UNIVERSIDAD LATINOAMERICANA DE CIENCIA Y TECNOLOGIA

Facultad de Ingeniería

Escuela de Ingeniería Informática

Trabajo final para optar por el grado de Licenciatura en Ingeniería Informática con Énfasis en Redes y Sistemas Telemáticos

Tema:
El correo electrónico como parte de la vida diaria: ¿Cómo obtener el mayor provecho con la menor molestia?

Estudiante: Ing. Sergio Montero Calderón

Cédula: 1-1293-0683

Profesor: Lic. Miguel Pérez Montero

III Cuatrimestre 2007

==========

Bachiller en Ingeniería en Sistemas. Candidato a Licenciatura en Ingeniería en Sistemas con énfasis en redes y sistemas telemáticos, ULACIT. Correo electrónico: supmontero@gmail.com

Índice

==========

Bachiller en Ingeniería en Sistemas. Candidato a Licenciatura en Ingeniería en Sistemas con énfasis en redes y sistemas telemáticos, ULACIT. Correo electrónico: supmontero@gmail.com

El correo electrónico como parte de la vida diaria: ¿Cómo obtener el mayor provecho con la menor molestia?

Sergio Montero Calderón

Resumen

En la actualidad, debido a los cambios tecnológicos, el ser humano necesita estar en contacto con el resto de las personas en el mundo.

En otros tiempos, no era posible a menos de que se tuvieran disponibles días, o incluso, meses para poder comunicarse con los demás; sin embargo, actualmente esto es posible gracias al uso de Internet, y principalmente a los correos electrónicos.

Se puede disfrutar de sus beneficios, pero, también es necesario protegerse de sus peligros, ya que existen muchas formas de hacerlo, sin embargo la mayoría son desconocidas por nosotros.

En un mundo que cambia constantemente, lo mejor es estar preparados para lo que podría venir, ya que solo de esta manera se podrá mantener la confidencialidad y seguridad personal.

Palabras Claves:
Correo electrónico, cambios tecnológicos Internet, confidencialidad, seguridad.

Abstract

At present, due to the technological changes, the human being needs to be in touch with the rest of the people in the world.

In other times, it was not possible unless they were available days or months to be able to communicate with the others; nevertheless nowadays this is possible thanks to the Internet use, and principally to the e-mails.

We can enjoy their benefits, but we should also protect ourselves of their dangers, since there exist many ways of doing that, nevertheless the majority are not known by us.

In a world that changes constantly, the best thing is to be prepared for what could come, since only in this way we will be able to support the confidentiality and personal safety.

Key Words:
E-mail, technological changes, Internet, confidentiality, safety.

==========

Bachiller en Ingeniería en Sistemas. Candidato a Licenciatura en Ingeniería en Sistemas con énfasis en redes y sistemas telemáticos, ULACIT. Correo electrónico: supmontero@gmail.com

Introducción:

¿Es usted una de esas personas que ya no recuerda como era su vida antes del correo electrónico y el Internet?, ¿Durante el día, su correo recibe al menos 10 mensajes y por lo menos la mitad son de propaganda o asuntos de trabajo?, de ser así, usted no está solo; con el pasar del tiempo cada vez son más las personas que se unen al mundo de la Internet, provocando a su vez un aumento del número de correos electrónicos que viajan en la red día a día.

Solamente en España, en el año 2003 existían 3 718 000 familias con acceso a Internet, para el 2004 este número creció hasta 4 544 000, y llega en la actualidad a 7 500 000 de familias (20minutos.es, 2005).

Más cerca de nuestras fronteras, en México se espera que para el 2012 existan alrededor de 70 millones de personas con acceso a Internet de banda ancha, esto es algo que llama la atención si se toma en cuenta que para el 2005 existían 17,1 millones de cibernautas (AFP, 2007).

Pero ¿qué pasa en Costa Rica? En nuestro país, cerca del 34 % de los hogares cuentan con una computadora, y cerca de la mitad de estas familias cuentan con acceso a Internet, a esto se le suman las personas que acceden en sus trabajos, en café Internet, en centros educativos, entre otros, haciendo circular cerca de 4 millones de correos electrónicos diarios (Racsa, 2007).

Un informe del Banco Mundial del 2006 indicaba que Costa Rica era el país de América Latina con más computadoras por cada 1.000 habitantes, con 238. Le seguían Chile con 133, Uruguay 125, México 108, Brasil 105, Argentina 96, Venezuela 82, y Guatemala 19, entre otros.

Entonces, urge la interrogante ¿qué hay de los correos electrónicos? En Costa Rica, alrededor de un millón de personas poseen correo electrónico, (de acuerdo con la página de Racsa), y este número aumenta con el pasar de los días, siendo su principal uso el intercambio de información entre amigos, comunicados de trabajo y propagandas o correos *spam*.

Antes de 1996, según Vásquez (2005), el método más utilizado para escribir a cualquier parte del mundo y hasta dentro de un mismo país, era el correo postal convencional; también, para hablar con una persona en cualquier otra parte del mundo se utilizaban las llamadas de larga distancia; luego de esta fecha es cuando empieza a despegar el correo electrónico, hasta llegar a nuestros días, en donde es el método más utilizado para comunicación en el mundo.

Ventajas de los correos electrónicos:

Las principales ventajas del correo electrónico frente a otros medios de intercambio de información tradicionales como el correo postal y el teléfono son:

- La ventaja más clara respecto al correo postal se centra en la velocidad. Mientras que en el correo ordinario una carta puede tardar muchos días, un mensaje enviado mediante 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).

- Otra ventaja se basa en la disponibilidad del acceso a Bases de Datos y Bibliotecas remotas en tiempo real.

- No es necesario que las dos personas que desean comunicarse estén presentes en el mismo momento, simplemente, se necesita que una de las dos lo envié y la otra cuando se conecte podrá ver su mensaje y responder.

- Respecto al precio de la conexión, cabe destacar que mientras una llamada telefónica a nivel nacional o internacional puede resultar de elevado costo, un e-mail permite el intercambio de una gran cantidad de correo a muy bajo precio, aun si la otra persona con la que se esté comunicando esté en el otro extremo del mundo.

- Es posible, la colaboración en un mismo proyecto de personas que se encuentran entre sí a varios kilómetros de distancia. Es muy utilizado en universidades y colegios, para, ponerse de acuerdo al momento de efectuar un trabajo, y si continúa avanzando de esta forma, falta poco para que en las escuelas se utilice diariamente.

- Actualmente, los servidores de correo electrónico como *Gmail* y *Hotmail* ofrecen cerca de cinco *Gigabytes* de almacenamiento y crece constantemente, por lo que prácticamente no faltará espacio para los correos.

Usos prácticos del correo electrónico en la casa (Virtualtamps, 2007**)**

- Mediante el correo electrónico, se pueden recibir ofertas de empresas que estén interesadas en dar a conocer ofertas de su negocio, enviar información de la misma y hacer llegar su página, mediante la cual se pueden efectuar pagos de manera segura.

