Este glosario se proporciona sólo para su información, y no se pretende que sea fiable como descripción completa o autorizada de los términos definidos a continuación, ni de las ramificaciones de seguridad o privacidad de las tecnologías descritas en él.

Glosario

administrador de certificados.
La parte del navegador que permite ver y administrar certificados. Para ver la ventana del administrador de certificados: abrir el menú Editar, elegir Preferencias, hacer clic en Privacidad y Seguridad, y luego elegir Administrar certificados.

administrador de contraseñas.
La parte del navegador que puede ayudar a recordar algunos o todos los nombres y contraseñas almacenándolas en el disco duro, e introduciéndolas automáticamente cuando se visitan esos sitios web.

administrador de cookies.
La parte del navegador que puede utilizar para controlar cookies.

algoritmos criptográficos.
Un conjunto de reglas o directrices usadas para realizar operaciones criptográficas tales como cifrado y descifrado.

aplicación auxiliar.
Cualquier aplicación que se use para abrir o ver un fichero descargado por el navegador. Un plugin es un tipo especial de aplicación auxiliar que se instala en el directorio de plugins y suele tener como función ejecutarse internamente en el navegador. Microsoft Word, Adobe Photoshop, y otras aplicaciones externas están consideradas aplicaciones auxiliares pero no plugins, ya que no se instalan automáticamente en el directorio del navegador, pero se pueden ejecutar desde el cuadro de diálogo al efectuar una descarga.

aplicación web
Una aplicación que no se está ejecutando en su equipo sino remotamente en un sitio web. Los ejemplos incluyen sistemas de correo web o sistemas basados en web en los que introduce información en un formulario y recibe una respuesta en forma de una página web. Una aplicación web *sin conexión* puede funcionar sin una conexión activa a Internet guardando las páginas relevantes localmente antes de ejecutar la aplicación.

asa
Un pequeño elemento cuadrado a la izquierda de la barra de menú y las barras de herramientas. El asa permite al usuario plegar rápidamente la barra de menú y las barras de herramientas.

asunto.
La entidad (persona, organización, o router) identificada por medio de un certificado. En particular, el campo asunto de un certificado contiene el nombre de asunto de la entidad certificada y otras características.

autoridad certificadora (CA).
Un servicio que emite un certificado tras verificar la identidad de la persona o entidad que se pretende identificar con el certificado. Una CA también renueva y revoca certificados y genera una lista de certificados revocados a intervalos regulares. Las CAs pueden ser independientes o una persona u organización que usa software servidor de emisión de certificados (como puede ser el sistema de gestión de certificados de SeaMonkey). Ver también certificado, CRL (lista de revocación de certificados).

barra de componentes.
Es la barra de herramientas que está situada en la esquina inferior izquierda de cualquier ventana de SeaMonkey. La barra de componentes permite que se pueda cambiar entre los componentes de SeaMonkey haciendo clic en los iconos del navegador, Correo y Noticias, Composer, etc.

barra de direcciones.
El campo (y botones asociados) que están cerca del borde superior de la ventana del navegador donde se puede escribir una URL o buscar término.

barra de estado.
Es la barra de herramientas situada en la parte inferior de cualquier ventana de SeaMonkey. Incluye la barra de componentes a la izquierda y los iconos de estado a la derecha.

barra de marcadores.
Es la barra de herramientas que se puede personalizar y que por defecto aparece justo debajo de la barra de direcciones en el navegador. Contiene botones estándar como Inicio, Marcadores, etc. que se pueden añadir o borrar. También se pueden añadir botones en los marcadores preferidos o en las carpetas que contienen grupos de marcadores.

Barra de menús
La barra de herramientas cerca de la parte superior de cualquier ventana de SeaMonkey que incluye los menús Archivo, Editar y Ver.

barra de navegación.
Es la barra de herramientas que se encuentra cerca de la parte superior de la ventana del navegador que incluye los botones

de Anterior y Siguiente.

barra de notificación
Una barra que aparece en la parte superior del área de contenido para informarle sobre algo que precisa de su atención, p.e. cuando el administrador de contraseñas puede guardar una contraseña para usted, cuando se ha bloqueado una ventana emergente o se necesita un plugin adicional.

CA.
Ver autoridad certificadora (CA).

CA raíz.
La autoridad certificadora (CA) con certificado firmado por sí misma en la parte más alta de una cadena de certificados. Ver también CA subordinada.

