que se requiera.

Según ISO 17799 el objetivo de la seguridad de información es proteger adecuadamente este activo para asegurar la continuidad del negocio y minimizar los daños en la organización.

A continuación se señalan ciertos esquemas de seguridad.

- **Privacidad del mensaje.**

  Los documentos sólo deben ser leídos por el destinatario deseado.

- **Origen del mensaje.**

  Probar la identidad de un individuo o autor de un documento, asegura la identidad del remitente del correo, de manera que podemos estar seguros de que fue escrito por quien lo envió y no ha sido falsificado.

- **Autenticidad.**

  Asegurar que la comunicación es auténtica, incluyendo dos etapas:

  Primero asegurándose de que el remitente y el destinatario son quienes dicen ser.

Segundo asegurándose de que una tercera persona no haya intervenido en la comunicación.

El problema de la autenticidad de un documento electrónico se soluciona firmando el documento antes de enviarlo, de forma que no quede duda al destinatario sobre la procedencia de dicho mensaje ni sobre la identidad del remitente. Garantizando así que el usuario que envió los mensajes, es quien dice ser.

- **Repudio del mensaje**

  Asegurar que no se pueda rechazar la validez legal del documento al igual que su información. Básicamente nos protege frente a que posteriormente el que envió el correo (o lo recibió de nosotros) diga en un futuro no haberlo enviado (o recibido si era el destinatario).

  Existe una diferencia entre la autenticidad y el no repudio. Por ejemplo, se puede afirmar que un documento fue escrito por una determinada persona, cuando se ha presenciado el acto de la firma.

Si un documento no está firmado autógrafamente nosotros podemos estar convencidos de su autenticidad, pero ésta no podrá ser probada, ya que sin la firma autógrafa, es imposible establecer vínculo entre la voluntad de la persona y el contenido del documento.

La consecuencia de estos esquemas de seguridad es que las empresas y hombres de negocio no los asumen perdiendo las oportunidades que brinda el Internet, muchas personas ignoramos estos esquemas, especialmente en nuestro país, haciendo más inseguro los mensajes de correo electrónico.

Para minimizar los riesgos y hacer del e-mail una herramienta confiable para la comunicación, en el mundo de los negocios y en otros sectores donde la información que se quiere transmitir es muy sensible, existe la criptografía.

2.5.2 Cifrado o Criptografía

2.5.2.1 Origen

La palabra criptografía proviene del griego kryptos, que

significa esconder y gráphein, que significa escribir; es decir, “escritura escondida”. La criptografía ha sido usada a través de los años para mandar mensajes confidenciales cuyo propósito es que sólo las personas autorizadas puedan entenderlos.

Esta herramienta es utilizada desde hace mucho tiempo atrás para preservar la confidencialidad de la información; especialmente las de origen militar y diplomático.

Podemos considerar las formas más primitivas de lenguaje escrito (por ejemplo; los jeroglíficos del antiguo Egipto) como técnicas criptográficas, ya que eran muy pocas las personas que podían interpretar estos símbolos.

Cuenta la historia que durante el Imperio Romano, en la época del Emperador Julio César, se utilizó un esquema criptográfico simple pero efectivo para comunicarse con sus generales. Este esquema consistía en desplazar cada letra del alfabeto un número determinado de posiciones. Por ejemplo; la letra “A” podría ser codificada como “M”, la “B” como “N”, la “C” como “O” y asi sucesivamente. En este caso, el número que se sumaría a cada letra para realizar la codificación sería 13. Así pues, el

mensaje “ATAQUEN HOY AL ENEMIGO” podría transformarse en “MFMCGQZ TAK MX QZQYUSA”, sin poder ser reconocido por el enemigo.

La criptografía moderna nace al mismo tiempo que las computadoras. Durante la segunda guerra mundial en un lugar llamado Bletchley Park.

Desde 1970 el interés por la criptografía ha ido creciendo ya que aplicación se enfoca en la protección de la confidencialidad, es así que ésta se ha ido ampliando en los últimos años hasta el punto de abarcar el mantenimiento de la integridad de los datos, la acreditación de la identidad de sus fuentes y la imposibilidad de su repudio.

2.5.2.2 Definición

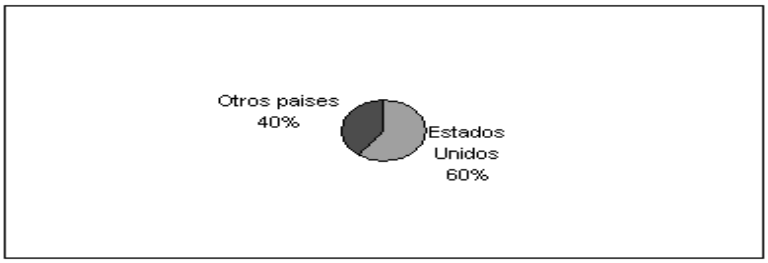
Criptografía es un conjunto de técnicas que tratan sobre la protección de la información frente a observadores no autorizados.

El método que utilizaba Julio César para reemplazar las letras de un mensaje ha ido evolucionando tanto así, que en la actualidad existen programas que encriptan el contenido de un archivo y lo desencriptan cuando se lo necesite.

Este tipo de herramienta es muy útil para manejar cualquier tipo de información confidencial y es aplicable no sólo para correo electrónico.

No es de sorprenderse de los resultados que arrojaron las encuestas realizadas en septiembre de 1997 por la firma de productos y servicios criptográficos Trusted Information System, TIS, refleje que son 1.601 los productos de ese carácter que se comercializan en el mundo, fabricados o distribuidos por 941 compañías, de 68 países, la mayor parte de las cuales – sobre un 60% - estadounidenses [(3)] .

[(3)] Revista: Boletín Escuela Nacional de Inteligencia, página 156



Fuente: Boletín Escuela Nacional de Inteligencia
FIGURA 2.1 Países que usan productos y servicios criptográficos en el mundo.

Estos datos surgen como consecuencia del aumento de interés y de las aplicaciones que atraviesa este campo de la seguridad de la información. Es la confusión que actualmente reina en el mismo y que podríamos nominar como “crisis de crecimiento”. Crisis por el surgimiento ininterrumpido de nuevos algoritmos de cifrado, técnicas y protocolos criptográficos para proteger la información.

Alguien que quiere mandar información confidencial aplica técnicas criptográficas para poder “esconder” el contenido del mensaje (cifrar o encriptar), manda el mensaje por una línea de comunicación que se supone insegura (Ver Figura 2.2) y después sólo el receptor autorizado o el destinatario legítimo del correo pueda leer el mensaje “escondido” (lo llamamos descifrar o

desencriptar). Con este mecanismo se garantiza la confidencialidad del correo.

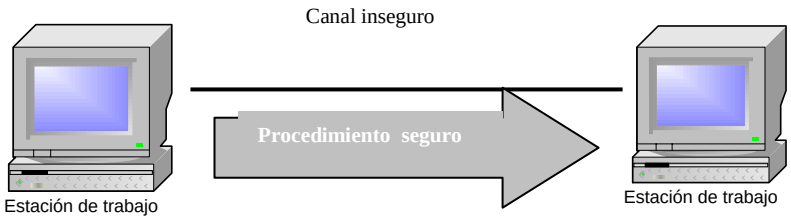


FIGURA 2.2 Canal inseguro.

Pero la “confidencialidad” no es lo único que permite la criptografía sino también resuelve otros problemas de seguridad, como certificar la “autenticidad” (firmar mensajes) e “integridad” (comprobar que la información recibida no ha sido modificada) de la información.

PGP, Pretty Good Privacy en español Muy Buena Privacidad (del que luego se dará más detalles) permite encriptar un mensaje para uno o varios destinatarios, y / o firmarlo, para que cualquiera pueda comprobar de quién es y que permanece tal y como fue emitido. Se definen dos métodos generales de cifrado:

2.5.2.2.1 Cifrado Simétrico

Surge a finales de los años 70 y básicamente consiste en que los usuarios que quieren intercambiar mensajes dispongan de una clave secreta que aplicada a un algoritmo como IDEA, RC5, DES, TRIPLE DES, etc. transforma el mensaje original en otro cifrado siendo responsabilidad de los usuarios conservar la clave.

Si se emplea la misma clave en las operaciones de cifrado y descifrado, se dice que el criptosistema es simétrico o de clave secreta. Estos sistemas son mucho más rápidos y resultan apropiados para el cifrado de grandes volúmenes de datos.

Ejemplo, el método de cifrado de Julio César, el desplazamiento de 13 letras es la clave que se utiliza para cifrar el mensaje, necesitándose la misma clave para descifrarlo. Este ejemplo nos muestra un criptosistema de clave simétrica. Es decir, se utiliza la misma clave para cifrar y descifrar el mensaje.

Ejemplo aplicado a la actualidad, Karen ha escrito un mensaje para Félix pero quiere asegurarse de que nadie más que él lo lea. Por esta razón decide cifrarlo con una clave

.

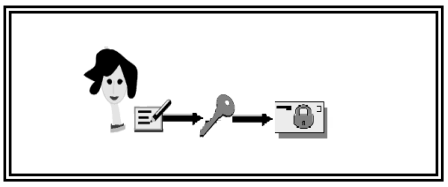


FIGURA 2.3 Cifrado del mensaje

Una vez que envía el mensaje cifrado y la clave, Félix realiza el descifrado.

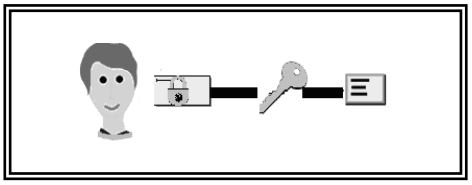


FIGURA 2.4 Descifrado del mensaje

Como podremos observar, este último ejemplo nos ilustra de mejor manera el cifrado simétrico. Mostrándonos el cifrado y descifrado de los mensajes.

La ventaja más importante de la criptografía de clave simétrica es su velocidad lo cual hace que éste tipo de algoritmos sean los más apropiados para el cifrado de grandes cantidades de datos.

La desventaja que presenta la criptografía de clave simétrica es la necesidad de distribuir la clave que se emplea para el cifrado.

DES (**Data Encryption Standard).**

Fue diseñado a principios de los años 70. Nació como consecuencia del criptosistema LUCIFER, creado por Horst Feiste, este criptosistema podía ser implementado fácilmente tanto en software como en hardware. Es así, que fue presentada en sociedad en el año 1975 y regulado en 1977 en Estados Unidos siendo posteriormente objeto de numerosos reconocimientos. Sin embargo como sus creadores previeron el paso del tiempo ha hecho desgastes en el mismo dirigiendo inevitablemente a sustituir dicho algoritmo por uno seguro.

En 1995 se reunieron varios de los más grandes criptógrafos estadounidenses para tratar este tema, dando a conocer sus conclusiones en Enero de 1996. Ellos concluyeron que la mínima longitud de clave aceptada en la actualidad para preservar informaciones durante los próximos 20 años debería ser de 90 bits lo que da una cardinalidad del espacio de claves de 2^{90}, aun así los expertos recomendaron usar claves de mayores longitudes todavía.

IDEA (Internacional Data Encryption Algorithm)

Es un algoritmo criptográfico bastante más joven que DES, este fue desarrollado por CASEWARE Corp., una prestigiosa compañía canadiense de desarrollo de software de auditoria.

Para muchos, constituye el mejor y más seguro algoritmo simétrico disponible en la actualidad. Como el caso de DES, se usa el mismo algoritmo para cifrar como para descifrar.

Debido al éxito que ha alcanzado este producto en todo el mundo éste posee miles de usuarios entre estos auditores, altos ejecutivos, etc.

2.5.2.2.2 Cifrado Asimétrico

Cuando se utiliza una pareja de claves para separar los procesos de cifrado y descifrado, se dice que el criptosistema es asimétrico o de clave pública. Una clave, la privada, se mantiene secreta, mientras que la segunda clave, la pública, es conocida por todos. Así mismo esta pareja de claves es complementaria lo que cifra una, sólo lo puede descifrar la otra y viceversa. Estas claves se obtienen mediante métodos matemáticos.

Los criptosistemas de clave pública, aunque más lentos que los simétricos, resultan adecuados para los servicios de autenticación, distribución de claves de sesión y firmas digitales, como se explicará posteriormente. Se utilizan los algoritmos de RSA, Diffie-Hellman, etc.

El cifrado asimétrico también se emplea para firmar documentos y autenticar entidades, como se describirá posteriormente, en el punto que trata sobre firmas digitales.

Podemos decir que sus usos más comunes son los dos siguientes:

- Garantizar que un archivo informático (mensaje de correo electrónico, archivo de texto, hoja de cálculo, etc.) ha sido creado por quien dice ser su creador (Firma Electrónica).
- Impedir que un archivo informático sea leído por personas sin autorización (encriptación).

Por ejemplo, Karen y Félix tienen sus pares de claves respectivas: una clave privada que sólo ha de conocer el propietario de la misma y una clave pública que está disponible para todos los usuarios.

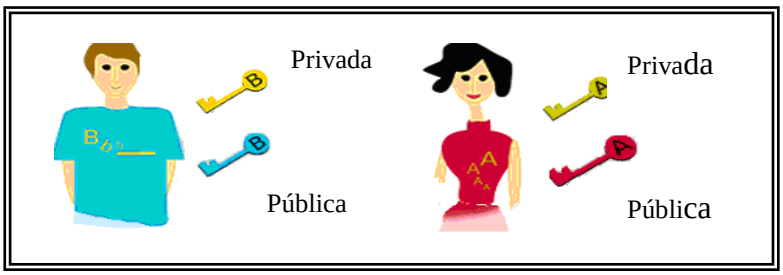


FIGURA 2.5 Par de Claves Privadas y Públicas

Y de igual forma que el ejemplo anterior Karen no quiere que nadie más que Félix pueda leer el mensaje. Por esta razón lo cifra con clave pública de Félix, accesible a todos los usuarios.

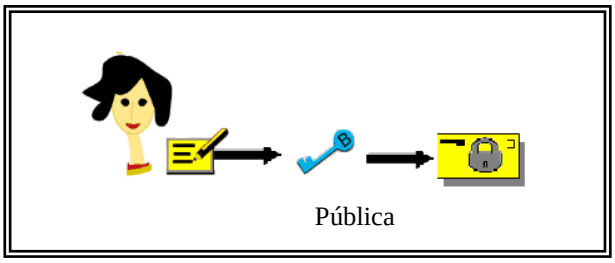


FIGURA 2.6 Cifrado del mensaje con la Clave Pública de Félix

Posteriormente se produce el envío del mensaje cifrado no siendo necesario el envío de la clave.

Sólo Félix puede descifrar el mensaje enviado por Karen ya que sólo él conoce la clave privada correspondiente.

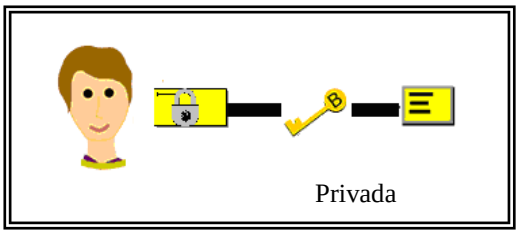


FIGURA 2.7 Descifrado del mensaje con la Clave Privada de Félix

RSA

Fue creado en 1978 por **R**ivest, **S**hamir y **A**dlman. Es el sistema criptográfico asimétrico más conocido, usado y rápido. Este sistema se basa en el hecho matemático de la dificultad de factorizar números muy grandes.

RSA presenta todas las ventajas de los sistemas asimétricos, incluyendo la firma digital, aunque resulta más útil a la hora de implementar la confidencialidad. Se suele usar también en los sistemas mixtos para encriptar y enviar la clave simétrica que se usará posteriormente en la comunicación privada.

2.5.3 PGP (Pretty Good Privacy, Muy Buena Privacidad)

Se trata de un proyecto iniciado a principios de los 90 por Phill Zimmerman. Es un programa que implementa una de las tecnologías más extendidas de encriptación.

Con el pasar de los años, PGP se ha convertido en uno de los mecanismos más populares y fiables para mantener la seguridad y privacidad en las comunicaciones.

Cuando enviamos una carta por el correo tradicional, la colocamos en el buzón de correo, pero previamente cerramos el sobre. Esto es así porque no queremos que otras personas lean su contenido. PGP es el programa que sirve de sobre a nuestras cartas por Internet ya que maneja la privacidad de tal forma que sólo aquellos para quienes el mensaje está dirigido puedan leerlo. Además permiten implementar mecanismos de verificación que hacen que puedan establecerse que el mensaje proviene de una determinada persona.

Sus características permiten que las personas intercambien archivos o mensajes con un alto grado de privacidad, pudiendo implementar la autenticación de su origen y destino.

PGP ha crecido a una gran velocidad tanto que en la actualidad es ampliamente utilizado, principalmente por las siguientes razones:

- Hay versiones gratuitas disponibles en la Web.
- Está basado en algoritmos que son considerados extremadamente seguros.
- No fue desarrollado ni es controlado por organizaciones gubernamentales.

PGP funciona con criptografía asimétrica (aunque por cuestiones de eficiencia también hace uso de criptografía simétrica), y su punto fuerte radica en la facilidad que ofrece a los usuarios comunes para generar las claves (algo que como antes he mencionado no es en absoluto trivial) y gestionarlas.

PGP proporciona lo que se denomina “anillo de claves” (llavero), que es un único fichero donde el usuario puede guardar todas

sus claves con facilidad, para realizar inserción y extracción de claves de manera sencilla.

Para autentificar claves, PGP permite que los usuarios “firmen claves”, por lo que podemos confiar en la autenticidad de una clave siempre que ésta venga firmada por una persona de confianza.

Además, cada clave tiene una “huella digital” (fingerprint), que se trata de una secuencia lo suficientemente larga para que sea única, pero lo suficientemente corta para poder ser comunicada de viva voz o escrita en papel. Así, si queremos asegurarnos de la autenticidad de una clave, solo hemos de preguntar (por ejemplo, por teléfono) a su autor la huella digital de su clave.

Cuando una clave secreta queda comprometida, o se sustituye por una nueva, puede ser revocada por su autor. Sólo tiene que generar y distribuir un “certificado de revocación” que informará a los usuarios de PGP que esa clave ya no es válida. Por supuesto, para poder emitir dicho certificado es necesario tener la clave secreta.

PGP proporciona un nivel de seguridad muy bueno y gran rendimiento si se utiliza correctamente. Sin embargo un uso inadecuado puede convertirlo en algo completamente inútil. Para que ésto no ocurra debemos cuidar estos aspectos:

- **Escoger contraseñas adecuadas:** Para extraer del anillo una clave privada requiere del usuario una contraseña. Por supuesto, ésta ha de ser segura (memorizable, larga, aleatoria, complicada, etc.)

- **Firmar sólo las claves de cuya autenticidad estemos seguros:** Debemos de ser cuidadosos para que las "redes de confianza" funcionen adecuadamente, o podemos certificar claves falsas (lo que nos engañaría a nosotros y a aquellos que confíen en nosotros como autoridad de certificación).

2.5.3.1 ¿Como funciona PGP al enviar correo encriptado?

Al enviar un mensaje encriptado a otro usuario de PGP, el programa crea una clave de sesión, la cual es independiente de nuestras claves privadas o públicas. Dicha clave de sesión es un número generado de forma aleatoria basándose en el

movimiento de nuestro ratón y las teclas que pulsamos. Esa clave de sesión se usa para encriptar el texto del mensaje, con lo que ya no hay forma de “VER” el mensaje.

Antes de enviar el mensaje la clave de sesión se encripta utilizando la clave pública del destinatario y ambos paquetes, texto encriptado y clave de sesión encriptada se envían juntos. Al recibir el mensaje, el destinatario desencripta la clave de sesión usando la clave privada. Una vez que tiene la clave de sesión, se desencripta el texto del mensaje con ella.

Para confiar totalmente en una clave pública o una firma, es necesario que se den una de las dos condiciones siguientes:

- La clave pública nos ha sido entregada directamente por la persona a la que pertenece. Esta puede ser enviada por correo electrónico y, al recibirla, podemos comprobar que lo que nos ha llegado es la clave pública de esa persona llamándola por teléfono y verificando los números de control.

- La clave pública está firmada por otras personas en las que confiamos. Al recibir una clave pública, es posible ver quien confía ya en esa clave y, si ellos son a su vez de

confianza, aceptarla e incluso firmarla nosotros mismos.Incluso así, puede quedarnos un poco de incertidumbre. Para resolverlo, lo mejor que se puede hacer es utilizar certificados digitales. Esto a diferencia de PGP no es gratuito.

PGP es totalmente gratuito para fines no comerciales.

2.5.3.2 El mayor problema de PGP

Pese a lo que pudiera parecer, el mayor problema de PGP no tiene nada que ver con los hackers, los algoritmos y demás cuestiones técnicas. Ciertamente su mayor desventaja es que son pocos sus usuarios, aunque su número aumenta a pasos agigantados.

Pese a que los internautas desconocen la existencia de PGP, su número de usuarios es infinitamente superior al de las demás aplicaciones gratuitas de seguridad que podemos encontrar, por lo que no deja de ser el líder en su sector con una gran ventaja sobre sus competidores.

2.5.4 Firmas y Documentos Digitales

2.5.4.1 Firmas digitales

Las firmas digitales proporcionan un medio de protección de la autenticidad e integridad de los documentos electrónicos; por ejemplo, puede utilizarse en el cierre de un negocio donde existe la necesidad de verificar quién firma un documento electrónico y comprobar si el contenido del documento no ha sido alterado.

Explicar en qué consiste una firma digital es sencillo: basta con imaginar una cerradura y su llave. Un mensaje de correo electrónico, o cualquier otro documento digital (transferencias de fondos, contratos, facturas, convenios de pago, etc.), pueden ser introducidos en una caja fuerte, de manera que sólo pueda ver su contenido quien posea una llave de su cerradura. El resto verá sólo el exterior: una caja fuerte.

La firma digital tiene dos finalidades:

- la encriptación del contenido y
- la autentificación del emisor.

Ciertamente, al igual que una cerradura puede ser violentada, la encriptación puede ser descubierta, pero eso puede llevar demasiado tiempo, incluso años, como para que alguien esté interesado en tomarse la molestia. **Una firma digital está compuesta por una clave privada**, la cerradura del ejemplo, **y una clave pública**, la llave, también llamada certificado digital. El emisor garantiza la seguridad y la privacidad de su mensaje firmándolo digitalmente por medio de su clave privada. Ésta codifica el contenido del mensaje, de tal manera que únicamente puede ser decodificado por una clave pública que corresponda, que encaje en la cerradura.

La creación de claves de privacidad es un proceso totalmente aleatorio y que garantiza niveles de seguridad tan difíciles de traspasar como se pretenda: a mayor calidad de cerradura y llave, mayor seguridad. La calidad de una firma digital se mide por su tamaño en bits.

En la práctica, la implementación de un sistema de firmas digitales es sencillo y seguro, aunque por supuesto siempre cuenta con el mismo riesgo: que no se tenga cuidado en la

protección de las claves. Efectivamente, si perdemos la llave de la cerradura, estamos perdidos, aunque no nos demos ni cuenta.

En principio, bastaba con cifrar un documento con la clave privada para obtener una firma digital segura, puesto que nadie excepto el poseedor de la clave privada puede hacerlo. Posteriormente, cualquier persona podría descifrarlo con la clave pública, demostrándose así la identidad del firmante. En la práctica, debido a que los algoritmos de clave pública son muy ineficaces a la hora de cifrar documentos largos, los protocolos de firma digital se implementan junto con funciones unidireccionales de resumen (hash), de manera que en vez de firmar un documento, se firma un resumen del mismo. Este mecanismo implica el cifrado, mediante la clave privada del emisor A, del resumen de los datos, que serán transferidos junto con el mensaje. Éste se procesa una vez en el receptor B, para verificar su integridad. Por lo tanto, los pasos del protocolo son:

1.- A: genera un resumen del documento.

2.- A: cifra el resumen con su clave privada, firmando el documento.

3.- A: envía el documento junto con el resumen firmado a B.

4.- B: genera un resumen del documento recibido de A, usando la misma función unidireccional de resumen. Después descifra con la clave pública de A el resumen firmado. Si el resumen firmado coincide con el resumen que él ha generado, la firma es válida.

De esta forma se ofrecen los servicios de no repudio, ya que nadie excepto A podría haber firmado el documento, y de autenticación, ya que si el documento viene firmado por A, podemos estar seguros de su identidad, dado que sólo él ha podido firmarlo. En último lugar, mediante la firma digital se garantiza asimismo la integridad del mensaje, ya que en caso de ser modificado, resultaría imposible hacerlo de forma tal que se generase la misma función de resumen que había sido firmada.

Por lo expuesto anteriormente podemos afirmar que:

- Cuando una persona firma digitalmente un documento, lo hace usando su llave primaria, a la cual sólo él tiene acceso.
- Su firma digital no puede ser copiada a un documento por alguien que no tenga acceso a su clave privada.

- La firma digital copiada no brinda acceso a la clave privada del individuo, la cual nunca es revelada.
- El documento no podrá ser modificado o alterado por terceros luego de ser firmado sin anular la firma.

Cómo funciona: Leer un documento Firmado

- Primero se obtiene generalmente la llave pública del certificado digital asociado a la firma digital usada.
- Dicho certificado puede ser incluído en el documento, o puede accederse a través de una red privada o Internet.
- El certificado digital certifica la autenticidad de la firma y la identidad del firmante.
- Si bien están asociadas, la llave pública no permite acceder a la llave privada del individuo.

2.5.4.2 Certificado Digital

- Un certificado digital es una garantía emitida por un tercero (Autoridad Certificadora) de que la firma digital ligada al certificado corresponde a la persona o institución que indica.

- Cuando recibimos un documento firmado digitalmente, podemos verificar la autenticidad de la firma al consultar el certificado digital.
- El certificado digital incluye la clave pública asociada a una firma digital.

2.5.4.3 Ventajas y beneficios del uso de firmas y documentos digitales.

1. *Ahorros en los costos de transacción y almacenamiento.*
   - No es necesario imprimir documentos si se pueden distribuir digitalmente y/o llenar en forma digital.
   - No es necesario preservar copias impresas de todos los documentos legales.
   - Captura de información: No tiene que ser digitalizada si se recibe digitalmente.
2. *Mayor eficiencia y agilidad.*
   - Se mejora la calidad de la información.
   - Los documentos pueden fluir más rápidamente, agilizándose procesos.

- Los documentos digitales pueden ser buscados, almacenados, consultados, e incluso distribuídos más fácil y ágilmente.

3. *Más transparencia.*
   - Dificulta la falsificación de firmas y documentos.
   - La recopilación y distribución íntegra de documentos y datos originales minimiza la posibilidad de su alteración.

4. *Avances tecnológicos.*
   - Fortalece e incentiva el uso de correo electrónico.
   - Permite la modernización de nuevos sectores: Salud, Arquitectura, etc.

2.5.5 Protección ante virus

Diariamente enviamos y recibimos una serie de mensajes, los mismos que muchas veces no conocemos su procedencia y mucho menos su contenido. Durante el proceso de envío de mensajes de correo electrónico cada uno es analizado y si no se detecta ningún virus es enviado al servidor de correo de la organización. El análisis de cada mensaje puede deteriorar la

performance del firewall o del retransmisor de correo, la cual dependerá de la carga de trabajo que tenga y la calidad del servicio requerido.

A continuación presentamos algunos beneficios de realizar este tipo de análisis:

- Los virus son detectados y detenidos antes de ingresar a la red.
- El análisis del virus puede ser implementado para todos los mensajes con solamente cambios menores en la configuración del servidor.
- Se pueden analizar mensajes que estamos enviando.
- El análisis de los mensajes puede ser administrado en forma centralizada asegurándose que se cumple con las políticas de seguridad de la organización y con las actualizaciones periódicas del software.
- La aplicación de análisis puede ser utilizada en los otros protocolos soportados por el firewall.

Así también mostramos las debilidades que puede causar el análisis en el firewall o en el retransmisor de mensajes.

- Puede requerir modificaciones significativas en la configuración del servidor de correo cuando se analizan correos salientes.
- No se pueden analizar correos encriptados.
- Puede requerir servidores potentes y costosos para poder manejar la sobrecarga de tareas si la organización es demasiado grande.

Otra opción es colocar el analizador directamente sobre el servidor de correo. Esta alternativa resulta interesante para detener aquellos mensajes contaminados que son enviados por usuarios internos a otros usuarios también internos ya que este tipo de mensajes no son alcanzados por el firewall.

A continuación presentamos algunas desventajas.

- La principal desventaja de esta opción es la caída que puede ocasionar sobre el servidor de correo causado por el incesante análisis de todos los mensajes administrados por el servidor.
- Al analizar los mensajes en el servidor puede requerir una importante modificación en la configuración del servidor de correo.

- No puede analizar mensajes encriptados.
- Puede requerir servidores potentes y costosos si la organización es demasiado grande.

Así también presenta algunas ventajas:

- El correo también puede ser analizado en ambas direcciones.
- El análisis de los mensajes puede ser administrado en forma centralizada asegurándose de que se cumple con las políticas de seguridad de la organización y con las actualizaciones periódicas requeridas por el software.
- Ofrece protección a los usuarios internos una vez que el virus ingresó a la red de la empresa.

En la actualidad los servidores de correo ya contienen antivirus.

Cuando considere un analizador de virus para un firewall o un servidor de correo, se debe tener en cuenta las siguientes características:

- Detectar y limpiar todos los virus conocidos u otro tipo de códigos maliciosos.

- Preveer algún grado de protección contra virus nuevos o desconocidos.
- Proveer filtro de contenido.
- Poder analizar archivos comprimidos.
- Simpleza y actualización en la administración.
- Actualización automática.

No es aconsejable instalar antivirus en el cliente por los siguientes puntos:

- Difícil de administrar centralizadamente.
- Los usuarios pueden no actualizar el antivirus con suficiente frecuencia y así exponer a toda la empresa.
- En general se analizan solamente los mensajes entrantes.
- Los virus no son detenidos en el perímetro de la red, ya sea en los firewall o en los retransmisores de correo.

Sin embargo, agregado a todo lo mencionado anteriormente podemos decir que el paso más importante de todos, es educar a los usuarios acerca del peligro de los virus inculcándole tomar en cuenta las siguientes acciones:

- Nunca abrir archivos adjuntos enviados por usuarios desconocidos.

- Nunca abrir archivos con extensiones sospechosas; por ejemplo, adjunto.txt.vbs
- Sospechar de los mensajes con títulos no acordes a la relación que nos vincula con el emisor; ejemplo, mensajes con el título “You are the best” enviado por un colega de trabajo.
- Analizar todos los archivos adjuntos con el antivirus antes de abrirlos, o configurar para que esta acción se realice automáticamente.
- Actualizar el antivirus periódicamente.

2.5.6 Firewall

Un cortafuego (o firewall en inglés), es un elemento de hardware o software utilizado en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según lo determine la organización. La ubicación habitual de un cortafuegos es el punto de conexión de la red interna de la organización con la red exterior, que normalmente es Internet; de este modo se protege la red interna de intentos de acceso no autorizados desde Internet, que puedan aprovechar vulnerabilidades de los sistemas de la red interna.

Es simplemente un filtro que controla todas las comunicaciones que pasan de una red a la otra y en función de lo que sean permite o deniega su paso. Para permitir o denegar una comunicación el firewal examina el tipo de servicio al que corresponde, como pueden ser el web, el correo. Dependiendo del servicio el firewall decide si lo permite o no. Además, el firewall examina si la comunicación es entrante o saliente y dependiendo de su dirección puede permitirla o no.

También es frecuente conectar al cortafuego una tercera red, llamada zona desmilitarizada o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

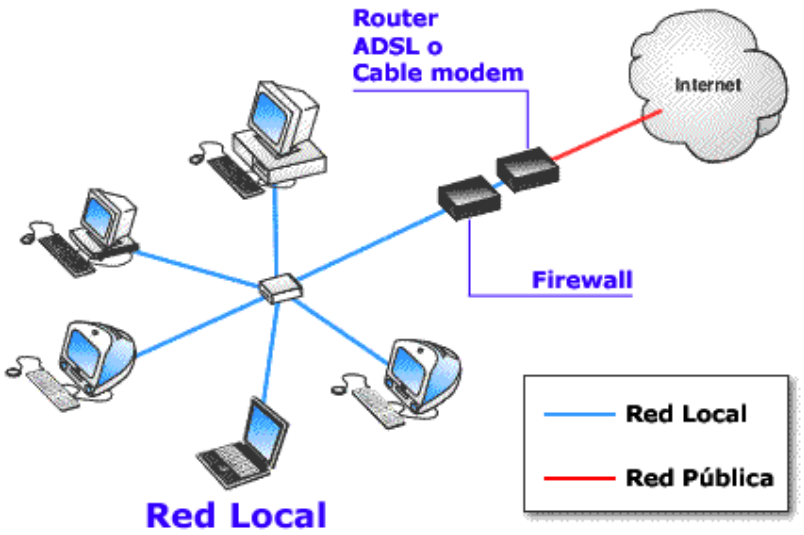


FIGURA 2.8 Firewall
Fuente: http://www.tecnyred.com/seguridad.php, 2006

2.6 Análisis de Riesgo (Metodología Delphi)

El método Delphi consiste en reunir a un grupo de expertos para solucionar determinados problemas. Dicho grupo realiza la categorización individual de las amenazas y de los objetos de riesgo.

El esquema completo de método Delphi es el siguiente:

1. **Crear matriz de Amenazas y Objetos:** Al comienzo se debe realizar una reunión con todo el personal involucrado en el trabajo. Esta reunión tiene por objeto no sólo identificar las amenazas y los objetos del área, sino también establecer nombres cortos para denominar las diferentes amenazas y objetos.

2. **Identificar los controles necesarios:** Este paso debe realizarse al comienzo, en la reunión con el grupo de personas involucradas en el área. Es allí donde se precisan los controles para salvaguardar los objetos en relación con las amenazas.

Los miembros del grupo deben discutir los controles que deberán incluirse. A medida que esos controles se van admitiendo, es necesario crear una lista con los siguientes datos:

- Número de identificación.
- Nombre corto que distingue cada control.

- Breve descripción sobre la funcionalidad y utilidad de los controles.
- Identificación de la persona responsable de la implementación de los controles.

3. **Categorizar los riesgos:** Identificar las áreas de alto, medio y bajo riesgo, colocándolas en orden de nivel de exposición. Para la ejecución de este paso se utiliza el método Delphi y la compasión de los niveles de riesgo.

El equipo Delphi sesiona conjuntamente para combinar sus experiencias en la realización de las siguientes tareas:

- Categorizar las amenazas por niveles de riesgo. (Ver Anexo 11). Para efecto de esta evaluación se ha organizado un grupo de tres personas, quienes se someten a votación hasta completar la matriz. (Ver Anexo 12). La categorización se obtiene sumando como se muestra en el Anexo 13. Posteriormente se suman los dos votos para obtener el total final de cada amenaza. El resultado se utiliza para elaborar una lista de categorización de amenazas, por niveles de riesgo de mayor a menor.

- Categorizar la sensibilidad de los objetos: Se inicia copiando los objetos que registra la matriz de control de riesgo en una hoja de comparación de categorías de riesgos. (Ver Anexo 14). Para categorizar la sensibilidad de los objetos se utiliza la apreciación que tenga cada uno de los expertos sobre cuál objeto de cada pareja de objetos puede causar mayor pérdida económica si se daña o causa demoras en el procesamiento. El grupo vota hasta completar. (Ver Anexo 15). Después se suman los resultados derechos de diagonales de las columnas (en forma vertical), y luego se suman los resultados izquierdos de las diagonales las columnas (en forma horizontal). Acabaremos sumando los resultados para obtener el total final. (Ver Anexo 16).

- Combinar ambas categorías: Terminada las dos categorías, se desarrolla una matriz de control de riesgos, en la cual se colocan los totales en orden (de mayor a menor), en ambos casos. (Ver Anexo 17).

- Posteriormente se multiplican los valores correspondientes y con los resultados obtenidos se organiza una nueva matriz. Concluida esta operación se procede a obtener el nivel de

riesgo / sensibilidad de las celdas de acuerdo con el valor del producto. Puede ser que al terminar este proceso se presenten repeticiones.

- A continuación se procede a dividir las celdas de regiones de mayor, medio y bajo riesgo. Este proceso se realiza dividiendo la cantidad de niveles de riesgo / sensibilidad para tres (número de expertos). El cociente se utiliza para establecer las celdas de mayor, mediano y bajo riesgo. (Ver Anexo 18 y Anexo 19).

4. **Diseñar controles definitivos:** Con los resultados obtenidos se diseñan los controles a nivel preventivo, detectivo y correctivo; de acuerdo con el área que se esté analizando.

- **Preventivos.-** Son aquellos que reducen la frecuencia con que ocurren las causas del riesgo.
- **Detectivos.-** Son aquellos que no evitan que ocurran las causas del riesgo sino que los detecta luego de ocurridos.
- **Correctivo.**- Ayudan a la investigación y corrección de las causas del riesgo.

CAPÍTULO 3

3. FUNDAMENTACIÓN NORMATIVA Y/O ESTANDARES EN AUDITORÍA DE SISTEMAS

3.1 Introducción

En el desarrollo de este trabajo hemos observado como el correo electrónico ha evolucionado de forma permanente con el pasar de los años, debido a ésto se ha dado origen al surgimiento a una serie de estándares y normas para que desarrollen en conjunto esquemas de seguridad y control en las organizaciones.

La importancia de mantener altos estándares de seguridad de información tanto en el sector público como privado deja de ser un sueño para convertirse en una realidad.

Así también se analiza de forma clara y resumida algunos estándares y normas de seguridad electrónica. Señalando de forma especial: COBIT, ISO 17799, COSO, SAC, la LEY DE COMERCIO ELECTRONICO vigente en el Ecuador.

Cabe señalar que las normas tienden a evolucionar o mejorar constantemente y pueda que durante el desarrollo del presente trabajo éstas hayan evolucionado.

3.2 Fundamentación normativa

3.2.1 Normas de control interno COSO

Debido al mundo económico que existe en la actualidad se ha visto la necesidad de integrar metodologías y conceptos en todas las áreas que pueden existir en una organización tanto administrativas como operativas, con el fin de ser competitivos y responder a las nuevas exigencias empresariales, surge así un nuevo concepto de control interno donde se brinda una estructura común el cual es documentado en el denominado informe COSO.

3.2.1.1 En qué consiste la Norma

COSO define al control interno como el proceso que involucra a todos los miembros de una organización con el fin de evaluar

operaciones específicas con seguridad razonable en tres principales categorías:

- Efectividad y eficiencia operacional.
- Confiabilidad de la información financiera.
- Cumplimiento de políticas, leyes y normas.

El control interno posee cinco componentes que pueden ser implementados e interrelacionados en todo tipo de organización de acuerdo a las características administrativas, operacionales y de tamaño; los componentes son:

- Ambiente de control
- Evaluación de riesgos
- Actividades de control (políticas y procedimientos)
- Información y comunicación
- Monitoreo o supervisión.

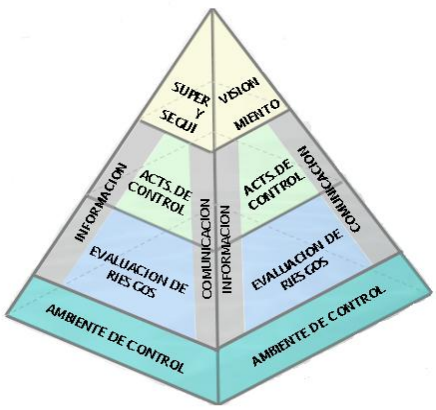


FIGURA 3.1 Estructura de Control Interno

Para poder implementar el control interno en una organización se debe establecer previamente los objetivos, políticas, lineamientos y estrategias relacionadas entre sí con el fin de garantizar el desarrollo organizacional y el cumplimiento de los objetivos;

Aplicado al correo electrónico podemos decir que el control a desarrollarse debe proveer de seguridad al mismo, analizando previamente las causas de los riesgos, observando si estos riesgos se deben a fallas humanas (descuidos en la administración de las contraseñas, divulgación no autorizada de información).

La norma señala la importancia de que la organización posea personal capacitado y con sólidos valores éticos, ya que de todos dependerá el logro de los objetivos propuestos.

Posteriormente a la evaluación es conveniente analizar los alcances encontrados, este análisis deben indicar como los cambios internos o externos en la organización pueden afectar o han afectado al cumplimiento de las políticas.

Ambiente de control.- COSO establece a este componente como el primero de los cinco y se refiere al establecimiento de un entorno que estimule las actividades con respecto al control de sus actividades. La Norma hace énfasis en la integridad y valores éticos de los trabajadores en la organización ya que la seguridad de la información y los equipos dependen de su integridad y sus valores.

Evaluación de riesgos.- Se requiere de un análisis e identificación de riesgos de seguridad de correo electrónico para lograr los objetivos propuestos. Los riesgos deberán ser evaluados periódicamente con el fin de desarrollar los respectivos controles y asi reducir su impacto (violación a la privacidad del correo electrónico, falta de confidencialidad de información, carencia de integridad, entre otros riesgos).

Actividades de control.- Verificar que se esté cumpliendo con los controles establecidos para preservar la seguridad de correo electrónico.

Información y comunicación.- El uso de correo electrónico no sólo abarca a nivel interno de la organización sino que es un

medio de comunicación con el mundo exterior, es a través del cual se obtiene o proporciona información relativa como; por ejemplo cartera de clientes, proveedores, contratistas, etc. Asimismo es necesario para proporcionar información a las entidades reguladoras sobre las operaciones de la empresa e inclusive sobre el funcionamiento de sus sistemas.

Supervisión y seguimiento de control.- Se debe comprobar que los controles establecidos estén cumpliendo con su función. Claro está que previamente se deben haber evaluado los posibles riesgos. Estas actividades de control no sólo son importantes porque implican la forma "correcta" de hacer las cosas, sino debido a que son el medio idóneo de asegurar en mayor grado el logro de la seguridad de correo electrónico. En caso de que algún control no esté cumpliendo a totalidad con su función deberá ser reforzado a la brevedad posible habiendo realizado previamente un respectivo análisis.

3.2.1.2 Características

La Norma señala claramente que todo el personal que labora en una organización debe tener bien definida sus responsabilidades

para una eficaz evaluación de riesgos. De igual manera señala al comité de auditoria como el órgano que no sólo tiene la facultad de cuestionar a la Gerencia en relación con el cumplimiento de sus responsabilidades, sino también asegurar que se tomen las medidas correctivas necesarias.

Básicamente la Norma nos dice que para lograr que los objetivos de seguridad correo electrónico de la organización se cumplan todo el personal debe tener claramente definida sus responsabilidades en la misma.

3.2.2 Ley de comercio electrónico, firmas electrónicas y mensajes de datos

Después del proceso de discusión y análisis esta Ley fue aprobada por El Congreso Nacional del Ecuador en el año 2002 en el registro Oficial Suplemento 557. Esta Norma tiene por objeto normar, regular, garantizar el secreto de comunicaciones y controlar el uso de sistemas de información y de redes electrónicas, incluida la Internet (correo electrónico) para que así éstas sean accesibles y transparentes al hacer uso de ellas, ya

que en la actualidad desempeñan un papel importante para el progreso del comercio y la producción y es a través de este medio que se logra definir múltiples negocios.

Así mismo analiza datos importantes; como mensajes de datos; los requisitos para poseer firma electrónica junto con sus características; el uso de certificados de firmas electrónicas, las obligaciones, responsabilidades y requisitos que deben cumplir las entidades que los emiten, entre otras.

Debido a la acogida que ha tenido el correo electrónico en la población se ve la necesidad de impulsar a los usuarios al uso adecuado de este medio de comunicación convirtiéndolo en una herramienta de desarrollo del comercio, la educación y la cultura.

La Ley señala aspectos interesantes respecto a la falsificación de documentos electrónicos, apropiación ilícita de información confidencial y cualquier otro tipo de delito informático. Dicha normativa es aplicable a delitos realizados por los funcionarios de las entidades afectadas o por hackers.

