UNIDAD 1

CORREO ELECTRÓNICO

OBSERVACION Este materia ha sido desarrollado por el Dr. Luciano Tamargo para el dictado de materias similares dentro del Dpto. de Ciencias e Ingeniería de la Computación de la Universidad Nacional del Sur (DCIC) y ha sido adaptado y completado para cubrir los contenidos de parte de la materia Informática y Nuevas Tecnologias II dictada por el DCIC.

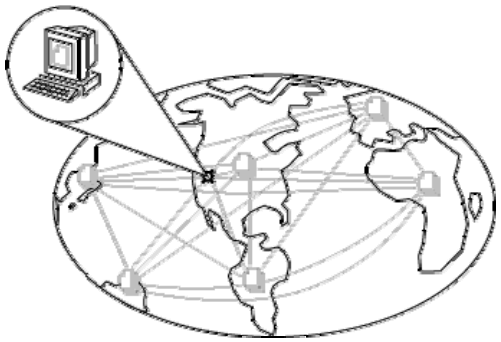
Parte del contenido y algunas imágenes de este apunte fueron tomados de los cursos gratuitos contenidos en aulaclick.es

Tabla de contenido

Internet

Internet es una red internacional que reúne una enorme cantidad de información, personas, computadoras y software funcionando e interactuando en forma cooperativa y global.

Internet conforma una especie de **laberinto virtual** que conecta computadoras de todo el mundo a través de diversos medios. Estos medios se presentan en muchas formas: desde cables de red local (varias máquinas conectadas en una oficina o empresa), a cables telefónicos convencionales, digitales y cables de fibra óptica. La transmisión también puede ser vía satélite o a través de servicios como la telefonía celular. Literalmente **Internet** significa "red de redes". En un día cualquiera se conectan a Internet millones de usuarios de cientos de países diferentes.



SERVICIOS

Internet brinda diferentes servicios:

- **Correo electrónico**: Para contactarse con personas en casi cualquier parte del mundo, a un costo muy bajo (también llamado e-mail por *electronic mail*).
- **Word-Wide Web (WWW)**: Servicios de noticias, deportes, cultura, entretenimientos, etc.
- **Software y publicaciones de distribución libre**: Como antivirus, manuales, tutoriales, archivos de audio, controladores para dispositivos, juegos, imágenes, animaciones,...
- **Grupos de discusión**: foros.
- **Transferencia de archivos**.
- **Comunicación remota en tiempo real**: por ejemplo chat o video llamadas.

En la actualidad el recurso más usado de Internet es el llamado Word-Wide Web que constituye todo el espacio de información.

Conexión a Internet

¿QUÉ SE NECESITA PARA CONECTARSE A INTERNET?

Para conectarse a Internet se necesitan varios elementos. Hay algunos elementos que varían según el tipo de conexión que elijamos y otros que son comunes a cualquier tipo de conexión. En general, necesitaremos:

- un equipo,
- una conexión,
- un módem,
- un proveedor de acceso a Internet y
- un navegador.

Equipo

El equipo es el elemento que **sirve al usuario para recibir y enviar información**. En el caso más común el equipo es una **computadora personal**, pero también puede ser un teléfono celular, como veremos más adelante.

Para utilizar Internet, es más aconsejable tener una buena conexión que un equipo muy potente, por eso cada vez más nos conectamos desde teléfonos celulares o pequeñas notebooks.

Conexión

La comunicación entre nuestra computadora e Internet necesita transportarse a través de algún **medio físico**. Existen diferentes tipos de conexiones:

- **Línea telefónica**: Es muy lenta y no permite que utilicemos el teléfono mientras estamos conectados. Sin embargo, existen las líneas RDSI y ADSL que permiten usar el teléfono aunque estemos conectados.
- **Cable**: Es una tecnología de banda ancha que transmite la información usando redes de fibra óptica y/o cable de antena de televisión. Este tipo de conexión se suele vender en conjunto con otros servicios como son telefonía o televisión digital. Nos permite permanecer conectados de manera permanente.

- **Telefonía móvil**: Utiliza diferentes sistemas para conectarse a Internet. Se elige el tipo de conexión según la cobertura que encontremos en nuestra zona. Cada vez más se utiliza el móvil para navegar.
- **Redes inalámbricas** (Wifi): Permite conectarse a Internet sin cables. Para ello necesitamos un modem o *router* WIFI que gestione la señal. También necesitamos un emisor-receptor en nuestro equipo.

La forma más simple es a través de la línea telefónica. En Argentina las más utilizadas son ADSL y el cable.