CA subordinada.
Una autoridad certificadora (CA) cuyo certificado está firmado por otra CA subordinada o por la CA raíz. Ver también cadena de certificados y CA raíz.

caché.
Una colección de copias de páginas web almacenadas en el disco duro del ordenador o en su memoria de acceso aleatorio (RAM, Random Access Memory). El navegador acumula estas copias mientras navega por la Web. Cuando se hace clic en un enlace o se escribe una URL para acceder a una página web cuyo contenido ya está en la caché, el navegador compara la copia almacenada con el original. Si no ha habido cambios, el navegador usa la copia de la caché en vez de volver a recuperar el original, ahorrando tiempo de procesamiento y descarga.

cadena de certificados.
Una serie jerárquica de certificados firmados por autoridades certificadoras sucesivas. Un certificado de una CA identifica a una autoridad certificadora (CA) y se usa para firmar certificados emitidos por esa autoridad. Un certificado de una CA también puede estar firmado por el certificado CA de una CA padre y así sucesivamente hasta la CA raíz.

canal
Una fuente actualizada con frecuencia de referencias a páginas web, normalmente noticias o artículos de blogs. Técnicamente es un documento XML disponible a través de una URL pública, compuesto de varios elementos en su interior, cada uno de los cuales contiene ciertos metadatos (posiblemente incluyendo un resumen) y una URL al artículo completo del blog o sitio de noticias. El documento XML se regenera a intervalos regulares, o siempre que se publica un nuevo artículo en el sitio web. Las aplicaciones web pueden suscribirse a la URL que sirve el canal y presentar los nuevos artículos a medida que se actualizan en el documento XML subyacente. Hay formatos XML específicos para los canales, lo más comunes de los cuales son RSS y Atom.

certificado.
El equivalente digital de una tarjeta fiscal. Un certificado especifica el nombre de una persona física, empresa u otra entidad y certifica que una clave pública, que está incluida en el certificado, pertenece a esa entidad. Cuando se firma un mensaje o datos digitalmente, la firma digital para ese mensaje se crea con la ayuda de la clave privada que corresponde a la clave pública en el certificado. Un certificado es emitido y firmado digitalmente por una autoridad certificadora (CA). La validez de un certificado se puede verificar comprobando la firma digital de la CA. También se llama identificación digital, pasaporte digital, certificado de clave pública X.509, y certificado de seguridad. Ver también criptografía con clave pública.

certificado de CA.
Un certificado que identifica a una autoridad certificadora. Ver también autoridad certificadora (CA), CA subordinada, CA raíz.

certificado de cifrado.
Un certificado cuya clave pública se usa sólo para cifrado. Los certificados de cifrado no se usan para operaciones de firma. Ver también pares de claves duales, certificado de firma.

certificado de firma.
Un certificado cuya correspondiente clave privada se usa para firmar los datos que se transmiten, para que el receptor pueda verificar la identidad de quien lo envía. Las Autoridades de Certificados (CAs) suelen emitir certificados de firma que sirven para firmar mensajes de correo electrónico y también para usarse como certificado de cifrado, usado para cifrar mensajes de correo electrónico. Ver también pares de claves duales, firma digital.

certificado de seguridad.
Ver certificado.

certificado para la firma de objetos.
Un certificado cuya clave privada correspondiente se usa para firmar objetos como ficheros de código. Ver también firma de objetos.

certificado SSL de cliente.
Un certificado que un cliente (como pueda ser un navegador) presenta a un servidor para acreditar la identidad del cliente (o la identidad de la persona que usa el cliente) usando el protocolo SSL (capa de conexiones seguras). Ver también identificación del cliente.

certificado SSL de servidor.

Un certificado que un servidor presenta a un cliente para verificar la autenticidad de la identidad del servidor usando el protocolo SSL (capa de conexiones seguras).

cifrado.
El proceso de juntar o separar información de manera que se enmascara su significado. Por ejemplo, las conexiones cifradas entre dos ordenadores hace que sea muy difícil de descifrar, o *desencriptar*, la información que viaja por la conexión. La información cifrada sólo puede ser descifrada por alguien que tenga la clave apropiada. Ver también criptografía con clave pública.

cifrado simétrico.
Un método de cifrado que usa una sola clave criptográfica para cifrar y descifrar un mensaje determinado.

cifrar.
Ver algoritmos criptográficos.

clave.
Un número de cierta longitud utilizado por algoritmos criptográficos para cifrar o descifrar datos. Por ejemplo, la clave pública de una persona permite que otras personas cifren mensajes para esa persona. Los mensajes cifrados deben descifrarse usando la clave privada. Ver también criptografía con clave pública.

clave de cifrado.
Una clave privada que se usa sólo para cifrado. Una clave de cifrado y su equivalente clave pública, más una clave de firma y su clave pública equivalente, constituyen un par de claves dual.

clave de firma.
Una clave privada usada sólo para firmar. Una clave de firma y su clave pública equivalente, junto con una clave de cifrado y su equivalente clave privada, constituyen pares de claves duales.

clave principal.
Una clave simétrica usada por el administrador de certificados para cifrar información. Por ejemplo, el administrador de contraseñas usa el administrador de certificados y la clave principal para cifrar contraseñas de correo electrónico, de páginas web y otra información confidencial que esté almacenada. Ver también cifrado simétrico.

clave privada.
Uno de los elementos del par de claves usadas en criptografía de clave pública. La clave privada se mantiene en secreto y se usa para descifrar los datos que han sido cifrados con la correspondiente clave pública.

