1. Consejos para su seguridad on-line

Lea atentamente estos consejos básicos de seguridad

Seguridad en servicios de banca a distancia

Cuando navegue por Internet y/o reciba correos electrónicos, es conveniente que **no introduzca su DNI, ni sus códigos de acceso a banca a distancia, ni los números secretos para realizar operaciones, ni otros datos sensibles** (como los números y las claves de sus tarjetas de débito y crédito) **en los siguientes casos**:

- En las **páginas a las que haya accedido** a través de un correo electrónico.
- En los **correos electrónicos** que usted envíe. Es conveniente que no lo haga ni siquiera en el caso de que se lo solicite alguien en nombre del Banco.
- **En caso de que dude de la autenticidad** de la página web en la que se encuentra.

Le informamos que **desde Banco Sabadell nunca le pediremos datos confidenciales**, como contraseñas o números secretos, ni por correo electrónico ni por formularios.

No guarde su código de acceso (PIN) **junto a su tarjeta personal de claves** de banca a distancia y evite **el acceso o la visualización** de los mismos **por parte de terceros**.

Para reforzar la protección de su ordenador

- **Aplique y active** la automatización de las **actualizaciones periódicas de seguridad** para el sistema operativo y aplicaciones de su equipo.
- Utilice un **sistema antivirus** incorporando "cortafuegos" (Firewall) y un **sistema "antiespía"** (Spyware) y manténgalos permanentemente actualizados.
- Utilice software, **servicios y sitios** de Internet **de confianza**.
- **Le recomendamos que se abstenga de ejecutar programas que le lleguen por correo electrónico**, aunque su origen parezca conocido, **cuando no esté totalmente seguro de su procedencia**.

Para su mayor seguridad y confianza, **el banco está incorporando** progresivamente **la certificación digital** en sus comunicaciones por correo electrónico.

Para ampliar esta información, puede llamar a nuestro servicio de atención telefónica, **902. 333 880**, o consultar las recomendaciones y la información de seguridad disponible en los distintos **portales del grupo Banco Sabadell**.

2. Seguridad del sistema

En SabadellUrquijo hemos incorporado la tecnología de seguridad más actualizada hasta el momento, así como medidas complementarias.

PROTOCOLO SSL EV DE CIFRADO 128 bits. SERVIDOR SEGURO

Esta tecnología permite que los datos introducidos en pantalla y que viajan a través de la red estén cifrados mediante un algoritmo, con claves variables en cada conexión. Estas claves son realmente el elemento esencial de lo que constituye la seguridad de un "servidor seguro".

SabadellUrquijo está hospedado en un servidor seguro y tiene incorporadas estas claves de 128 bits utilizando la última versión de certificados disponible, denominados certificados de validación extendida o certificados SSL EV. Dichos certificados incorporan mecanismos adicionales de seguridad que incorporan tecnologías de prevención del fraude, informando sobre el nivel de seguridad de la página visitada. Las últimas versiones de los navegadores, como por ejemplo Internet Explorer en su versión 7 o superior, o Firefox a partir de la versión 3, soportan estos tipos de certificados, indicando la autenticidad de la página web visitada, sombreando la barra de direcciones en color verde.

Adicionalmente, junto a la figura del candado de seguridad, se muestra información de la Sociedad Jurídica propietaria de la página web accedida (en nuestro caso Banco de Sabadell S.A.). Pulsando sobre este área se pueden obtener detalles adicionales acerca del certificado utilizado.

Si por el contrario la barra de direcciones aparece sombreada en color rojo, desconfíe de dicha página, ya que ésta podría ser fraudulenta.

Si utiliza versiones de navegadores que no soporten dichas funcionalidades, la barra de direcciones no aparecerá sombreada.

Más información:
http://www.verisign.es/ssl/ssl-information-center/extended-validation-ssl-certificates/index.html

CONTROLES DE LOS CÓDIGOS DE ACCESO

1. El código de acceso que Vd. introduce en SabadellUrquijo , ha de superar una serie de controles: un número máximo de equivocaciones por día, o acumulado de varios días, provocará que el código de acceso se cancele automáticamente. En ese caso, para reactivarla, habrá que solicitarlo por escrito o bien personalmente en su agencia de SabadellUrquijo .
2. Aquellas operaciones que precisan mayor seguridad (transferencias, órdenes de bolsa, etc.) solicitan una segunda clave. Esta segunda clave corresponde a una de las que constan en la tarjeta de claves de BS Online. Esta tarjeta de claves es distinta y personalizada para cada cliente. Cada operación de este tipo le solicita una clave distinta de forma aleatoria. La tarjeta de claves es un elemento absolutamente importante de la seguridad, debe conservarla siempre en su poder y comunicarnos inmediatamente su pérdida o extravío al servicio BS Online 902 323 000
3. En el momento de su conexión a BS Online, se le indica el día y hora de su anterior conexión. Verifique que realmente fue así. Esta facilidad le permite comprobar que sólo Vd. conoce sus claves de seguridad y por tanto sólo Vd. accede al servicio.

LIMITACIÓN DE IMPORTES DE LAS OPERACIONES

En algunas de las operaciones se limita, además, el importe por operación (y su acumulado en un período).

Además, en algunas de ellas, a partir de determinado importe, la oficina tiene conocimiento inmediato de su realización, por lo que de observar algo anormal, realizará las verificaciones que crea convenientes.

CONCLUSIÓN

Los tres elementos citados, cifrado de los mensajes, control de códigos de acceso y limitación de importes, configuran un nivel de seguridad que permite operar con el sistema BS Online con toda confianza.

RECOMENDACIONES

Hasta aquí le hemos comentado las medidas que hemos tomado en nuestro servicio, pero también hay medidas que Vd. debe tomar en su PC, no tanto para proteger la comunicación con el banco, sino para proteger su propio ordenador y la información que contenga. Su PC es el único punto cuya responsabilidad no puede corresponder al Banco sino a Vd. mismo.

1. VIRUS O PROGRAMAS MALICIOSOS. Es bien conocida la posibilidad de que su PC pueda quedar infectado por un virus informático o por un programa malicioso a través de discos, diskettes o simplemente navegando por Internet. DEBE vd. incorporar a su PC un detector de virus que se ejecute cada vez que arranque su ordenador. Además DEBE mantener actualizada la versión del programa antivirus.
2. Debe ser Vd. prudente al visitar webs desconocidas, sobre todo vigilar si le invitan a que descargue de la red ficheros y programas. Un virus o programa malicioso no es más que un programa dedicado a crear problemas en la información almacenada o incluso en el propio PC.
3. Procure no almacenar en su PC programas de los que no conozca su origen.
4. Debe realizar con cierta frecuencia una copia de seguridad (backup) de los archivos de su PC.