Modem

El modem establece la comunicación entre el equipo y el proveedor de Internet. Si el modem tiene *Wifi* nos podremos conectar a Internet sin cables.

Proveedor de acceso a Internet (ISP)

Los proveedores nos dan acceso a Internet. Para elegir bien un ISP (por *Internet Service Provider*) hay que tener en cuenta la rapidez de acceso, la calidad del servicio y por supuesto la tarifa. Algunos ejemplos de proveedores en Bahía Blanca son Speedy, BVC y Fibertel.

Navegador

Por último necesitaremos un programa que sea capaz de leer la información que hay en los servidores de Internet, y presentarla en pantalla. También son capaces de recoger la información que introduce el usuario mediante formularios y enviarla de vuelta al servidor.

Estos programas reciben el nombre de navegadores (*browsers*, en inglés) y el más conocido es *Internet Explorer* de Microsoft, que viene preinstalado en Windows lo que hace que sea el más usado, a pesar de existir navegadores más seguros y rápidos como *Firefox*, *Opera*, *Chrome* o *Safari*. Todos son gratuitos y se pueden descargar de Internet, por lo cual es fácil, además de recomendable, tener siempre una versión actualizada de los mismos. Más adelante en el apunte retomaremos este tema y lo abordaremos en detalle.

Correo electrónico

Correo electrónico (conocido también como *e-mail*), es un servicio de red que permite a los usuarios enviar y recibir mensajes y archivos rápidamente mediante sistemas de comunicación electrónicos. Principalmente se usa este nombre para denominar al sistema que provee este servicio en Internet, aunque por extensión también puede verse aplicado a sistemas análogos que usen otras tecnologías. Por medio de mensajes de correo electrónico se puede enviar no solamente texto, sino todo tipo de documentos digitales. Su eficiencia, conveniencia y bajo costo están logrando que el correo electrónico desplace al correo ordinario para muchos usos habituales.

ELEMENTOS

Para que una persona pueda enviar un correo a otra, cada una ha de tener una dirección de correo electrónico. Esta dirección la tiene que dar un proveedor de correo (yahoo, gmail, Hotmail, etc.), que son quienes ofrecen el servicio de envío y recepción. Es posible utilizar un programa específico de correo electrónico o una interfaz web, a la que se ingresa con un navegador web.

Dirección de correo

Una dirección de correo electrónico es un conjunto de palabras que identifican a una persona que puede enviar y recibir correo. Cada dirección es única y pertenece siempre a la misma persona.

Un ejemplo es *persona@servicio.com*, que se lee *persona arroba servicio punto com*. El signo **@** (llamado arroba) siempre está en cada dirección de correo, y la divide en dos partes: el nombre de usuario (a la izquierda de la arroba; en este caso, *persona*), y el dominio en el que está (a la derecha de la arroba; en este caso, *servicio.com*). Arroba también se puede leer "*en*", ya que *persona@servicio.com* identifica al usuario *persona* que está *en* el servidor *servicio.com* (indica una relación de pertenencia).

Lo que hay a la derecha de la arroba es precisamente el nombre del *proveedor* que da el correo, y por lo tanto, es algo que el usuario no puede cambiar, pero se puede optar por tener un dominio. Por otro lado, lo que hay a la izquierda depende normalmente de la elección del usuario, y es un identificador cualquiera, que puede tener letras, números, y algunos signos.

Es aconsejable elegir en lo posible una dirección fácil de memorizar para así facilitar la transmisión correcta de ésta a quien desee escribir un correo al propietario, puesto que es necesario transmitirla de forma exacta, letra por letra. Un solo error hará que no lleguen los mensajes al destino. Sin embargo, es indiferente que las letras que integran la dirección estén escritas en mayúscula o minúscula. Por ejemplo, *persona@servicio.com* es igual a *Persona@Servicio.Com*.

Proveedor de correo

Para poder enviar y recibir correo electrónico, generalmente hay que estar registrado en alguna empresa que ofrezca este servicio (gratuito o de pago). El registro permite tener una *dirección de correo* personal única y duradera, a la que se puede acceder mediante un nombre de usuario y una contraseña. Hay varios tipos de proveedores de correo, que se diferencian sobre todo por la calidad del servicio que ofrecen. Básicamente, se pueden dividir en dos tipos: los correos gratuitos y los que hay que pagar.

Gratuitos: Los correos gratuitos son los más usados, aunque incluyen algo de publicidad (unas incrustadas en cada mensaje y otros en la interfaz que se usa para leer el correo). Muchos sólo permiten ver el correo desde un sitio web propio del proveedor, para asegurarse de que los usuarios reciben la publicidad que se encuentra ahí. En cambio, otros permiten también usar un programa de correo configurado para que se descargue el correo de forma automática.