clave pública.
Uno de los elementos del par de claves que se usan en la criptografía de clave pública. La clave pública se distribuye libremente y se publica como parte de un certificado. Suele usarse para cifrar los datos que se mandan al propietario de la clave, que descifra los datos con la correspondiente clave privada.

cliente.
El software (como puede ser un navegador) que realiza peticiones y recibe información de un servidor, que normalmente se ejecuta en una máquina distinta. A un ordenador en el que se ejecuta software cliente se le suele llamar cliente.

complemento
Una pieza de software que puede añadirse a SeaMonkey para cambiar su apariencia, comportamiento, o para añadir nuevas características. También puede cambiar el idioma mostrado en la interfaz de usuario. Ver también extensión, paquete de idioma, plugin y tema.

conexión segura
Una conexión entre un cliente y un servidor que usa algún tipo de cifrado (normalmente, SSL) para asegurar que no puede ser interceptada por terceros. La mayoría de las veces, el servidor es el que proporciona el certificado para identificarse a sí mismo.

conexión segura
Una conexión que usa SSL o TLS. Toda la comunicación entre su equipo y el servidor está cifrada de modo que nadie que esté espiando su conexión podrá leerlo. Tenga en cuenta que los datos sólo se cifran durante la transmisión entre su aplicación cliente y el servidor, tras lo cual ya no está cifrada. Para probar su identidad al cliente, el servidor necesita identificarse a sí mismo usando un certificado. Un certificado no válido puede indicar un ataque en el servidor o la conexión, por lo que es importante hacer caso a los avisos sobre certificados.

consejo.
Una pequeña caja de texto que aparece cuando se mantiene el puntero del ratón unos segundos sobre ciertos elementos de la pantalla. Normalmente contienen información relativa al elemento sobre el que se ha situado el puntero.

consentimiento implícito.
También conocido como consentimiento “opt-out” (exclusión opcional). Se usa para describir las opciones de privacidad que pueden permitir a los sitios web recoger información sobre Vd. (por ejemplo, mediante cookies y formularios en línea) a menos que se niegue explícitamente a dar su consentimiento seleccionando una opción en la página web que el sitio proporciona para ese fin. Mientras la información se recoge, puede que no se solicite ningún consentimiento. Vea también rastreo del usuario

contraseña cifrada
Usada para la identificación basada en contraseña para conseguir la identificación segura. La contraseña del usuario se cifra antes de ser enviada al servidor (p.e., por métodos como CRAM-MD5) para evitar que nadie espiando la conexión pueda verla en texto en claro. Este mecanismo se usa frecuentemente cuando no hay disponible una conexión segura.

contraseña de copia de seguridad para certificados.
Una contraseña que protege un certificado del que se está haciendo una copia de seguridad o ya se ha hecho con anterioridad. El administrador de certificados pide que se ponga una contraseña cuando se hace una copia de seguridad de un certificado, que será necesaria para restaurar un certificado del cual se ha hecho una copia de seguridad.

contraseña maestra.
Una contraseña usada por el administrador de certificados para proteger la clave principal u otras claves privadas almacenadas en un dispositivo de seguridad. El administrador de certificados necesita acceso a las claves privadas, por ejemplo, cuando se firman mensajes de correo o se usa uno de los certificados propios para identificarse en una página web. Se necesita acceder a la clave maestra cuando el administrador de contraseñas o el administrador de formularios leen o añaden datos a la información personal. Se puede establecer o cambiar contraseña maestra desde el panel de preferencias de contraseñas. Cada dispositivo de seguridad necesita una contraseña maestra independiente. Ver también clave privada, clave principal.

cookie.
Una pequeña cantidad de información almacenada en el ordenador generada por algunos sitios web. Cuando se visita uno de estos sitios web, se pide al navegador que ponga una o más cookies en el disco duro. Después, cuando se vuelve a ese sitio web, el navegador manda las cookies pertenecientes a ese sitio. Las cookies ayudan a las páginas web a guardar información acerca de usted, como el contenido de un carro de la compra. Se puede controlar en las preferencias cómo se usan las cookies y cuánta información deseamos que los sitios web puedan almacenar en ellas. Ver también cookie externa.

cookie externa.
Vea cookie de terceros.

cookie de terceros.
Una cookie de un sitio web que se almacena en el ordenador cuando se visita un sitio web distinto. A veces un sitio web muestra contenido que es albergado en otro sitio web. Ese contenido puede ser cualquier cosa, desde una imagen a texto o un anuncio. El segundo sitio web que alberga tales elementos también tiene la capacidad de guardar cookies en su navegador, incluso si Vd. no lo visita directamente. Las cookies de terceros también se conocen como “cookies externas”.