3. Medidas de seguridad

Glosario de términos

A continuación encontrará una serie de consejos que le ayudarán a preservar la confidencialidad y seguridad en su navegación por Internet y los Servicios de Banca a Distancia del Banco Sabadell:

1. Desconfíe de aquellos mensajes de correo electrónico que provengan de sitios desconocidos o que contengan información incoherente.
2. Nunca entregue su identificador y contraseña u otros datos personales cuando éstos le sean requeridos por mensajes SMS, fax, un mensaje de correo electrónico, o por un enlace contenido en el mismo, que no apunte a una dirección segura (https:).
3. Recuerde que su código de acceso es personal e intransferible. Se recomienda cambiarlo periódicamente para evitar el acceso por parte de terceros. Además, recuerde memorizarlo y evite su anotación.
4. Guarde con cautela su tarjeta de claves o su Tarjeta de Identificación Digital, sin permitir su acceso a terceros. Estas tarjetas son la llave que permite la realización de operaciones.
5. Evite la visualización o el acceso de su tarjeta de claves por parte de terceros y no realice copias de la misma. Si utiliza una Tarjeta de Identificación Digital, recuerde retirarla del lector cuando haya dejado de utilizarla; asimismo, cambie periódicamente el PIN de su tarjeta, recuerde memorizarlo y evite su anotación.
6. Utilice un sistema antivirus y antispyware, actualizándolo con frecuencia, preferiblemente de forma automática.
7. Actualice su navegador y sistema operativo con las mejoras de seguridad que aportan los fabricantes y siempre siguiendo sus indicaciones.
8. Si dispone de conexión permanente (del tipo ADSL, cable o similar) es conveniente instalar un firewall (cortafuegos) personal.
9. Tome precauciones adicionales cuando utilice ordenadores públicos o compartidos.
10. Si detecta o sospecha algún problema de seguridad, contacte inmediatamente con el Banco.
11. Política de Seguridad
12. Ley y jurisdicción aplicables

Puede contactar con el Banco por motivos de seguridad a través de **diferentes canales**. Si utiliza el formulario electrónico, seleccione como motivo de su comunicación la opción "Seguridad".

1. Desconfíe de aquellos mensajes de correo electrónico que provengan de sitios desconocidos o que contengan información incoherente.

Los mensajes de correo electrónico que provienen de direcciones desconocidas tienen una alta probabilidad de contener virus informáticos o programas maliciosos, especialmente cuando el asunto o tema que observamos antes de abrirlo contiene información incoherente: está escrito en un lenguaje no habitual o no está relacionado con los temas tratados comúnmente con quien lo envía.

Se debe tener en cuenta que, incluso si el remitente del mensaje es conocido, cuando el asunto o tema que visualizamos no es coherente con dicho remitente, el mensaje podría estar siendo enviado por un virus informático o programa malicioso, ya sea desde el ordenador del propio remitente o desde otro ordenador infectado conocedor de su dirección de correo electrónico.

2. Nunca entregue su identificador y contraseña u otros datos personales cuando éstos le sean requeridos por mensajes SMS, fax, por un mensaje de correo electrónico, o por un enlace contenido en el mismo, que no apunte a una dirección segura (https:).

   Banco Sabadell no le solicitará, mediante mensajes SMS, fax, correo electrónico o formularios datos confidenciales o personales como claves, números de cuentas, de tarjetas, etc.

   Banco Sabadell únicamente le dirigirá a sus portales a través de páginas seguras (https:), que le mostrarán un candado cerrado en su navegador. Haciendo "doble-clic" sobre dicho elemento, usted podrá visualizar un certificado digital expedido por una tercera empresa de confianza (Verisign) y así comprobar que la identidad existente en dicho certificado pertenece a Banco Sabadell (Organization = BANCO SABADELL).

   Compruebe que, al entrar en el servicio de Banca Electrónica, éste le indica correctamente su nombre y apellidos y la última fecha y hora de conexión.

3. Recuerde que su código de acceso es personal e intransferible. Se recomienda cambiarlo periódicamente para evitar el acceso por parte de terceros. Además, recuerde memorizarlo y evite su anotación.

   Como medida adicional, deberá abstenerse de escoger un número relacionado con sus datos personales, así como cualquier otro código que pueda resultar fácilmente predecible por terceras personas (fecha de nacimiento, teléfono, series de números consecutivos, repeticiones de la misma cifra, etc.). Deberá abstenerse asimismo de anotar dichos códigos o claves en cualquier soporte físico, y en todo caso junto a elementos de identificación complementarios (tarjetas).

4. Guarde con cautela su tarjeta de claves o su Tarjeta de Identificación Digital, sin permitir su acceso a terceros. Estas tarjetas son la llave que permite la realización de operaciones.

5. Evite la visualización o el acceso de su tarjeta de claves por parte de terceros y no realice copias de la misma. Si utiliza una Tarjeta de Identificación Digital, recuerde retirarla del lector cuando haya dejado de utilizarla; asimismo, cambie periódicamente el PIN de su tarjeta, recuerde memorizarlo y evite su anotación.

   Compruebe si la fecha y hora del último acceso que se le informa al entrar en los servicios de Banca a Distancia coincide realmente con la última vez que los utilizó.

   Recuerde que si usted está dado/a de alta en algún servicio agregador de cuentas de otra entidad, dicho servicio puede realizar periódicamente accesos a los servicios de Banca a Distancia que usted le haya indicado, quedando reflejada la fecha y hora del último acceso realizado de esta forma.

   Si usted sospecha que la fecha y hora del último acceso no coincide con un acceso efectuado por usted o por el servicio agregador de otra entidad en la que esté dado/a de alta, notifique inmediatamente al Banco dicha situación.

6. Utilice un sistema antivirus y antispyware, actualizándolo con frecuencia, preferiblemente de forma automática.

   La proliferación de virus informáticos es cada día más común. Asegúrese de disponer de un buen sistema antivirus y, lo más importante, de mantener permanentemente actualizadas sus tablas de detección de virus. Disponer de un sistema antivirus le puede servir de poco si el mismo no dispone de las últimas tablas de detección para los virus más recientes.