Una desventaja de estos correos es que en cada dirección, la parte que está a la derecha del @ muestra el nombre del proveedor; por ejemplo, el usuario *juan* puede tener *juan@correo-gratuito.net*. Este tipo de direcciones desagradan a algunos (sobre todo, a empresas) y por eso es común comprar o registrar gratuitamente (en ciertos países) un dominio propio, para dar un aspecto más profesional.

Pagos: Los correos que hay que pagar normalmente ofrecen todos los servicios disponibles. Es el tipo de correo que un proveedor de Internet da cuando se contrata la conexión. También es muy común que una empresa registradora de dominios venda, junto con el dominio, varias cuentas de correo para usar junto con ese dominio (normalmente, más de 1).

Correo web

Casi todos los proveedores de correo dan el servicio de *correo web*: permiten enviar y recibir correos mediante un sitio web diseñado para ello, y por tanto usando sólo un navegador web. La otra alternativa es usar un *programa de correo* especializado.

El *correo web* es cómodo para mucha gente, porque permite ver y almacenar los mensajes desde cualquier sitio (en un servidor remoto, accesible por el sitio web) en vez de en una computadora en particular. Como desventaja, es difícil de ampliar con otras funcionalidades, porque el sitio ofrece un conjunto de servicios concretos y no podemos cambiarlos. Además, suele ser más lento que un *programa de correo*, ya que hay que estar continuamente conectado a sitios web y leer los correos de uno en uno.

Cliente de correo

También están los *clientes de correo electrónico*, que son programas para gestionar los mensajes recibidos y poder escribir nuevos. Suelen incorporar muchas más funcionalidades que el *correo web*, ya que todo el control del correo pasa a estar en la computadora del usuario. Por ejemplo, algunos incorporan potentes filtros anti-*correo no deseado* (el llamado *SPAM*).

Los clientes de correo necesitan que el proveedor de correo ofrezca este servicio, ya que no todos permiten usar un programa especializado (algunos sólo brindan *correo web*). En caso de que sí lo permita, el proveedor tiene que explicar detalladamente cómo hay que configurar el programa de correo. Esta información siempre está en su sitio web, ya que es imprescindible para poder hacer funcionar el programa, y es distinta en cada proveedor. Entre los datos necesarios están: tipo de conexión, *dirección del servidor de correo*, *nombre de usuario* y *contraseña*. Con estos datos, el programa ya es capaz de obtener y descargar nuestro correo.

El funcionamiento de un *programa de correo* es muy diferente al de un *correo web*, ya que un programa de correo descarga *todos* los mensajes que tenemos disponibles, y luego pueden ser leídos sin estar conectados a Internet (además, quedan grabados en el disco). En cambio, en un sitio web se leen de uno en uno, y hay que estar conectado a la red todo el tiempo. Algunos ejemplos de programas que realizan las funciones de cliente de correo electrónico son *Mozilla Thunderbird*, *Outlook Express* y *Eudora*.

FUNCIONAMIENTO

Escritura del mensaje

Se pueden mandar mensajes entre computadores personales o entre dos equipos de una computadora central. Los mensajes se archivan en un buzón (una manera rápida de mandar mensajes). Cuando una persona decide escribir un correo electrónico, su programa (o correo web) le pedirá como mínimo tres cosas:

- **Destinatario**: una o varias direcciones de correo a las que ha de llegar el mensaje
- **Asunto**: una descripción corta que verá la persona que lo reciba antes de abrir el correo
- El propio **mensaje**. Puede ser sólo texto, o incluir formato, y no hay límite de tamaño

Además, se suele dar la opción de incluir *archivos adjuntos* al mensaje. Esto permite traspasar datos informáticos de cualquier tipo mediante el correo electrónico.

Para especificar el destinatario del mensaje, se escribe su dirección de correo en el campo llamado *Para* dentro de la interfaz (ver Figura 8). Si el destino son varias personas, normalmente se puede usar una lista con todas las direcciones, separadas por comas o punto y coma.

Además del campo **Para** existen los campos *CC* y *CCO*, que son opcionales y sirven para hacer llegar copias del mensaje a otras personas:

- Campo **CC** (*Copia de Carbón*): quienes estén en esta lista recibirán también el mensaje, pero verán que no va dirigido a ellos, sino a quien esté puesto en el campo **Para**. Como el campo **CC** lo ven todos los que reciben el mensaje, tanto el destinatario principal como los del campo **CC** pueden ver la lista completa.
- Campo **CCO** (*Copia de Carbón Oculta*): una variante del **CC**, que hace que los destinatarios reciban el mensaje sin aparecer en ninguna lista. Por tanto, el campo **CCO** nunca lo ve ningún destinatario.