CRAM-MD5
Un algoritmo criptográfico usado para el cifrado de contraseñas para conseguir identificación segura.

criptografía.
El arte y práctica de ensamblar (cifrar) y desensamblar (descifrar) información. Por ejemplo, las técnicas criptográficas se usan para componer y descomponer la información que circula entre páginas web comerciales y nuestro navegador. Ver también criptografía con clave pública.

criptografía con clave pública.
Un conjunto de estándares y técnicas ampliamente conocidas que permiten a una entidad (una persona, una organización, o hardware, como un router) verificar electrónicamente su identidad o firmar y cifrar datos. Para ello, se necesitan dos claves: una clave pública y una clave privada. La clave pública se publica como parte de un certificado, que asocia esa clave con una identidad concreta. La correspondiente clave privada se mantiene en secreto. Los datos cifrados con la clave pública sólo se pueden descifrar con la clave privada.

CRL (lista de revocación de certificados).
Una lista de certificados revocados que se genera y está firmada por una autoridad certificadora (CA). La última CRL se puede descargar al navegador o a un servidor, luego haga una comprobación contra él para asegurarse que los certificados todavía son válidos antes de permitir su uso para identificaciones.

descifrado.
El proceso de descomponer datos que han sido cifrados. Ver también cifrado.

detección de alteraciones.
Un mecanismo que asegura que los datos recibidos en formato electrónico no han sido alterados; es decir, que los datos recibidos se corresponden en su totalidad con la versión original de los mismos datos.

dirección IP (dirección de protocolo de Internet.
La dirección de una máquina en una red TCP/IP. Cada ordenador en Internet tiene una dirección IP. Los clientes tienen una IP permanente o una asignada dinámicamente cada vez que se conectan a la red. Las direcciones IP se escriben como cuatro conjuntos de números, de esta forma: 204.171.64.2.

dispositivo de seguridad.
Hardware o software que proporciona servicios criptográficos como cifrar y descifrar y puede almacenar certificados y claves. Una tarjeta inteligente es un ejemplo de un dispositivo de seguridad implementado en hardware. El administrador de certificados tiene su propio dispositivo de seguridad interno, llamado dispositivo de seguridad software, que está siempre disponible mientras se ejecuta el navegador. Cada dispositivo de seguridad está protegido por su propia contraseña maestra.

dispositivo de seguridad software.
El dispositivo de seguridad predeterminado que usa el administrador de certificados para almacenar claves privadas asociadas con los certificados. Adicionalmente al uso de claves privadas, el dispositivo de seguridad software almacena la clave principal usada por el administrador de contraseñas para cifrar contraseñas de correo, de páginas web, y otra información importante. Ver también clave privada y contraseña maestra.

DN, nombre distinguido (Distinguished Name).
Un nombre indicado de una manera especial que identifica de manera única el asunto de un certificado.

Do Not Track
Un mecanismo que permite a los usuarios informar a los sitios web que no quieren ser rastreados por sitios web de terceros y aplicaciones web. Se añade una preferencia sobre el rastreo del usuario en la cabecera HTTP y se envía al sitio web. SeaMonkey permite enviar solicitudes “Do Not Track”, pero los sitios web no están obligados a respetar lo indicado en ella.

extensión
Un tipo de complemento que cambia el comportamiento de SeaMonkey o le añade nuevas funcionalidaes.

FIPS PUBS 140-1.
Siglas de Federal Information Processing Standards Publications (FIPS PUBS) 140-1, es un estándar del gobierno de EEUU para implementar módulos criptográficos -es decir, hardware o software que cifra y descifra datos o realiza otras operaciones criptográficas, como la creación o comprobación de firmas digitales. Muchos productos vendidos al gobierno de EEUU deben ser compatibles con uno o más de los estándares de FIPS.

firma de objetos.
Una tecnología que permite a los desarrolladores de software firmar el código Java, scripts en JavaScript, o cualquier otro tipo de fichero, y que permite a los usuarios identificar a los firmantes y controlar el acceso por el código firmado a los recursos locales.

firma digital.
Un código creado a partir de los datos a firmar y la clave privada del firmante. Este código es único para cada nueva porción de datos. Una simple coma añadida a un mensaje cambia la firma digital para ese mensaje. Cuando una firma digital se valida correctamente con el software apropiado, no indica sólo que el mensaje o transacción son correctos, sino que también es una garantía de que los datos del mensaje no han cambiado desde que se firmó digitalmente. Una firma digital no tiene nada que ver con una firma escrita a mano, aunque a veces puede tener propósitos legales similares. Ver también no repudio, detección de alteraciones.

FTP (protocolo de transferencia de ficheros).
Un estándar que permite a los usuarios transferir ficheros de un ordenador a otro a través de la red. Se puede usar el navegador para obtener ficheros usando FTP.

GSSAPI (Generic Security Services Application Program Interface, Interfaz de programación de aplicaciones de servicios genéricos de seguridad)
Ver Kerberos.

HTML (lenguaje de hipertexto basado en marcas).
El formato que se usa en las páginas web. El estándar HTML define marcas (tags) o códigos para definir las propiedades del texto, tipos de letra, estilos, imágenes y otros elementos que forman parte de una página web.