   Adicionalmente, no instale software de fuentes desconocidas ni navegue por sitios que le inspiren poca confianza.

   Igualmente, es conveniente disponer de protección contra el "Spyware". Puede utilizar un programa antivirus que también le proteja contra el "Spyware" o utilizar un programa específico para "Spyware".

7. Actualice su navegador y sistema operativo con las mejoras de seguridad que aportan los fabricantes y siempre siguiendo sus indicaciones.

   Periódicamente, van apareciendo mejoras y nuevas versiones de los navegadores y del sistema operativo que aportan mayor seguridad a la navegación y al uso de Internet.

   Lea las recomendaciones de los fabricantes de dichos productos y actualice su navegador y el sistema operativo según sus instrucciones.

8. Si dispone de conexión permanente (del tipo ADSL, cable o similar) es conveniente instalar un firewall (cortafuegos) personal.

   Mientras su ordenador permanece conectado a Internet, él mismo se puede comunicar con cualquier usuario de dicha red. Para evitar un posible acceso a información ubicada en su ordenador, se recomienda la instalación de un firewall (cortafuegos) personal, en especial, si usted utiliza una conexión permanente (ADSL, cable o similar).

9. Tome precauciones adicionales cuando utilice ordenadores públicos o compartidos.

   Utilice ordenadores públicos solamente para consultas que no tengan un carácter privado. Recuerde que puede ser observado por terceras personas o, incluso, por medios electrónicos de vigilancia.

10. Si detecta o sospecha algún problema de seguridad, contacte inmediatamente con el Banco.

    Puede contactar con el Banco a través de **diferentes canales**. Si utiliza el formulario, seleccione como motivo de su comunicación la opción "SEGURIDAD".

11. Política de Seguridad

    SabadellUrquijo ha incorporado la tecnología de seguridad más avanzada hasta el momento, así como una serie de medidas complementarias para asegurar la confidencialidad en las transacciones. A tales efectos el Usuario deberá cumplir las condiciones siguientes:

    En general: el Usuario deberá disponer de los dispositivos y elementos que en cada momento se determinen como "requerimientos del sistema" en las páginas del Portal y, por razones de seguridad, deberá disponer de las versiones más modernas de navegación. Se advierte expresamente al Usuario que éste no deberá abandonar su ordenador cuando esté operando a través del Portal.

    Banco de Sabadell, S.A. se reserva el derecho de adoptar todas las normas y medidas de seguridad que en cada momento considere oportunas a fin de garantizar el buen uso y confidencialidad del servicio. El Usuario autoriza a Banco de Sabadell, S.A. para no ejecutar las solicitudes u órdenes recibidas cuando la identificación no sea correcta o tenga dudas razonables sobre la identidad de la persona que las emite.

    El Usuario autoriza irrevocablemente a Banco de Sabadell, S.A. para el registro y archivo de las comunicaciones y transacciones que se produzcan a través del Portal.

    Es bien conocida la posibilidad de que un PC pueda quedar infectado por un virus informático a través de disquetes o simplemente navegando por Internet. El Usuario deberá incorporar a su PC un detector de virus que se ejecute cada vez que arranque su ordenador, el cual deberá mantenerse permanentemente actualizado, debiendo además efectuar con frecuencia copias de seguridad ("backup") en relación con los archivos contenidos en el ordenador del Usuario. Banco de Sabadell, S.A. no garantiza ni controla la ausencia de virus ni de otros elementos en los servicios prestados por terceros a través del Portal (ficheros; correos; documentos electrónicos; etc.), ni tampoco puede garantizar ni se responsabiliza de las alteraciones o defectos que puedan producirse en el sistema informático del Usuario por causa de cualquier virus informático o elemento lesivo que haya afectado o se haya transmitido por tercero a través del Portal. El Usuario debe ser prudente al visitar webs desconocidas, sobre todo vigilar si le invitan a que descargue de la red ficheros y programas. Un virus no es más que un programa dedicado a crear problemas en la información almacenada o incluso en el propio PC. El Usuario procurará no almacenar en su PC programas de los que no conozca su origen.

    BS Online: los Usuarios que sean además clientes del servicio BS Online deberán adoptar las medidas necesarias al objeto de custodiar debidamente los elementos de identificación personal propios del servicio y recurrir inmediatamente a los sistemas de suspensión o bloqueo de los servicios previstos al efecto. Asimismo se recomienda no teclear o utilizar dichos elementos de identificación en ordenadores que se hallen en lugares públicos o emplazamientos que puedan facilitar la intervención de las comunicaciones o visualización de las claves por parte de terceros. Tampoco deberán anotarse el número secreto o códigos de acceso en ninguno de los documentos u objetos que el Usuario guarde o lleve consigo o junto a tarjetas de identificación digital, advirtiéndose en forma expresa que, en caso de elección o modificación voluntaria de claves, no resulta conveniente escoger un número de clave relacionado con los datos personales, al ser fácilmente deducidos o previstos (fecha de nacimiento, teléfono o similares).

12. Ley y jurisdicción aplicables

    Las presentes condiciones generales se rigen por el ordenamiento jurídico español, sometiéndose las partes para cualquier controversia que se suscite en relación al portal a los Juzgados y Tribunales correspondientes al domicilio de Banco de Sabadell, S.A.

4. Prevenciones

Virus informáticos y programas malignos

Los virus y programas malignos son pequeños programas que se instalan en el ordenador, sin conocimiento del usuario, y que tienen fines maliciosos como, por ejemplo, destruir o robar información o provocar disfunciones en el equipo o la red a la que se conecta.

Un virus, además de actuar en la máquina afectada, se propaga a otros ordenadores con los que dicha máquina pueda tener relación o conexión, utilizando para ello formas muy variadas que han ido evolucionando con el tiempo. Años atrás, los virus se propagaban principalmente a través de disquetes. Con la aparición de las redes, Internet y el correo electrónico, los virus han encontrado su forma de propagación idónea aunque los soportes de información continúan siendo un medio utilizado.

Diariamente aparecen nuevos virus en Internet aunque no todos tienen el mismo peligro.