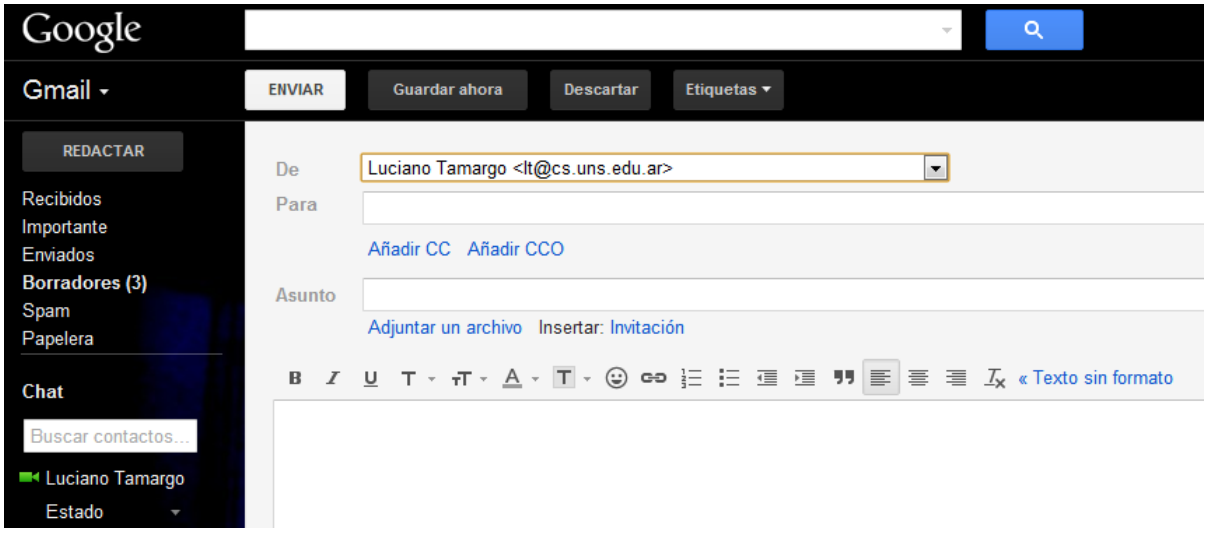


Figura 8. Ejemplo de mensaje electrónico

PROBLEMAS

El principal problema actual es el ***correo no deseado***, que se refiere a la recepción de correos no solicitados, normalmente de publicidad engañosa, y en grandes cantidades, promoviendo pornografía y otros productos y servicios de calidad sospechosa.

Usualmente los mensajes indican como remitente del correo una dirección falsa. Por esta razón, es difícil localizar a los verdaderos remitentes, y no sirve de nada contestar a los mensajes de correo no deseado: las respuestas serán recibidas por usuarios que nada tienen que ver con ellos. Por ahora, el servicio de correo electrónico no puede identificar los mensajes de forma que se pueda discriminar la verdadera dirección de correo electrónico del remitente de una falsa. Esta situación, que puede resultar chocante en un primer momento, es semejante por ejemplo a la que ocurre con el correo postal ordinario: nada impide poner en una carta o postal una dirección de remitente aleatoria, el correo llegará en cualquier caso.

Además del *correo no deseado*, existen otros problemas que afectan a la seguridad y veracidad de este medio de comunicación:

- los **virus informáticos**, que se propagan mediante archivos adjuntos infectando la computadora de quien los abre,
- la **suplantación de identidad**, que es correo fraudulento que generalmente intenta conseguir información bancaria,
- los **bulos** (bromas, burlas, o hoax), que difunden noticias falsas masivamente, y
- las **cadenas de correo electrónico**, que consisten en reenviar un mensaje a mucha gente; aunque parece inofensivo, la publicación de listas de direcciones de correo contribuye a la propagación a gran escala del correo no deseado y de mensajes con virus, suplantadores de identidad y engaños.