HTTP (protocolo de transferencias de hipertexto).
El protocolo usado para transferir páginas web (documentos hipertexto) entre navegadores y servidores a través de la World Wide Web.

HTTPS (protocolo seguro de transferencias de hipertexto).
La versión segura del protocolo HTTP que usa SSL para asegurar la privacidad de los datos del cliente (como la información de tarjetas de crédito) mientras se transmiten por Internet.

huella (certificado).
Ver huella de un certificado.

huella (navegador)
Un método de rastreo de usuarios por el cual se identifica a un usuario basándose en características del navegador como las versiones del navegador y del sistema operativo, las preferencias de idioma establecidas o los plugins instalados.

huella de un certificado.
Un número único asociado con un certificado. El número no es parte del certificado en sí pero es el resultado de aplicar una función matemática al contenido del certificado. Si el contenido del certificado cambia, incluso en un sólo carácter, la función produce un número distinto. Por tanto, las huellas de certificados pueden usarse para verificar que los certificados no han sido modificados.

identificación.
El uso de una contraseña, certificado, número de identificación personal (PIN), u otra información para validar una identidad en una red de ordenadores. Ver también identificación con contraseñas, identificación con certificados, identificación del cliente, identificación del servidor, identificación segura.

identificación con certificados.
Verificación de la identidad basada en certificados y cifrado mediante clave pública. Ver también identificación con contraseñas.

identificación con contraseñas.
Identificación confidencial usando un nombre y una contraseña. Ver también identificación.

identificación del cliente.
El proceso de identificar un cliente en un servidor, por ejemplo con un usuario y contraseña o con un certificado SSL de cliente y algunos datos firmados digitalmente. Ver también SSL (capa de conexiones seguras), identificación en el servidor.

identificación del servidor.
El proceso de identificarse el servidor a un cliente usando un certificado SSL de servidor. Ver también identificación del cliente, SSL (capa de conexiones seguras).

identificación digital.
Ver certificado.

identificación falsa.
La presentación de una entidad como una persona u organización que no es. Por ejemplo, una página web puede aparentar ser un almacén de muebles cuando en realidad es un sitio web que toma números de tarjetas de crédito y no manda nada. Ver también spoofing.

identificación segura
Un tipo de identificación que se puede conseguir mediante el cifrado de la contraseña o por mecanismos como Kerberos y NTLM. No debe confundirse con una conexión segura.

indiscreción.
Intercepción no deseada de la información enviada a través de la red por una entidad a la que dicha información no está destinada.

IMAP (protocolo de acceso a mensajes de Internet).
Un protocolo estándar para servidores de correo que permite almacenar todos los mensajes y los cambios en el servidor en vez del disco duro del ordenador. Usar IMAP en vez de POP ahorra espacio en disco y permite acceder a las carpetas del correo, incluyendo mensajes enviados, borradores y carpetas personalizadas, desde cualquier lugar. Usar un servidor IMAP con una conexión de módem es por lo general más rápido que usar un servidor POP, ya que inicialmente se descargan sólo las cabeceras de los mensajes. No todos los ISPs ofrecen servicios IMAP.

Internet.
Una red mundial de millones de ordenadores que se comunican entre sí usando protocolos estándar como TCP/IP. Desarrollado originalmente para el ejército de EEUU en 1969, Internet creció para incluir instituciones de educación e investigación y, a finales los años 90, a millones de empresas, organizaciones y particulares. Hoy en día Internet se usa para correo electrónico, navegar por la World Wide Web (WWW), mensajería instantánea, grupos, y otros muchos servicios.

IRC (charla retransmitida por Internet).
Un protocolo usado para charlar con otras personas en tiempo real usando un cliente IRC.

ISP (proveedor de servicios de Internet).
Una institución o compañía que proporciona conexiones a Internet.

Java.
Un lenguaje de programación desarrollado por Sun Microsystems. Un programa Java puede ejecutarse en muchos tipos distintos de ordenadores, evitando así que los programadores tengan que crear versiones distintas de un mismo programa para cada tipo de ordenador. Los programas y applets escritos en Java no son directamente compatibles con su navegador.

JavaScript.
Un lenguaje de *scripting* usado comúnmente para construir páginas web. Los programadores usan JavaScript para hacer las páginas web más interactivas; por ejemplo, para mostrar formularios y botones. JavaScript no debe ser confundido con Java. Son dos lenguajes técnicamente distintos. No es necesario tener Java instalado para que JavaScript funcione correctamente.

Kerberos
Un mecanismo para usar *single-signon* (inicio de sesión único), tarjetas inteligentes, u otros métodos personalizados para identificar el acceso sin utilizar contraseñas para cada servicio individual. Se usa sobre todo en grandes redes empresariales/institucionales donde la identificación se proporciona por servicios centralizados como LDAP.