Para evitar ser contagiado (afectado), se deben tomar una serie de precauciones:

- Navegar únicamente por sitios conocidos de los que tengamos referencias y que nos inspiren confianza, puesto que algunos virus y programas maliciosos se encuentran ocultos en páginas de Internet de dudosa confianza.
- No utilizar ficheros o programas de los que se desconoce el origen.
- No abrir mensajes de correo electrónico de origen desconocido.
- Ser precavidos con mensajes de correo electrónico que provengan de personas conocidas y que tengan un título sin sentido o inesperado. Antes de abrir estos mensajes contactar con el presunto emisor y constatar que realmente él ha enviado dicho mensaje ya que podría tratarse de un mensaje enviado por un virus.
- Disponer de un programa antivirus reconocido y mantener permanentemente actualizadas sus tablas de detección de virus. No es suficiente con disponer de la última versión del programa antivirus. Para que este sea efectivo con los últimos virus aparecidos, deberemos mantener actualizadas sus tablas.
- No abrir directamente los ficheros anexos en mensajes de correo. Es más seguro guardarlos primero en el ordenador y abrirlos desde fuera del programa de correo electrónico.

Los usuarios expertos deberían proteger la información confidencial mediante programas de cifrado.

Enlaces de interés sobre virus

A continuación le facilitamos a efectos meramente informativos los siguientes enlaces:

Alertas

http://www.alerta-antivirus.es/
http://www.hispasec.com/
http://www.virusprot.com/

Fabricantes

http://www.trendmicro.es/
http://www.mcafee.com/ (INGLÉS)
http://www.pandasoftware.es/
http://www.symantec.com/ (INGLÉS)
http://www.avp-es.com/
http://www.norton.com/ (INGLÉS)
http://esp.sophos.com/

Enlaces de interés sobre "Spyware"

http://lavasoft.de/spanish/default.shtml
http://microsoft,com/athome/security/spyware/software/default.mspx (INGLÉS)
http://ca.com/products/pestpatrol/ (INGLÉS)
http://www.webroot.com/es/index.php

Enlaces de interés sobre cifrado

http://www.pgp.com/products/personal/index.html (INGLÉS)
http://www.pgpi.org/ (INGLÉS)

Intento de robo de códigos de acceso u otra información confidencial ("Phishing")

Uno de los fraudes existentes en Internet consiste en la creación de páginas y/o portales falsos y la falsificación del origen de mensajes de correo electrónico.

Combinadas estas dos técnicas, se utilizan para la captación fraudulenta de códigos de acceso a servicios y aplicaciones de terceros, u otra información confidencial como números de cuentas y de tarjetas (incluyendo la fecha de caducidad), con la finalidad de acceder a su información o realizar operaciones en su nombre.

La forma de realizar el robo de códigos de acceso mediante esta técnica consiste en crear una dirección y páginas en Internet cuyo nombre es prácticamente idéntico al de la empresa o portal que se intenta suplantar. El nombre difiere en unos pocos caracteres, muchas veces en uno sólo. En la dirección fraudulenta se han creado páginas que pueden ser idénticas o muy parecidas a las verdaderas.

Las víctimas del fraude reciben correos electrónicos supuestamente enviados por la empresa real (en este caso, la dirección de correo que los emite es imitada totalmente), en los que se les invita, argumentando algún motivo de interés, a dirigirse a las páginas fraudulentas, en las cuales se les pide su identificación, contraseña u otros datos de acceso. Si se introduce dicha información en las páginas fraudulentas, ésta habrá sido robada y con ella se podrá acceder al sitio real realizando las funciones u operaciones que la información robada permita.

Algunas variantes de la técnica anterior consisten en solicitar la misma información mediante mensajes SMS, fax o teléfono.

¿Cómo prevenirse?

Siga las instrucciones anteriores y los comunicados e información de seguridad que Banco Sabadell le ofrece. Contacte con el Banco ante cualquier duda al respecto. Puede contactar a través de **diferentes canales**. Si utiliza el formulario electrónico, seleccione como motivo de su comunicación la opción "Seguridad".

Enlaces de interés sobre intentos de robo de códigos de acceso e información confidencial ("Phishing").

A continuación le facilitamos a efectos meramente informativos los siguientes enlaces:

http://www.msn.es/security/phishing/
http://es.wikipedia.org/wiki/Phishing
http://www.consumer.gov/idtheft/ (INGLÉS)

5. Protecciones

Las protecciones que se describen a continuación son complementarias entre ellas y ninguna substituye a las demás.

Certificado digital

Un certificado digital es una garantía sobre la identidad de un determinado servidor y páginas asociadas que prestan un servicio en el mundo electrónico (principalmente Internet).

El certificado digital es emitido por una empresa de confianza (Prestador de Servicios de Certificación), como Verisign o la FNMT (Fábrica Nacional de Moneda y Timbre), que después de verificar exhaustivamente la identidad del solicitante, le asigna dicho certificado mediante la creación del mismo.

El certificado digital contiene los datos correspondientes a la dirección a certificar (ej.: www.sabadellurquijo.com), la identidad de quien opera en dicha dirección, la fecha de caducidad del certificado y otra información de carácter técnico. El certificado digital, a su vez, está firmado digitalmente por el Prestador de Servicios de Certificación.

La confianza de un certificado digital vendrá dada, por tanto, además de por la información contenida en el mismo, por la confianza que nos merezca el Prestador de Servicios de Certificación que lo ha emitido y firmado. Los Prestadores de Servicios de Certificación muestran públicamente los procesos utilizados para realizar la

certificación: son las llamadas Políticas y Prácticas de Certificación. De esta forma, podemos evaluar la confianza que un determinado Prestador de Servicios de Certificación nos merece.

¿Cómo validar las páginas de un servicio en Internet?

Un certificado digital se nos puede mostrar en diferentes situaciones. La más común es la de verificar que las páginas de un determinado servicio en Internet pertenecen a quien deberían y no a un impostor que las ha copiado. De esta forma, nos aseguramos que la información personal y confidencial que entreguemos será recibida por la identidad adecuada.

Es recomendable no facilitar nunca datos confidenciales a partir de páginas activadas a partir de un enlace contenido en un correo electrónico. Le recomendamos que acceda a las páginas de nuestras webs siempre a través de las direcciones Internet comunicadas por el Banco.

Pasos para validar las páginas de un servicio en Internet (páginas seguras):

1. Compruebe que la dirección (url) de las páginas comienza con el prefijo https y que su navegador muestra el icono con un candado cerrado en el lado inferior derecho de su ventana (en Internet Explorer, en Netscape Navigator).
2. Pulse sobre el candado (doble clic en Internet Explorer y un clic en Netscape Navigator) para ver el certificado digital y comprobar la identidad de quien está mostrando las páginas que van a recoger su información:
   a. En Internet Explorer:

      Comprobar la dirección (URL), el emisor del certificado y la validez del mismo.