- Cotizar con una sola solicitud. Si se cotiza por ejemplo: partes para el motor de tu automóvil y se tuvieran todas las especificaciones, se podría enviar el listado de las partes a todos los mecánicos que tuvieran correo electrónico y cada uno de ellos respondería cuánto seria el monto en su taller y de esta forma elegir el mejor sin moverse de la casa o trabajo.

- Se pueden enviar fotos escaneadas o tomadas con cámaras digitales a cualquier parte del mundo en cuestión de segundos, así como chatear con cualquier persona en tiempo real, ya sea que viva en Costa Rica o en China.

- Se puede enviar el currículo a varias empresas que tengan correo electrónico en un mensaje, así como también se recibe la respuesta en el correo en lugar de una llamada telefónica.

- El usuario puede recibir o impartir un curso a través de correo electrónico y, a la vez, recibir las calificaciones de los cursos de la universidad o de los cursos virtuales en que está matriculado.

- Puede recibir asesoría sobre tu tesis o investigación de algún investigador reconocido de cualquier parte del mundo o de tus profesores de la universidad y coordinar la entrega de avances y revisión de la misma.

- El usuario puede crear su propio medio de información, periódico, revista, galería de imágenes, música, etc. por medio de correo electrónico. Por ejemplo: periódico escolar, imágenes del país.

- Posibilita formar foros de discusión con compañeros o profesores y coordinar trabajos del colegio o universidad, permitiendo así que personas de Limón puedan trabajar con compañeros de Guanacaste en segundos.

- Se pueden enviar quejas o sugerencias a empresas, mediante el correo electrónico, normalmente estas empresas tienen un correo específico para estos casos.

Usos prácticos del correo electrónico en las empresas o instituciones

- Se pueden enviar ofertas a los clientes, así como fotografías de sus productos y diferentes negocios. Los clientes ingresan a la página Web de la empresa y se inscriben para que les envíen las ofertas a su correo electrónico, el punto negativo es que algunas veces el filtro de nuestro correo lo puede enviar al correo *spam*.

- Enviar cotizaciones de precios a los clientes que lo han pedido, ahorrando en uso de papel y sin tener que esperar a que la persona a quien va dirigido atienda el teléfono o que un fax este disponible.

- En el caso de contar con varias sucursales, ya sea en la misma ciudad o en diferente ciudad o país, permite mantener los inventarios relativamente actualizados, esto conjugado con algún programa de inventarios que permita leer la información desde el correo electrónico podría ser automático.

- Con la conjugación con programas de uso común, por ejemplo Excel de Microsoft, se podría enviar un archivo (hoja de cálculo) de ventas de cada sucursal y generar una consolidación diaria de ventas y gastos.

- Ahorro en costos de telefonía, ya que mediante el uso del correo electrónico se puede sustituir en la mayoría de los casos el teléfono al momento de comunicarse con otras sucursales.

- Ser informado de oportunidades por los proveedores sobre actualizaciones de precios, ofertas y existencias de sus inventarios.

- Contar con varias cuentas de correo para la mejor atención de sus clientes, para que estos envíen sus quejas o sus sugerencias mediante las mismas, un ejemplo de este tipo de correos es el siguiente: atencionclientes@suempresa.com.

- Los trabajadores de una empresa se pueden comunicar entre ellos, de la misma manera que pedir permisos o justificar alguna ausencia en caso de enfermedad.

- En el caso de consultores o prestadores de servicios, se podría brindar consultoría a cualquier parte del mundo a través de correo electrónico.

- Con respecto a diseño gráfico o programas de cómputo, se pueden enviar muestrarios o demos de diseños o programas en venta. Normalmente se brinda una licencia por 30 días para que el cliente lo pruebe y decida si lo compra o no.

Desventajas de los correos electrónicos:

Una de las grandes quejas de los usuarios es que su correo está lleno de *spam*, y que esto aumenta el tiempo de revisarlo, así, cabe preguntar, ¿Qué son correos *spam*?

El correo basura o *Spam* es básicamente todo aquel correo que el usuario no ha pedido con anticipación y aun así lo recibe, esto no solo ocurre con respecto a los correos electrónicos, sino también en mensajes de teléfono, en foros, o *blogs* de la Internet; por consiguiente, aunque no es exclusivo del correo electrónico, éste es el que más se ve afectado.

Los correos *spam* se hacen con el objetivo de hacer propaganda masiva, y así, lograr mayores ventas o mayores visitas en los sitios *web*.

Formas de evitar el spam

Lo principal es poseer dos cuentas de correo, una en la que se va a manejar toda la información importante o personal, y otra que va a ser usada en el momento de registros en foros, o de dar en encuestas.

De estas dos direcciones, nunca se debe publicar la personal en páginas de acceso público de Internet.

Al crear una cuenta de correo privada, debe evitarse el empleo del nombre o apellido del dueño en ella, ya que de esta manera, es mucho más fácil para los demás intentar adivinar el correo; se deben utilizar combinaciones de números, letras y símbolos especiales.

La dirección pública debe ser algo temporal. Son altas las posibilidades de que los *spammers* (personas dedicadas a enviar correos *spam*) recolecten su dirección pública rápidamente. Intente cambiarla con frecuencia.

Cuando se registre en foros, cuartos de *chat* o suscribirse a listas de correo y promociones se debe utilizar siempre el correo público y nunca el privado. También, se debe considerar el uso de varias direcciones públicas para determinar cuales son las páginas o servicios que venden direcciones a los *spammers*.

Nunca responda a los mensajes no solicitados. La mayor parte de los *spammers* emplean las respuestas para verificar qué direcciones son reales. Mientras más responda, más *spam* recibirá.

Si los *spammers* descubren su dirección pública o privada, lo recomendable es que la cambie. Esto puede ser inconveniente, pero al cambiar su dirección de correo electrónico le ayudará a evitar el *spam*, al menos por un tiempo.

Bachiller en Ingeniería en Sistemas. Candidato a Licenciatura en Ingeniería en Sistemas con énfasis en redes y sistemas telemáticos, ULACIT. Correo electrónico: supmontero@gmail.com

Virus:

Otra gran desventaja de los correos es la cantidad de virus que existen hoy y que están propensos a dañar el equipo de cualquier usuario que se descuide.

¿Qué es un virus? Como su mismo nombre lo indica, al igual que los virus de los que se pueden contagiar los humanos, los virus informáticos están diseñados para dañar el equipo del usuario, sus programas o archivos.

¿Cómo nacieron estos virus?, Hacia finales de los años 60, Douglas McIlory, Victor Vysottsky y Robert Morris idearon un juego al que llamaron *Core War* que se convirtió en el pasatiempo de algunos de los programadores de los laboratorios *Bell* de *AT&T*.

El juego consistía en que dos jugadores escribieran cada uno un programa llamado *organismo*, cuyo hábitat fuera la memoria de la computadora. A partir de una señal, cada programa intentaba forzar al otro a efectuar una instrucción inválida, ganando el primero que lo consiguiera.