LaTeX
Un procesador de textos y lenguaje de marcas de documentos para documentos de imprenta, ampliamente usado en el mundo académico. En particular, proporciona una sintaxis de texto sencillo para escribir fórmulas matemáticas complejas.

LDAP (protocolo ligero de acceso a directorios).
Un protocolo estándar para acceder a servicios de directorio, como libros de direcciones corporativos, desde cualquier plataforma. Se puede configurar el navegador para acceder a directorios LDAP desde la libreta de direcciones. También se pueden configurar el correo y las noticias para usar un servidor de directorio LDAP para autocompletar direcciones de correo

electrónico.

Malware
Abreviatura de “Software Malicioso” y un término general para una variedad de software diseñado para dificultar la operación del equipo, recopilar información confidencial u obtener acceso a su equipo. Pueden ser distribuidos por páginas web infectadas o como adjunto de mensajes de correo. Entre los ejemplos se incluyen virus, gusanos, troyanos, spyware o adware. El malware puede redistribuirse a sí mismo enviando mensajes para infectar otros equipos.

marcador.
Una dirección de página web almacenada (URL) a la que se puede acceder fácilmente haciendo clic en un icono en la barra de marcadores o eligiendo el nombre del marcador en el menú Marcadores.

marco.
Los marcos son páginas web contenidas dentro de una “meta” página que las mantiene coordinadas. A menudo se les conoce por su término en inglés, *“frame”*.

MathML (Mathematical Markup Language, lenguaje de marcado matemático)
El lenguaje de marcado usado para escribir notaciones matemáticas en páginas web.

módulo de seguridad.
Ver módulo PKCS #11.

módulo PKCS #11.
Un programa en el ordenador que gestiona los servicios criptográficos como el cifrado y descifrado usando el estándar PKCS #11. Otros nombres son *módulos criptográficos*, *proveedores de servicios criptográficos*, o *módulos de seguridad*. Los módulos PKCS #11 controlan dispositivos tanto hardware como software. Un módulo PKCS #11 siempre controla una o más ranuras, que pueden implementarse mediante algún lector físico (por ejemplo, para leer tarjetas inteligentes) o mediante software. Cada ranura de un módulo PKCS #11 puede, sin embargo, contener un dispositivo de seguridad (también llamado *token*) que es el dispositivo hardware o software que proporciona los servicios criptográficos y almacena certificados y claves. El administrador de certificados lleva dos módulos internos PKCS #11. Se pueden instalar módulos adicionales en el ordenador para controlar lectores de tarjetas inteligentes u otros dispositivos hardware.

motor de búsqueda o buscador.
Un programa basado en una página web que permite a los usuarios buscar y recuperar información específica de la World Wide Web (WWW). El motor de búsqueda puede buscar en todo el texto de los documentos web o una lista de palabras clave, o usar técnicas de revisión de documentos web e indexarlos manualmente para poder ser recuperados. Normalmente, el usuario escribe una palabra o una frase, también llamada consulta, en un cuadro de búsquedas, y el motor de búsqueda muestra los enlaces a las páginas web relevantes.

navegación basada en ubicación
Un método para determinar la ubicación de un usuario para proporcionar servicios personalizados para la ubicación actual, o para el propósito de rastrear al usuario. Además de la dirección IP, se usa información específica del proveedor como puntos de acceso inalámbricos para determinar la longitud y latitud y altitud así como la velocidad y dirección (si están disponibles) que se entrega al sitio web solicitante. Es proporcionada por un servicio de geolocalización.

navegación con cursor
Una característica de SeaMonkey que le permite desplazarse por el texto en las páginas web y los mensajes de correo (o esta ventana de ayuda) con un cursor. Usando su teclado, puede desplazarse y seleccionar texto como lo haría en un editor de textos. Puede activar y desactivar el modo del cursor pulsando la tecla F7. El modo de navegación con cursor también puede activarse y desactivarse en las preferencias Avanzadas - Navegación con teclado.

navegación privada
Navegar en una sesión en la que no se conservan datos privados (tales como el historial de navegación, las cookies, y el contenido cacheado) más allá de la duración de la sesión privada. La navegación privada no debe confundirse con la navegación anónima y no evita el rastreo de usuario ni la monitorización de la actividad web por un proveedor de Internet o el empleador.

navegación segura
Protección contra amenazas habituales de malware y phishing mediante la comprobación de cada página web contra una lista de sitios web identificados como tales. Si la página web que está a punto de visitar ha sido identificada como contenedora de contenido malicioso, SeaMonkey evita su carga y muestra en su lugar una advertencia.

no repudio.
Característica del correo electrónico seguro que asegura que el remitente de un mensaje no puede negar la evidencia de que ha sido él quien lo ha enviado. Una firma normal escrita a mano proporciona una forma de no repudio. Una firma digital proporciona otra.

nombre de asunto.
Un DN (nombre distinguido) que describe de manera única el asunto de un certificado.

NTLM (NT LAN Manager)
Un protocolo para la identificación en redes locales que es propietaria de Microsoft Windows. Se usa sobre todo en redes empresariales/institucionales.

OCSP (protocolo de estado del certificado en línea).
Un conjunto de reglas que el administrador de certificados sigue para realizar una comprobación en línea de la validez del certificado cada vez que éste se usa. Este proceso supone comprobar el certificado contra una lista de certificados válidos mantenidos en una página web específica. El ordenador debe estar en línea para que funcione el OCSP.

OPML (lenguaje de marcado para procesadores de esquemas)
Un formato XML usado para listas colecciones de canales. Aunque más genérico en su especificación, hoy en día se usa principalmente para exportar e importar colecciones de canales entre diferentes agregadores o lectores de canales, como SeaMonkey.

página de inicio.
Es la página que se visitará al abrir el navegador o al pulsar en el botón de Inicio. También se usa para referirse a la página principal de un sitio web, a partir de la cual se puede explorar el resto de ese sitio web.

página web.
Un único documento en la World Wide Web que se especifica por una dirección única o URL y que puede contener texto, hiperenlaces y gráficos.

pares de claves duales.
Dos pares de clavespública y privada -cuatro claves en total- que corresponden a dos certificados separados. La clave privada de un par se usa para firmar operaciones, y las claves pública y privada del otro par se usan para operaciones de cifrado y descifrado. Cada par corresponde a un certificado separado. Ver también criptografía con clave pública.

paquete de idioma
Un tipo de complemento que añade un nuevo idioma a la interfaz de usuario de SeaMonkey.

Phishing
Phishing es el término en inglés dado a un modelo de actividad fraudulenta en el cual un tercero crea sitios web falsos, haciéndose pasar por los de entidades bancarias, compañías de tarjetas de crédito y sitios de compra en línea, intentando recopilar información personal de las víctimas que caigan engañados por ellos.

PKCS #11.
El estándar en criptografía de clave pública que gobierna los dispositivos de seguridad como tarjetas inteligentes. Ver también dispositivo de seguridad, tarjeta inteligente.

PKI (infraestructura de clave pública).
Los estándares y servicios que facilitan el uso de criptografía de clave pública y certificados en una red.

plugin.
Un tipo de aplicación auxiliar que añade nuevas funcionalidades al navegador, como poder reproducir audio o vídeo. Al contrario de lo que sucede con otras aplicaciones auxiliares, un plugin se autoinstala en el directorio de plugins en el directorio principal de la instalación y lo normal es que sea el navegador el que lo ejecute internamente. Por ejemplo, un plugin de audio permite escuchar archivos de audio en una página web o en un mensaje de correo electrónico.

POP (protocolo de oficina postal).
Un protocolo estándar en servidores de correo que requiere que se descarguen los mensajes nuevos al disco duro; aunque se puede elegir dejar las copias en el servidor. Con POP, se pueden almacenar todos los mensaje, incluyendo el correo enviado, borradores y carpetas personalizadas, en un ordenador solamente. Por otro lado, IMAP permite almacenar permanentemente todos los mensajes así como los cambios en el servidor, al cual se puede acceder desde cualquier ordenador. La mayoría de los ISPs admiten el uso de POP.

proxy.
Es un programa intermediario que actúa tanto como servidor como cliente, con la finalidad de realizar peticiones en el nombre de otros clientes.

ranura.
Una parte del hardware, o su equivalente en software, controlada por un módulo PKCS #11 y diseñada para contener un dispositivo de seguridad.

rastreo de usuario
Métodos que algunos sitios web, incluyendo anunciantes y servicios de análisis, emplean para determinar patrones de cómo navega usted por la web (p.e., qué sitios web ha visitado, qué preferencias ha hecho públicas al usar botones incrustados por redes sociales y su historial de compras). Esta información se usa principalmente para mostrar ofertas o anuncios de productos o servicios dirigidos. Los mecanismos de rastreo de usuario incluyen cookies y huella del navegador. Vea también Do Not Track.

renovación de certificados.
El proceso de renovar un certificado que está a punto de caducar.

RSS (Sindicación realmente simple)
Un formato de datos XML para feeds web.

servicio de geolocalización

Un servicio web para la navegación basada en ubicación.

servidor.
Es el software (como el que sirve páginas web) que recibe peticiones de un cliente al que le manda la información solicitada, que normalmente se ejecuta en una máquina distinta. Una máquina en la que se ejecuta software de servidor, se le llama servidor.

sitio web.
Un grupo de páginas web relacionadas vinculadas por hiperenlaces y gestionadas por una única compañía, organización, o particular. Un sitio web puede incluir texto, gráficos, ficheros de audio y vídeo, y enlaces a otros sitios web.

spoofing.
Aparentar ser alguien que no se es. Por ejemplo, una persona puede aparentar tener la dirección de correo `jdoe@mozilla.com`, o una máquina puede identificarse como un sitio web llamado `www.mozilla.com` sin serlo en realidad. El spoofing es una forma de identificación falsa.

SMTP (protocolo de transferencia simple de correo).
Un protocolo que envía mensajes de correo electrónico a través de Internet.

SOCKS
Un protocolo que un servidor proxy puede utilizar para aceptar solicitudes de usuarios cliente en una red interna y re-enviarlas a través de Internet.

SSL (capa de conexiones seguras).
Un protocolo que permite una identificación recíproca entre un cliente y un servidor con la finalidad de establecer una conexión comprobada y cifrada. SSL se ejecuta por encima del protocolo TCP/IP y por debajo de HTTP, LDAP, IMAP, NNTP, y otros protocolos de red de alto nivel. El nuevo estándar de la Internet Engineering Task Force (IETF) llamado Transport Layer Security (TLS) está basado en SSL. Ver también cifrado, identificación.

STARTTLS
Una extensión a protocolos estándares TCP comunes (como SMTP, POP o IMAP) de manera que el cliente puede pedir al servidor que use TLS en el mismo puerto TCP que las conexiones no seguras.

tarjeta inteligente.
Un pequeño dispositivo, normalmente de tamaño similar a una tarjeta de crédito, que contiene un microprocesador y puede almacenar información criptográfica como claves y certificados, además de realizar operaciones criptográficas. Las tarjetas inteligentes usan el estándar PKCS #11. Una tarjeta inteligente es una clase de dispositivo de seguridad.

TCP.
Ver TCP/IP (protocolo de control de la transmisión/protocolo de Internet.

TCP/IP (protocolo de control de la transmisión/protocolo de Internet).
Un protocolo de sistemas Unix utilizado para conectar ordenadores independientemente del sistema operativo. TCP/IP es un protocolo esencial de Internet y se ha convertido en un estándar global.

tema
Un tipo de complemento que cambia la apariencia de SeaMonkey.

TLS
Seguridad en la Capa de Transporte (Transport Layer Security, TLS) es el nuevo estándar del Grupo de Trabajo de Ingeniería de Internet (Internet Engineering Task Force, IETF) basado en SSL (Capa de Conexiones Seguras, Secure Sockets Layer). Ver también SSL y cifrado.

token.
Ver dispositivo de seguridad.

***token* de seguridad.**
Ver dispositivo de seguridad.

trust.
Relación de confianza en una persona u otra entidad. En el contexto de la PKI (infraestructura de clave pública), trust se refiere a la relación entre el usuario de un certificado y la autoridad certificadora (CA) que emitió el certificado. Si se usa el administrador de certificados para especificar que se confía en una CA, el administrador de certificados confiará en los certificados válidos emitidos por esa CA a menos que se especifique lo contrario en las opciones de certificados individuales. En la pestaña de autoridades del administrador de certificados se pueden especificar los tipos de certificados de las CAs en que confía o no.

URL (localizador uniforme de recursos).
El formato estándar de direcciones que le dice al navegador cómo localizar un archivo u otro recurso en la Web. Por ejemplo: `http://www.mozilla.org`. Se pueden escribir URLs en la barra de direcciones del navegador para acceder a páginas web. Las URLs también se usan en los enlaces de las páginas para poder ir a otras al pinchar en ellos. También se conoce como dirección de Internet o dirección Web.

verificación de certificados.
Cuando el administrador de certificados verifica un certificado, confirma que la firma digital fue creada por una CA cuyo propio certificado está almacenado en el administrador de certificados y marcado como de confianza para emitir ese tipo de certificados. También confirma que el certificado a verificar no está en los sitios en los que no se confía. Finalmente, si el OCSP (protocolo de estado del certificado en línea) está activado, el administrador de certificados también realiza una comprobación en línea, buscando el certificado en una lista de certificados válidos mantenidos en una URL especificada bien en el propio certificado o bien en las preferencias de validación del navegador. Si cualquiera de estos controles falla, el administrador de certificados marca el certificado como no verificado y no reconocerá la identidad a la que certifica.

World Wide Web.
También conocida como la Web. Una parte de Internet que se refiere al conjunto de páginas web almacenadas en servidores web y mostradas en los clientes llamados navegadores web (como SeaMonkey).

WPAD (autodescubrimiento de proxies web).
Una propuesta de protocolo de Internet que permite a un navegador web localizar automáticamente y conversar con servidores proxy en una red.

XML (lenguaje extensible basado en marcas).
Un estándar abierto para describir datos. A diferencia de HTML, XML permite al desarrollador de una página web definir marcas especiales. Para más información, vea el documento en Internet de W3C Lenguaje Extensible basado en Marcas (XML)  .

XSLT (transformaciones del lenguaje extensible de hojas de estilo).
Un lenguaje usado para convertir un documento XML en otro documento XML o en otro formato.

XUL (Lenguaje de interfaz de usuario XML).
Un lenguaje de marcas XML para crear interfaces de usuario en aplicaciones.