      A continuación, seleccionar la pestaña "Detalles" para poder comprobar la identidad de quien presenta las páginas web en las que visualizamos e introducimos nuestra información.

      En la ventana superior que aparezca, seleccionaremos el campo "Asunto". En ese momento, podremos visualizar la información correspondiente en la ventana inferior. En el caso de las empresas de Banco Sabadell, el campo O (Organization) deberá contener la información "BANCO SABADELL" y, como información complementaria, los campos L, S y C son Sabadell, Barcelona y ES, respectivamente.

   b. En Netscape Navigator:

      Pulsar en el botón "Ver" en la anterior ventana.

      Esta acción hará que aparezca una nueva ventana con la información sobre el certificado digital:

      Comprobar en la misma la dirección (URL) de las páginas con las que se está tratando, el emisor del certificado y la validez del mismo.

      En el caso de las empresas de Banco Sabadell, el campo O (Organization) deberá contener la información "BANCO SABADELL".

   c. En otros navegadores:

      La forma de mostrar el certificado en otros navegadores es similar. Recuerde comprobar que el campo O (Organización) tiene como valor la identidad de quien espera (en el caso de las empresas de Banco Sabadell, O = BANCO SABADELL).

Cifrado de datos

Adicionalmente, al utilizar páginas seguras (páginas protegidas mediante un certificado digital), toda la información transmitida entre su navegador y el servidor que aloja dichas páginas se transmite de forma cifrada. Así, dicha información permanece inmune a la interceptación por terceros.

Para conseguir la máxima protección de cifrado en las comunicaciones con páginas seguras (protección necesaria para el uso de servicios financieros y cualquier otro tipo de información confidencial), es necesario utilizar un navegador que proporcione cifrado fuerte (cifrado de 128 bits).

Políticas y Prácticas de Certificación

Mediante las políticas y prácticas de certificación los Prestadores de Servicios de Certificación muestran al público, de manera abierta, los mecanismos y pasos (comprobaciones de identidad) que utilizan para expedir los certificados digitales a quienes los solicitan. De esta forma, quien vaya a verificar un certificado podrá confiar en mayor o menor medida en los certificados emitidos por dicho prestador.

En la práctica, dado que las políticas y prácticas son documentos extensos, se confía en uno u otro prestador de servicios de certificación según el grado de conocimiento que previamente se tenga de él, siendo Verisign el más conocido a nivel mundial para la certificación de páginas de servicios en portales y servidores.

Políticas de Certificación (CP).

Las políticas indican qué realizan los prestadores de servicios de certificación y los tipos de servicios y certificados que realizan.

En el enlace siguiente, se muestran las políticas de certificación (CP o Certificate Policies) de Verisign, líder mundial en servicios de certificación https://www.verisign.com/repository/vtnCp.html (INGLÉS).

Prácticas de Certificación (CPS)

Las prácticas de certificación detallan cómo se garantizan las políticas, es decir, qué procedimientos y mecanismos concretos se utilizan para la emisión de certificados digitales.

En el enlace siguiente, se muestran las prácticas de certificación (CPS o Certification Practice Statements) de Verisign, líder mundial en servicios de certificación:

http://www.verisign.com/repository/CPS/ (INGLÉS).

Enlaces de interés sobre certificados digitales y Prestadores de Servicios de Certificación:

Verisign (INGLÉS)
ACE
Thawte (INGLÉS)
Camerfirma

Cortafuegos ("Firewall") personal

Un cortafuegos o "Firewall" personal es un programa que bloquea al acceso no autorizado desde Internet hasta nuestro ordenador y también el acceso incontrolado (producido por algún nuevo virus, programa o código maligno) desde nuestro ordenador hacia Internet.

Hoy en día, podemos encontrar cortafuegos en programas separados o integrados dentro de otros programas de seguridad (como antivirus) o en los propios sistemas operativos (como Windows XP).

Se llama cortafuegos personal para distinguirlo de los cortafuegos perimetrales, que habitualmente realizan esta función para la protección de todo un grupo de ordenadores en red frente a la conexión a otra red desconocida (habitualmente Internet u otra red de terceros).

Mediante el uso de un cortafuegos personal podremos controlar las conexiones que se realizan con Internet u otras redes desde y hacia todos los programas existentes en nuestro ordenador. Cuando el cortafuegos se instala, todas las conexiones están prohibidas y se deberán autorizar expresamente aquellas que sean habituales según el uso que hagamos de nuestro ordenador. Cuando el cortafuegos nos avise del intento de inicio de una conexión que no ha sido expresamente autorizada, deberemos indicarle si la queremos autorizar o no, dependiendo de si dicha conexión está relacionada con el uso que estemos realizando en ese momento del ordenador o, por el contrario, la conexión se produce debida a un agente externo (intento de acceso desde Internet, virus o similar). El cortafuegos personal es un programa pensado para usuarios ya iniciados en el uso de Internet.

También es conveniente actualizar periódicamente la versión de nuestro cortafuegos, según las recomendaciones del fabricante correspondiente.

Enlaces de interés sobre cortafuegos.

A continuación le facilitamos a efectos meramente informativos los siguientes enlaces:

http://www.pc-actual.com/Actualidad/Reportajes/Seguridad/Virus/20030130012/6
http://www.zonealarm.com
http://www.symantec.com/region/mx/product/consumer/npf/
http://www.protegerse.com/outpost/

6. Buenas prácticas

Actualizaciones de seguridad del navegador y sistema operativo

Para prevenir posibles problemas de seguridad derivados de las vulnerabilidades que se descubren ocasionalmente en el software utilizado, es conveniente visitar las páginas de seguridad de los fabricantes de los programas que utilizamos, en especial el navegador y el propio sistema operativo.

Navegador.

El navegador, como principal herramienta de acceso a Internet, es el principal programa que debe mantenerse actualizado con las últimas recomendaciones de seguridad.

Utilice cifrado fuerte (cifrado de 128 bits) para las comunicaciones con páginas seguras (https).

Visite periódicamente las páginas en Internet del fabricante de su navegador y actualícelo según las recomendaciones de seguridad que en ellas aparezcan.

Enlaces de interés sobre nuevas versiones y actualizaciones de seguridad para el navegador.