Al término del juego, se borraba de la memoria todo rastro de la batalla, ya que estas actividades eran severamente sancionadas por los jefes, por ser un gran riesgo dejar un *organismo* suelto que pudiera acabar con las aplicaciones del día siguiente. De esta manera, surgieron los programas destinados a dañar en la escena de la computación. (Monografías, 2007)

Sin embargo, no fue sino hasta 1984 que se adoptó el nombre de virus y que se han ido expandiendo en el mundo mediante *diskettes*, disco compacto, llave maya y correo electrónico.

No existe solo un virus, existen múltiples tipos de ellos, cada uno con una finalidad diferente. Entre los más conocidos y peligrosos se pueden destacar:

***Worms* o gusanos:** Un gusano está diseñado para copiarse de un equipo a otro, pero lo hace automáticamente. En primer lugar, toma el control de las características del equipo que permiten transferir archivos o información. Una vez que un gusano esté en su sistema, puede viajar solo. El gran peligro de los gusanos es su habilidad para reproducirse en grandes números. Por ejemplo, un gusano podría enviar copias de sí mismo a todos los usuarios de su libreta de direcciones de correo electrónico, lo que provoca un efecto dominó de intenso tráfico de red que puede hacer más lentas las redes empresariales e Internet en su totalidad.

Troyanos: Del mismo modo que el caballo de Troya mitológico, apareció como un mensaje de correo electrónico que incluye archivos adjuntos que aparentaban ser actualizaciones de seguridad de Microsoft, pero que resultaron ser virus que intentaban deshabilitar el software antivirus y del servidor de seguridad. (Microsoft, 2007)

Algunos ejemplos de nombres de correos famosos que contenían virus son los siguientes (Monografías, 2007):

- *3b Trojan (alias PKZIP Virus).*
- *AOL4Free Virus Hoax.*
- *Baby New Year Virus Hoax.*
- *BUDDYLST.ZIP*
- *BUDSAVER.EXE*
- *Budweiser Hoax*
- *Death69*
- *Deeyenda*
- *E-Flu*
- *FatCat Virus Hoax*
- *Free Money*
- *Get More Money Hoax*
- *Ghost*
- *Good Time*

Muchas personas afirman que cada vez que tienen correo nuevo y quien lo envía es desconocido, lo mejor es utilizar un antivirus, para estar más seguro; sin embargo, no hay que hacerlo solo con los correos desconocidos, sino con todos, ya que aunque usted tenga cuidado con sus archivos, no significa que sus amigos lo tengan también y pueden ser perfectamente sus mismos amigos quienes lo contagien de un virus sin saberlo ninguno de los dos.

Formas de combatir los virus:

Existen muchas armas para combatir en esta guerra contra los virus, entre ellos están. Ferreyra Cortés, Gonzalo (1991):

Antivirus: Estos son programas que se instalan en la computadora, e incluso algunos se pueden ejecutar desde Internet, y están diseñados para revisar los archivos de discos internos y extraíbles con el fin de encontrar los que contengan virus y eliminarlos. Pero hay que tener cuidado, ya que las mismas personas que hacen los virus muchas veces crean un “antivirus”, que en realidad es un virus más, por esto solo hay que confiar en las empresas que pertenezcan a la A. V. P. D. que son los encargados de desarrollar los productos antivirus reconocidos a nivel mundial, entre las que se cuentan:

- *Cheyenne Software*
- *I. B. M.*
- *Intel*
- *McAfee Associates*
- *Stiller Research Inc.*
- *S&S International*
- *Symantec Corp.*
- *ThunderByte*

- **Copias de seguridad**: Al tener un respaldo de los datos, solo se perderá lo que se haya hecho desde el momento del respaldo hasta el momento de la infección, así disminuye drásticamente las pérdidas. Por lo general, se realizan respaldos en DVD por la gran capacidad de los mismos.

- **Desconfiar**: Utilice siempre un antivirus, no importa si el correo electrónico es de una persona conocida o no, a los correos electrónicos hay que respetarlos, ya que estos pueden acabar en un parpadear con muchas horas o días de trabajo, nunca descargue correos que estén en otro idioma, ni de propagandas o encuestas, ya que esto podría salirle muy caro.

- **Hacer reenvíos seguros de email**: Cuando reciba un mensaje de correo electrónico sospechoso de contener virus o que hable de algo desconocido, conviene consultar su posible infección o veracidad. Sólo si se está seguro de la ausencia de virus del mensaje o de que lo que dice es cierto e importante, de ser conocido por nuestros contactos, lo reenviaremos, teniendo cuidado de poner las direcciones de correo electrónico de los destinatarios en la casilla CCO. Así se evitará la propagación de mensajes con virus, tanto del spam como la de aquellos mensajes con phishing u hoax.

- **Informar a nuestros contactos**: Conviene que se le haga saber lo mencionado en el punto anterior a los contactos en cuanto nos reenvían mensajes con virus o contenido falso o sin utilizar la casilla CCO.

- **Limpiar y eliminar el virus**: En el momento en que nos damos cuenta de que la máquina en uso fue infectada por un virus, lo recomendable es desconectarse de la red, ya que existen virus que mandan la información contenida a otras personas a través de la red, por lo que al desconectarse de la misma se disminuye un poco el riesgo de perder información, la cual en casos es vital, como lo son cuentas de tarjetas al realizar pagos por Internet. Inmediatamente de haberse desconectado de la red se ejecuta el antivirus actualizado, para así eliminar el virus

- **Restauración completa**: Este es el paso más drástico, ya que eliminará todos los archivos que contenga la unidad, este se efectuará solo cuando el virus sea demasiado fuerte para un antivirus, y dejará el disco o la unidad como vino de la fábrica, totalmente en blanco.

¿Cómo saber si está infectado con un virus en la computadora?

Algunos datos que pueden indicar si la computadora esta infectada por un virus

- La velocidad del equipo disminuye drásticamente.
- Aparece el rótulo: “poco espacio en disco duro”.
- El equipo no responde o se bloquea con frecuencia
- El equipo se bloquea y se tiene que reiniciar cada pocos minutos
- El equipo se reinicia solo y no puede ejecutarse normalmente
- Ciertas aplicaciones del equipo no funcionan correctamente
- No se tiene acceso a los discos o a las unidades de disco
- No se puede imprimir correctamente
- Aparecen mensajes de error poco comunes
- Aparecen menús y cuadros de diálogo distorsionados

Claro está, que esto no siempre indica que es un virus, también puede ser perfectamente un error de software o hardware.

Certificados de seguridad.

Pero afortunadamente para los usuarios, no todo son virus y troyanos, gracias al talento y la dedicación de miles de personas la navegación es día a día más segura en la red.

Actualmente, Microsoft creó el certificado de correo electrónico de Outlook, el cual reduce el correo no deseado (Microsoft, 2007)

Enviar correo electrónico Antes de que los mensajes salgan de la bandeja de salida, Office Outlook 2007 sella cada mensaje con un certificado de correo electrónico. El certificado incorpora características únicas del mensaje, incluida la lista de destinatarios y la hora cuando se envió el mensaje. Como resultado, el certificado sólo es válido para ese mensaje de correo electrónico. Es necesario algún tiempo adicional de procesado para construir el certificado. Como resultado, los mensajes tardan algo más en abandonar la bandeja de salida. Este es el costo en cómputo en el que se incurre al usar el Certificado de correo de Outlook.