PRECAUCIONES RECOMENDABLES

Cuando recibamos un mensaje de correo electrónico que hable de algo que desconocemos (aunque nos lo haya mandado alguien que conocemos) conviene consultar su veracidad (por ejemplo a partir de buscadores de la web, tratando de consultar en el sitio web de la supuesta fuente de la información, o en webs serias, fiables y especializadas en el tipo de información en cuestión). Sólo si estamos seguros de que lo que dice el mensaje 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 (puede ser necesario poner sólo nuestra dirección de correo electrónico en la casilla Para) y borrando del cuerpo del mensaje encabezados previos con direcciones de correo electrónico (para facilitar la lectura es preferible copiar la parte del cuerpo del mensaje sin los encabezados previos y pegarla en un mensaje nuevo en el que aparece tras cliquear en reenviar tras borrar todo el texto, repetido a partir de previos envíos). Así evitaremos la propagación del correo no deseado así como la de mensajes con virus. Conviene que hagamos saber esto a nuestros contactos en cuanto nos reenvían mensajes con contenido falso, sin utilizar la casilla CCO o sin borrar encabezados previos con direcciones de correo electrónico.

Cuando el mensaje recibido lleve uno o varios archivos adjuntos tendremos cuidado, especialmente si el mensaje nos lo manda alguien que no conocemos. Hay peligro de que los archivos contengan virus. Sólo los abriremos si estamos seguros de su procedencia e inocuidad. Si, tras esto, comprobamos que los ficheros son inofensivos e interesantes para nuestros contactos podremos reenviarlo siguiendo las precauciones del párrafo anterior (en este caso, para que lleguen los ficheros adjuntos es más rápido hacer clic en reenviar que crear un mensaje nuevo y volverlos a adjuntar -aunque tendremos cuidado de borrar todo el texto que repite previos reenvíos; quizá pegando después el cuerpo principal del mensaje recibido si tiene información de interés o relacionada con los archivos adjuntos).

Cuando en un mensaje sospechoso se nos ofrezca darnos de baja de futura recepción de mensajes o de un boletín no haremos caso, es decir, no responderemos el mensaje, ni escribiremos a ninguna dirección supuestamente creada para tal fin (del tipo bajas@xxxx.es o unsubscribe@xxxxxxx.com), ni cliquearemos sobre un enlace para ello. Si hiciéramos algo de lo citado confirmaríamos a los remitentes de correo basura que nuestra cuenta de correo electrónico existe y está activa y, en adelante, recibiríamos más mensajes no deseados. Si nuestro proveedor de correo lo ofrece podemos cliquear en "*Es spam*" o "*Correo no deseado*" o "*Marcar como spam*". Así ayudaremos a combatir el correo basura.

SERVICIOS DE CORREO ELECTRÓNICO

Los principales proveedores de servicios de correo electrónico gratuito: *Gmail*, *Hotmail* y *Yahoo!*.

Los servicios de correo pagos los suelen dar las compañías de acceso a Internet o los registradores de dominios. También hay servicios especiales, como *Mailinator*, que ofrece cuentas de correo temporales (caducan en poco tiempo) pero que no necesitan registro.

Seguridad en el envío de datos por Internet

SEGURIDAD EN LA NUBE O CLOUD COMPUTING

La seguridad y la privacidad en la nube son las grandes preocupaciones en estos tiempos. Las ventajas de la computación en la nube están influyendo enormemente en nuestra forma de usar las computadoras: cada vez usamos más aplicaciones en nube: Gmail, Twitter, Facebok, Youtube. Paradójicamente estas maravillosas ventajas -la facilidad de acceso, lo asequible que resulta, su centralización y flexibilidad- podrían ser también la causa de nuevos tipos de inseguridad. La seguridad siempre ha sido uno de los principales problemas en el ámbito de la transmisión de datos y la computación. Con la aparición del Cloud Computing se ha convertido en un problema especialmente relevante, pues los datos del usuario pasan a estar almacenados en servidores ajenos, gestionados por proveedores que en principio no presentan garantías de confiabilidad. La escala es mucho más grande, y no hay tanto control físico como en la computación tradicional. Cuantos más usuarios utilicen un software más barato es contratarlo. Pero cuando miles de clientes distintos utilizan el mismo hardware a gran escala, cualquier fallo en el sistema o ataque por parte de hackers podría afectar negativamente a mucha gente. Hay que tener en cuenta los siguientes aspectos:

- Integridad de los datos: es necesario poder asegurar que los datos no han sido modificados por entidades no autorizadas, y que la información es la original.
- Pérdidas de información: debido a que los datos se dejan de almacenar en el cliente y pasan a estar ubicados en servidores en la nube, existe la probabilidad de pérdida de la información en el caso de fallo en el sistema ajeno al usuario.
- Confidencialidad o privacidad: es la garantía de que sólo puedan acceder a los datos usuarios autorizados. El usuario, en principio, no tiene control completo del acceso del proveedor a sus datos

Estos aspectos son especialmente importantes en el caso de determinadas aplicaciones que trabajan con datos sensibles, que no pueden verse comprometidos en manera alguna. Entre dichas aplicaciones se contarán las propias de bancos, empresas u hospitales, el sistema penitenciario, etc; a menudo por imperativo legal.

Como respuesta a la problemática anterior surge un nuevo servicio asociado a la computación e la nube: la seguridad como servicio, que se relaciona con los siguientes ítems:

- Seguridad del navegador utilizado: en el entorno de la nube, los servidores remotos son usados para la computación. Tu computadora se usa solo para entrada/salida de

operaciones, y para la autorización y autenticación de la información en la nube. Un navegador web estándar es una plataforma normalmente utilizada para todos los usuarios del mundo. Utilizar un navegador seguro es primordial. El protocolo Transport Layer Security (TLS) se suele utilizar para la encriptación de datos y la autentificación del host.

- Autenticación: en el entorno de la nube, la base para el control de acceso es la autenticación, el control de acceso es más importante que nunca desde que la nube y todos sus datos son accesibles para todo el mundo a través de internet. Trusted Platform Module (TPM) es extensamente utilizado y un sistema de autenticación más fuerte que el nombre de usuario y la contraseña. Trusted Computing Groups (TCG's) es un estándar sobre la autorización de usuarios y otras herramientas de seguridad de comunicación en tiempo real entre el proveedor y el cliente.
- Pérdida de gobernanza: en las infraestructuras de la nube, el cliente necesariamente cede el control al proveedor (Cloud Provider) en un número de asuntos, los cuáles afectan a la seguridad. Al mismo tiempo, el acuerdo de nivel de servicio no suele tener el cometido de surtir este tipo de servicios en la parte del proveedor de la nube, dejando una brecha en las defensas de seguridad.
- Protección de los datos: La computación en la nube pone en riesgo la protección de datos para los usuarios de la nube y sus proveedores. En muchos casos, ocasiona dificultades para el proveedor (en el rol del controlador de la información) para asegurar la efectividad práctica del manejo de los datos del proveedor de la nube y para cerciorar que los datos van por el camino correcto. Este problema se suele agravar en casos de múltiples transferencias de datos, por ejemplo entre sistemas de gobierno incluido el sistema penitenciario. Por otra parte, algunos proveedores de la nube, proporcionan información de sus prácticas de cercenamiento de datos. También hay algunas ofertas de certificaciones en el procesamiento de datos, las actividades de seguridad, y los controles de datos que tienen lugar Las corrientes de datos de internet están unidas al malware y de paquetes señuelo para meter al usuario en una desconocida participación en actividades delictivas.

Ej: la empresa Gradiant está trabajando en el editor de textos online Google Docs, de forma que los usuarios puedan almacenar sus documentos de forma cifrada en los servidores y que de este modo tengan la garantía de que sus datos estarán seguros y permanecerán inalterados.

CRIPTOGRAFIA Y SEGURIDAD EN LA NUBE

Por definición la criptografía es la ciencia de ocultar información, de manera que los usuarios no autorizados no puedan leerlo. La criptografía permite convertir los datos en texto sin formato legible o datos codificados llamados texto cifrado. Por definición la criptografía es la ciencia de ocultar información, de manera que los usuarios no autorizados no puedan leerlo. El secreto en la escritura es una práctica antigua que se remonta al antiguo Egipto, pero sigue siendo fundamental para asegurar los datos en la actualidad. De hecho, la encriptación es absolutamente necesaria cuando se transmiten datos confidenciales a través de medios no seguros como Internet.

La criptografía es una parte importante de la prevención de los datos privados de ser robados. Incluso si un atacante para entrar en una computadora o intercepta los mensajes todavía no será capaz de leer los datos si está protegido por la criptografía o cifrado. Además de ocultar el significado de los datos, la criptografía realiza otras necesidades críticas de seguridad para los datos, incluidos los certificados, confidencialidad e integridad.

La aparición de la computación en la nube y el uso masivo de las comunicaciones digitales han producido un número creciente de problemas de seguridad. Las transacciones que se realizan a través de la red pueden ser interceptadas, y por tanto, la seguridad de esta información debe garantizarse. Este desafío ha generalizado los objetivos de la criptografía para ser la parte de la criptología que se encarga del estudio de los algoritmos, protocolos (se les llama protocolos criptográficos), y sistemas que se utilizan para proteger la información y dotar de seguridad a las comunicaciones y a las entidades que se comunican.

La criptografía se puede utilizar para autenticar que el remitente de un mensaje es el remitente real y no un impostor. La criptografía también prevé el repudio, que es similar a la autenticación, y se utiliza para probar que alguien llega a enviar un mensaje o realiza una acción. En efecto, instancia que puede usarse para probar algún asunto penal a cabo en una transacción financiera específica.