A continuación le facilitamos a efectos meramente informativos los siguientes enlaces:

http://windowsupdate.microsoft.com
http://www.microsoft.com/downloads/search.aspx?langid=18&displaylang=es
http://wp.netscape.com/es/es/index.html
http://wp.netscape.com/security/index.html (INGLÉS)
http://www.netscape.com/download (INGLÉS)

Sistema operativo.

Algunos sistemas operativos, como Windows con su funcionalidad Windows Update, tienen utilidades para verificar la existencia de actualizaciones del sistema operativo, incluyendo actualizaciones de seguridad.

Haga uso de dichas utilidades o visite periódicamente las páginas en Internet del fabricante de su sistema operativo y actualice el mismo según las recomendaciones de seguridad que en ellas aparezcan.

Enlaces de interés sobre actualizaciones de seguridad para el sistema operativo.

A continuación le facilitamos a efectos meramente informativos los siguientes enlaces:

http://windowsupdate.microsoft.com
http://www.microsoft.com/spain/technet/seguridad/default.asp
http://www.microsoft.com/security/ (INGLÉS)

Uso de cifrado fuerte (cifrado de 128 bits) en comunicación con páginas seguras

El cifrado fuerte (implantado mediante el uso de claves de cifrado de 128 bits) se consigue mediante el uso combinado de software específico en los servidores que muestran las páginas seguras y el uso de navegadores capacitados para usar dicho cifrado.

Debido a su potencia, su uso acostumbra a estar autorizado únicamente a servidores de páginas pertenecientes a entidades financieras y otras empresas con requerimientos de seguridad similares. En cambio, es de libre utilización para cualquier navegador.

Por ello, los servicios de banca a distancia de las entidades financieras están habitualmente capacitados para utilizar cifrado fuerte. El uso de cifrado fuerte en las comunicaciones con estos servicios depende entonces de que el navegador tenga la capacidad de cifrado fuerte.

Compruebe que utiliza una versión de su navegador preferido con capacidades de cifrado fuerte (128 bits). Si no es el caso, actualice su navegador a una versión que permita cifrado fuerte.

¿Cómo saber si un servidor permite el cifrado fuerte (128 bits)?

Normalmente, un servidor que utilice cifrado fuerte lo anunciará en sus páginas, habitualmente en un apartado específico de seguridad. Si no es el caso, deberá disponer de un navegador con cifrado fuerte para averiguar el tipo de cifrado que utiliza un servidor determinado.

¿Cómo saber si estoy utilizando comunicaciones con cifrado fuerte (128 bits)?

Para saber si estamos intercambiando la información mediante cifrado fuerte primero deberemos observar que el candado existente en el extremo inferior derecho de la ventana de nuestro navegador esté cerrado. Una vez hecho esto:

- En Internet Explorer colocar, moviendo el ratón, el apuntador sobre dicho candado y dejarlo encima unos instantes hasta que aparezca la longitud de la clave de cifrado, que deberá ser 128 bits.
- En Netscape Navigator, pulsar una vez sobre el candado cerrado. Se nos abrirá una ventana que nos indicará el tipo de cifrado, que deberá ser de 128 bits (cifrado de grado alto).

Si usted dispone de un navegador habilitado para el uso de cifrado fuerte podrá igualmente comunicarse de forma segura con servidores que no dispongan de esta característica. En ese caso, de forma automática se utilizará para la comunicación el tipo de cifrado más alto que soporte el servidor y como longitud de clave de cifrado aparecerá un valor inferior a 128 (normalmente 40 o 56 bits).

¿Cómo actualizar mi navegador para que utilice cifrado fuerte (128 bits)?

Diríjase a las páginas de descarga y actualizaciones del fabricante de su navegador preferido y busque las versiones o actualizaciones de 128 bits para su navegador. Recuerde que sólo podrá comunicarse mediante cifrado fuerte con aquellos servidores que dispongan de dicha característica.

Enlaces de interés sobre cifrado de 128 bits

A continuación le facilitamos a efectos meramente informativos los siguientes enlaces:

http://www.microsoft.com/windows/ie_intl/es/download/128bit/intro.asp
http://www.aola.com/netscape/download/

Copias de seguridad

Con el objetivo de poder recuperar la información disponible en el ordenador con anterioridad a la existencia de algún problema en el mismo, debemos realizar copias de seguridad y mantenerlas siempre actualizadas.

Un aspecto importante para poder conseguir la recuperación de las copias de seguridad es el lugar donde éstas se guarden. Las copias deberán custodiarse en un lugar separado del equipo que contiene los datos originales para que, en caso de incidente con el mismo, no se pierdan también las copias. Esto es especialmente importante en el caso de un ordenador portátil, situación en la que no es nada recomendable guardar las copias en la misma funda o maleta que el portátil.

Las copias de seguridad se realizan sobre soportes de información llamados "removibles", que tienen la característica de poderse extraer del ordenador que contiene los datos originales. Estos soportes "removibles" pueden ser disquetes, CDs o DVDs gravables, unidades de cinta, unidades ZIP, dispositivos conectables por puerto USB (Universal Serial Bus) como discos externos, memorias persistentes, etc.

Enlaces de interés sobre copias de seguridad

A continuación le facilitamos a efectos meramente informativos los siguientes enlaces:

http://www.conozcasuhardware.com/quees/almacen4.htm#backups
http://www.iomega-europe.com/eu/en/products/products_en.aspx (INGLÉS)
http://www.pricingcentral.com/best/backup_utility_software.html (INGLÉS)

7. Firma electrónica

Banco Sabadell ha iniciado el uso de la firma electrónica en sus envíos de correo electrónico.

La firma electrónica de los correos garantiza la identidad del emisor, que ha recibido la validación de su dirección de correo electrónico mediante la firma electrónica de Verisign, autoridad de certificación digital reconocida mundialmente, y que, al mismo tiempo, garantiza técnicamente que el contenido del mensaje no ha sido alterado en tránsito por terceros.

Adicionalmente, para una mayor facilidad y confianza en la identificación del emisor, en cada mensaje de correo electrónico emitido se incluye al pie una imagen aleatoria asociada al destinatario, con un número que se incrementa en cada envío y que ayuda a identificar rápidamente el origen del mensaje.

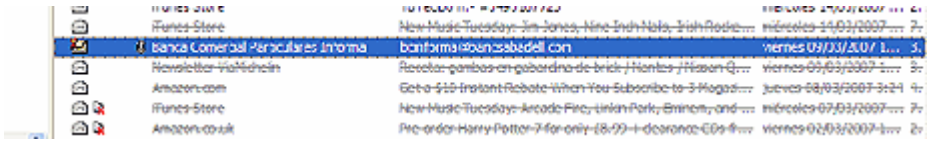
La imagen siempre es la misma para un determinado emisor y destinatario, mientras que el número se incrementa con cada envío.