Mensajes de datos

La ley reconoce igual valor jurídico a los mensajes de datos junto con la información que se encuentre como anexo accesible mediante un enlace electrónico a los documentos escritos. Es así que cuando se requiera que la información conste por escrito ésto se dará cumplido con un mensaje de datos.

Los mensajes de datos también serán sometidos a leyes, reglamentos y acuerdos internacionales relativos a la propiedad intelectual.

Queda claro que cualquier violación a la confidencialidad, transferencia ilegal de mensajes, de datos o violación del secreto profesional será sancionado conforme a las leyes.

La Ley además especifica que se puede considerar íntegro un mensaje si se mantiene completa e inalterable su información, salvo cambios de presentación pero no en contenido.

Firmas electrónicas y certificados de firmas electrónicas

La firma electrónica cumple la función de indicar que el titular de la firma aprueba y reconoce la información contenida en el

mensaje de datos. Esta hará las veces de una firma manuscrita. Para que la firma electrónica tenga validez debe cumplir los siguientes requisitos:

- Ser individual y estar vinculada a su titular.
- Permitir verificar la autoría e identidad del signatario, mediante dispositivos técnicos establecidos por esta ley.
- Debe ser seguro, confiable e inalterable.
- Al momento de su creación, los datos con los que se creare se hallen bajo control del signatario.
- Debe ser controlada por la persona a quien pertenece.

Asimismo el titular de la firma electrónica tiene obligaciones y responsabilidades que debe cumplir. La duración de la firma electrónica es indefinida pero puede ser extinguida por los siguientes motivos:

- Voluntad
- Fallecimiento del titular
- Liquidación de la persona jurídica, titular; y por causa judicialmente declarada; pero la extinción de la firma no libra al titular de responsabilidades previamente contraídas.

Junto con las firmas electrónicas encontramos los certificados de firmas electrónicas que como su palabra lo indica sirven para certificar la identidad del titular de una firma electrónica. De la misma forma ésta debe cumplir ciertos requisitos.

La extinción de dicho certificado será por solicitud del titular, extinción de la firma electrónica y por expiración del plazo de validez del certificado de firma electrónica. Si el certificado de firma electrónica es suspendido de forma temporal, inmediatamente dicha situación debe ser comunicada al titular y al organismo de control señalando previamente las causas y podrá ser nuevamente habilitado una vez que hayan desaparecido las causas que lo originó.

Reconocimiento internacional de certificados de firma electrónica

Todos los certificados electrónicos emitidos por entidades de certificación extranjeras, que cumplieren con los requisitos señalados en esta ley, tendrán el mismo valor legal que los certificados acreditados, expedidos en el Ecuador. El Consejo Nacional de Telecomunicaciones dictará el reglamento correspondiente para la aplicación de este valor.

Las firmas electrónicas creadas en el extranjero, para el reconocimiento de su validez en el Ecuador se someterán a lo previsto en la ley y su reglamento.

Salvo aquellos casos en los que el Estado, en virtud de convenios o tratados internacionales haya pactado la utilización de medios convencionales, los tratados o convenios que sobre esta materia se suscriban, buscarán la armonización de normas respecto de la regulación de mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluído el comercio electrónico, la protección a los usuarios de estos sistemas, y el reconocimiento de los certificados de firma electrónica entre los países suscriptores.

Entidades de certificación de información

Se considera como tales a toda empresa que emita certificados de firma electrónica y pueden prestar otros servicios relacionados con la firma electrónica, autorizadas por el Consejo Nacional de Telecomunicaciones, según lo dispuesto en esta ley y el reglamento que deberá expedir el Presidente de la República

Su función es garantizar la protección de los datos conforme lo establecido en esta ley. Dichas entidades tienen responsabilidades y obligaciones que cumplir. Para cesar sus funciones, ésta deberá notificar al Organismo de Control por lo menos con noventa días de anticipación y se sujetará a las normas y procedimientos establecidos para el efecto.

Como podemos observar la ley es muy clara sobre las obligaciones y responsabilidades que debe cumplir el acreedor de la firma electrónica, certificación de firma electrónica así como para los organismos de control y entidades de certificación.

3.2.3 Normas de Control Interno SAC

SAC, Systems Auditability and Control Study (Auditoria de Sistemas y Estudios de Control) es un conjunto de procesos, funciones, actividades, subsistemas y gente integrada para asegurar el logro efectivo de los diferentes objetivos y metas planteadas.

De forma específica y aplicada a la seguridad de correo electrónico podemos decir que, establece los medios para

proporcionar una seguridad razonable de que los objetivos y metas de la organización sean logrados en forma eficiente, eficaz y económica.

Los componentes de un sistema de control incluyen:

- Ambiente de control.- Se refiere a la estructura de la organización. Capacitar al personal sobre el uso que debe prestarle a sus cuentas de correo.
- Sistemas automatizados.- Abarca procesamiento, reporte, almacenaje y transferencia de información.
- Procedimientos de control.- Controles generales o específicos que ayuden a preservar la seguridad de información de correo electrónico. Controles de seguridad física (servidores, red, etc.) y lógica (transporte de la información). Controles sobre telecomunicaciones, entre otros. Básicamente son controles de aplicación que aseguran un proceso, desde la entrada, el proceso y la salida de la información (previenen, detectan y corrigen) cualquier adulteración de la información.

3.3 Estándares Internacionales

3.3.1 Estándar de control de sistemas COBIT

Dentro de los principales estándares internacionales tenemos COBIT, que es muy utilizado para desarrollar trabajos de Auditoria Informática así como por profesionales de TI para asegurar y salvaguardar la información.

3.3.1.1 En qué consiste la Norma

A continuación explicaremos los fundamentos del estándar COBIT, por sus siglas en inglés Control Objetives for Information and Related Technology (Objetivos de Control para la información y tecnología relacionada). Es un estándar internacional de uso diario por los administradores de negocios y los auditores a nivel mundial, facilitando la compresión por parte de la alta gerencia de los riesgos de seguridad relacionados con la tecnología de información.

COBIT tiene como misión: Investigar, desarrollar, publicar y promover un conjunto internacional y actualizado de objetivos de

control para tecnología de información que sea de uso cotidiano para gerentes y auditores.

En el año 1996 COBIT fue presentada por ISACA (Asociación de Auditoría y Control de Sistemas de Información), la cual se ha caracterizado por estar a la vanguardia en la emisión de normas, guías y procedimientos referentes a la auditoria y administración de Tecnología de la Información.

Esta normativa puede ser implementada en cualquier organización que desee implementar un proyecto de TI sustentable y con altos estándares de control y seguridad de sus sistemas de información; sin importar su tamaño o la tecnología que utilice.

3.3.1.2 Características

Está dirigida a la gerencia, los auditores y los usuarios finales con un propósito específico; apoyar decisiones de inversión y control sobre la seguridad de correo electrónico.

Entre sus principales características señalamos las siguientes:

- Es orientado al negocio.
- Basado en una revisión critica y analítica de las tareas y actividades desarrolladas.
- Está alineado con estándares de control y Auditoria (COSO, IFAC, IIA, ISACA, AICPA)

Podemos decir que en el caso de correo electrónico la norma lo abarca completamente ya que involucra tanto a usuarios como a los administradores en la responsabilidad de mantener segura la información.

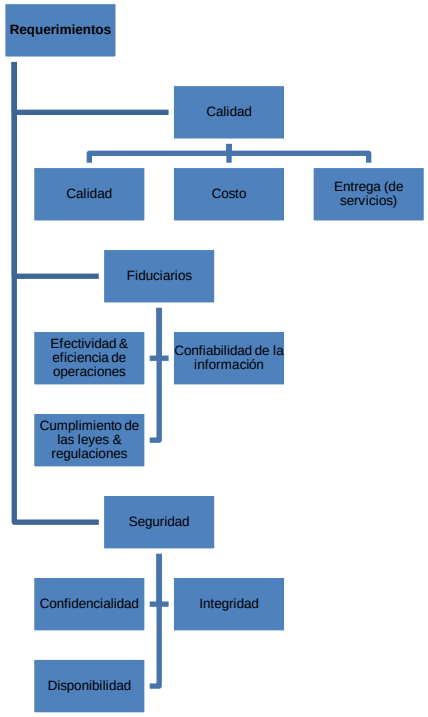
3.3.1.3 Estructura de la Norma

ISACA a través de diversos medio de difusión como por ejemplo su sitio Web, ha logrado difundir ampliamente la estructura fundamental de COBIT por todo el mundo.

Esta Norma esta basada en tres principios fundamentales que son:

1. **Requerimiento de Información del Negocio.**

Toda organización debe establecer de forma específica los requerimientos necesarios para preservar la seguridad de la información que viaja por correo electrónico.



Requerimientos de Calidad.- La organización debe establecer la calidad, costo y oportunidad de la información. Si una organización o una persona considera que la información que esta siendo transmitida vía correo electrónica amerita algún tipo de seguridad, debe tomar acciones que eviten posibles riesgos.

Requerimientos Financieros.- Básicamente deberá definir los mínimos controles de efectividad y eficiencia de operaciones. Asi

como la confiabilidad de la información cumpliendo con leyes y regulaciones. La información que viaja por la red debe ser segura y por ende confiable.

Efectividad.- Se refiere a que la información que se está manejando debe de ser pertinente para el desarrollo del negocio. De igual manera su entrega debe ser oportuna, correcta y consistente

Eficiencia.- La organización debe contar con los más óptimos recursos en la provisión de información.

Confiabilidad de la información.- La información que se provea debe ser la apropiada con el fin de operar correctamente en la entidad.

Cumplimiento.- Se debe cumplir las leyes, regulaciones y acuerdos contractuales a los que el proceso del negocio está sujeto.

Requerimientos de Seguridad.- La organización debe asegurar la confidencialidad, integridad y disponibilidad de información que viaje vía e-mail. Se debe garantizar que la información llegue íntegra sin haber sufrido ningún tipo de alteración a su destinatario.

Confidencialidad.- La información debe ser protegida contra cualquier divulgación o intento no autorizado.

Integridad.- Se refiere a la validez que ésta debe tener así como a la precisión y suficiencia de la información.

Disponibilidad.- La información debe estar disponible cuando sea requerida. También nos indica que se debe salvaguardar los recursos necesarios y capacidades asociadas al correo electrónico.

2. Recursos de TI.

Estos recursos son necesarios para todo tipo organización que haya implantado un sistema de Tecnología de información.

Datos**.-** Cualquier información que viaje por correo electrónico es considerada como dato.

Sistemas de Aplicación**.-** Se refiere a los sistemas de información del correo electrónico que integran procedimientos manuales y sistematizados.

Tecnología.- Abarca software y hardware básico también sistemas operativos, de redes, telecomunicaciones, correo electrónico, etc.

Instalaciones.- Se refiere a los recursos necesarios para alojar y dar soporte al correo electrónico.

Personal**.-** Se refiere a todo el personal que de forma directa o indirecta interviene con el correo electrónico (usuarios, administradores, proveedor, etc.).

3. Procesos de TI.

Así mismo, para lograr que una organización implemente de forma exitosa sus recursos debe hacerlo mediante una serie de procesos asociados para que así proporcionen la información que la empresa necesita para alcanzar sus objetivos. Estos procesos se encuentran agrupados de la siguiente forma:

***Dominios*.-** Agrupación neutral de procesos, que normalmente corresponden a una responsabilidad organizacional. A continuación se describen los cuatro dominios principales:

- Planeación y Organización.- Se refiere a la mejor manera de lograr la seguridad de correo electrónico.
- Adquisición e implementación.- Las posibles soluciones para preservar la seguridad de correo electrónico deben ser claramente identificadas y desarrolladas, así como implementadas e integradas dentro del proceso del negocio.
- Prestación de servicios y Soporte.- Hace referencia a la entrega de los servicios requeridos por los usuarios de correo electrónico que va desde las operaciones

tradicionales hasta el entrenamiento y lógicamente pasando por seguridad.

- Seguimiento.- Todos los procesos necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de seguridad de correo electrónico.

Procesos.- Es una serie de conjuntos o actividades unidas con delimitación de control. COBIT nos presenta 34 Objetivos de Control repartidos en los cuatro dominios. Se debe tener en cuenta que estos procesos pueden ser aplicados a diferentes niveles dentro de una organización.

También debe ser tomado en cuenta que el criterio de efectividad de los procesos que planean o entregan soluciones a los requerimientos del negocio, cubrirán en ciertas ocasiones los criterios de disponibilidad, integridad y confidencialidad. En la práctica se han convertido en requerimientos del negocio.

Resulta claro que las medidas de control no satisfarán necesariamente los diferentes requerimientos de información del negocio en la misma medida. Se lleva a cabo una clasificación

dentro del marco referencial *COBIT* basada en rigurosos informes y observaciones de procesos por parte de investigadores, expertos y revisores con las estrictas definiciones determinadas previamente.

Primario: Es el grado al cual el objetivo de control definido impacta directamente en la seguridad del correo.

Secundario: Es el grado al cual el objetivo de control definido satisface únicamente de forma indirecta o en menor medida el requerimiento seguridad de correo.

Blanco (vacío): Podría aplicarse; sin embargo, los requerimientos son satisfechos más apropiadamente por otro criterio en este proceso y/o por otro proceso.

Ciertamente, todas las medidas de control no necesariamente tendrán impacto en los diferentes recursos de TI a un mismo nivel. Por lo tanto, el Marco Referencial de COBIT indica específicamente la aplicabilidad de los recursos de TI que son administrados en forma específica por el proceso bajo consideración no por aquellos que simplemente toman parte en el proceso. Esta clasificación está basada en el mismo proceso riguroso de información proporcionada por los investigadores,

expertos y revisores utilizando definiciones indicadas previamente.

A continuación mencionaremos algunos procesos que tratan sobre la seguridad de correo electrónico. Dentro de la Planeación y Organización podemos encontrar los siguientes:

- **Definición de un plan estratégico de tecnología de información.**

  Se deben implantar planes a corto y largo plazo los mismos que deberán contener metas claras y concretas a corto plazo. Se refiere a la mejor manera de alcanzar la seguridad de correo electrónico.

- **Definición de la organización y de las relaciones de TI.**

  Satisfacer los requerimientos del negocio. Lo cual se hace posible a través de una organización conveniente en número y habilidades, con tareas y responsabilidades definidas. Tomando previamente en consideración:

  - Supervisión
  - Rol y responsabilidades
  - Personal clave

Responsabilidad de seguridad física y lógica: Se debe asignar formalmente la responsabilidad de la seguridad física y lógica de los activos de información de la organización a un Gerente de seguridad de la información, quien su vez reportará a la alta gerencia.

Así mismo la gerencia deberá diseñar una estructura para designar formalmente a los custodios del correo para que éste no presente problemas. También sus funciones y responsabilidades deberán estar claramente definidas.

Se debe evaluar si todo el personal cuenta con los recursos adecuados para llevar a cabo sus tareas y sus responsabilidades de la mejor forma posible.

- **Comunicación de la dirección y aspiraciones de la gerencia.**

  Asegurar que el usuario comprende y conoce las responsabilidades sobre el uso del correo electrónico. Lo cual se logra a través de políticas establecidas y transmitidas en este caso a los usuarios tomando en consideración ciertos aspectos:

- Código de ética/ conducta. La Gerencia deberá desarrollar y difundir dicho código de ética entre sus colaboradores.
- Políticas de seguridad y de control interno. La gerencia deberá asumir la responsabilidad de desarrollar, promulgar y controlar que éstas se cumplan.

- **Asegurar el cumplimiento de requerimientos externos.**

  Cumplir con obligaciones legales, regulatorias y contractuales a través del desarrollo de medidas apropiadas para su cumplimiento.

- **Evaluación de riesgos**

  La finalidad de la evaluación de los riesgos es asegurar el logro de objetivos de seguridad de correo electrónico. Se debe tener en cuenta los siguientes puntos:

  - Actualización de evaluación de riesgos. (Constantemente evaluarlos para de esta manera tenerlos actualizados y por ende estar preparados ante ellos).
  - Metodología de evaluación de riesgos.

- Medición de riesgos (cualitativos y/o cuantitativos)
- Plan de acción de riesgos.

Dentro de la Adquisición e Implementación podemos señalar las siguientes:

- **Identificar soluciones**

  Asegurar un mejor enfoque para asi cumplir con los requerimientos de los usuarios. Realizando previamente un análisis de las diferentes alternativas comparadas contra los requerimientos de los usuarios. Teniendo en consideración los siguientes puntos:

  - Estudios de factibilidad (costos-beneficio, alternativas, etc.). Estos deben ser examinados en forma monetaria y no monetaria.
  - Adquisición de productos de software. Estos deberán obedecer las políticas de adquisición de la empresa.
  - Reporte de análisis de riesgo. Se debe asegurar que cada proyecto de desarrollo, implementación y modificación de correo contenga el análisis y documentación de las posibles amenazas a la seguridad.

- **Adquisición y mantenimiento de arquitectura de software**

  Poseer el software apropiado para soportar las diversas aplicaciones. La cual se hace posible por medio de la evaluación del desempeño de hardware y software, brindando mantenimiento preventivo de hardware y seguridad al correo electrónico. Se debe tener en cuenta los siguientes puntos:

  - Evaluación de tecnología.
  - Mantenimiento preventivo de hardware.
  - Seguridad del software de sistema, instalación, mantenimiento y control sobre cambios.

- **Desarrollo y mantenimiento de procedimientos relacionados con tecnología de información.**

  Asegura el uso apropiado del correo electrónico a través del desarrollo de manuales de procedimientos de operaciones para usuarios.

- **Administración de Cambios**

  Minimiza la probabilidad de interrupciones, alteraciones no autorizadas y errores. Llevar un registro que permita el

análisis, implementación y seguimiento de todos los cambios requeridos y llevados a cabo.

- Autorización de cambios. Toda solicitud de cambio deberá realizarse por escrito. Y estas posteriormente se procederán a categorizar y priorizar de acuerdo al grado de importancia.
- Distribución de software. Diseñar medidas de control específicas. Asegurar la correcta distribución de software. La cual se debe realizar de forma integra.
- Evaluar su impacto. Deberá establecerse un procedimiento para asi asegurar que todos los cambios sean evaluados, analizando asi su impacto.
- Control de cambios. La administración de cambio como la distribución de software deben estar integrados apropiadamente.

Dentro de Servicios y Soporte encontramos los siguientes:

- **Garantizar la seguridad de sistemas.**

  Salvaguardar la información contra cualquier uso, divulgación, modificación no autorizada; daño o pérdida. La cual se logra a través de controles que aseguren que el

acceso a sistemas, datos y programas esté restringido para usuarios no autorizados.

- **Capacitar a los usuarios.**

  Asegurar que los usuarios estén utilizando de forma eficiente la tecnología disponible. Al hablar de correo electrónico en una compañía podríamos decir que éste sea para uso exclusivamente laboral.

  Lograr que los usuarios estén concientes de los riesgos y responsabilidades en el manejo del correo electrónico. Esto se logra a través de un plan de entrenamiento y desarrollo.

- **Administración de la configuración.**

  Prevenir alteraciones no autorizadas (acceso al servidor de correo), verificar existencias físicas de los equipos. Se hace posible a través de una serie de controles que identifiquen y registren todos los activos de la organización que intervienen en el uso del correo electrónico así como su ubicación. Se debe tener en consideración los siguientes puntos:

  - Registro de activos.

- Administración de cambios en la configuración.
- Chequeo de software no autorizado.

- **Administración de datos.**

  Asegurar que los datos permanezcan completos, precisos e íntegros durante su entrada, salida, actualización y almacenamiento. A través de una combinación de controles generales y de aplicación sobre las operaciones de TI. Teniendo en cuenta los siguientes puntos:

  - Controles de entrada.
  - Controles de salida.
  - Administración de almacenamiento y respaldo.
  - Integridad.

- **Evaluar lo adecuado del Control Interno**

  Asegurar el logro de los objetivos de control interno establecidos. A través del compromiso de la Gerencia de monitorear los controles internos, evaluar su efectividad y emitir reportes sobre ellos en forma regular. Se debe realizar auto evaluaciones.

- **Proveer auditoria independiente**

  Incrementar los niveles de confianza beneficiándose de recomendaciones pasadas en mejores prácticas. Por medio de auditorías independientes desarrolladas en intervalos regulares a la seguridad del correo electrónico.

  Actividades.- Son las acciones requeridas para lograr un resultado medible.

3.3.2 Estándar ISO 17799

Pertenece a la familia de las ISO y presenta las "mejores prácticas" para la implementación de un Sistema de de Control y Seguridad de Tecnología de la Información. Se encuentra estructurada en 10 áreas de control.

3.3.2.1 En que consiste la Norma

ISO 17799:2000 es una norma internacional basada en la norma BS 7799, un código de buenas prácticas para la gestión de la seguridad de la información, la cual, fue publicada en

1995 por el Instituto Británico de Normas Técnicas y que posteriormente fue actualizada en el año 1999., siendo su organismo emisor ISO (Organización Internacional de Estándares).

BS 7799 fue desarrollada con el objetivo de tratar aspectos de la seguridad informática en los negocios electrónicos. A pesar de ésto tuvo muy poca acogida debido a que para muchos esta Norma era muy general y exigente para la realidad tecnológica de ese entonces. Debido a se comenzó a trabajar en una segunda versión que abarque de manera más amplia la seguridad y que sea flexible, para que así cualquier organización esté en capacidad de implementarla. Es así que en el año 1999 se publicó la segunda versión mejorada de BS 7799.

En base a esta evolución en la Norma, el Comité internacional de ISO participó junto al Instituto Británico de Normas Técnicas para la emisión de la nueva ISO 17799; la cual, incluía la posibilidad para todo tipo de organización de obtener la Certificación ISO 17799.

ISO 17799 nos presenta una serie de recomendaciones para realizar la gestión de la seguridad de información dirigidas a los responsables de iniciar, implantar o mantener la seguridad de información en una organización.

Sin lugar a dudas ISO 17799 en la actualidad se ha convertido en uno de los estándares más utilizados al momento de implementar un Sistema de Seguridad Informática.

El objetivo de la norma ISO 17799 es proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones. Proteger adecuadamente la información de correo electrónico para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocio.

La seguridad de la información se define como la preservación de:

- **Su confidencialidad**. Sólo quienes estén autorizados pueden acceder a la información.
- **Su integridad**. Los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

- **Su disponibilidad**. Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.

Se fundamenta en la presentación de 10 áreas de control que deben ser cuidadosamente cubiertas por los responsables de TI de las organizaciones, sin importar el tamaño o estructura que éstas tengan ya que como se expresó anteriormente ésta recoge las “mejores prácticas” de seguridad sugeridas por los expertos.

En estos momentos muchas empresas multinacionales poseen una certificación ISO 17799 ya que así como la calidad juega un papel muy importante la seguridad de la información también.

Toda información transmitida por correo electrónico debe estar protegida de forma adecuada.

¿Por qué es necesaria la seguridad de la información?

La información que viaja por correo electrónico debe ser confidencial, llegar de forma integra a su destino y estar disponible para quienes estén autorizados a hacer uso de ella.

Constantemente el correo electrónico se enfrenta a una serie de amenazas como son: fraude, espionaje, sabotaje, suplantaciones, spam, vandalismo, etc. Daños tales como los ataques mediante virus informáticos y denegación de servicio, estos y otros más con el pasar del tiempo se han vuelto más comunes. Por estos y otros motivos las organizaciones han visto la necesidad de desarrollar e implantar controles que ayuden a minimizar su impacto manteniendo asi la seguridad del mismo.

La administración de la seguridad de la información, exige, como mínimo, la participación de todos los empleados de la organización. También puede requerir la participación de proveedores (Internet), clientes y accionistas. Así mismo, puede requerirse el asesoramiento experto de organizaciones externas.

Los controles de seguridad de información resultan considerablemente más económicos y eficaces si se incorporan en la etapa de especificación de requerimientos y diseño.

¿Qué es gestionar?

Es llevar a cabo las actividades necesarias para lograr un determinado fin. La gestión de la seguridad de correo electrónico consiste en la realización de las tareas necesarias para garantizar los niveles de seguridad exigibles en una organización.

Algunas consideraciones:

- Los problemas de seguridad no son únicamente tecnológicos.
- Los riesgos no se eliminan. Se gestionan.
- La seguridad no es un producto, es un proceso.

¿Por qué gestionar?

- Garantizar la confidencialidad, integridad y disponibilidad de sus activos es lo primordial para cualquier organización.
- Nuevas amenazas.

- La dependencia creciente de los recursos de TI aumenta los impactos.
- No siempre se pueden eliminar los riesgos.
- Es necesario gestionar la seguridad de la información.

3.3.2.2 Gestión de la seguridad

Sistema de gestión de la seguridad de la información (SGSI)

Sistema de gestión que comprende la política de seguridad de correo electrónico, la estructura organizativa, los procedimientos, los procesos y los recursos necesarios, para implantar la gestión de la seguridad de la información. Es aplicable en todo tipo de organización.

3.3.2.3 Estructura de la Norma

El ISO 17799 establece diez dominios de control que cubren por completo la gestión de la Seguridad de la Información, las cuales se resumen a continuación:

1. Política de seguridad

La organización debe tener bien claro cuales son sus objetivos de control y la metodología que va a emplear para establecer un subsistema de Control Interno Informático.

La alta dirección debe definir una política que refleje las líneas directrices de la organización en materia de seguridad, aprobarla y publicitarla de la forma adecuada a todo el personal implicado en el uso del correo electrónico.

La política se constituye en la base de todo el sistema de seguridad de la información. De igual manera la alta dirección debe apoyar visiblemente la seguridad de información electrónica.

2. Aspectos organizativos para la seguridad.

Se busca gestionar la seguridad de la información dentro de la organización manteniendo la seguridad de los recursos de tratamiento de la información y de los activos de información de la organización que son accedidos por terceros.

Debe diseñarse una estructura organizativa dentro de la compañía que defina las responsabilidades que en materia de seguridad tiene cada usuario. Dicha estructura debe poseer un enfoque multidisciplinario los problemas de seguridad no son exclusivamente técnicos.

3. Clasificación y control de activos.

Es de suma importancia definir una clasificación de los activos relacionados con la seguridad de correo electrónico y a nivel general, manteniendo un inventario actualizado de los recursos informáticos que posee la empresa para llevar a cabo una adecuada protección de dichos activos.

4. Seguridad ligada al personal.

Se refiere a la importancia de mantener informado y capacitado al personal respecto a la seguridad y confidencialidad de la información con el objetivo de reducir los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones y los servicios. Asegurando que los usuarios son conscientes de las amenazas y riesgos en el ámbito de la seguridad electrónica de la información, y que están preparados para sostener la política de seguridad de la organización en el desarrollo normal

de su trabajo y así minimizar los daños provocados por incidencias de seguridad y por el mal funcionamiento, controlándolos y aprendiendo de ellos.

Vale indicar que los procesos de notificación de incidencias deben ser claros, ágiles y conocidos por todos.

5. Seguridad física y del entorno.

Es importante establecer un Plan general de seguridad de la información dentro de la compañía. Evitando los accesos no autorizados, daños e interferencias contra los locales y la información de la organización.

Prevenir pérdidas, daños o comprometer los activos así como la interrupción de las actividades de la misma. De igual manera prevenir las exposiciones a riesgo o robos de información y de recursos de tratamiento de información.

Por lo señalado anteriormente podemos decir que las áreas de trabajo de la organización y sus activos deben ser clasificadas y protegidas en función de su criticidad, siempre de una forma

adecuada y frente a cualquier riesgo factible de índole física (robo, inundación, etc.)

6. Gestión de comunicaciones y operaciones.

Se asegura la operación minimizando los riesgos de fallos de información. Se busca proteger la integridad del software y de la información. Manteniendo la disponibilidad de los servicios de tratamiento de información y comunicación.

Prevenir la pérdida, modificación o mal uso de la información intercambiada entre organizaciones.

Básicamente debe garantizarse la seguridad de las comunicaciones del negocio, el medio por el que viaja el correo electrónico.

7. Control de accesos.

En esta sección se enfatiza en los controles que deben implementarse para controlar el acceso a la información de la organización y los procesos del negocio.

Para cumplir lo expuesto anteriormente se debe tener establecido una política la cual debe abarcar diversos puntos

como por ejemplo políticas de divulgación y autorización de información. En las reglas de control se debe tener en cuenta los cambios en los permisos de usuarios que son iniciados automáticamente.

De igual manera la Norma hace referencia a la administración de contraseñas, indica que éste es el medio por el cual los usuarios van a tener acceso a la información, es por ésto que la asignación de contraseñas debe controlarse a través de un proceso de administración formal.

La Norma recomienda el uso de otras tecnologías de identificación y autenticación de usuarios; por ejemplo, verificación de firma.

Con el fin de mantener un control eficaz del acceso a información la gerencia debe llevar a cabo periódicamente un proceso formal con el fin de revisar los accesos de usuarios.

Asimismo nos indica que la colaboración por parte de los usuarios desempeña un papel importante y esencial en la

eficacia de los controles en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento.

Para prevenir el mal uso del correo electrónico debe tenerse en cuenta los siguientes puntos:

- Mantener en secreto las contraseñas.
- Evitar en lo posible escribir en papeles las contraseñas a menos que esta pueda ser guardada en algún lugar seguro.
- Cambiar las contraseñas siempre que exista un posible riesgo
- Seleccionar contraseñas de calidad, con una longitud mínima de 6 caracteres, pero al mismo tiempo fácil de recordar.
- Evitar en lo posible que las contraseñas estén basadas en información personal que otra persona pueda adivinar fácilmente; por ejemplo, nombres, números de teléfono, fecha de nacimiento, etc.
- No tengan caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabéticos.
- Cambiar las contraseñas cada cierto tiempo.

8. Desarrollo y mantenimiento de sistemas.

Se debe establecer los controles de acceso adecuado para proteger la información que se intercambien por correo electrónico.

La norma señala los lineamientos respecto a la seguridad interna de los sistemas de información durante las etapas de diseño y desarrollo, bajo los principios de confidencialidad, autenticidad e integridad de la información; con la finalidad de prevenir ingresos, modificaciones o eliminación de la información. Evitando asi: los accesos no autorizados a los sistemas de información, acceso de usuarios no autorizados, acceso no autorizado a ordenadores, acceso a información contenida en el sistema.

9. Gestión de continuidad del negocio.

En esta sección se busca que la organización identifique cuales son las principales amenazas que pondrían en riesgo la continuidad operativa del negocio, se busca proteger los procesos críticos frente a grandes fallos o desastres hallando posibles alternativas a tales amenazas, se establezcan los recursos necesarios y se elabore un Plan de Contramedidas,

que debería verse reflejado en un documento denominado Plan de Contingencias.

10. Conformidad con la legislación.

La norma establece de forma clara los lineamientos respecto al cumplimiento de las leyes, reglamentos, normas y políticas referentes a la seguridad informática y al correo electrónico. Garantizar la alineación de los sistemas con la política de seguridad de la organización y con la normativa derivada de la misma.

El correo electrónico está sujeto a leyes de comercio electrónico de esta forma nuestro proyecto integrará los diferentes controles establecidos en dicha normativa y/o marco legal. Como por ejemplo, la Ley de Comercio Electrónico en su Art. 4 Propiedad intelectual señala que todos los mensajes de datos estarán sometidos a leyes, reglamentos y acuerdos internacionales que hagan referencia a la propiedad intelectual. Claramente podremos darnos cuenta que ésta ley se aplica también a los mensajes de correo electrónico.

CAPÍTULO 4

4. CASO PRÁCTICO: Evaluación de Seguridad de Correo Electrónico

4.1 Información Preliminar

4.1.1 Descripción de la empresa

Por ética profesional denominaremos a la empresa real como TecMotors Tecnicentro Guayaquil S.A. Esta empresa fue fundada en los años 80, es una empresa de ErcoParts S.A. que pertenece a Continental General Tire de Alemania. Se encuentra ubicada en la ciudadela FAE, su número total de trabajadores es 43. TecMotors se dedica a la venta de llantas, aditivos y amortiguadores.

TecMotors S.A. tiene como misión ser una compañía sólidamente estructurada orientada al desarrollo de soluciones en cada producto y servicio que los diferentes sectores que la economía

demande, creando satisfacción y bienestar a sus colaboradores y rentabilidad a sus accionistas.

Su visión es, ser la compañía número uno por excelencia en la comercialización de neumáticos y productos a fines con una total cobertura dentro de la provincia del Guayas.

Sus principales clientes son: Conecel, Consejo Provincial, CATEG, Muy Ilustre Municipalidad de Guayaquil, Reybanpac, Interagua, entre otros.

Sus principales competidores son: Tecfaroni, Importadora Andina, entre otros.

Debido a que TecMotors S.A. es una filial de Continental General Tire de Alemania, su principal medio de comunicación es el correo electrónico, por este motivo el Gerente General de la empresa solicitó la Evaluación de la seguridad de su correo electrónico. (Ver Anexo 3)

4.1.2 Motivos del trabajo

Previa reunión con el Gerente y el Jefe de Sistemas se pudo determinar que entre los principales motivos o justificativos de este análisis de Evaluación de Seguridad de Correo Electrónico son los siguientes:

- Desconocimiento de la Gerencia acerca de la seguridad de correo electrónico que debe poseer la organización.

- Interés del Gerente por alcanzar los más óptimos niveles de seguridad, garantizando la integridad de la información que viaja por la red.

- Preocupación de parte de los directivos de que la información que se transmite sea obtenida por la competencia.

- Deseo de la Gerencia de evaluar la seguridad de la información que viaja por la red para así incrementar o fortalecer dichos niveles de seguridad.

Estos justificativos son detallados a continuación:

Desconocimiento de la Gerencia acerca de la seguridad de correo electrónico que debe poseer la organización.

La Gerencia desconoce los niveles de seguridad que existen y deben implementarse en la organización dentro del correo electrónico.

Para la Gerencia de TecMotors ésto constituye un justificativo para la realización del trabajo.

Interés del Gerente por alcanzar los más óptimos niveles de seguridad garantizando la integridad de la información que viaja por la red

Existe preocupación e interés por parte de la Alta Gerencia por salvaguardar la integridad de la información que viaja por la red pues ésta es muy sensible y confidencial. Partiendo de que los riesgos no son eliminados sino más bien controlados.

Los controles y las seguridades cada vez se vuelven más indispensables para salvaguardar la información del correo de TecMotors.

Preocupación de parte de los directivos de que la información que se transmite sea obtenida por la competencia

Debido a que la empresa intercambia información respecto a innovaciones y productos especiales con filiales de otros países es necesario preservar la privacidad de la misma. Las tablas de valores de tasas de descuento, el costo de la mercadería, el precio de venta al por mayor, entre otros; constituye la información que se debe preservar.

Deseo de los directivos de evaluar la seguridad de su información que viaja por la red para así incrementar o fortalecer dichos niveles

Debido a los riesgos que puede sufrir la información que es transmitida por correo electrónico se ve la necesidad de evaluar la seguridad de información permitiendo obtener los controles mínimos a implementar en materia de seguridad. La información que viaja por correo electrónico es de vital importancia para TecMotors de allí la necesidad de fortalecer los esquemas de seguridad.

4.1.3 Objetivos

4.1.3.1 Objetivo General

Evaluar la Seguridad de Correo Electrónico identificando los riesgos potenciales que afectan al mismo, desarrollando controles con el de fin de minimizar y contrarrestar dichos riesgos.

4.1.3.2 Objetivos específicos

Los objetivos específicos de la evaluación de la seguridad de correo electrónico de TecMotors son:

1. Determinar las seguridades existentes en el correo electrónico de la empresa. (Ver Anexo 4)

2. Identificar riesgos y problemas relativos a la seguridad de correo electrónico. (Ver Anexo 9)

3. Establecer controles y recomendaciones al gerente de la empresa para preservar la seguridad de correo electrónico. (Ver Anexo 20)

4. Garantizar la seguridad de la información de la organización que viaja por correo electrónico considerando los aspectos de confidencialidad, integridad y disponibilidad.

5. Dar a conocer normas de seguridad de correo electrónico que deben aplicar los usuarios. (Ver capítulo 3)

A continuación cada uno de estos objetivos son detallados:

Determinar las seguridades existentes en el correo electrónico de la empresa

Conocer las diferentes seguridades vigentes en la organización a la fecha de evaluación, para así determinar si el correo de la empresa mantiene la información de forma confidencial, confiable, íntegra y privada.

Identificar riesgos y problemas relativos a la seguridad de correo electrónico

Se busca tener claramente identificados los riesgos potenciales para así proponer diferentes alternativas de control y minimizar sus efectos.

En caso de que ya existan controles e igual se esté incurriendo en riesgos, éstos deberán ser mejorados y en caso de que no existan se deberán implementar a la brevedad posible.

Establecer controles y recomendaciones al gerente de la empresa para preservar la seguridad de correo electrónico

Después de realizar la evaluación a la seguridad del correo electrónico debemos informar a la Gerencia los resultados de la evaluación con sus respectivas recomendaciones, en este informe se incluirán los controles mínimos que deben existir.

A la Gerencia se le presentará una serie de controles preventivos, detectivos y correctivos; y recomendaciones con la finalidad de minimizar los riesgos encontrados y así alcanzar los objetivos propuestos. Así mismo, se dará a conocer el orden en el cual los controles deben ser implementados, dependiendo exclusivamente de TecMotors considerarlos y ponerlos en práctica.

Garantizar la seguridad de la información de la organización que viaja por correo electrónico considerando los aspectos de confidencialidad integridad y disponibilidad

Se entiende por integridad que toda la información de la empresa que viaja a través del correo electrónico debe ser completa, veraz y legítima.

Garantizar la confidencialidad de la información del correo se refiere a que la misma debe ser protegida contra cualquier divulgación o intento no autorizado de lectura.

Disponibilidad se refiere a que la información debe estar lista para su uso en el momento en que sea requerida.

Dar a conocer normas de seguridad de correo electrónico que deben aplicar los usuarios

Se debe tener en claro que los usuarios desempeñan un papel muy importante ya que también depende de ellos mantener la seguridad del correo electrónico, por ello es interés de la Gerencia contar con normas de seguridad de correo electrónico que deben aplicar los usuarios.

4.1.4 Alcance

La evaluación comprende únicamente la central o matriz de Guayaquil de TecMotors, no incluye las filiales. Dicha evaluación fue realizada a finales del mes de mayo, junio y el mes de julio, revelando lo que hasta esa fecha en materia de seguridad se haya implementado en el correo electrónico de TecMotors y cubre el período de enero a junio del 2006.

4.1.4.1 Duración de la evaluación

La "Evaluación de la Seguridad del Correo Electrónico" fue realizada durante 40 días. (Ver Anexo 2).

4.2 Descripción del entorno informático

La empresa cuenta con equipos informáticos que se detallan a continuación:

4.2.1 Arquitectura informática

Entorno de red: La empresa cuenta con una red que tiene un servidor del sistema operativo con Windows 2000 Server.

TecMotors posee un total de treinta máquinas interconectadas en la red. De las cuales veintisiete tienen acceso al correo electrónico.

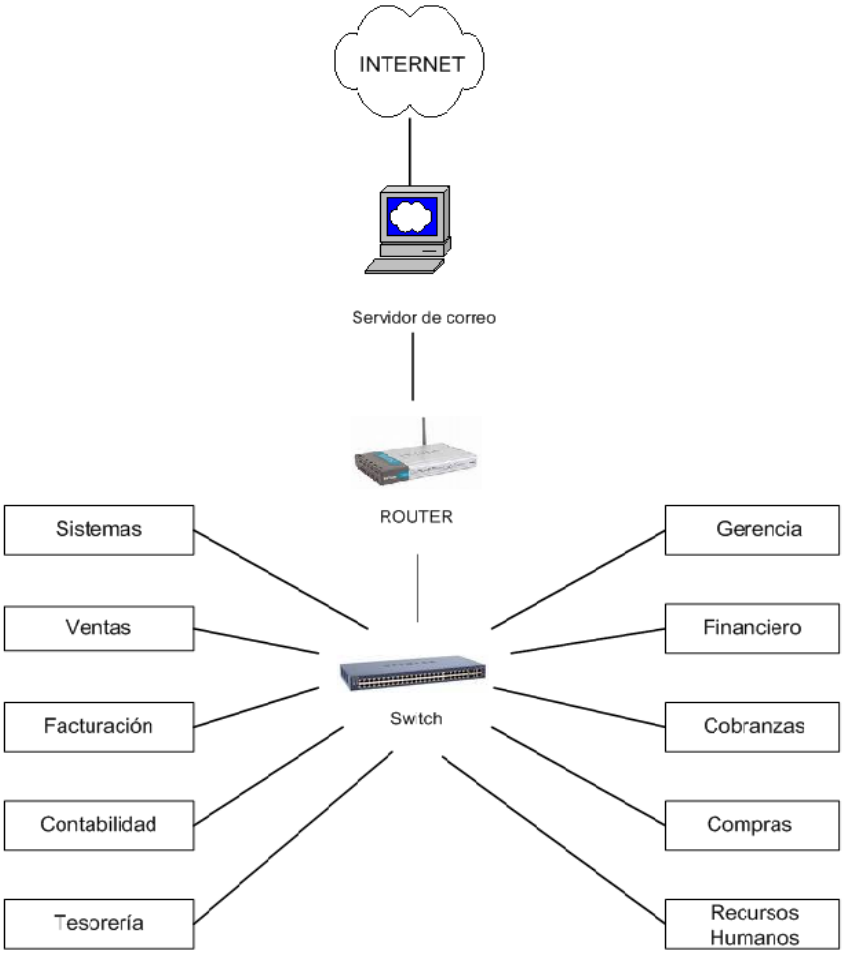


FIGURA 4.1 Diagrama de red de TecMotors

Equipos disponibles: Los veintisiete equipos que al momento se encuentran operativos con el correo electrónico poseen las siguientes características: (Ver Anexo 7)

- Procesador AMD
- Disco duro 80 Gb, 7200 rpm
- 256 Mb de ram
- 1 unidad de CD writer
- 1 unidad de CD rom
- 1 tarjeta de red incorporada
- 1 monitor, Mouse y teclado genérico

El departamento de sistemas cuenta con dos servidores de correo: Un servidor que tiene instalado el sistema operativo Linux y otro servidor con Windows; las características son: (Ver Anexo 8)

Servidor Linux

- Pentium IV 3.0
- Disco duro 80 Gb
- 256 Mb ram de memoria
- 1 unidad de CD rom
- 1 unidad de diskette
- 2 tarjetas de red

Servidor Windows

- Pentium IV 3.0
- Disco duro 36 Gb de 10.000 rpm
- 1 disco SATA de 250 Gb y 7.200 rpm
- 1 unidad de CD writer
- 1 tarjeta de red incorporada

4.2.2 Software de sistemas y utilitarios

Sistema Operativo: El sistema Operativo que utilizan es Windows XP en el Server Windows y Linux en el otro servidor.

Lenguajes de programación: La empresa utiliza el lenguaje Microsoft Visual Basic 6.0

Sistemas de Aplicación: TecMotors S.A. para el desarrollo eficiente de sus actividades y así satisfacer las necesidades de sus clientes cuenta con cinco módulos, los cuales son:

- Cuentas por Pagar
- Bancos
- Contabilidad
- Cobranzas

- Inventario

Siendo el más importante el módulo de cobranzas según criterio emitido por el Gerente y el Jefe de sistemas debido a que TecMotors S.A. realiza ventas a crédito.

Dicho sistema fue diseñado por la Compañía Austro Cía. Ltda., que se encarga de brindar a la empresa asesoría técnica del sistema (modificaciones) y cuenta con un período de diseño, prueba e implementación de 2 años aproximadamente.

Utilitarios: Los principales utilitarios usados en esta empresa son:

- Office XP: Word, Excel, Power Point para el desarrollo de presentaciones gerenciales, Access, entre otros.
- Internet Explorer.

4.3 Estrategia de Evaluación de Seguridad de Correo Electrónico

4.3.1 Planeación

Para iniciar el trabajo desarrollamos un plan cronológico de trabajo (Ver Anexo 1) y programa de trabajo. (Ver Anexo 2)

4.3.2 Reunión con la Gerencia

Se llevó a cabo una reunión con la Gerencia y el Jefe de Sistemas para conocer los motivos que tiene la Gerencia para evaluar la seguridad de su correo electrónico y de esta forma determinar los objetivos que se persiguen (Ver puntos 4.1.2 y 4.1.3).