Recibir correo electrónico Cuando una aplicación de correo electrónico de un destinatario que admite el Certificado de correo electrónico de Outlook recibe un mensaje certificado, lo reconoce. Este certificado indica a la aplicación de correo electrónico del destinatario que no es probable que el mensaje sea correo no deseado, algo que tiene en cuenta el filtro de la aplicación de correo electrónico al evaluar el mensaje.

Pero aún de esta manera se puede seguir enviando correo no deseado; sin embargo, las personas que lo quieran hacer necesitarán invertir más en sus equipos para poder enviar la misma cantidad de correos, ya que el tiempo de procesamiento es mayor, por lo cual disminuiría bastante este tipo de correos.

¿Qué tipos de mensajes no se certifican?

En los casos siguientes, un mensaje de correo electrónico no se certifica:

- El destinatario del mensaje está en la Lista global de direcciones (GAL) de Microsoft Exchange de la organización del remitente. Si un destinatario, tal como un proveedor de la empresa, tiene una dirección de correo electrónico externa pero aparece en la lista GAL de la organización, el mensaje saliente no se certifica.
- Usted o el administrador de correo electrónico de la organización ha desactivado la función de certificado.
- Antes de enviar un mensaje, el filtro de correo no deseado de Outlook evalúa si el mensaje tiene características de este tipo que hagan probable que sea clasificado así por el filtro del destinatario. Si el mensaje no tiene estas características, Outlook no certifica el mensaje porque es poco probable que el filtro de correo del destinatario vaya a determinar que el mensaje contiene correo no deseado.

Y es que existen personas que se dedican a tratar de leer los correos de las personas, sin importar para el uso que sean estos (diversión o trabajo), y para ellos es muy sencillo, ya que existen métodos por los cuales pueden leerlos como si hubieran sido el destinatario.

Afortunadamente, existen métodos para poder mantener seguros los datos del usuario, por medio del cifrado que es una forma de codificar los datos para que se escondan a la vista de los demás y por medio de las firmas digitales, para asegurarse de que el correo no ha sido alterado.

La ventaja que esto ofrece, además de ocultar el mensaje, es poder estar seguros de la integridad del mensaje y que quien dice enviar el correo es una persona conocida.

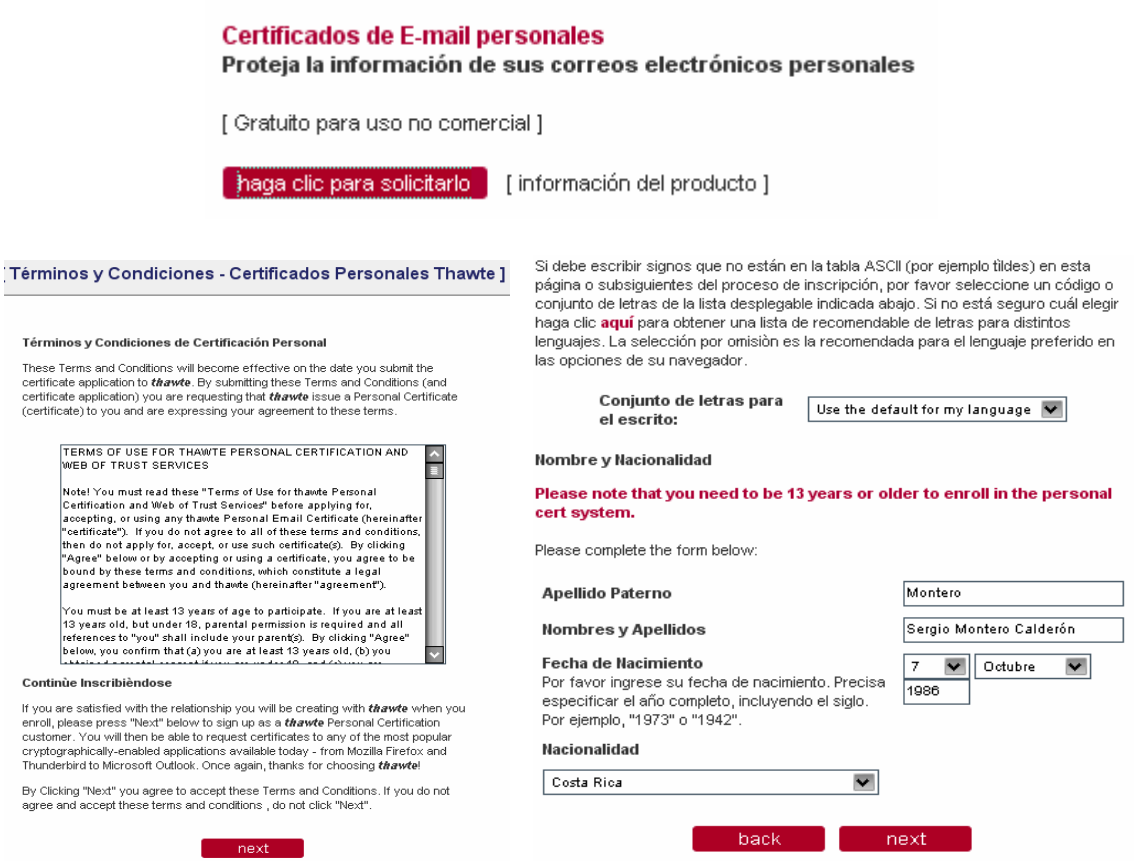
¿Cómo funcionan estos certificados?, se basan en la tecnología PKI (*Public Key Infraestructure*) la cual permite la identificación de usuarios entre ellos y a la vez utilizar la información de los certificados de identidad en el momento de cifrar los mensajes o utilizar las firmas digitales.

Para que esto pueda darse se requieren 3 elementos:

- Un usuario iniciador de la operación
- Unos sistemas servidores que dan fe de la ocurrencia de la operación y garantizan la validez de los certificados implicados en la operación.
- Un destinatario de los datos cifrados/firmados/enviados garantizados por parte del usuario iniciador de la operación.

¿Entonces que se tiene que hacer para empezar a enviar correos seguros?, lo primero es conseguir un Certificado de Seguridad Personal, existen muchas empresas certificadores que los ofrecen como Verisign y Thawte. Thawte ofrece un certificado personal gratuito, solo hay que seguir un sencillo asistente, el cual lo llevará a un panel en el que podrá solicitar el certificado personal, como se muestra en el cuadro #1: (Dahousecat, 2007)

Cuadro # 1
¿Cómo solicitar certificados personales gratuitos?



Thawte 2007. Certificados personales de e-mail, recuperado el 14 de noviembre de: http://www.thawte.com/secure-email/personal-email-certificates/index.html

==========

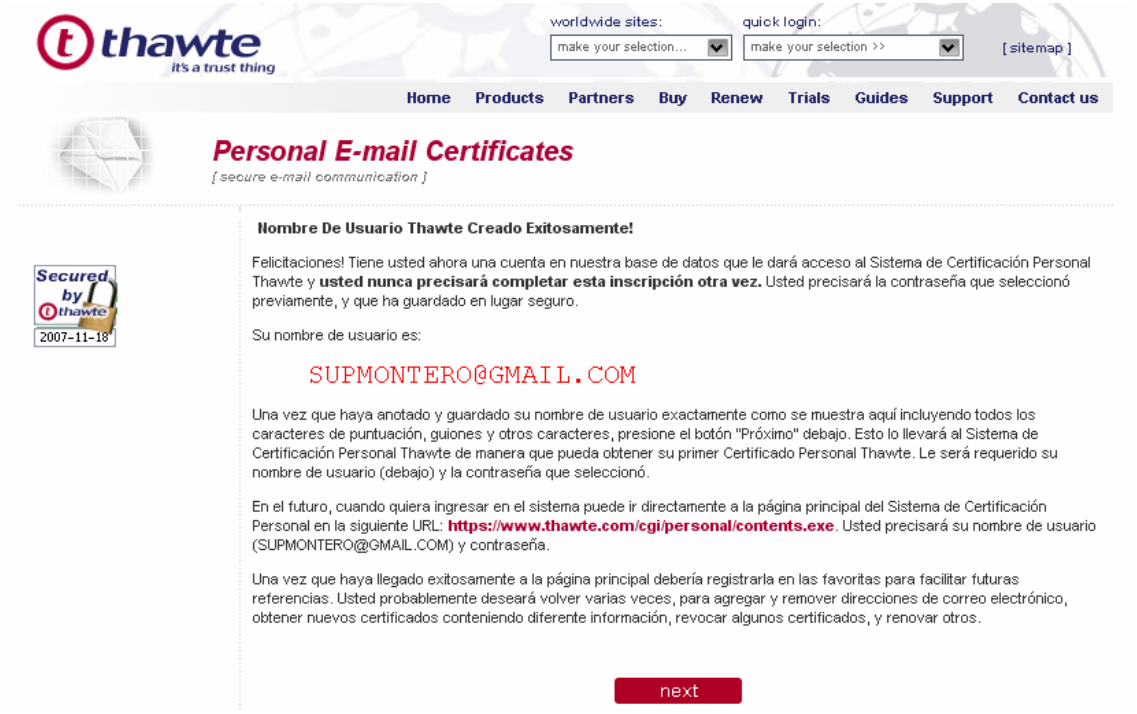
Bachiller en Ingeniería en Sistemas. Candidato a Licenciatura en Ingeniería en Sistemas con énfasis en redes y sistemas telemáticos, ULACIT. Correo electrónico: supmontero@gmail.com

Para crearlo, simplemente, debe seguir el asistente, rellenando los datos solicitados, como el nombre, fecha de nacimiento, correo electrónico, contraseña, navegador (en este caso se hará con M*ozilla Thunderbird*) entre otros. A menos de que haya escogido una opción no gratuita, en la cual sí tiene que ingresar números de tarjeta de crédito y muchos datos más, estas opciones se utilizan principalmente en empresas.

Luego recibirá un correo para confirmar la solicitud, una vez confirmado se presentará la siguiente pantalla mostrada en el cuadro #2:

Cuadro # 2

Confirmación de creación de cuenta

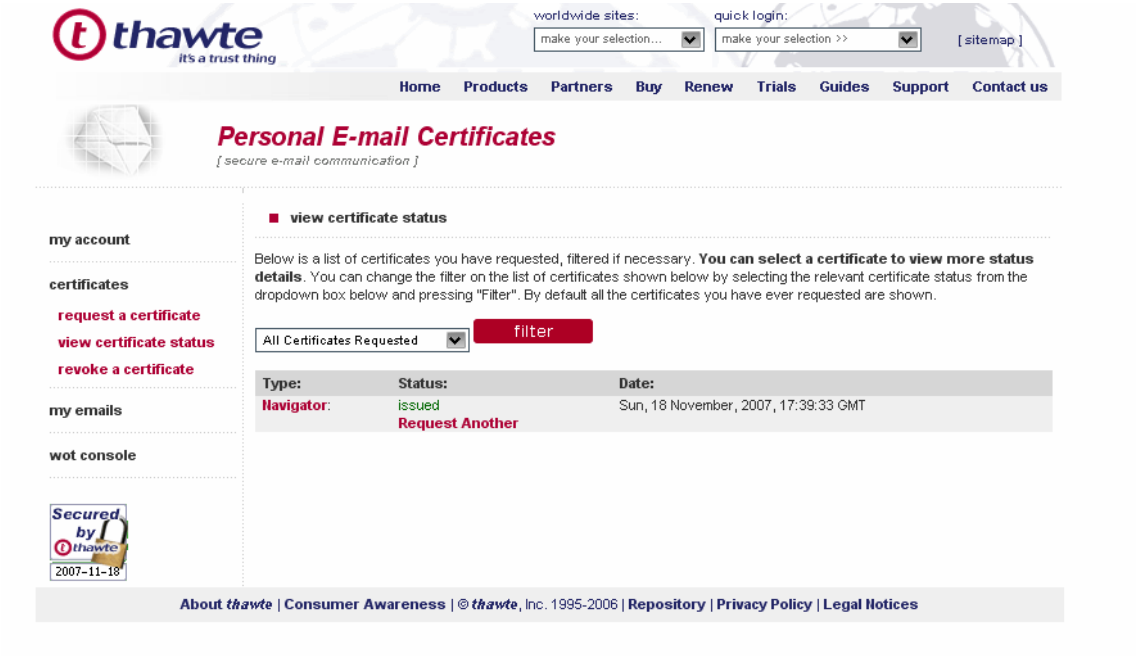


Thawte 2007. Certificados personales de e-mail, recuperado el 14 de noviembre de: http://www.thawte.com/secure-email/personal-email-certificates/index.html

Luego ingresa al sistema y solicita un certificado, sabrá cuando está listo si visualiza la siguiente pantalla mostrada en el cuadro #3:

Cuadro # 3

Confirmación de creación de certificados

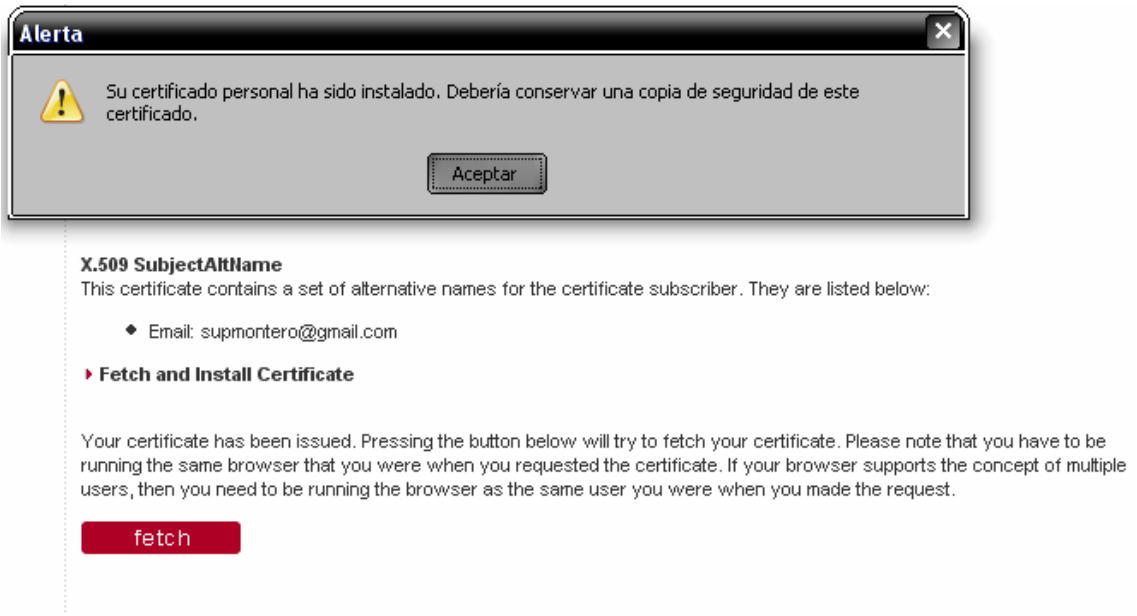


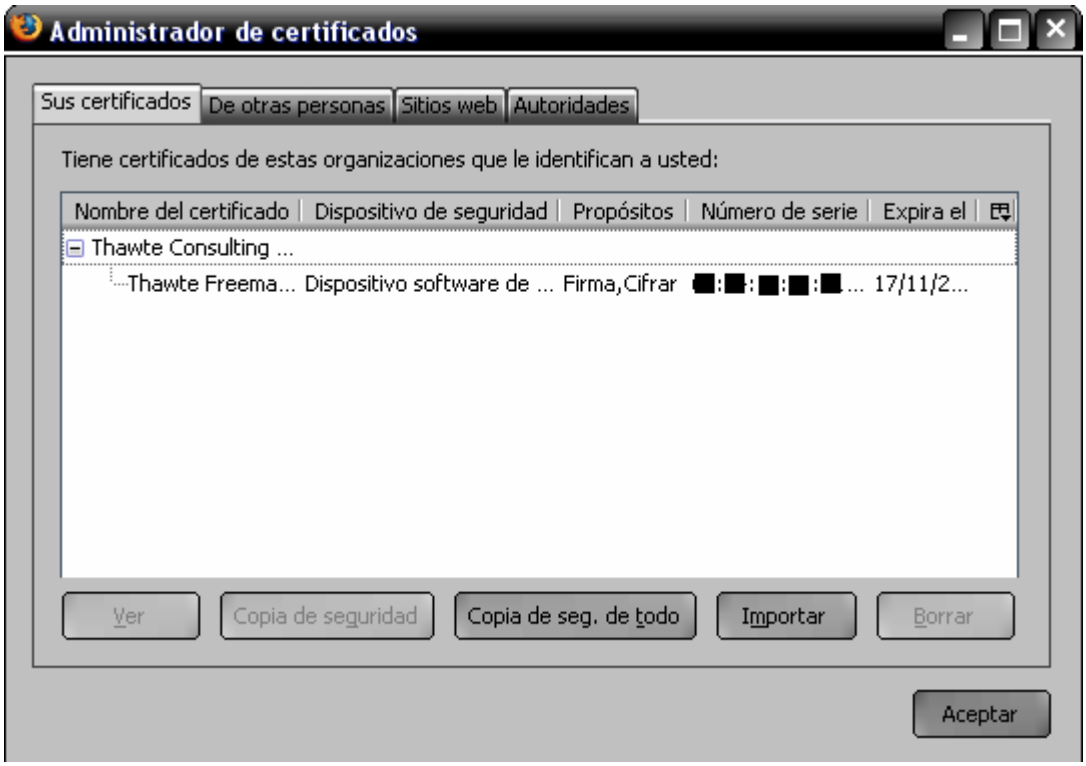
Thawte 2007. Certificados personales de e-mail, recuperado el 14 de noviembre de: http://www.thawte.com/secure-email/personal-email-certificates/index.html

Se le da clic sobre *Navigator*, en la siguiente página encontrarán un resumen de toda nuestra información y al final el botón FETCH y el certificado se instalará en su navegador, ahora solo irá a *Herramientas - Opciones - Avanzado* y de ahí seselecciona la pestaña *Cifrado* y pulsara el botón *Ver Certificados* ahí encontrará uno que dice "*Thawte Freenmail Member*" ahora se pulsa "Copia de Seguridad" y la guarda en algún directorio; este generará un archivo con extensión ".p12" que es un certificado de acuerdo con el estándar PKCS12 y este será el que se podrá instalar en nuestro cliente de correo electrónico.

Cuadro # 4

Confirmación de instalación de certificados





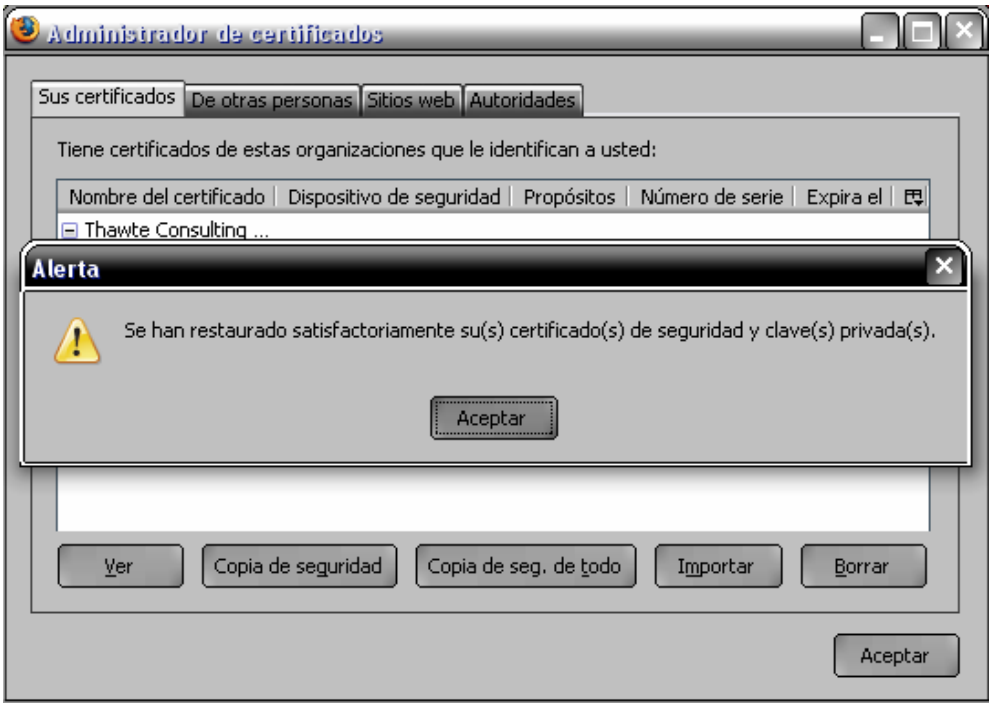
Thawte 2007. Certificados personales de e-mail, recuperado el 14 de noviembre de: http://www.thawte.com/secure-email/personal-email-certificates/index.html

Se pueden tener tantos certificados como cuentas de correo se utilicen. Luego se debe configurar el certificado para que sea utilizado por la cuenta de correo del usuario correspondiente.

Para ello iremos a *Herramientas - Opciones - Avanzado"* y se seleccionará la pestaña que dice *"Certificados"* y de ahí el botón *Importar*, pedirá primero la contraseña para el dispositivo de seguridad y luego el que se utilizó para crear el certificado, este último es el que se usa en *thawte*.

Cuadro # 5

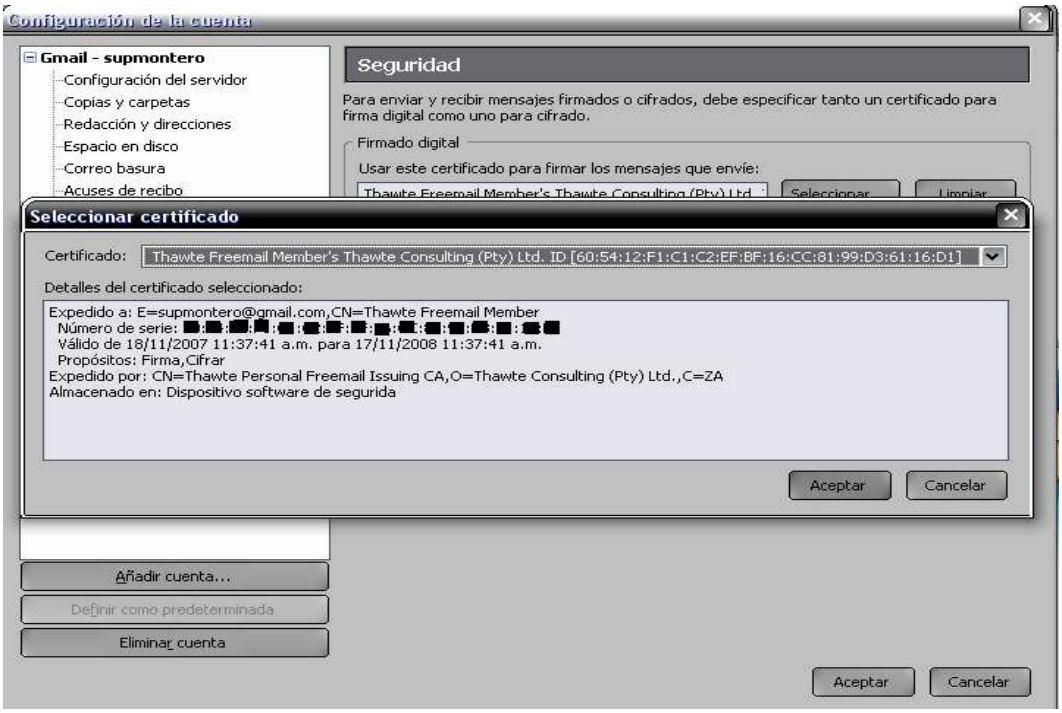
Instalación de certificados en *Thundebird*

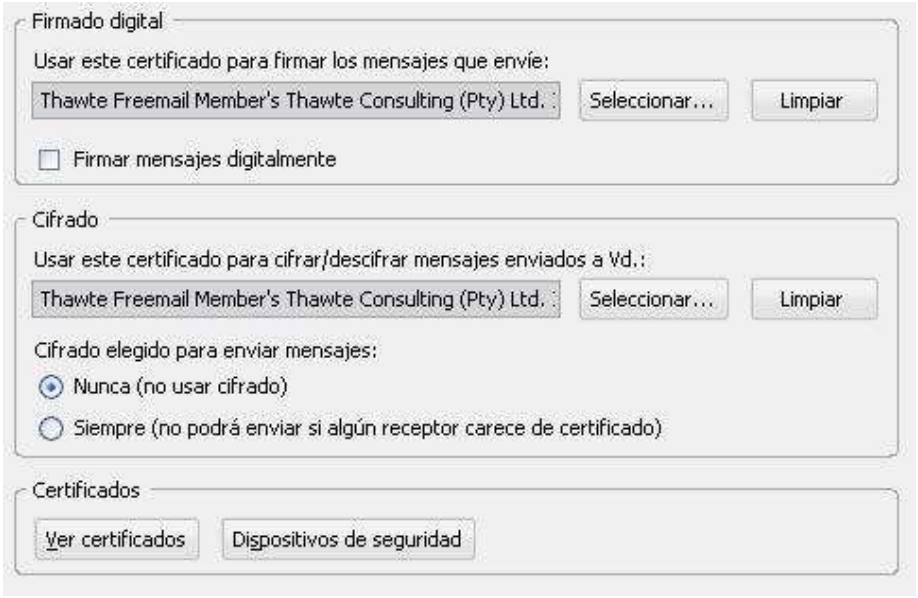


Thawte 2007. Certificados personales de e-mail, recuperado el 14 de noviembre de: http://www.thawte.com/secure-email/personal-email-certificates/index.html

Ahora se deberá configurar la cuenta de correo electrónico para que utilice el certificado, para ello irá a *Herramientas - Configuración de las Cuentas"* y buscará la opción de *Seguridad* de la cuenta que necesita emplear el certificado, cuando seleccione la opción *Seleccionar, esta,* automáticamente mostrará el certificado que creado para esa cuenta, así que solo debe darse *Aceptar*.

Cuadro # 6
Selección de certificado





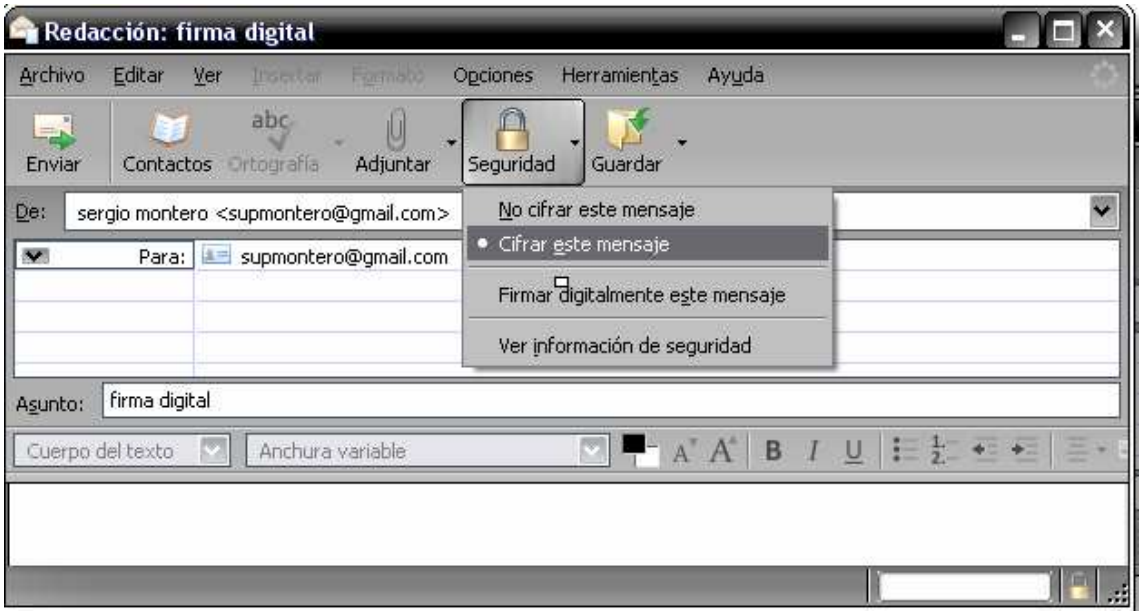
Thawte 2007. Certificados personales de e-mail, recuperado el 14 de noviembre de: http://www.thawte.com/secure-email/personal-email-certificates/index.html

Luego, pregunta si desea usar el mismo Certificado para Cifrar mensajes, debido a que el certificado que ofrece Thawte tiene esa posibilidad se debería aceptar, pero esto queda a criterio del usuario, la recomendación es Aceptar, de todas formas desde el editor de Correo Electrónico se podrá escoger entre: mandar un correo firmado digitalmente, cifrado, o mandarlo sin seguridad.

De esta forma se está listo para poder enviar mensajes de manera segura. Ahora solo falta ver cómo activar estas opciones a la hora de enviar los correos electrónicos.

Cuadro # 7

Enviando Correo electrónico seguro



Thawte 2007. Certificados personales de e-mail, recuperado el 14 de noviembre de: http://www.thawte.com/secure-email/personal-email-certificates/index.html

Enviar un correo seguro es tan sencillo como activar y desactivar opciones en el menú de Thunderbird, las consideraciones que se deben tener en cuenta son las siguientes:

En clientes de *Webmail* el usuario receptor no podrá ver que el email está firmado digitalmente, en el caso de *Gmail* te aparece con un archivo adjunto llamado “smime.p7s” y los cifrados con “smime.p7m”, así que para que esto funcione debemos utilizar algún cliente de correo electrónico.

Para poder cifrar, se debe tener la clave pública del destinatario, esta la pueden conseguir si el receptor nos envía un correo electrónico firmado digitalmente, o que el mismo nos proporcione su llave pública.

Lo mencionado anteriormente se puede realizar mediante correos de *Gmail, Hotmail, Yahoo* entre otros, ya que estos disponen de opciones para conectarse vía *POP3* y *SMTP*, y se puede utilizar en *Thunderbird, Outlook* o cualquier otro cliente de correo.

Bachiller en Ingeniería en Sistemas. Candidato a Licenciatura en Ingeniería en Sistemas con énfasis en redes y sistemas telemáticos, ULACIT. Correo electrónico: supmontero@gmail.com

Recomendaciones:

En el desarrollo de este artículo, se han indicado las ventajas de contar con el correo electrónico, pero, a su vez los peligros que conlleva el no tener cuidado con este.

Entre los principales cuidados que deberían tener todos los que utilizan este servicio que, actualmente, es parte vital de la vida diaria de las personas y empresas, están los siguientes:

Mantenga un Antivirus actualizado
Cuente con un filtro de correos *spam*
Nunca abra archivos de correos *spam* o de personas desconocidas
Mantenga cuentas de correo separadas para amigos y para subscripciones
Cambie, frecuentemente, la dirección para subscripciones en Internet

Estos son consejos sencillos que cualquier persona puede seguir para tener un poco más de seguridad; sin embargo, existen otros tipos un poco más avanzados, los cuales permiten tener una mayor confianza y confidencialidad en los datos:

Realizar una copia de seguridad de nuestros datos.
Certificados de seguridad

Estos consejos son normalmente para personas cuyo trabajo depende del correo electrónico y de la información de su computadora, sin embargo, esto no implica que el resto de las personas no puedan utilizarlos, ya sea si lo empleamos solo para hablar con amigos o para hacer trabajos del colegio o la universidad en grupo, ya que es seguro que cualquier persona que posea una computadora, pasaría un muy mal rato si por abrir su correo electrónico se infecta de un virus y pierde todos y cada uno de sus datos, no hay que confiarse, debe recordarse lo ya mencionado antes, que usted tenga cuidado no quiere decir que sus amigos lo tengan. Utilice siempre antivirus y proteja sus herramientas de uso diario.

Finalmente, se recomienda tener mucho cuidado al enviar y recibir correos electrónicos, ya que de la misma manera que los antivirus se actualizan constantemente, así también se actualizan los virus, por lo que se debe de ser sumamente precavido con esta valiosa herramienta, para así obtener el mayor provecho, minimizando las molestias que podrían surgir.

==========
Bachiller en Ingeniería en Sistemas. Candidato a Licenciatura en Ingeniería en Sistemas con énfasis en redes y sistemas telemáticos, ULACIT. Correo electrónico: supmontero@gmail.com

Referencias Bibliográficas

20minutos.es, 2005. Un millón mas de hogares con Internet en el ultimo año. Recuperado el 7 de octubre del 2007, de: http://www.20minutos.es/noticia/7098/0/internet/hogares/estadistica/

AFP, 2007. México espera contar con 70 millones de cibernautas en 2012. Recuperado el 11 de octubre del 2007, de: http://afp.google.com/article/ALeqM5i_S9Rg14YHBk8WkqfC1KCJwYeueg

Racsa, 2007. Disminuye Brecha digital en el país. Recuperado el 16 de octubre del 2007, de: https://www.racsa.co.cr/racsa_noticias/brecha_digital.htm

Monografías, 2007. Estudio sobre virus informáticos. Recuperado el 1 de noviembre de 2007, de: http://www.monografias.com/trabajos/estudiovirus/estudiovirus.shtml

Microsoft, 2007, ¿Qué son virus, gusanos y troyanos? Recuperado el 4 de noviembre de 2007 de: http://www.microsoft.com/latam/athome/security/viruses/virus101.mspx

Ferreyra Cortés, Gonzalo (1991), *VIRUS en las Computadoras*, México: Macrobit Editores, S.A. ISBN 970-604-077-3.

Virtualtamps, 2007. Temas de Computación. Recuperado el 10 de noviembre de 2007 de: http://www.virtualtamps.com.mx/computacion/ventajascorreo.html

Microsoft, 2007. Cómo el certificado de correo electrónico de Outlook reduce el correo no deseado, Recuperado el 10 de noviembre de: http://office.microsoft.com/es-es/downloads/FX101321103082.aspx?pid=CL100570423082

Dahousecat, 2007.Correo electrónico seguro, recuperado el 10 de noviembre de 2007 de: http://blog.dahousecat.net/2007/06/30/correo-electronico-seguro-certificado-digital-personal/