La criptografía respeta la confidencialidad, ya que sólo un lector con el algoritmo de descifrado correcto puede leer el mensaje cifrado. Por último, la criptografía puede proteger la integridad de la información, garantizando que los mensajes no han sido alterados.

Los tres tipos de algoritmos utilizados para el cifrado son:

- Hashing: Un algoritmo hash se utiliza para crear un código irreversible de una parte de la información. Este código hash se llama un hash y es exclusiva de la información y se puede utilizar como una firma de los datos. Un hash se utiliza para la comparación de datos para asegurarse de que no se han cambiado, por lo que asegura la integridad de un mensaje
- Algoritmos de Cifrado Simétrico: también llamada criptografía privada o de clave secreta. Un algoritmo de cifrado simétrico puede ser descifrado, en lugar de ser irreversibles. Existen varios tipos de algoritmos simétricos. Algunos de los más populares son:

- Estándar de cifrado de datos (Data Encryption Standard) DES: fue uno de los primeros algoritmos ampliamente utilizados sin embargo, se ha resquebrajado y ya no se considera seguro
- Estándar de cifrado avanzado (Advanced Encryption Standard) AES: no se ha resquebrajado y es utilizado por el gobierno de los EE.UU., mientras que
- Rivest Cipher (RC): significa "Ron's Code" y es una familia de algoritmos escrito por Ron Rivest en 1987. Blowfish es un fuerte algoritmo simétrico de código abierto creado en 1993.
- Algoritmo Internacional de cifrado de datos (International Data Encryption Algorithm) IDEA): se ve favorecida por las naciones europeas
- Blowfish

- Algoritmos de Cifrado Asimétrico: Los algoritmos criptográficos asimétricos se diferencian de los algoritmos simétricos, ya que requiere de dos "claves" para cifrar y descifrar datos en comparación con el algoritmo de clave única simétrica. Asimétrica o cifrado de clave pública utiliza dos claves matemáticamente relacionadas: una clave pública conocida por todos para cifrar mensajes y una clave privada, conocida sólo por el receptor del mensaje a descifrar la información.

Criptografía Asimétrica y Protocolo PGP

La criptografía asimétrica (en inglés asymmetric key cryptography), también llamada criptografía de clave pública (en inglés public key cryptography) o criptografía de dos claves1 (en inglés two-key cryptography), es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona que ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier persona, la otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella. Además, los métodos criptográficos garantizan que esa pareja de claves sólo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves.

Si el remitente usa la clave pública del destinatario para cifrar el mensaje, una vez cifrado, sólo la clave privada del destinatario podrá descifrar este mensaje, ya que es el único que la conoce. Por tanto se logra la confidencialidad del envío del mensaje, nadie salvo el destinatario puede descifrarlo.

La criptografía asimétrica es ampliamente utilizada y sirve de base a los protocolos Transport Layer Security (TLS) y PGP (Pretty Good Privacy). Algunos algoritmos asimétricos comunes son RSA y Diffie-Hellman. Es importante mencionar que la criptografía asimétrica es normalmente más

costosa computacionalmente que la criptografía simétrica, es decir, que una computadora necesita realizar más cálculos para cifrar y descifrar los mensajes cifrados con criptografía asimétrica. Como ventaja, la criptografía asimétrica

- provee de autenticidad e integridad. Cuando se envía un mensaje cuya autenticidad e integridad
- es verificable, se dice que está firmado digitalmente. Así, el usuario tiene la posibilidad de enviar mensajes firmados y/o cifrados a sus destinatarios. Sé consiente y selectivo de la información que debes firmar y/o cifrar.
- se usa para proteger una gran variedad de comunicaciones, por ejemplo el correo electrónico, que es uno de los medios de comunicación más utilizados en la actualidad
- crea un revocado del certificado de tu clave. Así, en caso de que por algún motivo tu clave privada fuera comprometida, puedes revocarla y evitar que los usuarios no autorizados puedan hacer mal uso de ella.

Los sistemas de cifrado de clave pública o sistemas de cifrado asimétricos se inventaron con el fin de evitar por completo el problema del intercambio de claves de los sistemas de cifrado simétricos. Con las claves públicas no es necesario que el remitente y el destinatario se pongan de acuerdo en la clave a emplear. Todo lo que se requiere es que, antes de iniciar la comunicación secreta, el remitente consiga una copia de la clave pública del destinatario. Es más, esa misma clave pública puede ser usada por cualquiera que desee comunicarse con su propietario. Por tanto, se necesitarán sólo n pares de claves por cada n personas que deseen comunicarse entre sí.

Las dos principales ramas de la criptografía de clave pública son:

- **Cifrado de clave pública:** un mensaje cifrado con la clave pública de un destinatario no puede ser descifrado por nadie (incluyendo al que lo cifró), excepto un poseedor de la clave privada correspondiente--presumiblemente, este será el propietario de esa clave y la persona asociada con la clave pública utilizada. Se utiliza para confidencialidad.
- **Firmas digitales:** un mensaje firmado con la clave privada del remitente puede ser verificado por cualquier persona que tenga acceso a la clave pública del remitente, lo que demuestra que el remitente tenía acceso a la clave privada (y por lo tanto, es probable que sea la persona asociada con la clave pública utilizada) y la parte del mensaje que no se ha manipulado. Sobre la cuestión de la autenticidad.

Una analogía con el cifrado de clave pública es la de un buzón con una ranura de correo. La ranura de correo está expuesta y accesible al público; su ubicación (la dirección de la calle) es, en esencia, la clave pública. Alguien que conozca la dirección de la calle puede ir a la puerta y colocar un mensaje escrito a través de la ranura; sin embargo, sólo la persona que posee la llave (clave privada) puede abrir el buzón de correo y leer el mensaje. Una analogía para firmas digitales es el

sellado de un sobre con un sello personal. El mensaje puede ser abierto por cualquier persona, pero la presencia del sello autentifica al remitente.

CRIPTOGRAFIA Y CORREO ELECTRÓNICO

La mayor parte de los mensajes de correo electrónico que se transmiten por Internet no incorporan seguridad alguna, por lo que la información que contienen es fácilmente accesible a terceros. Para evitarlo, la criptografía también se aplica al correo electrónico. Entre las diversas ventajas que tiene usar un certificado al enviar un email, podríamos destacar la seguridad que nos aporta ya que así evita que terceras personas (o ''hackers'') puedan leer su contenido, o bien que tenemos la certeza de que el remitente de éste correo electrónico es realmente quien dice ser.

Normalmente el correo electrónico sólo provee cifrado en el proceso de autenticación. Es decir, cuando un usuario inicia sesión en su correo electrónico, la contraseña va protegida en su transmisión, pero el resto de la información, incluyendo los correos electrónicos viaja sin ser codificada por lo que pueden ser capturada y leída por usuarios no autorizados. Es importante cifrar el correo electrónico para asegurar que los mensajes son leídos sólo por los usuarios autorizados, así como firmar los correos electrónicos enviados para permitir que los destinatarios de nuestros mensajes corroboren la autenticidad de los mismos.

Una de las tecnologías más utilizadas para la implementación de criptografía asimétrica en el correo electrónico es PGP (Pretty Good Privacy), la cual se distribuye gratuitamente y puede ser agregada a interfaces existentes de correo desde donde los usuarios pueden crear y administrar sus claves. También existen alternativas como Enigmail que permiten cifrar el correo desde clientes de coreo como Thunderbird, siempre y cuando sea soportada por el proveedor del servicio de correo.

BUENAS PRÁCTICAS PARA MEJORAR EL CIFRADO DE DATOS

- Utiliza una clave robusta para proteger tu información. Si la clave es débil es probable que un atacante logre adivinarla con facilidad, utilizando una variedad de ataques de diccionario, fuerza bruta y estadísticos.
- Establece un mecanismo para recuperar la clave de cifrado en caso de olvidarla. Si no lo haces, es probable que no haya manera de recuperar los archivos y se pierdan para siempre. Es recomendable que la clave usada para cifrar un activo de información, a su vez sea cifrada y almacenada utilizando una clave maestra, con el fin de recuperarla en caso de que se olvide.
- Dependiendo del tamaño y de la importancia de la información cifrada, puede ser recomendable realizar una o varias copias de ésta, de manera que si ocurre algún problema con

el medio de almacenamiento (disco duro, CD/DVD, memoria usb, etc.), haya forma de recuperar la información original. La criptografía puede usarse para proteger cualquier información digital. Se usa para proteger discos completos, particiones, carpetas y archivos, incluyendo la información que se transmite de un sistema de cómputo a otro. Determina qué grado de protección requieres en tus sistemas, en función del grado de protección que desees proveer a la información y el grado de funcionalidad y eficiencia que necesites.

- Durante el proceso de generación de claves, en ocasiones se permite indicar una “frase de contraseña”, la cual se usa para proteger tu clave y controlar tu acceso. De esta manera, funciona como una capa de protección adicional, para que en caso de que te sea robada no pueda ser usada de manera no autorizada. Proporciona una frase de contraseña robusta pero que puedas recordar