Así mismo esta reunión sirvió para que el Gerente, el Jefe de Sistemas y dos delegados del personal que usan el correo electrónico de TecMotors se comprometan a colaborar en el desarrollo eficiente de dicha evaluación.

4.3.3 Cuestionario de Visita previa

Se realizó una entrevista “Guía de visita previa” (Ver Anexo 3), la misma que permitió conocer la estructura orgánica del departamento de sistemas, así mismo, se pudo constatar la ausencia del manual de funciones dentro del departamento, dicha entrevista también permitió conocer el número total de trabajadores que posee TecMotors S.A.; en fin se pudo obtener información general de la empresa.

4.3.4 Evaluación de controles

Para la evaluación de los controles existentes en el correo electrónico de la empresa, fueron aplicadas varias técnicas de auditoría, entre ellos la observación, entrevistas, cuestionarios, constatación física. (Ver Anexo 4, 5, y 6)

Dicha revisión desempeña un papel importante ya que permite determinar la existencia de seguridades y controles generales en la organización con particular énfasis en el correo electrónico.

4.3.5 Establecer Metodología de Riesgo

Luego de evaluar las diferentes metodologías que existen para analizar los riesgos, se escogió la metodología Delphi, que consiste en reunir a dos o más personas que conozcan del negocio y del correo electrónico.

4.3.6 Identificar los riesgos de Seguridad de Correo Electrónico

Para la identificación de los riesgos se entrevistó al Jefe de Sistemas y al Asistente Técnico (Ver Anexo 4, 5, y 6), quienes indicaron las seguridades con que cuenta el correo electrónico así como se identificaron los posibles riesgos y problemas que afectan a la seguridad del mismo.

Se estableció la Matriz de Ponderaciones, proceso que mediante una lluvia de ideas proporcionó todos los riesgos observados así como su impacto. De esta manera, empezamos por analizar los riesgos más relevantes:

1. Las claves proporcionadas por el Jefe de Sistemas son sencillas y de fácil deducción.

2. Falta de concientización sobre el uso del correo electrónico de TecMotors.
3. Ausencia de política de seguridad de correo electrónico.
4. Carencia de bitácora de control sobre las cuentas de usuario creadas, eliminadas y los perfiles.
5. No existe respaldo de información.
6. Accesos no autorizados a las cuentas de correo (divulgación y manipulación de información).
7. Ausencia de medidas de seguridad en los equipos.
8. Virus en los equipos.
9. Carencia de firma electrónica.
10. Fácil acceso al servidor de correo por personas no autorizadas.
11. Saturación de servidor por SPAMS adjuntos a los mensajes.
12. Falta de disponibilidad de información (perdida de información).
13. Suplantación de identidad.
14. Intercepción de mensajes.

Para un mejor manejo de los riesgos encontrados, los expertos determinaron clasificar dichos riesgos y determinar las

amenazas, ésto se mostrará en la matriz ponderada. (Ver Anexo 9 y 10)

4.3.7 Análisis de riesgos

Método matricial para el análisis de riesgos

Este método consiste en utilizar una matriz que muestra gráficamente las amenazas a que está expuesto el correo electrónico de TecMotors y los objetos que intervienen para su uso.

Los pasos para el análisis de riesgo son:

A continuación describiremos los pasos para su desarrollo:

1. Identificar las amenazas (causas de riesgo) y los objetos del sistema.
2. Categorizar los riesgos.

Crear la matriz de amenazas y de objetos del sistema

Luego de identificar las amenazas existentes en el correo electrónico, (trabajo realizado previa reunión con el grupo de expertos), se determinó los que compondrán la Matriz de Control de Riesgos (Amenazas y Objetos). (Ver Anexo 11)

Categorización de riesgos

Se categorizan las amenazas por niveles de riesgo, de mayor a menor, como haya sido determinado en reunión con el grupo, luego del proceso de votación. (Ver Anexo 12 y 13).

Posteriormente se procede a sumar primero los votos de las columnas y luego los votos de las filas; y finalmente para obtener la cifra total se suman los dos resultados antes obtenidos. (Ver Anexo 14).

Categorización de objetos

A continuación se procede a categorizar la sensibilidad de los objetos, el cual se inicia pasando los objetos que registra la matriz de control de riesgos en una hoja de comparación de objetos. Para categorizar la sensibilidad de los objetos se utiliza como criterio la percepción que tenga el grupo de trabajo. (Ver Anexo 15).

Posteriormente se procede a la votación del grupo de igual forma como se realizó con la categorización de las amenazas (Ver Anexo 16).

Subsiguientemente se procede a sumar, de igual manera que se realizó con las amenazas (Ver Anexo 17).

Una vez realizada la categorización tanto de las amenazas como de los objetos se realiza una combinación de ambas categorías, elaborando una matriz de combinaciones. Se procede a colocar los totales en orden descendente (de izquierda a derecha y de arriba hacia abajo), en los dos casos (Ver Anexo 18).

Inmediatamente después se procede a realizar los cálculos correspondientes, multiplicando los valores de las amenazas y objetos para así poder obtener el nivel de riesgo / sensibilidad de las celdas. Al terminar este proceso se presentaron repeticiones, las cuales no serán consideradas para determinar el nivel de riesgo de las celdas, posteriormente dividimos las celdas en regiones de mayor, mediano y menor riesgo (Ver Anexo 19).

Como podemos observar en este caso existen repeticiones en los productos, por lo cual se consideran 23 celdas para la determinación del nivel de riesgo. Se procede a dividir las 23 celdas para 3 (el número de expertos) obteniendo 7,6. La escala de valoración es Semicuantitativa ya que se asignan rangos

numéricos a las características Alto, Medio y Bajo. Se toman las siete celdas con los productos más altos para determinarlas con un nivel de riesgo alto, las siete celdas con los productos más bajos para determinarlas con un nivel de riesgo bajo; y las nueve celdas restantes se las determina con un nivel de riesgo medio.

Riesgo Alto	de 1 a 8 celdas	= 8
Riesgo Medio	de 9 a 15 celdas	=7
Riesgo Bajo	de 16 a 23 celdas	= 8

(Ver Anexo 19)

4.4 Diseño de controles definitivos

Finalmente, con los resultados obtenidos, apoyados en el método Delphi y en el modelo matricial Riesgo / Sensibilidad, se diseñan, analizan y documentan controles a nivel: preventivos, detectivos y correctivos que servirán como referencia a la seguridad del correo electrónico (Ver Anexo 20).

Así mismo se estableció el orden en el cual los controles diseñados deben ser implementados en TecMotors los cuales fueron aprobados por la directiva y el Jefe de Sistemas de la compañía. (Ver Anexo 21)

4.5 Presentar los resultados

Finalmente la Gerencia debe conocer el resultado del análisis de la evaluación de seguridad de correo electrónico de manera oportuna, el mismo que será presentado en un informe detallado que se muestra a continuación en los resultados de la evaluación, así la Gerencia podrá tomar las acciones necesarias para preservar la seguridad de su correo electrónico.

4.5.1 Resultados de la Evaluación

Las debilidades encontradas, los efectos y una serie de recomendaciones y controles orientados a minimizar dichos riesgos detectados en el uso de correo electrónico, así también encontraremos algunos indicadores que servirán para determinar si los controles están minimizando los riesgos al correo electrónico.

Cuentas de Correo

1. Manual de políticas de seguridad de correo electrónico no existe en la organización.

Situación Actual:

Durante la revisión realizada pudimos observar que no se cuenta con una política de seguridad de correo electrónico.

Efectos:

Esta situación puede causar que:

- Existe mal uso de las cuentas de correo.
- Falta de seguridad por parte de los nuevos usuarios al tratar de utilizarlo.
- Se ignoren las responsabilidades que se están adquiriendo.

Recomendaciones:

Desarrollar a la brevedad posible la política de seguridad de correo electrónico en la que se describa las responsabilidades que adquiere el usuario al momento de la creación de su cuenta.

De igual manera se debe señalar que el correo de la empresa sólo será usado para fines laborales.

Poner los puntos claves de la política de seguridad de correo electrónico como papel tapiz en todas las computadoras con acceso a correo electrónico de TecMotors.

Indicador:

Proporción de usuarios que conocen la política de seguridad de correo electrónico de TecMotors.

$$\frac{\text{\# de usuarios que conocen la política de seguridad de correo de TecMototors}}{\text{\# total de usuarios de correo electrónico de TecMotors}}$$

Escala:

Muy Bueno	= 1
Bueno	> 0.7 y < 1
Regular	> 0.5 y $\leq$ 0.7
Malo	$\leq$ 0.5

2. Las cuentas de los usuarios de correo pueden quedar abiertas y activas durante tiempo indefinido aunque no se las esté usando.

Situación Actual:

Durante la revisión se pudo observar que las cuentas de correo pueden quedar abiertas durante tiempo indefinido aunque éstas no estén siendo usadas.

Efectos:

Este tipo de errores puede causar:

- Acceso a información confidencial.
- Divulgación de información confidencial.
- Personas no autorizadas hagan uso de una cuenta.
- Se reste privacidad a los mensajes.
- Manipulación de información.

Recomendación:

El Gerente de Sistemas debe configurar de manera general las cuentas de todos los usuarios para que después de cinco minutos de inactividad se cierre la sesión. Se debe tener en

cuenta que el tiempo de espera no debe ser muy extenso (mínimo 5 minutos y máximo 10).

Las cuentas de trabajadores que no laboren en la organización deben ser dadas de baja.

Indicador:

Proporción de cuentas de correo electrónico que continúan abiertas después de 5 minutos de inactividad en el mes.

$$\frac{\text{\# de cuentas que continúan abiertas transcurrido 5 minutos de inactividad en el mes}}{\text{\# total de cuentas usadas en el mes}}$$

Escala:

Muy bueno = 0

Bueno > 0 y ≤ 0.1

Regular > 0.1 y ≤ 0.3

Malo > 0.3

3. Accesos no autorizados a las cuentas de correo

Situación actual

Mediante cuestionario y observación se pudo constatar que la empresa no cuenta con medidas de seguridad para evitar el acceso de personas no autorizadas a las cuentas de correo.

Efecto:

- Divulgación no autorizada de información.
- Pérdidas monetarias en el negocio.
- Acceso a información reservada.
- Adulteración de información.
- Falta de privacidad.

Recomendación:

El jefe de sistemas debe desarrollar e implementar la firma electrónica para los usuarios de la empresa.

Capacitar a los usuarios sobre las responsabilidades y precauciones con que debe usar sus cuentas de correo.

Indicador:

Proporción de accesos no autorizados a las cuentas de correo de TecMotors en el mes.

$$\frac{\text{\# de usuarios que presentan quejas por accesos no autorizados a sus cuentas de correo en el mes}}{\text{\# de usuarios en el mes}}$$

Escala:

Muy Bueno	≤ 0.1
Bueno	> 0.1 y ≤ 0.3
Regular	> 0.3 y ≤ 0.5
Malo	> 0.5

4. No hay respaldo de las cuentas de usuario (Backups)

Situación actual:

Mediante confirmación, cuestionario y observación (Anexo 4) pudimos constatar que la empresa no cuenta con respaldo de las cuentas de usuario.

Efecto:

- Se pierda el usuario.

- Se pierda el pasword.
- Se pierdan los mail guardados del usuario (pérdida de información)
- Pérdida de tiempo.
- En caso de fallas no se puede recuperar estos datos.

Recomendaciones:

Respaldar las cuenta de usuario semanalmente para asi evitar pérdida de información.

Hacer backups de las cuentas.

Indicador:

Proporción de cuentas de usuarios respaldadas semanalmente.

$$\frac{\text{\# de cuentas respaldadas semanalmente}}{\text{\# total de cuentas}}$$

Escala:

Muy Bueno	= 1
Bueno	> 0.8 y < 1
Regular	> 0.6 y $\leq$ 0.8
Malo	$\leq$ 0.6

5. No existe bitácora de control de las cuentas de usuario.

Situación Actual:

Producto del análisis se pudo constatar que el Jefe de Sistemas no posee un documento donde se registre en forma ordenada y actualizada todas las cuentas de usuario creadas con sus características.

Efecto:

Esta situación puede originar que:

- No se tenga un control de las cuenta de usuario creadas.
- No se posea las características principales de cada cuenta de usuario.

Recomendación:

Elaborar una bitácora de control donde se registre la creación y eliminación de las cuentas de usuario así como una descripción detallada de todas las características del usuario de la cuenta.

Indicador:

Proporción de cuentas de usuarios creadas que estén registrados en la bitácora de control.

$$\frac{\text{\# de cuentas de usuarios creados y registrados en la bitácora}}{\text{\# cuentas de usuarios creados}}$$

Escala:

Muy Bueno	= 1
Bueno	> 0.8 y < 1
Regular	> 0.6 y $\leq$ 0.8
Malo	$\leq$ 0.6

Usuarios y contraseñas

6. Se pudo observar que las claves proporcionadas por el Jefe de Sistemas son sencillas y de fácil deducción.

Situación Actual:

Producto de la revisión conocimos que las contraseñas proporcionadas por el Jefe de Sistemas a los usuarios son sencillas y por ende fáciles de deducir.

Efecto:

Este tipo de situaciones puede causar:

- Se reste confidencialidad y seguridad al correo ya que las claves son fáciles de deducir y por ende de copiar.
- Se produzca accesos no autorizados a la cuenta de un usuario produciendo una violación a la privacidad.

Recomendaciones:

Es aconsejable utilizar claves con un mínimo de ocho caracteres con una combinación de letras y números. Para esto es recomendable implementar un software que cumpla con los parámetros antes establecidos. Así mismo no es adecuado utilizar paswords de: nombres, fechas, entre otros que son de fácil deducción.

De igual manera se debe recordar al usuario cambiar sus contraseñas cada tres meses como máximo y como mínimo de forma mensual. Debemos tener en mente que toda protección que tomemos para salvaguardar la seguridad de nuestro correo no esta de más.

El Jefe de Sistemas deberá revisar si las contraseñas establecidas cumplen con los parámetros señalados asi mismo debe mantener un registro de las contraseñas previas del

usuario; por ejemplo, de los 12 meses anteriores, y evitar la reutilización de las mismas.

Finalmente informar a los usuarios que todas las contraseñas que no cumplan con los parámetros establecidos deben ser cambiadas inmediatamente.

Indicador:

Proporción de claves menores a 8 caracteres.

$$\frac{\text{\# de claves activas menores a 8 caracteres}}{\text{\# de claves activas}}$$

Escala:

Muy Bueno	≤ 0.1
Bueno	> 0.1 y ≤ 0.3
Regular	> 0.3 y ≤ 0.5
Malo	> 0.5

7. Falta de concientización de los usuarios acerca del uso del correo electrónico de la organización.

Situación Actual:

Durante el análisis conocimos que los usuarios hacen uso de su cuenta de correo no solamente para fines laborales sino también para uso personal.

Efecto:

Esta situación permite que:

- Al utilizar el correo de la organización para otros fines aumenta las probabilidades de que las máquinas se infecten de virus.
- Posible saturación del servidor de correo.
- Elevar costos de la empresa.
- Baja productividad.

Recomendaciones:

Al momento que el Gerente de Sistemas crea una nueva cuenta de correo estará en la obligación de indicarle a cada usuario las responsabilidades y obligaciones que adquiere en su uso asi como de enseñarles a gestionar con efectividad sus correos electrónicos garantizando que guarden y borren mensajes

cuando sea necesario. De igual manera se le debe indicar a cada usuario que dicha cuenta ha sido creada exclusivamente para fines laborales. Establecer una política de correo en la cual se indique:

1. No se debe utilizar la cuenta de correo de la empresa para recibir horóscopo, chistes, entre otros ya que algunos de estos mensajes podrían tener virus.
2. No abrir mensajes de personas desconocidas o con asuntos inusuales como por ejemplo: “Eres millonario”.
3. Las claves proporcionadas por el Jefe de sistemas deben ser personalizadas por los usuarios.

El jefe de sistemas debe tener identificado quienes son los usuarios que no están cumpliendo con la política establecida.

Indicador:

Proporción de usuarios de correo electrónico que conocen lo que es un SPAM.

$$\frac{\text{\# de usuarios de correo que conocen lo que es un SPAM}}{\text{\# total de usuarios de correo electrónico}}$$

Escala:

Muy Bueno	= 1
Bueno	> 0.8 y < 1
Regular	> 0.6 y ≤ 0.8
Malo	≤ 0.6

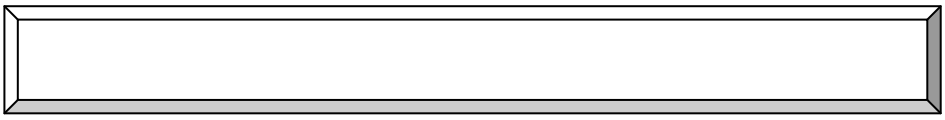
Indicador:

Proporción de SPAM en el correo electrónico de TecMotors por mes.

$$\frac{\text{\# de correos SPAM por mes}}{\text{\# total de correos enviados y recibidos}}$$

Escala:

Muy Bueno	≤ 0.1
Bueno	> 0.1 y ≤ 0.3
Regular	> 0.3 y ≤ 0.5
Malo	> 0.5



8. Las cuentas de usuario poseen capacidad ilimitada de almacenamiento.

Situación Actual:

Mediante entrevista realizada al jefe de sistemas pudimos conocer que las cuentas de usuario poseen capacidad ilimitada de almacenamiento.

Efecto:

Esta situación puede afectar en:

- Saturación del servidor de correo.
- Falta de disponibilidad del servicio.

Recomendaciones:

El Gerente de Sistemas debe asignar capacidad de almacenamiento a cada cuenta de usuario de acuerdo a las necesidades del cargo y/o función que desempeñe en TecMotors o también puede asignarlas de manera general, es decir, a todos

los usuarios asignarles por igual una cantidad mínima de almacenamiento.

Indicador:

Promedio de almacenamiento por usuario.

$$\frac{\text{Capacidad de almacenamiento utilizado por usuario}}{\text{Capacidad de almacenamiento asignado por usuario}}$$

Escala:

Muy Bueno	≤ 0.4
Bueno	> 0.4 y ≤ 0.6
Regular	> 0.6 y ≤ 0.7
Malo	> 0.7

9. El servidor de correo se encuentra en un lugar de fácil acceso a las personas. (Sabotajes, daños, errores)

Situación Actual:

Durante la revisión se pudo observar que el lugar donde se encuentra el servidor de Correo Electrónico es de fácil acceso a

las personas, cualquiera que desee puede tener contacto a poca distancia.

Efectos:

Esta situación implica que:

- Que cualquier persona que posea conocimientos superiores de informática acceda al Server para cometer un sabotaje, una travesura, entre otras y por ende la pérdida total o parcial de la información del servidor.
- El servidor se encuentre vulnerable a fallas de seguridad físicas como un daño parcial o total del equipo ya sea voluntaria o involuntariamente, robo, destrucción, entre otros.
- Puede ocurrir que alguien por descuido o imprudencia tropiece con el equipo provocando daños.

Recomendaciones:

Resguardar en un lugar seguro y restringido el servidor de tal manera que la probabilidad de que exista un incidente contra el computador sea mínima al igual que la probabilidad de que exista manipulación del equipo por cualquier persona no autorizada. Esto ayudará a resguardar las aplicaciones en términos de confidencialidad, integridad y disponibilidad.

Se deben colocar letreros prohibiendo el ingreso al área de sistemas de parte de personal no autorizado y mantener la puerta siempre cerrada.

Asi también mediante el monitoreo se puede detectar e identificar el ingreso de personal no autorizado a dicha área.

Dar a conocer a todos los trabajadores de TecMotors sobre la restricción del acceso a dicho departamento.

Indicador:

Proporción de visitas por mes al lugar donde se encuentra el servidor.

$$\frac{\text{\# de accesos no autorizados por mes}}{\text{\# total de visitas por mes}}$$

Escala:

Muy Bueno	≤ 0.1
Bueno	> 0.1 y ≤ 0.3
Regular	> 0.3 y ≤ 0.5
Malo	> 0.5

Partes y/o piezas del computador

10. Ausencia de medidas de seguridad en los equipos.

Situación actual:

Mediante cuestionario y observación se constató que los equipos servidores (Linux y Windows) carecen de seguridad física.

Efecto:

- Pérdida parcial o total de los equipos, sus partes y/o piezas.
- Perdida de dinero.
- Perdida de información

Recomendación:

Establecer un área restringida para ubicar los servidores.

Prohibir el ingreso de personas no autorizadas al departamento de sistemas.

Dar mantenimiento a la red y a los equipos cada vez que se crea necesario.

Indicador:

Proporción de equipos buenos por mes.

$$\frac{\text{\# de equipos trabajando}}{\text{\# total de equipos}}$$

Escala:

Muy Bueno	≥ 0.9
Bueno	≥ 0.7 y < 0.9
Regular	≥ 0.5 y < 0.7
Malo	< 0.5

Archivos (Imágenes y Texto)

11. Recibir mensajes infectados.

Situación actual:

Mediante reuniones y entrevistas realizadas se pudo comprobar que a las cuentas de correo llegan mensajes con imágenes y texto infectados por algún virus.

Efecto:

- Pérdida de información.
- Dañar las máquinas.
- Infectar toda la red.
- Pérdidas económicas para el negocio.

Recomendación

Implantar filtros de spam para controlar la cantidad de mensajes no deseados que reciben los usuarios.

Levantar un firewall para de esta forma proteger la red contra intentos de accesos no autorizados.

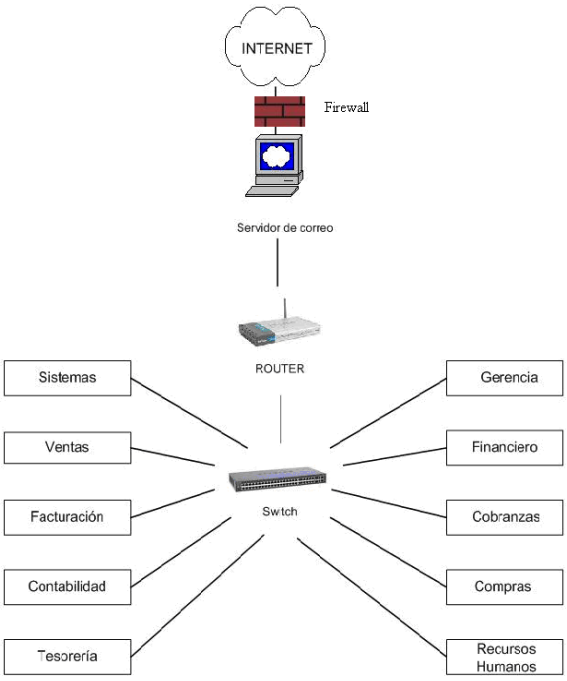


FIGURA 4.2 Implementación de Firewall en TecMotors

Advertir a los usuarios de nunca abrir archivos enviados por desconocidos ni de extensiones desconocidas.

Analizar los archivos adjuntos con el antivirus antes de abrirlos.
El jefe de sistemas debe actualizar el antivirus y realizar monitoreos a la red periódicamente.

Al momento de considerar un analizador de virus para servidor de correo se deben tener en cuenta ciertos puntos como: poder analizar archivos comprimidos, actualización automática, simpleza en la administración.

Indicador:

Proporción de mensajes infectados.

$$\frac{\text{\# de mensajes infectados}}{\text{\# total de mensajes recibidos}}$$

Escala:

Muy Bueno	≤ 0.1
Bueno	> 0.1 y ≤ 0.3
Regular	> 0.3 y ≤ 0.5
Malo	> 0.5

12. Carencia de una firma electrónica.

Situación Actual:

Durante la revisión se pudo observar que la empresa no posee firma digital, aunque no descartan la idea de implantarla con el tiempo.

Efecto:

Estas situaciones permiten que:

- Personas con los conocimientos necesarios y no autorizadas accedan a la información de la empresa y hagan uso de ella.
- Violación a la privacidad de los mensajes.
- Violación a la integridad de los mensajes.
- Falta de confidencialidad de información.
- Mal uso de información.
- Divulgación no autorizada de información.

Recomendaciones:

La pronta implantación de una firma digital que permita al receptor verificar la integridad de los mensajes. Posteriormente obtener un certificado digital para garantizar la autenticidad de la firma digital.

CONCLUSIONES

Para las empresas y usuarios en general.

- Podemos decir que en la actualidad el correo electrónico es un recurso básico con un funcionamiento sencillo de gran uso que debe protegerse, lo que demanda la implementación de esquemas de seguridad.

- Es a través de este medio de comunicación que algunos negocios se logran concretar día a día, sin importar la ubicación geográfica.

- En la era de la conectividad electrónica, donde abundan los virus, los hackers y el fraude electrónico no podemos obviar la importancia de la seguridad en el correo electrónico.

- La seguridad de correo electrónico es un conjunto de técnicas que tratan sobre la protección de la información frente a observadores no autorizados. Enmarcándose en los principios de confidencialidad, integridad y disponibilidad.

- Este trabajo tiene como finalidad mostrar que toda información que viaje por la red es de fácil acceso para una persona que tenga los

conocimientos necesarios para hacerlo y más aún cuando no se han establecido esquemas de seguridad básicos, por lo que debemos tomar las medidas necesarias de protección de información.

- El presente trabajo es un apoyo y guía no sólo para esta empresa sino para todas aquellas empresas y personas que desarrollen sus actividades comerciales y/o productivas a través de este importante medio de comunicación.

Para TecMotors S.A.

- El análisis de la seguridad de correo electrónico, desarrollado en la empresa, ha contribuido a ampliar conocimientos en materia de seguridad para todos los integrantes que poseen cuenta de correo electrónico en la organización.

- Los usuarios no están conscientes de los riesgos, responsabilidades y del buen uso que le deben dar a sus cuentas de correo.

- En el trabajo se pudieron determinar una serie de hallazgos como:

Usuarios y Contraseñas

1. Se pudo observar que las claves proporcionadas por el Jefe de Sistemas a los usuarios son sencillas y de fácil deducción.
2. Falta de concientización de los usuarios acerca del uso del correo electrónico de la organización.

Servidor de correo

3 Las cuentas de usuario poseen capacidad ilimitada de almacenamiento.

4 El servidor de correo se encuentra en un lugar de fácil acceso a las personas (sabotajes, daños, errores).

Cuentas de correo

5 Las cuentas de los usuarios pueden quedar abiertas durante tiempo indefinido aunque no se las esté usando.

6 Accesos no autorizados a las cuentas de correo.

7 No hay respaldo de las cuentas de usuario (Backups).

8 No existe manual de políticas de seguridad de correo electrónico.

9 No existe bitácora de control de las cuentas de usuario.

Partes y/o piezas de computador

10 Ausencia de medidas de seguridad en los equipos.

Archivo (Imágenes y texto)

11 Recibir mensajes infectados.

12 Carencia de una firma electrónica.

RECOMENDACIONES

Para las empresas y usuarios en general

- Los riesgos de violación a la seguridad de correo electrónico están constantemente presente, es por ésto que se debe implantar y desarrollar controles preventivos, detectivos y correctivos.

- Tener una cuenta de correo implica que nosotros como usuarios somos responsables del uso de la misma, por eso debemos tener en consideración los siguientes puntos.
    - Cerrar nuestra cuenta de usuario si nos vamos a ausentar por más de cinco minutos.
    - Usar contraseñas con un mínimo de ocho caracteres en combinación de números y letras.
    - No divulgar nuestra contraseña.
    - Cambiar nuestra contraseña cada vez que lo creamos necesario o como mínimo cada mes.
    - No abrir mensajes que han sido enviados por desconocidos.

Para TecMotors S.A.

- La organización debe darle la importancia necesaria a la seguridad de correo electrónico.

- Se debe redactar una política de seguridad de correo electrónico, que incluya los siguientes puntos:
    - Como prevenir ataques al correo electrónico.
    - Protección de archivos adjuntos de correo electrónico, revisión de un antivirus.
    - Lineamientos sobre cuando no utilizar correo electrónico.
    - Responsabilidad de los usuarios (empleados) de no comprometer a la organización, por ejemplo, realizando compras no autorizadas, enviando correos electrónicos difamatorios.
    - Uso de técnicas criptográficas para proteger la confidencialidad e integridad de los mensajes de correo electrónico.
    - Controles adicionales para examinar mensajes electrónicos que no pueden ser autenticados.

- Los administradores del correo electrónico de la empresa deben crear sólamente las cuentas de correo electrónico necesarias y esta

creación debe estar debidamente respaldada por una solicitud de creación de la cuenta firmada por el Gerente de la empresa.

- Se debe concienciar a los usuarios acerca del buen uso del correo electrónico de la empresa por medio de charlas y cursos de capitación sobre la información que se está transmitiendo vía correo electrónico al igual como en los riegos en que se está incurriendo

- Levantar un firewall a la brevedad posible con la finalidad de proteger la red interna.

- Se debe crear una bitácora de control en la cual se registre la creación, eliminación y modificación de las cuentas de correo.

- Desarrollar políticas de contraseñas así como configurar las cuentas de usuario para que éstas se ajusten a la misma.
    - Una cantidad mínima de caracteres. Lo recomendable es que esté compuesta de 8 caracteres entre letras (mayúsculas y minúsculas) y números.
    - El tiempo que puede permanecer una clave sin modificarse es 30 días.

- Solicitar al usuario que cambie periódicamente su clave de acceso (mínimo 30 días).
- Prohibir la reutilización de claves del usuario, es decir, por comodidad algunos usuarios prefieren librarse del cambio de la clave modificándola levemente.
- Establecer jerarquías. Determinar quién está autorizado a modificar claves con un control respectivo.
- Configurar el correo electrónico para denegar el ingreso luego de 3 de intentos fallidos.

- Dar a conocer a los usuarios sobre la política de seguridad de correo electrónico.

- Capacitar a los usuarios sobre el uso de sus cuentas asi como las responsabilidades que contraen.

- Llevar un registro claro de la creación, eliminación y modificación de cuentas.

- Cada cierto tiempo comunicar a los usuarios que realicen el cambio de contraseñas a sus cuentas de correo, mínimo 30 días.

- Cambiar periódicamente las claves de acceso al servidor de correo, mínimo 30 días.

- El correo de TecMotors debe ser utilizado exclusivamente para fines laborales.

- Respaldar las cuentas de usuario periódicamente.

- El Jefe de Sistemas junto con el Gerente de TecMotors deben delegar a una persona que se encargue de medir si los controles establecidos están cumpliendo con su función, a través de los indicadores desarrollados.

ANEXOS

ANEXO 1

CRONOGRAMA DE TRABAJO

Nombre de la tarea	Duración	may-06										jun-06																										jul-06	
		20	22	23	24	25	26	27	29	30	31	1	2	3	5	6	7	8	9	10	12	13	14	15	16	17	19	20	21	22	23	24	26	27	28	29	30	1	3
		S	L	M	M	J	V	S	L	M	M	J	V	S	L	M	M	J	V	S	L	M	M	J	V	S	L	M	M	J	V	S	L	M	M	J	V	S	L
Análisis Preliminar																																							
Reunión con la gerencia y/o el Jefe de Sistemas.	7 días																																						
Elaboración programa de trabajo (Anexo 3)	1 día																																						
Diseño de la Guía de Visita Previa y entrevistas.	1 día																																						
Elaboración de la Guía de Visita Previa (Anexo 4)	1 día																																						
Evaluación de Controles y Seguridad del Correo Electrónico																																							
Entrevista al Jefe de Sistemas (Anexo 5)	1 día																																						
Entrevista al Asistente Técnico (Anexo 6 y Anexo 7)	1 día																																						
Análisis y desarrollo de los resultados obtenidos en las entrevistas.	3 días																																						
Constatación física del inventario de computadoras. (Anexo 8)	1 día																																						
Identificación y Análisis de Riesgo																																							
Determinación y clasificación de riesgos (Anexo 9)	1 día																																						
Preparación de papeles de trabajo y análisis de los resultados obtenidos.	6 días																																						
Desarrollo de Matriz de Control de Riesgos (Anexo 10)	2 días																																						
Comparación de las categorías de riesgo. (Anexo 11)	3 días																																						
Proceso de Votación (Amenazas - Objetos) (Anexo 12 y Anexo 15)	1 día																																						
Comparación de categorías de riesgo (Anexo 14)	1 día																																						
Suma de ambas votaciones. (Anexo 13 y Anexo 16)	1 día																																						
Elaboración de la matriz de combinación de categorías. (Anexo 17)	1 día																																						
Elaboración de la matriz de resultados (Anexo 18)	2 días																																						

ANEXO 1

CRONOGRAMA DE TRABAJO

Nombre de la tarea	Duración	may-06										jun-06																												
		20	22	23	24	25	26	27	29	30	31	1	2	3	5	6	7	8	9	10	12	13	14	15	16	17	19	20	21	22	23	24	26	27	28	29	30			
		S	L	M	M	J	V	S	L	M	M	J	V	S	L	M	M	J	V	S	L	M	M	J	V	S	L	M	M	J	V	S	L	M	M	J	V			
Análisis de Areas Críticas Establecimientos de Controles																																								
Matriz de identificación de los niveles de riesgo: alto, medio, bajo (Anexo 19)	1 día																																							
Análisis y elaboración de controles (Anexo 20)	5 días																																							
Reunión de equipo de trabajo	7 días																																							
Informe																																							
Comunicación de resultados	1 día																																							

Elab por: B. Salazar **Fecha**: 15/05/06

ANEXO 2

PROGRAMA DE TRABAJO

Empresa: TecMotors S.A.	**Dpto:** Sistemas		
OBJETIVOS/PROCEDIMIENTOS	**REF.**	**ELAB. POR**	**FECHA**
RELEVAMIENTO DE INFORMACIÓN			
Objetivo			
Adquirir conocimiento de la seguridad de correo electrónico que posee la organización.			
Procedimientos:			
1. Elaborar una guía de visita previa que nos permita identificar los objetivos la estructura organica de TecMotors S.A. Información general de la empresa.	Anexo 3	B. Salazar	24-May
2. Entrevistar al Jefe del Dep. de Sistemas para asi obtener información precisa acerca de la evaluación de controles y seguridad del correo electrónico.	Anexo 4	B. Salazar	24-May
IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS			
Objetivo			
Establecer los niveles de riesgo / sensibilidad de correo electrónico en la empresa.			
Procedimientos			
1. Entrevistar al Asistente Técnico acerca de sus funciones y responsabilidades en TecMotors.	Anexo 5	B. Salazar	24-May
2. Entrevistar al Asistente Técnico 2 acerca de sus funciones y responsabilidades en TecMotors.	Anexo 6	B. Salazar	24-May
3, Realizar constatción física de los equipos configurados con acceso a correo electrónico y los servidores de correo.	Anexo 7	B. Salazar	06-Jun
4, Servidores	Anexo 8	B.Salazar	06-Jun

PROGRAMA DE TRABAJO

5. Riesgos de Seguridad de correo electrónico	Anexo 9	B. Salazar	06-Jun
6, Establecer la Clasificación de Riesgos Existentes.	Anexo 9	B. Salazar	06-Jun
7, Establecer Matriz de Control de Riesgos (Amenazas y Objetos).	Anexo 10	B. Salazar	06-Jun
8. Realizar la Comparación de Categorías de Riesgos (Amenazas).	Anexo 11	B. Salazar	15-Jun
9. Realizar Proceso de Votación del Grupo Delphi (Amenazas).	Anexo 12	B. Salazar	16-Jun
10. Realizar la Suma de Votos de las Amenazas.	Anexo 13	B. Salazar	19-Jun
11. Elaborar la Comparación de Categorías de Riesgo (Objetos).	Anexo 14	B. Salazar	15-Jun
12. Elaborar el Proceso de Votación (Objetos).	Anexo 15	B. Salazar	16-Jun
13, Realizar la Suma de Votos de los Objetos.	Anexo 16	B. Salazar	19-Jun
14, Realizar la Matriz de Combinación de las 2 Catagorías.	Anexo 17	B. Salazar	20-Jun
15, Realizar la Matriz de Resultados con Riesgos de Sensibilidad e Identificación de Niveles de Riesgo.	Anexo 18	B. Salazar	21-Jun
16, Establecer y documentar Controles Definitivos.	Anexo 20	B. Salazar	28-Jun
17, Implementación de controles	Anexo 21	B Salazar	13-Abr

Elaborado por: B. Salazar **Fecha:** 23/05/06
Revisado por: A. Naranjo **Fecha:** 11/02/07

ANEXO 3

GUIA DE VISITA PREVIA
INFORMACIÓN GENERAL

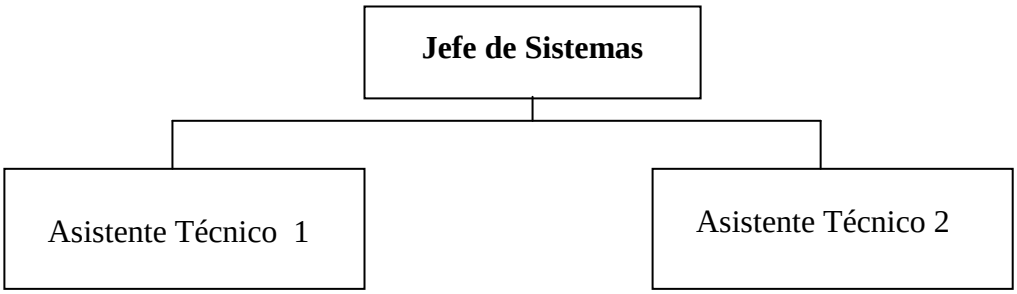
Nombre de la Entidad: TecMotors S.A.
Nombre del Departamento: Sistemas
Persona Entrevistada: Jefe del Departamento **Fecha:** 24 de Mayo/06

1. **¿Cuál es el objetivo de TecMotors?**
   La venta de llantas y aditivos al por mayor y menor creando satisfacción y bienestar a sus clientes, colaboradores y rentabilidad a sus accionistas.

2. **¿Cuál es el número de trabajadores que posee TecMotors?**
   Un total de 43 empleados.

3. **¿Cuál es el objetivo del Departamento de Sistemas?**
   El objetivo principal del departamento de Sistemas es satisfacer las necesidades y exigencias de los usuarios que conforman el personal de la empresa. Asi como salvaguardar la integridad de la información.

4. **¿Cuál es la estructura orgánica del Departamento?**

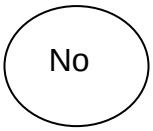


5. **¿Cuál es su función como Jefe de Sistemas de Tecmotors?**
   Dar soporte técnico a toda la empresa (software y hardware).

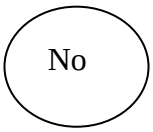
6. **¿Existe manual de funciones del departamento?**

   Si No

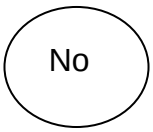
7. ¿Existe manual de procedimientos del departamento?

Si 

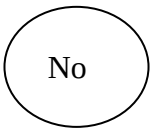
8. ¿Existe un manual de política de seguridad de correo electrónico?

Si 

9. ¿Cuenta con algún tipo de seguridad física el departamento de Sistemas?

Si 

10. ¿Poseen seguro contra robo de los equipos?

Si 

11. ¿Cuáles son los motivos de la evaluación de seguridad de correo electrónico?

Uno de los motivos de esta evaluación es el desconocimiento por parte de la gerencia de la seguridad que debe poseer el correo electrónico de la empresa. Así mismo se muestra un interés por parte de la Gerencia en poseer un correo seguro (que la información viaje segura).

La Gerencia desea garantizar la seguridad del correo electrónico y para ello requiere realizar una evaluación de la seguridad de correo electrónico.

Elaborado por: B. Salazar **Fecha:** 24/05/06
Revisado por: A. Naranjo **Fecha:** 11/02/07

ANEXO 4

ENTREVISTA
EVALUACIÓN DE CONTROLES Y SEGURIDAD DEL CORREO ELECTRÓNICO

Empresa: TecMotors S.A.
Departamento: Sistemas
Persona entrevistada: Jefe del Departamento **Fecha:** 24 de Mayo/06

1. **¿Posee correo electrónico la organización?**

   Si (circled) No

2. **¿Cuál es el sistema de correo electrónico que usa?**
   Internet explorer.

3. **¿Cuál es su proveedor de Internet y por qué?**
   Ecutel es nuestro proveedor de Internet. Tenemos Internet las 24 horas al día los 7 días de la semana. Los 365 días al año a un costo de $100.00 al mes.

Seguridad de los equipos y control de accesos

4. **¿Poseen seguro de equipos?**

   Si (circled) No

5. **¿Con cuantos equipos cuenta TecMotors para uso de correo electrónico y como están distribuidos los equipos?**
   Tenemos un total de treinta máquinas con acceso a correo electrónico y dos servidores de correo uno en Linux y el otro en Windows.

6. **¿Dónde se encuentran ubicados los servidores de correo?**
   Se encuentran ubicados en el departamento de sistemas.

7. **¿Quienes tienen acceso al departamento de sistemas?**
   Cualquier persona de la empresa. Por ahora el departamento de sistemas no cuenta con seguridad física ya que la puerta tiene dañado el seguro.

8. **¿Quiénes tienen acceso al servidor de correo?**
   El Jefe de Sistemas y dos asistentes técnicos con autorización.

Claves de acceso

9. **¿Poseen claves de acceso los servidores de correo y como están compuestas?**
   Sí, están compuestas de 10 caracteres entre número y letras las cuales son asignadas y cambiadas únicamente por el Jefe de sistemas.

10. **¿Cada cuánto tiempo son cambiadas éstas claves?**
    Las claves de acceso son cambiadas cada vez que el Jefe de Sistemas lo crea necesario. No en un tiempo especifico.

11. **¿Las contraseñas de usuario asignadas inicialmente bajo qué parámetros son establecidas?**
    No se tiene establecido un parámetro específico para la asignación de claves. Las contraseñas asignadas inicialmente son iguales a los nombres de usuario. Ejemplo:
    Usuario: jgarcia
    Contraseña: jgarcia

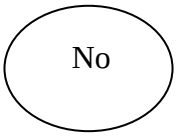
12. **¿Cada cuánto tiempo los usuarios cambian sus contraseñas y bajo qué parámetros?**
    Pueden cambiar sus contraseñas cuantas veces ellos lo crean necesario, pero bajo la supervisión del Jefe de Sistemas. No tenemos establecido un parámetro específico de cómo deben estar compuestas las contraseñas. En algunos casos las contraseñas que asignan los usuarios son sus fechas de cumpleaños o la de sus hijos o sus nombres. Algunos de los usuarios conservan las contraseñas iniciales igual al nombre de usuario creado como se indicó anteriormente, es decir la que fue asignada al momento de la creación de la cuenta.

Cuentas de usuario

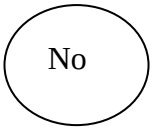
13. **¿Quién es el encargado de la creación y eliminación de cuentas de correo de TecMotors?**
    El Jefe de Sistemas o los Asistentes Técnicos son los encargados de crear o eliminar las cuentas a los usuarios y asignarles una contraseña inicial como se explico anteriormente, la cual posteriormente podrá ser cambiada por el usuario cuando crea conveniente.

14. **¿La solicitud de creación de una cuenta de usuario se la realiza de forma verbal o escrita?**
    En el momento que una persona empieza a forma parte de TecMotors se le crea una cuenta de correo electrónico. Este procedimiento no necesita autorización. Es algo que se debe hacer.

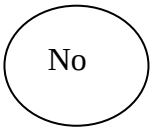
15. **¿Posee respaldo de las cuentas de usuario?**

    Si 

16. **¿Posee un registro o bitácora de control de las cuentas de usuario?**

    Si 

17. **¿Posee un registro actualizado de la creación y eliminación de cuentas de correo de TecMotors?**

    Si 

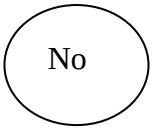
18. **¿Cuántas cuentas de usuario de TecMotors se encuentran activas al momento?**
    En este momento tenemos 35 cuentas de usuario.

19. **De las cuentas de usuario antes mencionadas, ¿Todas pertenecen a trabajadores actuales?**
    No, sólo 33 son de trabajadores actuales. Lo que sucede es que las otras dos cuentas son de trabajadores que fueron despedidos el mes pasado y no han sido eliminadas por falta de tiempo.

20. **¿Cuál es la capacidad de almacenamiento de cada cuenta de usuario?**
    Su capacidad es ilimitada.

Política de Seguridad

21. **¿Se cuenta con un manual de políticas de seguridad de correo electrónico?**
    Si



22. **¿Al momento de crear una cuenta de correo se le indica al usuario las responsabilidades que está adquiriendo así como el uso que le debe dar?**
    No, se asume que ellos ya las conocen.

23. **¿Los usuarios utilizan el correo de TecMotors para actividades ajenas a la empresa? Explique**
    Algunos usuarios utilizan la cuenta de correo de TecMotors para recibir y/o enviar mensajes personales. Esto depende de cada usuario. He visto que algunos reciben propagandas de tiendas, mensajes de amigos.

Seguridad de Información

24. **¿Por cuánto tiempo pueda permanecer abierto un correo sin ser usado?**
    El correo puede quedar abierto por tiempo indefinido aunque no se ésta usando.

25. **¿Qué posibilidad existe de que los equipos se infecten por algún mensaje que contenga virus?**
    En el momento que llega un correo infectado, el servidor automáticamente lo intenta desinfectar, pero si no puede hacerlo borra el mensaje automáticamente y al destinatario le llega un mensaje

indicándole de que un correo ha sido eliminado de su cuenta por contener virus.

26. **¿Cuál es la capacidad de archivos adjuntos que puede recibir y enviar en un mail?**
    La capacidad de archivos adjuntos que pueden recibir es ilimitada mientras que la de enviar es de 2 GB.

27. **¿Posee Firma electrónica?**
    No, pero si hemos considerado la idea de implantarla.

28. **¿Posee certificado digital?**

    Si No

29. **¿Poseen estándares escritos de mejora continua?**

    Si No

30. **¿Se tiene conciencia de la seguridad que debe poseer el correo electrónico de la empresa?**
    Si, pero todo cambio lleva tiempo.

31. **¿Cuáles son los problemas que se han presentado en el uso del correo electrónico?**
    Uno de los problemas que se ha presentado es que los usuarios utilizan su cuenta de correo electrónico para almacenar y enviar información personal, es decir ajena a TecMotors aumentando la posibilidad de que el servidor se sature o que los equipos se infecten de virus.

32. **¿A la presente fecha se ha realizado una auditoria informática a la empresa?**
    A nivel informático nunca.

Elaborado por: B. Salazar **Fecha:** 24/05/06
Revisado por: A. Naranjo **Fecha:** 11/02/07

ANEXO 5

EVALUACIÓN DE FUNCIONES Y RESPONSABILIDADES

Empresa: TecMotors S.A.
Departamento: Sistemas
Persona entrevistada: Asistente Técnico 1 **Fecha:** 24 de Mayo/06

1. **¿Cuál es su función dentro de TecMotors?**
   Brindar ayuda y asesoría informática al departamento y a todas las personas que trabajan en TecMotors. El Jefe de Sistemas me llama o me hace llamar por teléfono y en un máximo de dos horas yo debo estar presente en la compañía. De igual manera al finalizar mi labor se lo comunico al Jefe del Departamento de Sistemas.

2. **¿Esta Usted autorizado a crear cuentas de usuario en el correo de TecMotors?**
   Si (X) No ( )

3. **¿Por quién debe estar autorizado para crear cuentas de usuario en el correo de TecMotors?**
   Por el Jefe de Sistemas o por el Gerente. Cualquier actividad que yo vaya a realizar debe estar previamente autorizada por cualquiera de las dos personas nadie más.

4. **¿Esta autorización de qué forma se la realiza?**
   Verbal (X) Escrita ( )

5. **¿Posee un registro o bitácora de control de las cuentas de usuario?**
   Si No (X)

6. **¿Usted conoce las claves de acceso a los servidores?**
   Si (X) No ( )

7. **¿Al momento de asignar las contraseñas a los usuarios en la creación de una cuenta de correo bajo qué patrones lo realiza?**
   La empresa ya tiene definida la estructura de las claves de acceso. Sólo se sigue un orden.

8. **¿Lleva un registro detallado de las actividades que realiza?**
   Si (X) No ( )

9. ¿Tiene usted conciencia de la seguridad que debe poseer el correo electrónico de la empresa?

Si, y por eso mismo esta en discusión la implantación de una firma digital.

10. ¿Qué seguridades existen en el correo electrónico?

Cifrado ( )
Firma Digital ( )
Certificado Digital ( )
Ninguna (x)

11. ¿Cuáles son los problemas que se han presentado en el uso del correo electrónico?

Los problemas que se presentan son a nivel de usuario debido a que éstos se suscriben para recibir publicidad en la cuenta de correo de TecMotors que poseen, Infectando en ciertas ocasiones los equipos.

Elaborado por: B. Salazar **Fecha:** 24/05/06
Revisado por: A. Naranjo **Fecha:** 11/02/07

ANEXO 6

EVALUACIÓN DE FUNCIONES Y RESPONSABILIDADES

Empresa: TecMotors S.A.
Departamento: Sistemas
Persona entrevistada: Asistente Técnico 2 **Fecha:** 24 de Mayo/06

1. ¿Cuál es su función dentro de TecMotors?

En primer lugar yo no soy trabajador estable de TecMotors, yo solamente presto servicios cuando el Jefe de Sistemas lo solicita. Mi labor es prestar ayuda al Jefe de Sistemas y a todo el personal de la organización. El Jefe de Sistemas me llama o me hace llamar por teléfono y en un máximo de dos horas yo debo estar presente en la compañía. De igual manera al finalizar mi labor se lo comunico al Jefe del Departamento de Sistemas.

2. ¿Esta Usted autorizado a crear cuentas de usuario en el correo de TecMotors?

Si (X) No ( )

3. ¿Por quién debe estar autorizado para crear cuentas de usuario en el correo de TecMotors?

Por el Jefe de Sistemas o por el Gerente. Toda actividad que se realice debe estar previamente autorizada por el Jefe de Sistemas.

4. ¿Esta autorización de qué forma se la realiza?

Verbal (X) Escrita ( )

5. ¿Posee un registro o bitácora de control de las cuentas de usuario?

Si No (X)

6. ¿Usted conoce las claves de acceso a los servidores?

Si (X) No ( )

7. ¿Al momento de asignar las contraseñas a los usuarios en la creación de una cuenta de correo bajo qué patrones lo realiza?

La empresa ya tiene definida la estructura de las claves de acceso. Sólo se sigue un orden. Ejemplo:
Usuario: bsalazar
Contraseña: bsalazar

8. ¿Lleva un registro detallado de las actividades que realiza?

Si (X) No ( )

9. ¿Tiene usted conciencia de la seguridad que debe poseer el correo electrónico de la empresa?

Si, y por eso mismo esta en discusión la implantación de una firma digital.

10. ¿Cuáles son los problemas que se han presentado en el uso del correo electrónico?

Algunas veces no nos llegan los correos. Otro problema que vale señalar es el uso que le dan los usuarios a sus cuentas de correo.

Elaborado por: B. Salazar **Fecha:** 24/05/06

Revisado por: A. Naranjo **Fecha:**11/02/07

ANEXO 7

CONSTATACIÓN FÍSICA DEL INVENTARIO DE COMPUTADORAS CONFIGURADAS CON ACCESO A CORREO ELECTRÓNICO Y SERVIDORES DE CORREO

Hardware

Nº	UBICACIÓN			Procesador	Sistema Operativo	Observación
	Área	Departamento	Encargado			
1	Financiera y Administrativa	Gerencia	Gerente General	AMD	Windows XP	Sin novedad
2		Financiero	Asistente de Gerencia	AMD	Windows XP	Sin novedad
3		Financiero	Gerente Financiero	AMD	Windows XP	Sin novedad
4		Financiero	Asistente Financiero	AMD	Windows XP	Sin novedad
5		Compras	Jefe de Compras e Importaciones	AMD	Windows	Sin novedad
6		Compras	Asistente de Compras	AMD	Windows XP	Sin novedad

CONSTATACIÓN FÍSICA DEL INVENTARIO DE COMPUTADORAS CONFIGURADAS CON ACCESO A CORREO ELECTRÓNICO Y SERVIDORES DE CORREO

Hardware

Nº	UBICACIÓN			Procesador	Sistema Operativo	Observación
	Área	Departamento	Encargado			
7		Facturación	Facturadora 1	AMD	Windows XP	Sin novedad
8		Facturación	Facturadora 2	AMD	Windows XP	Sin novedad
9		Facturación	Facturadora 3	AMD	Windows XP	Sin novedad
10		Facturación	Facturadora 4	AMD	Windows XP	Sin novedad
11		Contabilidad	Jefe de Contabilidad	AMD	Windows XP	Sin novedad
12		Contabilidad	Nómina y rol de pago	AMD	Windows XP	Sin novedad

CONSTATACIÓN FÍSICA DEL INVENTARIO DE COMPUTADORAS CONFIGURADAS CON ACCESO A CORREO ELECTRÓNICO Y SERVIDORES DE CORREO

Hardware

Nº	UBICACIÓN			Procesador	Sistema Operativo	Observación
	Área	Departamento	Encargado			
13		Tesorería	Tesorero	AMD	Windows XP	Sin novedad
14	Ventas	Ventas	Gerente Ventas/Mercadeo	AMD	Windows XP	Sin novedad
15		Ventas	Publicidad	AMD	Windows XP	Sin novedad
16		Ventas	Asistente de Ventas	AMD	Windows XP	Sin novedad
17		Ventas	Asistente de Ventas	AMD	Windows XP	Sin novedad
18	Crédito	Cobranzas	Jefe de Crédito y Cobranzas	AMD	Windows XP	Sin novedad

CONSTATACIÓN FÍSICA DEL INVENTARIO DE COMPUTADORAS CONFIGURADAS CON ACCESO A CORREO ELECTRÓNICO Y SERVIDORES DE CORREO

Hardware

Nº	UBICACIÓN			Procesador	Sistema Operativo	Observación
	Área	Departamento	Encargado			
19		Cobranzas	Asistente de Crédito y Cobranzas 1	AMD	Windows XP	Sin novedad
20		Cobranzas	Asistente de Crédito y Cobranzas 2	AMD	Windows XP	Sin novedad
21		Cobranzas	Asistente de Crédito y Cobranzas 3	AMD	Windows XP	Sin novedad
22		Cobranzas	Asistente de Crédito y Cobranzas 4	AMD	Windows XP	Sin novedad
23		Bodega	Jefe de Bodega	AMD	Windows XP	Sin novedad
24	Recursos Humanos	Recursos Humanos	Jefe de Recursos Humanos	AMD	Windows XP	Sin novedad
25	Sistemas	Sistemas	Jefe de Sistemas	AMD	Windows XP	Sin novedad

CONSTATACIÓN FÍSICA DEL INVENTARIO DE COMPUTADORAS CONFIGURADAS CON ACCESO A CORREO ELECTRÓNICO Y SERVIDORES DE CORREO

Hardware

Nº	UBICACIÓN			Procesador	Sistema Operativo	Observación
	Área	Departamento	Encargado			
26		Sistemas	Jefe de Sistemas	Pentium IV 3.0	Linux	Disco duro de 80 (Servidor de correo)
27		Sistemas	Jefe de Sistemas	Pentium IV 3.0	Windows XP	Disco duro de 36 Gb. (Servidor de correo)

Software

El sistema de aplicación que utiliza TecMotors para el desarrollo de sus actividades contiene cinco módulos:

- Cuentas por Pagar
- Bancos
- Contabilidad
- Cobranzas
- Inventario

Dicho sistema fue desarrollado por la Compañía Austro Cia Ltda.

Elaborado por: B. Salazar **Fecha:** 06/06/06

Proporcionado por: Jefe de Sistemas **Fecha:**24/05/06

ANEXO 8

Servidores

Elaborado por: B. Salazar **Fecha:** 06/06/06
Proporcionado por: Jefe de Sistemas **Fecha:** 24/05/06

ANEXO 9

RIESGOS DE SEGURIDAD DE CORREO ELECTRONICO

1	Las claves proporcionadas por el Jefe de Sistemas son sencillas y de fácil deducción.
2	Falta de concientización sobre el uso del correo electrónico de TecMotors.
3	Ausencia de política de seguridad de correo electrónico.
4	Carencia de bitácora de control sobre las cuentas de usuario creadas, eliminadas y los perfiles.
5	No existe respaldo de información.
6	Accesos no autorizados a las cuentas de correo (divulgación y manipulación de información).
7	Ausencia de medidas de seguridad en los equipos.
8	Virus en los equipos.
9	Carencia de firma electrónica.
10	Fácil acceso al servidor de correo por personas no autorizadas.
11	Saturación de servidor por SPAMS adjuntos a los mensajes.
12	Falta de disponibilidad de información (perdida de información).
13	Suplantación de identidad.
14	Intercepción de mensajes.

Elaborado por: B. Salazar **Fecha:** 06/06/06
Revisor por: A. Naranjo **Fecha:** 11/02/07

ANEXO 10

CLASIFICACIÓN DE RIESGOS EXISTENTES

No.	OBJETOS	# RIESGO
1	**Usuarios y contraseñas.**	
	Las claves proporcionadas son sencillas y de fácil deducción.	1
	Falta de concientización de los usuarios acerca del uso del correo electrónico de la organización.	2
2	**Servidor de correo.**	
	Las cuentas de usuario poseen capacidad ilimitada de almacenamiento provocando saturación del servidor.	11
	El servidor de correo se encuentra en un lugar de fácil acceso a las personas. (sabotajes, daños, errores)	10
3	**Cuentas de correo.**	
	Las cuentas de los usuarios de correo electrónico pueden quedar abiertas durante tiempo indefinido aunque no se las esté usando.	13
	Accesos no autorizados.	6
	No hay respaldo de las cuentas de usuario (backups).	5-12
	Inexistencia de un manual de política de seguridad de correo electrónico.	3
	Ausencia de bitácora de control de las cuentas de usuario.	4
4	**Partes y/o piezas del computador.**	
	Ausencia de medidas de seguridad en los equipos.	7
5	**Archivos**	
	Recibir mensajes infectados.	8
	Carencia de firma electrónica.	9-14

Las amenazas Generales que fueron determinadas y que afectan tanto a la

parte física como lógica son:

No.	AMENAZAS	# AMENAZA
1	Accesos no autorizados a las cuentas de correo y/o uso inadecuado del correo y de la información.	1
2	Pérdidas monetarias en el negocio.	2
3	Pérdida de información y/o equipos.	3
4	Infectar las máquinas con virus.	4
5	Saturación del servidor.	5

ANEXO 11

MATRIZ DE CONTROL DE RIESGO (AMENAZAS Y OBJETOS)

Amenazas / Objetos	Accesos no autorizados y/o mal uso de la información.	Pérdidas monetarias.	Pérdida de información y/o equipos.	Virus	Saturación del servidor.
Usuarios y Contraseñas.					
Servidor de correo.					
Cuentas de correo.					
Partes y/o piezas del computador.					
Archivos					

Elaborador por: B. Salazar. **Fecha:** 06/06/06
Revisado por: Ing. A Naranjo. **Fecha:** 11/02/07

ANEXO 12
COMPARACIÓN DE CATEGORIA DE RIESGO (AMENAZAS)

Accesos no autorizados y/o mal uso de la información.	Accesos no autorizados.				
Pérdidas monetarias.		Pérdidas monetarias.			
Pérdida de información y/o equipos.			Pérdida de información y/o equipos.		
Virus				Virus	
Saturación del servidor.					Saturación del servidor.

Elaborador por: B. Salazar **Fecha:** 15/06/06
Revisado por: Ing. A. Naranjo **Fecha:** 11/02/07

ANEXO 13
PROCESO DE VOTACIÓN DEL GRUPO DELPHI (AMENAZAS)

Accesos no autorizados y/o mal uso de la información.	Accesos no autorizados.				
Pérdidas monetarias.	III / III	Pérdidas monetarias.			
Pérdida de información y/o equipos.	II / 0	II / I	Pérdida de información y/o equipos.		
Virus	I / II	II / III	I / III	Virus	
Saturación del servidor.	III / I	III / I	II / I	III / II	Saturación del servidor.

ANEXO 13
PROCESO DE VOTACIÓN DEL GRUPO DELPHI (AMENAZAS)

Valoración del riesgo:

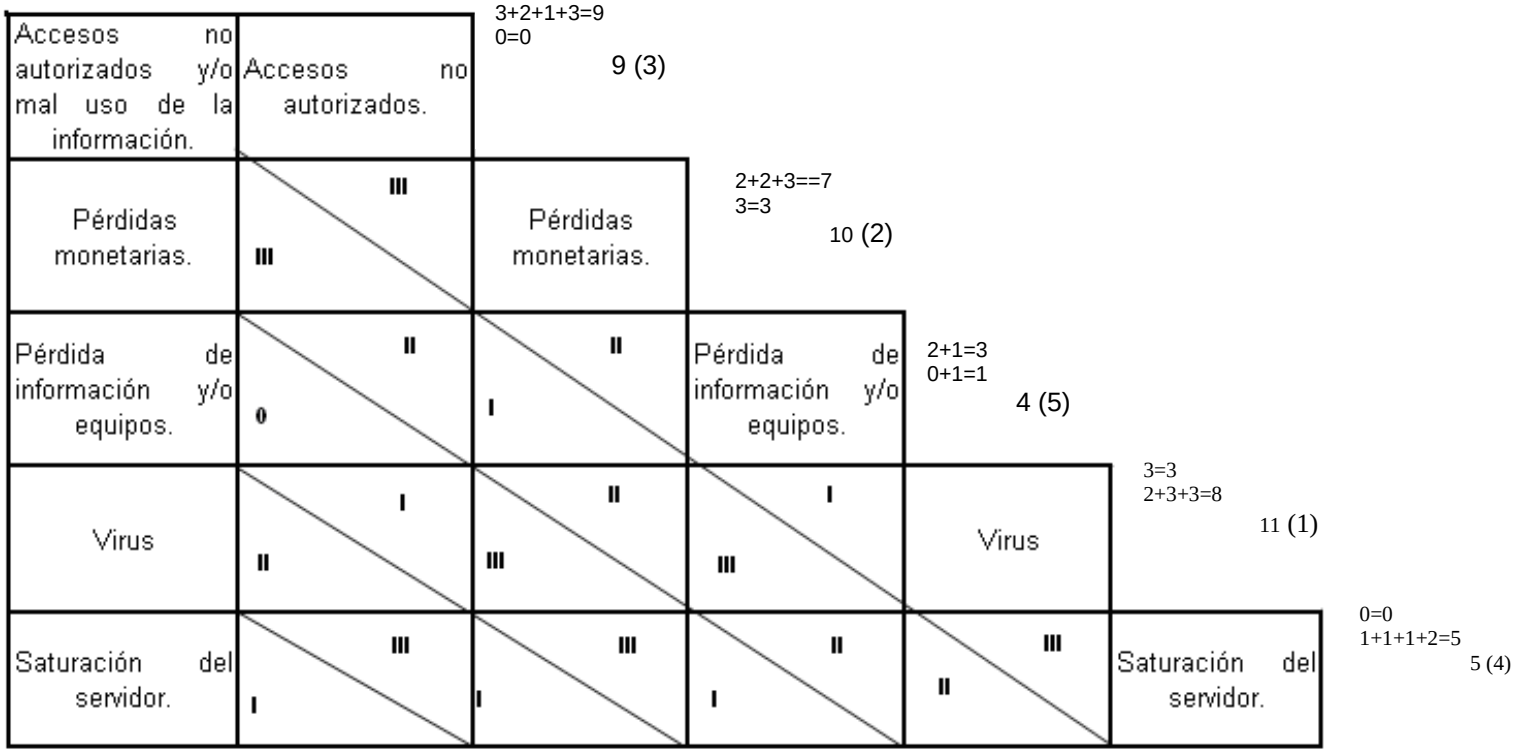
Voto	Interpretación
I	Bajo
II	Medio
III	Alto

Explicación de la votación (vertical)

- Primero procedemos a evaluar Pérdida y/o destrucción de información con cada una de las siguientes que en este caso sería divulgación no autorizada de información. El grupo delphi dió la ponderación de tres al primero y dos al segundo.
- Ahora evaluamos pérdida y/o destrucción de información con fraude y sabotajes. Otorgándole el grupo delphi al primero la valoración de tres y al segundo uno.
- Y así sucesivamente con cada uno hasta llegar a saturación del servidor de correo.

Elaborador por: B. Salazar **Fecha:** 16/06/06
Revisado por: Ing. A. Naranjo **Fecha:** 11/02/07

ANEXO 14
SUMA DE LOS RESULTADOS (AMENAZAS)

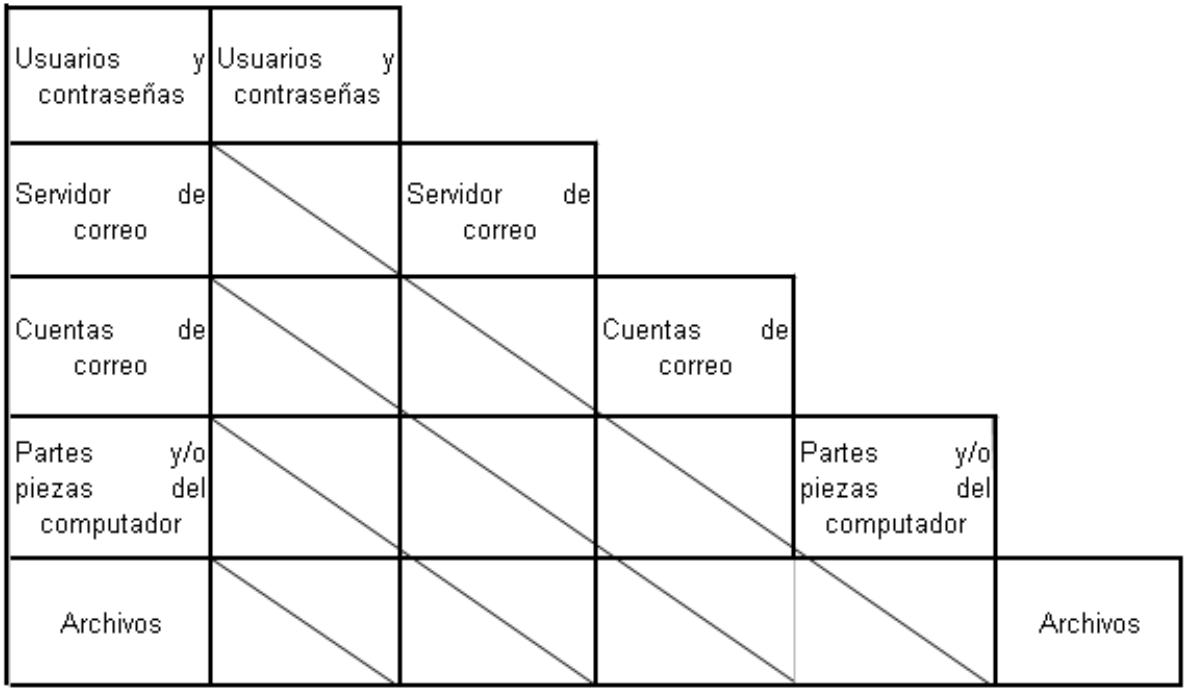


Elaborador por: B. Salazar
Revisado por: Ing. A. Naranjo

Fecha: 19/06/06
Fecha: 11/02/07

ANEXO 15

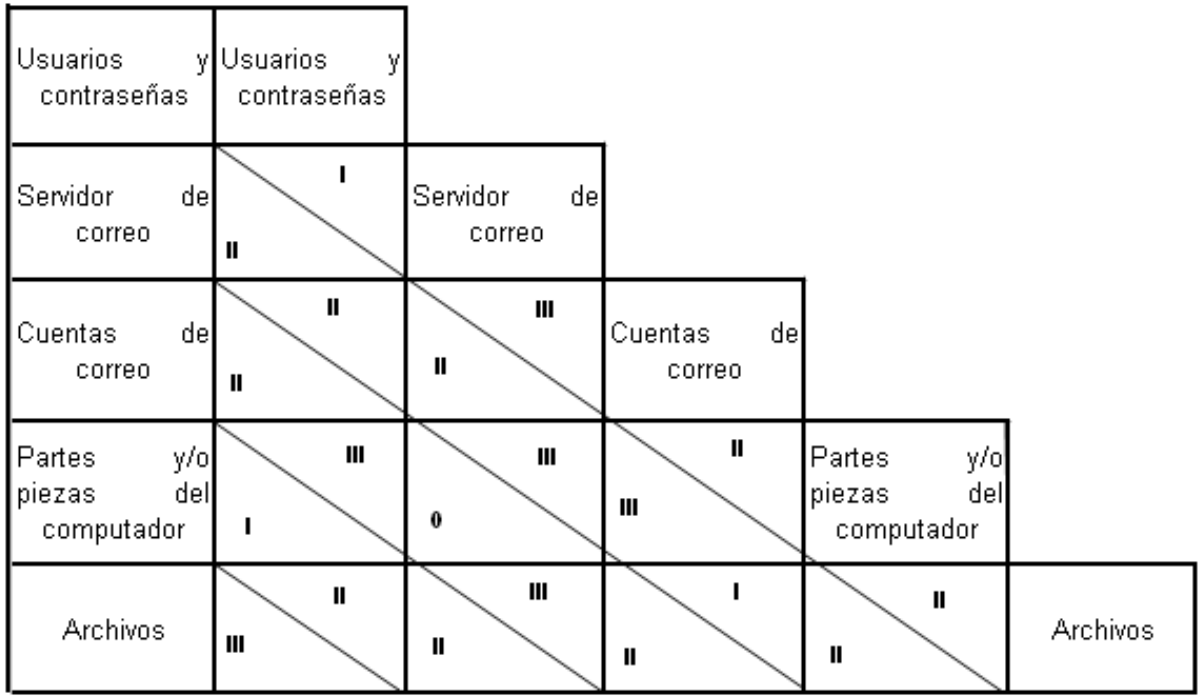
COMPARACIÓN DE CATEGORIAS DE RIESGOS (OBJETOS)



Elaborador por: B. Salazar **Fecha:** 15/06/06
Revisado por: Ing. A. Naranjo **Fecha:** 11/02/07

ANEXO 16

PROCESO DE VOTACIÓN DEL GRUPO DELPHI OBJETOS



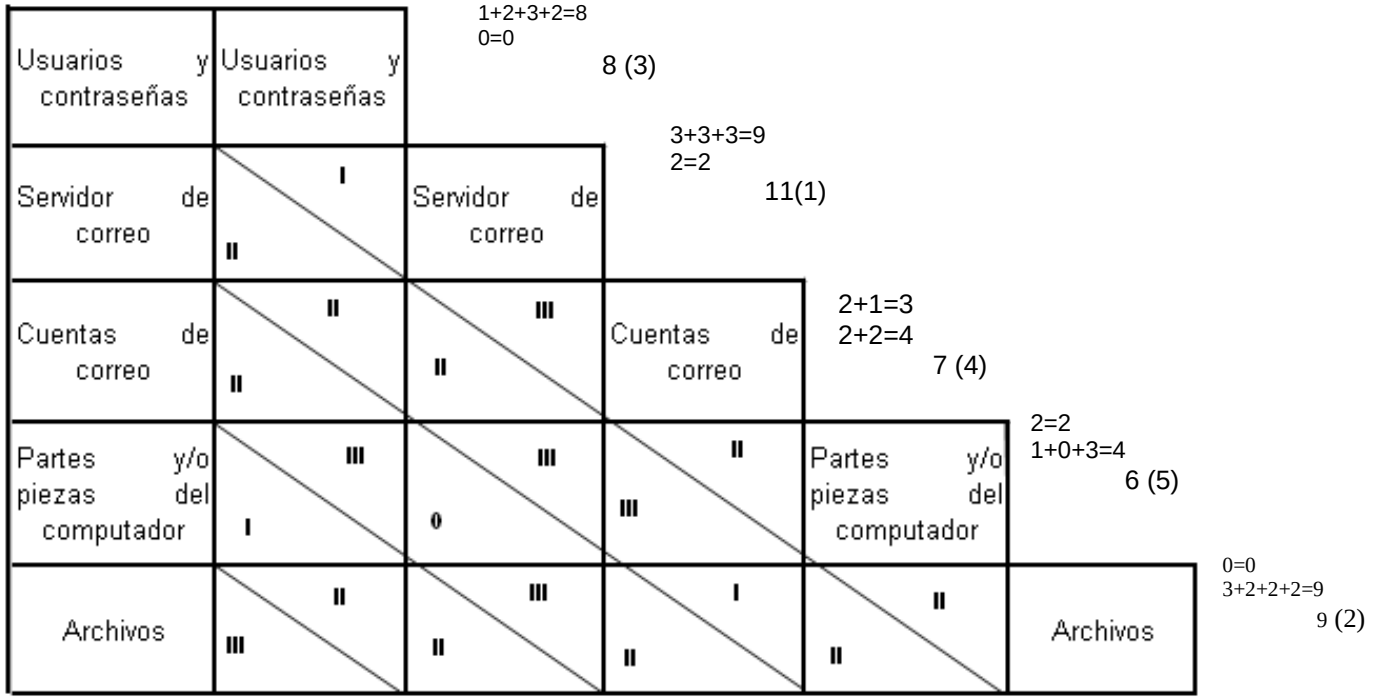
* Se realiza el mismo proceso que se realizó en el Anexo 11

Elaborador por: B. Salazar **Fecha:** 16/06/06

Revisado por: Ing. A. Naranjo **Fecha:** 11/02/07

ANEXO 17

SUMA DE LOS RESULTADOS (OBJETOS)



Elaborador por: B. Salazar
evisado por: Ing. A. Naranjo

Fecha: 19/06/06
Fecha: 11/02/07

ANEXO 18
MATRIZ DE COMBINACIONES DE LAS 2 CATEGORIZACIONES (AMENAZAS Y OBJETOS)

Amenazas / Objetos	Virus (11)	Perdidas Monetarias. (10)	Accesos no Autorizados. (9)	Saturación de Servidor. (5)	Perdida de Información y/o equipos. (4)
Servidor de correo (11)	121	110	99	55	44
Archivos. (9)	99	90	81	45	36
Usuarios y Contraseñas. (8)	88	80	72	40	32
Cuentas de coreo. (7)	77	70	63	35	28
Partes y/o piezas del computador. (6)	66	60	54	30	24

Elaborador por: B. Salazar **Fecha:** 20/06/06
Revisado por: Ing. A. Naranjo **Fecha:** 11/02/07

ANEXO 19

MATRIZ DE RESULTADOS CON RIESGOS DE SENSIBILIDAD DE IDENTIFICACIÓN DE NIVELES DE RIESGO (ALTO, MEDIO, BAJO)

Amenazas / Objetos	Virus (11)	Perdidas Monetarias. (10)	Accesos no Autorizados. (9)	Saturación de Servidor. (5)	Perdida de Información y/o equipos. (4)
Servidor de correo (11)	121 **1**	110 **2**	99 **3**	55 **14**	44 **16**
Archivos. (9)	99 **3R**	90 **4**	81 **6**	45 **15**	36 **18**
Usuarios y Contraseñas. (8)	88 **5**	80 **7**	72 **9**	40 **17**	32 **20**
Cuentas de coreo. (7)	77 **8**	70 **10**	63 **12**	35 **19**	28 **21**
Partes y/o piezas del computador. (6)	66 **11**	60 **13**	54 **14R**	30 **21**	24 **22**

Elaborador por: B. Salazar
Revisado por: Ing. A. Naranjo

Fecha: 21/06/06
Fecha: 11/02/07

ANEXO 20
CONTROLES ESTABLECIDOS

No. Ident.	Nombre Corto	Nivel Preventivo	Nivel Detectivo	Nivel Correctivo	Responsabilidad	Amenazas y/o Objetos que cubren
1.	Claves de Acceso	Asignar claves con un mínimo de ocho caracteres en combinación de números y letras.	Revisar si las contraseñas establecidas por los usuarios cumplen con el mínimo de caracteres establecidos	Informar a los usuarios que todas las contraseñas que no cumplan con los requerimientos establecidos deben ser cambiadas.	Jefe de Sistemas	**Amenazas**: Accesos no autorizados, Violación a la privacidad. **Objetos:**Usuarios y contraseñas, Cuentas de correo, Texto e Imágenes y Archivo.
2.	Administración de Contraseñas	Informar a los usuarios que las contraseñas proporcionadas por el Jefe de Sistemas posteriormente debe de ser cambiada.	Revisar si las contraseñas asignadas por el Jefe de Sistemas han sido cambiadas.	Configurar las cuentas de correo para disponer al usuario cambiar el pasword inmediatamente que se observe que este no ha sido cambiado.	Jefe de Sistemas	**Amenazas:** Accesos no autorizados, Violación a la privacidad**. Objetos:** Usuarios y contraseñas, Cuentas de correo, Texto e Imágenes y Archivo.

ANEXO 20
CONTROLES ESTABLECIDOS

No. Ident.	Nombre Corto	Nivel Preventivo	Nivel Detectivo	Nivel Correctivo	Responsabilidad	Amenazas y/o Objetos que cubren
3	Seguridades en la empresa	Restringir la entrada al Departamento de Sistemas a personal no autorizado. Manteniendo la puerta cerrada y colocando un aviso de "area restringida o prohibido el ingreso a personal no autorizado"	Mediante monitoreo y observación se puede detectar e identificar el ingreso de personal no autorizado a dicho departamento.	Comunicar a todos los trabajadores de TecMotors sobre la restricción de acceso al Departamento.	Gerencia y Dpto. de Sistemas	**Amenazas**:Accesos no autorizados, Robo y/o pérdida, Violación a la privacidad, Fraude y/o sabotaje. **Objetos:** Servidor de correo, partes y/o piezas del computador, Archivo.
4	Respaldo de las Cuentas de Usuario	Se necesita respaldar las cuentas de usuario periódicamente.	Revisar si se han respaldado las cuentas de correo para así evitar futuros incovenientes.	Respaldar las cuentas de correo con una frecuencia semanal o diaria.	Jefe de Sistemas	**Amenazas:** Robo y/o pérdida. **Objeto:** Cuentas de correo, Texto e imágenes y Archivo.

ANEXO 20
CONTROLES ESTABLECIDOS

No. Ident.	Nombre Corto	Nivel Preventivo	Nivel Detectivo	Nivel Correctivo	Responsabilidad	Amenazas y/o Objetos que cubren
5.	Tiempo de espera	Comunicar a los usuarios que las cuentas de correo se cierran automáticamente después de 5 minutos de presentar inactividad.	Configurar el cierre de sesión.	Corregir errores de configuración.	Jefe de Sistemas	**Amenazas**: Accesos no autorizados, robo y/o pérdida de información, Violación a la privacidad, Fraude y/o sabotajes. **Objetos:** Usuarios y/o contraseñas, Cuentas de correo, Texto e imágenes y Archivo.
6	Evaluar uso del correo electrónico	Informar a los usuarios que el correo de TecMotors es para fines laborales. Estableciendo políticas de uso del mismo.	Tener identificado quienes son los usuarios que no están cumpliendo con la política establecida.	Capacitar a los usuarios sobre el uso óptimo que deben darle a su cuenta. Recalcando que su uso es exclusivamente laboral.	Gerente y Jefe de Sistemas	**Amenazas**: Correos no deseados (infectados). **Obejtos:** Servidor de correo, Texto e imágenes y Archivo.

Elaborador por: B. Salazar
Revisado por: Ing. A. Naranjo

Fecha: 28 de Junio/06
Fecha: 11/02/07

ANEXO 21
IMPLEMENTACIÓN DE LOS CONTROLES

C1: Claves de Acceso
C2: Administración de contraseñas
C3: Seguridades en la empresa
C4: Respaldo de las cuentas de usuario
C5: Tiempo de espera
C6: Evaluar uso del correo electrónico

Controles	Abril	Mayo				Junio				Julio
	4° Semana	1° Semana	2° Semana	3° Semana	4° Semana	1° Semana	2° Semana	3° Semana	4° Semana	1° Semana
C1										
C2										
C3										
C4										
C5										
C6										

Elaborador por: B. Salazar **Fecha**: 13/04//07

GLOSARIO

Antivirus.- Son programas cuya función es detectar y eliminar virus informáticos y otros programas maliciosos.

ASCII.- Estándar definido y establecido para representar los caracteres (letras, números, signos de puntuación, caracteres especiales, etc.) de forma numérica.MODEM.- Su objetivo fundamental es aprovechar el canal telefónico (de una rango de 300 a 340 hertz) de forma da transmitirse por el información digital a la mayor velocidad posible.

Bandeja de entrada.- Es una carpeta existente en los programas de correo electrónico, que contiene todos los mensajes que se han recibido.

Características.- Cualidades o rasgos que sirven para distinguir una persona o cosa de sus semejantes.

Cronograma.- Relación de actividades por desarrollar en fechas determinadas, las cuales hacen parte de los planes y programas de las organizaciones y a su vez se constituye en un mecanismo del control interno.

Esquema.- Bosquejo, proyecto, diseño.

Estafetas.- Casa u oficina del corre donde se entregan las cartas que se envían y se recogen las que se recibe.

Exploit.- Es una técnica o un programa que aprovecha un fallo o hueco de seguridad -una vulnerabilidad - existente en un determinado protocolo de comunicaciones, sistema operativo, o herramienta informática.

Firewall / Cortafuegos.- Su traducción literal es *muro de fuego*, también conocido a nivel técnico como *cortafuegos*. Es una *barrera* o protección que permite a un sistema salvaguardar la información al acceder a otras redes, como por ejemplo Internet.

Función.- Es el conjunto de actividades u operaciones que dan características propias y definidas a un cargo, para determinar niveles de responsabilidad y autoridad que deben estar formuladas y documentadas en un manual de funciones y procedimientos.

Hardware.- Es el conjunto de elementos materiales que componen un ordenador (circuitos, cables, tarjetas). Es la parte fisica.

IP (Internet Protocol) / TCP-IP. - La IP es la dirección o código que identifica exclusivamente a cada uno de los ordenadores existentes. El protocolo

TCP/IP es el sistema utilizado para la interconexión de dichos ordenadores, sin provocar conflictos de direcciones. Se utiliza en Internet.

ISP (Internet Service Provider).- Es un proveedor de acceso a Internet que además ofrece una serie de servicios relacionados con Internet (Proveedor de Servicios Internet).

Módem.- Es un elemento físico (un periférico), también conocido como MOdulador DEMmodulador, que se utiliza para convertir las señales eléctricas (analógicas y digitales). Su objetivo es facilitar la comunicación entre ordenadores y otros tipos de equipos. Su utilidad más habitual, en la actualidad, es conectar los ordenadores a Internet.

Nodo.- Cada uno de los usuarios de la red se denomina NODO. Cada NODO esta definido por un numero clave (dirección).

Normas.- Son los requisitos de calidad relativos a la persona del auditor, al trabajo que realiza y a la emisión de su opinión.

RAM (Random Access Memory).- Es la memoria principal del ordenador, donde se colocan todos los ficheros cuando se utilizan y todos los programas cuando se ejecutan.

Recomendación.- Encargo que se hace a una persona respecto de otra o de alguna cosa.

Red.- Es una organización que intercambia correo en forma de mensajes.

Red LAN.- Local Area Network, Es una red cuyo ámbito es el de un departamento, edificio o campus. Ejemplo, Red de toda la ESPOL.

Red MAN.- Metropolitan Area Network, es una red que interconecta equipos de una ciudad o una red de área local.

Red Wan.- Wide Area Network, es una red cuyo ámbito geográfico es un entorno regional, nacional e internacional. Ejemplo, laboratorio Beta.

Riesgos.- Puede definirse como el efecto de una causa. Es un incidente o situación, que ocurre en un sitio concreto durante un intervalo de tiempo determinado, con consecuencias negativas o positivas que podrían afectar el cumplimiento de los objetivos.

Riesgo Alto.- Cuando el riesgo hace altamente vulnerable a la entidad.

Riesgo Bajo.- Cuando el riesgo presenta vulnerabilidad baja.

Riesgo Medio.- Cuando el riesgo presenta una vulnerabilidad media.

Router.- Enrutador, encaminador. Dispositivo de hardware para interconexión de redes de las computadoras. Hace pasar paquetes de datos entre redes tomando como base la información de la capa de red.

Servidor.- Sistema informático (ordenador) que presta ciertos servicios y recursos (de comunicación, aplicaciones, ficheros, etc.) a otros ordenadores (denominados clientes), los cuales están conectados en red a él.

SMTP.- El protocolo SMTP (Simple Mail Transfer Protocol) es el que se encarga del envío y recepción de los mensajes en TCP/IP.

Software.- Es la parte lógica del ordenador, esto es el conjunto de programas que puede ejecutar el hardware para la realización de tareas de computación.

Spam.- Es correo electrónico no solicitado, normalmente con contenido publicitario, que se envía de forma masiva. Este tipo de mensajes pueden causar graves molestias y provocar pérdidas de tiempo y recursos.

TCP/IP.- TCP.- Transmisión Control Protocol, Protocolo de la Transmisión de Control. **IP.-** Internet Protocol, Protocolo Internet. Permiten conectar computadoras y redes. Su misión es que al transmitir la información dentro de Internet.

Verificar.- Probar que es verdad una cosa que se duda. La auditoria es un examen que verifica y evalúa determinadas áreas de una empresa.

VPN.- Acrónimo de Virtual Private Network, que en castellano significa Red Privada Virtual (RPV), es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada. (Internet)

BIBLIOGRAFÍA

Libros y Publicaciones:

1. Harley Hahn Rick Stoot, Internet Manual de referencia, S/N edición, Mc Graw – Hill de Informática, Páginas (17,18, 23-26, 49)

2. Los Medios de Comunicación y las Tecnologías de la Información, Convergencia de los sectores de telecomunicaciones, Unión Europea.

3. Dvorak Nick Anis, Telecomunicaciones para PC modems, software, BBS, correo electrónico, interconexión, Prólogo de Meter Nortor, Mc Graw Hill. Paginas (57-88)

4. José Antonio Echenique, Auditoria Informática, editorial McGraw-Hill, 2nd edición Octubre 2001.
5. Rodao Jesús de Marcel, Piratas Cibernéticos, Seguridad Informática e Internet, Editorial: Alfa Omega, 2002, páginas 5-69

6. Enciclopedia de la Auditoria, Grupo Océano, Febrero 1999.

7. Mario Piattini, Auditoría Informática un enfoque practico, Editoria:l Alfa Omega, agosto 2001

8. Mc. Connel Steve, 1996. Desarrollo y Gestión de Proyectos Informáticos: Gestión de Riesgos, Primera Edición, McGraw-Hill, España.

9. Siyan & Hare, Internet Firewalls and Network Security, Primera Edición, New Riders Publishers, 1995

10. Ley 59/2003, Firma electrónica. Títulos I - VI, de 19 de diciembre

11. ISACA – Information Systems Audit. And Control Association, COBIT 3rd Edition Control Objetives Edición, IT Governance Institute, 2000.

12. CONACYT - Consejo Nacional de Ciencia y Tecnología - Vol. 10 No. 2 Diciembre 1991.

Direcciones Web

13. http://www.monografias.com/trabajos5/queint/queint.shtml - 2005 - Díaz Pablo.

14. http://www.monografias.com/trabajos26/correo-electronico/correo-electronico.shtml - Agosto 2005 - Alosi Jorge Gabriel.

15. www.icann.org - 4-04-2007 - Internet Corporation for Assignet Names and Numbers –

16. http://www.unav.es/capellania/fluvium/textos/documentacion/eti164.htm - 17-06-2003 - Sueiro Enrique

17. http://www.virtualtamps.com.mx/computacion/ventajascorreo.html - 2005 - Ing. Garza Juan José

18. www.aui.es – 2007 - Asociación de usuarios de Internet

19. http://www.proasetel.com/paginas/articulos/mercado_internet.htm#_internet3 - 2006 – Proasetel.

20. www.supertel.gov.ec – 2007 - Super Intendencia de Telecomunicaciones.

21. http://es.wikipedia.org/wiki/Portada - 15-04–2007 – Wikimedia Foundation.

22. http://www.tecnyred.com/seguridad.php - 2006 - TECNYRED SCP