Ejemplo de correo firmado electrónicamente

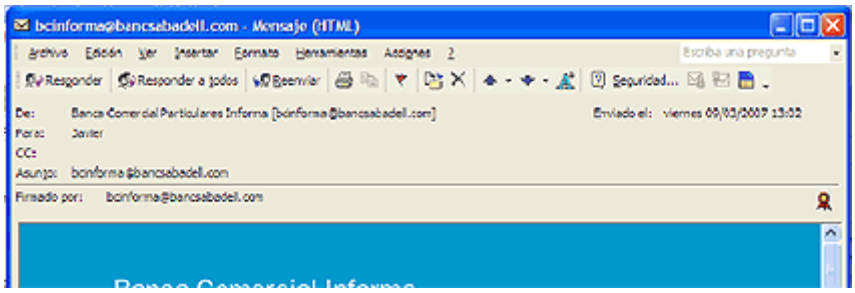
A continuación, se puede ver cómo distinguir un correo firmado electrónicamente en la «bandeja de entrada». El correo se muestra con un icono que lo diferencia como un correo firmado electrónicamente:

En el programa de correo Microsoft Outlook:

- Al abrir la «bandeja de entrada», observamos un icono diferenciado para los mensajes firmados electrónicamente:

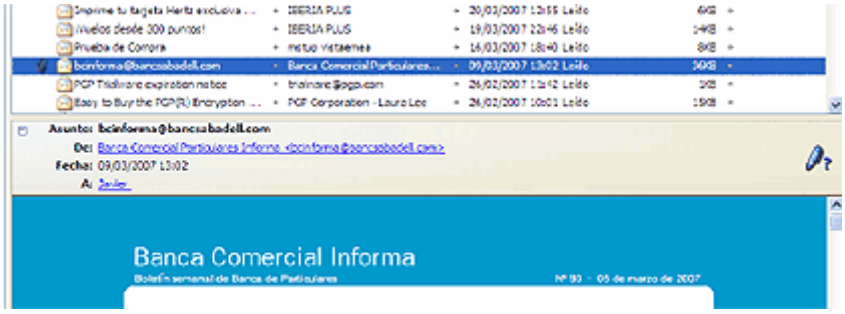


- Al pulsar "doble-clic" sobre el mensaje, también observamos que el mensaje tiene en su parte derecha un icono correspondiente a la firma electrónica:



En el programa de correo Thunderbird:

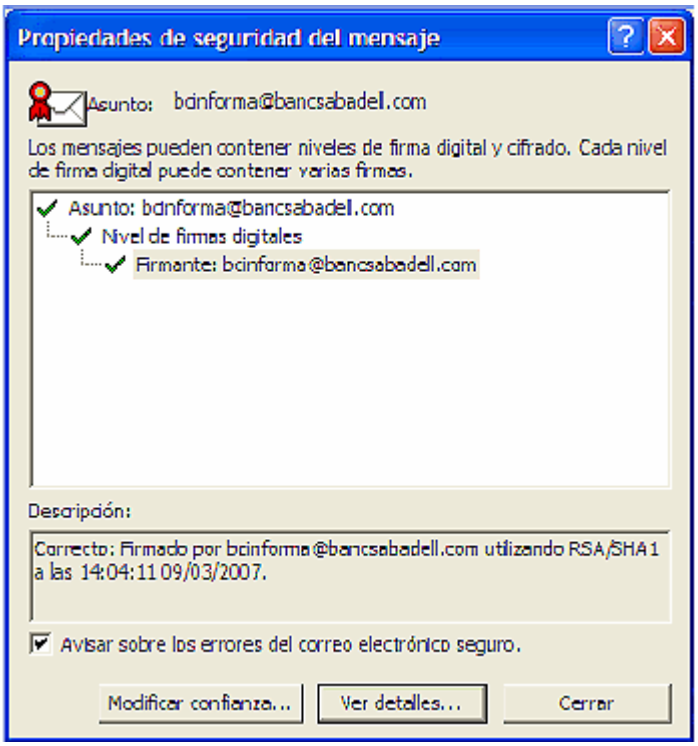
- Al seleccionar el mensaje, observamos que éste muestra en su parte derecha un icono diferenciado que indica que el mensaje está firmado electrónicamente:



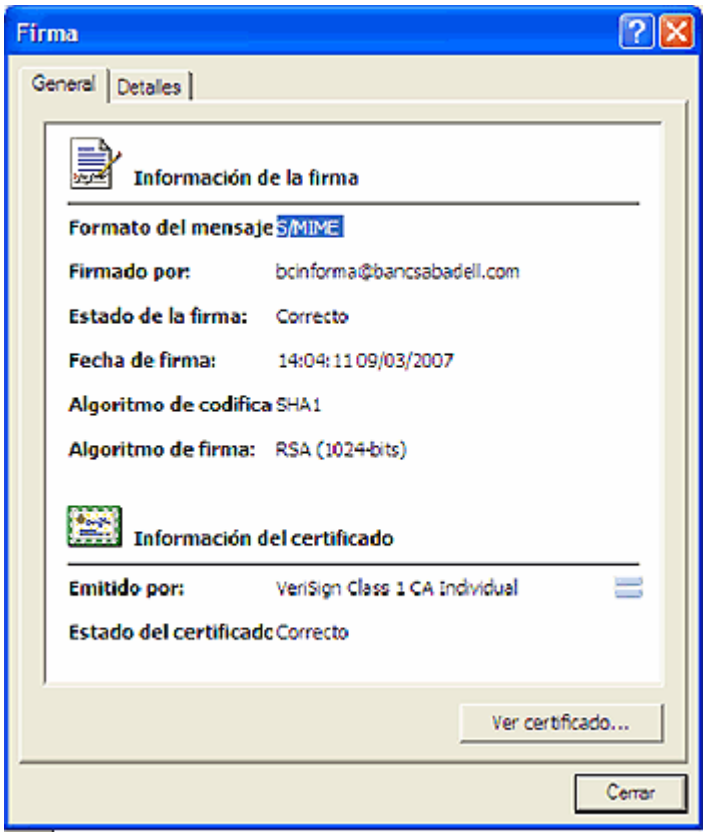
Si pulsamos doble clic sobre el icono anterior ubicado en la parte derecha del mensaje, en ambos sistemas de correo obtendremos información sobre la firma electrónica y sobre el certificado emitido por Verisign:

En el programa de correo Microsoft Outlook:

Aparecerá la siguiente ventana:



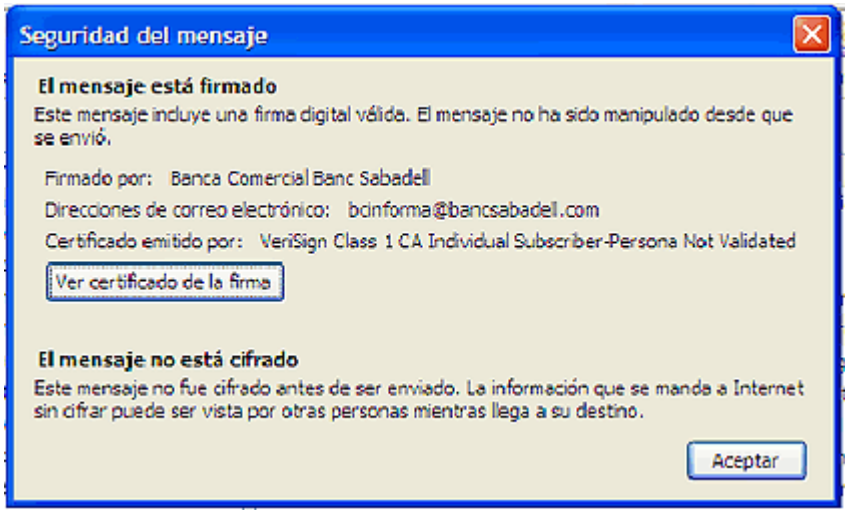
Pulsando el botón para obtener más detalles, nos aparecerá la ventana siguiente, en la que pulsando el botón para ver el certificado, podremos obtener los detalles del mismo en una nueva ventana:



Donde finalmente, después de pulsar sobre la pestaña «Detalles» y sobre la línea «Asunto», podremos observar todos los detalles correspondientes al certificado obtenido de Verisign, acreditando así la autenticidad del emisor (dirección emisora del correo electrónico, conteniendo el sufijo «@bancsabadell.com», y el resto de información del emisor y de Verisign).

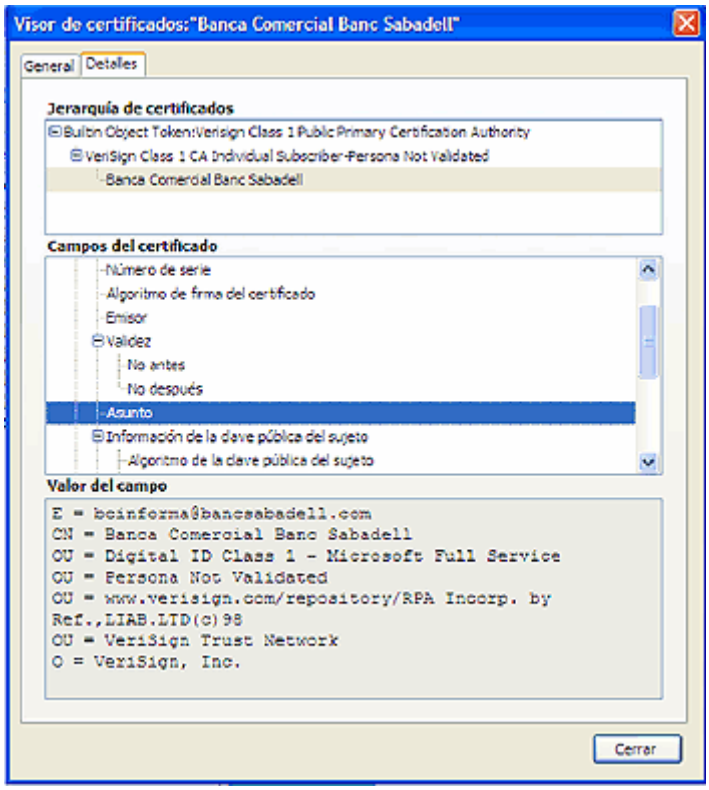
En el programa de correo Thunderbird:

Aparecerá la ventana siguiente:



Indica que el mensaje está firmado electrónicamente, con una firma válida, quién lo ha firmado (dirección emisora del correo electrónico, conteniendo el sufijo «@bancsabadell.com») y el resto de información del certificador Verisign.

Si pulsamos el botón para ver el certificado de la firma electrónica, podremos ver sus detalles en una nueva ventana.



Donde, finalmente, después de pulsar en la pestaña "Detalles" y sobre la línea «Asunto», podremos observar todos los detalles correspondientes al certificado obtenido de Verisign, acreditando la autenticidad del emisor (dirección

emisora del correo electrónico, conteniendo el sufijo «@bancsabadell.com», y el resto de información del emisor y de Verisign).

En otros programas de correo:

En otros programas de correo, la forma de reconocer la autenticidad de los mensajes firmados electrónicamente es similar.

La mayoría de los sistemas de correo que no necesitan de un programa de correo para ser accedidos, sino que se acceden con un navegador web (sistemas de correo del tipo «webmail»), no disponen de las facilidades anteriores para reconocer los correos firmados. En este tipo de sistemas de correo podemos ayudarnos de la medida adicional que se explica a continuación para validar mejor al emisor de un correo, aunque este mecanismo para reconocer al emisor del correo electrónico no es tan seguro como el anterior

Medida adicional de confianza:

Como medida adicional de confianza, para facilitar el reconocimiento de los mensajes firmados electrónicamente por las sociedades del grupo, al pie del mensaje firmado encontraremos una imagen, escogida aleatoriamente en función de la dirección del destinatario, de forma que cada destinatario recibe una imagen diferente, que siempre será la misma mientras no cambie su dirección de correo electrónico de destino. Sobre esta imagen aparece un número secuencial, que se incrementará con cada envío que se reciba en la misma dirección de destino.

De esta forma, un destinatario siempre recibirá la misma imagen añadida al pie del mensaje firmado y, sobrepuesto, un número que se incrementará en cada envío.

Al lado de la imagen y el número secuencial figuran los datos correspondientes al certificado digital emitido por Verisign que se ha utilizado para firmar electrónicamente el mensaje.

Ejemplo de pie de mensaje: