

MEDIDAS DE SEGURIDAD PARA TRANSACCIONES ONLINE

Utilizar Internet para realizar transacciones económicas – tanto gestiones bancarias como pagos de comercio electrónico – es algo muy habitual tanto en la actividad empresarial como en la de los ciudadanos en su faceta de consumidores. Por ello, es fundamental seguir una serie de buenas prácticas y medidas para garantizar que todo el proceso se realice con seguridad, reforzando nuestra confianza como usuarios de estos servicios.

Este artículo se divide en tres apartados: medidas de autenticación (para legitimar la identidad), medidas de seguridad durante el proceso, y buenas prácticas en general, que incluyen consejos para hacer que los pagos online y operaciones bancarias se realicen de forma segura.

I Medidas de autenticación

La autenticación es el proceso mediante el cual se confirma que quien se conecta y solicita acceso a un servicio es realmente quien dice ser, es decir, el legítimo usuario. Los siguientes elementos son los principales encargados de autenticar el proceso desde su inicio (tras la conexión con el servidor destino).

La elección de unos u otros dependerá siempre de la infraestructura proporcionada por el comercio o banco online y las posibilidades de la conexión o dispositivo mediante el que se realice el proceso.

Claves de acceso

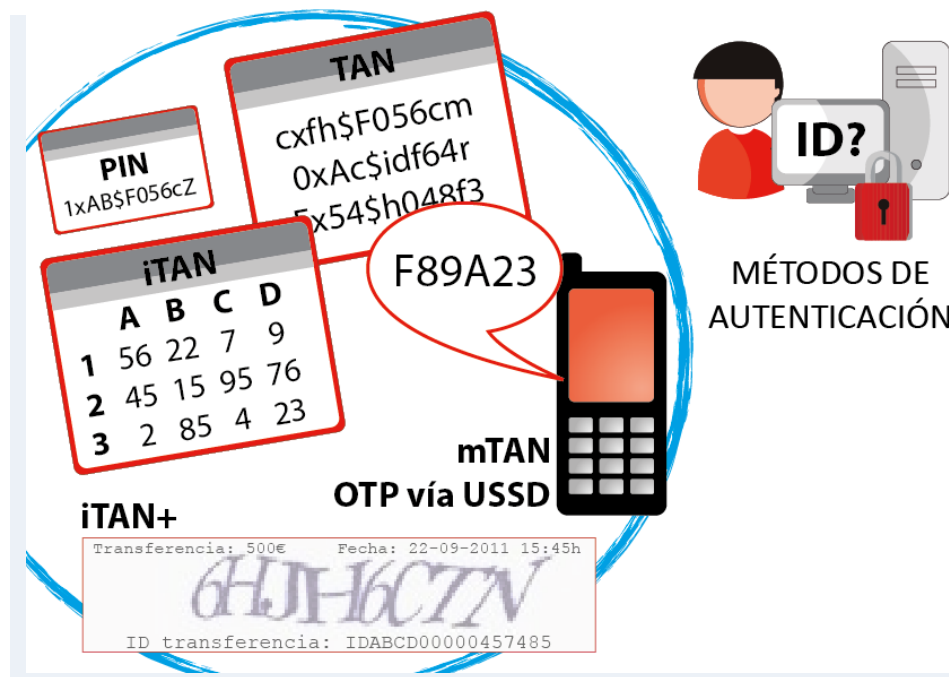
Hasta ahora, el elemento más utilizado para comprobar la legitimidad del usuario que solicita realizar la transacción ha sido el uso de claves de acceso. Existen multitud de mecanismos que se han ido mejorando y adoptando lo largo de los años, los ejemplos más significativos son:

- PIN (Personal Identification Number), número de identificación personal o contraseña. El número de identificación personal es la medida más sencilla y clásica de identificación: el banco o tienda online facilita una clave numérica o código alfanumérico para identificarnos, que deberá ser introducido en el formulario correspondiente en el momento de la autenticación.
- TAN (Transaction Authentication Number) o número de autenticación de transacción. Se trata de una evolución del PIN. Está formado por una lista o tabla de códigos que, en función de las circunstancias, pueden haber sido previamente generados y distribuidos de manera física (papel o tarjetas) o distribuirse instantes antes de la transacción a través de medios digitales o dispositivos electrónicos. En

cada transacción se solicitará una clave distinta. Algunas variantes de este sistema son:

- **mTAN:** Antes de la transacción el banco envía el número de identificación a través del móvil del cliente, en un SMS por ejemplo.
- **iTAN:** Tabla de códigos que utiliza índices y que se corresponde con las conocidas tarjetas de coordenadas bancarias que facilitan las entidades para realizar la confirmación de pagos o transacciones. Por ejemplo, se puede solicitar introducir la clave correspondiente con la fila C columna 2.
- **iTANplus:** Nueva variante que añade CAPTCHAS¹ al proceso. Los CAPTCHAS son imágenes con información en su interior que se supone solo podrán ser leídas por humanos y no por programas automatizados. El CAPTCHA mostrado puede identificar el TAN a introducir, o utilizarse como método de comprobación de identidad (mostrando por ejemplo la fecha de nacimiento del usuario).

Ilustración 1: Ejemplos de diferentes medios de autenticación



Fuente: INTECO

¹ Completely Automated Public Turing test to tell Computers and Humans Apart (Prueba de Turing pública y automática para diferenciar máquinas y humanos). Un ejemplo son las imágenes en las que se incluyen letras o números suficientemente distorsionados como para que un software no puede reconocerlos de forma automática, mientras que un ser humano sí podría identificarlos.

- **Generadores de TANs:** dispositivos electrónicos que generan los códigos según un patrón interno. Se hablará de ellos en el apartado de tokens.
- **OTP (One Time Password)** o contraseña de un solo uso. Se trata de una clave de un solo uso, que generalmente es enviada por correo electrónico o SMS y que también puede ser generada a través de dispositivos tokens. El código OTP deja de ser efectivo en el momento en el que se realiza la transacción.

Tokens

Son dispositivos electrónicos independientes o con conexión USB a un PC. Permiten generar claves privadas aleatorias según un patrón o mediante sincronización con un servidor externo. En un momento dado el banco solicita que se introduzca la clave de acceso generada por el token del cliente. Generalmente sólo se tendrá que activar un botón para que se calcule.

Smartcards

También conocidas como tarjetas inteligentes. Son dispositivos de identificación del mismo tamaño que las tarjetas de crédito, que cuentan con un *chip* en el que guardan información. Muchas de las nuevas tarjetas de crédito son en realidad *smartcards*, abandonando progresivamente la obsoleta banda magnética para la identificación.

Este tipo de tarjetas necesitan lectores conectados al ordenador y permiten la identificación cuando el software o web que se está utilizando lo necesite. Su potencial es la capacidad de albergar información privada dentro del *chip* y, dependiendo del tipo de *chip* utilizado, pueden ser reprogramados posteriormente para incorporar o actualizar los datos internos.

Su principal función es guardar los certificados personales de usuario. Un ejemplo claro de *smartcard* es el actual DNI electrónico español.

Dispositivos biométricos²

Los dispositivos biométricos se basan en una cualidad e incorporan el factor de autenticación "cómo se es", es decir, buscan una manera precisa e inequívoca de identificar al usuario utilizando para ello partes de su cuerpo. Los más usados son:

- Lectores de huellas dactilares.
- Lectores de palma de la mano.

² Para ampliar conocimientos sobre la biometría se recomienda la consulta de la [Guía sobre las tecnologías biométricas aplicadas a la seguridad publicada](#) por INTECO.

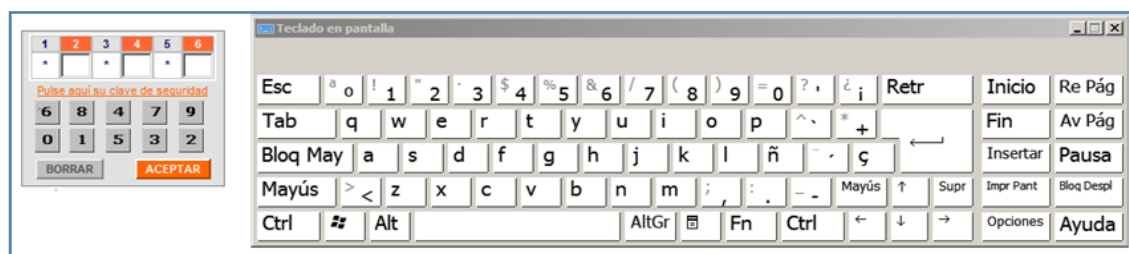
- Lectores de retina.
- Identificadores de voz.

Aunque puedan parecer dispositivos destinados a grandes empresas y organismos, en realidad están siendo adoptados a todos los niveles de forma gradual y ya existen iniciativas bancarias para implementarlo como medida principal de identificación de usuario.

Teclados virtuales

No son un sistema de identificación en sí, sino un medio de introducir (de manera más o menos segura) las credenciales de usuario, por ejemplo su PIN. Este método está recibiendo una gran aceptación en muchas webs bancarias para los formularios de introducción de contraseña o en el momento de solicitar las coordenadas. Los teclados virtuales también existen dentro del sistema operativo o el software antivirus como mecanismo de introducción de datos de manera virtual sin utilizar el teclado físico. Su objetivo es evitar los *keyloggers* o registradores de pulsaciones en el teclado.

Ilustración 2: Ejemplos de teclados virtuales



Fuente: INTECO

Firmas Digitales

Estas firmas están destinadas a comprobar la integridad de los datos transferidos durante una comunicación. Permiten comprobar si la comunicación sobre la transacción ha sido alterada en algún momento en su paso por las redes que separan origen y destino. Trabajan conjuntamente con los certificados digitales y los diferentes sistemas de cifrado disponibles.

Certificados digitales

Junto a las firmas digitales, son un elemento imprescindible para iniciar una conexión segura. Los certificados digitales son archivos que identifican usuarios, empresas, organismos y, más comúnmente, la página a la que se accede. En resumen, se trata de una serie de datos personales unidos a una clave pública, y todo ello firmado por una

entidad que les da validez. Normalmente los certificados son expedidos por las CA, Autoridades de Certificación. Los certificados se pueden utilizar:

- A través de los navegadores, que utilizan los certificados digitales (personales o corporativos) instalados en el equipo cuando los necesitan.
- A través de *smartcards* o tarjetas inteligentes donde residen y que añaden una capa física de seguridad.

Un certificado típico está compuesto por:

- Nombre completo de la persona u organismo a identificar.
- Nombre de la autoridad CA.
- Número de serie.
- Firma digital de la CA.

Es estándar tecnológico más usado por los certificados es el UIT-T X.509, que regula su contenido antes de ser asignados por una CA.

Infraestructura PKI

Se trata de un concepto abstracto. Es una combinación de diferentes mecanismos y protocolos, tanto hardware como software, que permiten realizar transacciones electrónicas con seguridad, basándose en la criptografía de clave pública.

De manera global se refiere al conjunto formado por las autoridades de certificación y el resto de elementos que intervienen en la comunicación:

- El certificado y las diferentes autoridades de certificación (CA).
- La clave, pública o no.
- Los servidores de certificación.
- El cifrado utilizado.
- Las firmas digitales.
- Los canales seguros de transporte de la información.
- Las garantías de aceptación de la transacción (no revocación).

Según el **Ministerio de Industria, Energía y Turismo**, actualmente existen multitud de CAs en nuestro país, como la Dirección General de la Policía (DNIe), FNMT-CERES, RedIRIS³ (SCS y pkIRISGrid), ipsCA... Se pueden consultar todas las entidades en: <https://www11.mityc.es/prestadores/busquedaPrestadores.jsp>

Ilustración 3: Ejemplo de certificado de DNI-e

Información del certificado

Este certif. está destinado a los siguientes propósitos:

- Asegura la identidad de un equipo remoto
- Prueba su identidad ante un equipo remoto
- Protege los mensajes de correo electrónico
- Confirma que el software procede de un editor de software
- Protege el software de alteraciones después de su publicación

* Para ver detalles, consulte la declaración de la entidad de ce

Campo	Valor
Versión	V3
Número de serie	00 d2 85 70 fd ae a7 d6 5f 11 84 15 c6 3
Algoritmo de firma	sha1RSA
Algoritmo hash de firma	sha1
Emitor	AC RAIZ DNIe, DNIe, DIRECCION GENER
Válido desde	jueves, 16 de febrero de 2006 12:37:25
Válido hasta	sábado, 09 de febrero de 2036 0:59:59

Emitido para: AC RAIZ DNIe

Emitido por: AC RAIZ DNIe

Válido desde: 16/ 02/ 2006 **hasta:** 09/ 02/ 2036

CN = AC RAIZ DNIe
OU = DNIe
O = DIRECCION GENERAL DE LA POLICIA
C = ES

Fuente: INTECO

II Medidas de seguridad durante la transacción

Actualmente el cifrado es el elemento conocido más adecuado para asegurar el proceso de principio a fin, garantizando la integridad y confidencialidad de la transacción.

El cifrado es la alteración de las comunicaciones de forma que se dificulte su comprensión por agentes no autorizados en caso de que puedan interceptarlas. Cualquier transacción online debe estar cifrada criptográficamente, puesto que es el único método matemático que, si se realiza en ausencia de malware u otros elementos distorsionadores, garantiza la seguridad de la operación.

SSL y HTTPS

A través del protocolo SSL "Secure Socket Layer", protocolo de autenticación y cifrado entre servidores web y clientes (navegadores), se ha desarrollado HTTPS, un protocolo de seguridad de aplicación basado en SSL (o TLS) y derivado del HTTP. Se identifica comúnmente por utilizar el operador <https://> al inicio de la URL en lugar del habitual <http://>.

³ www.rediris.es.

Durante una conexión HTTPS, existe una primera fase de acuerdo o "handshake" donde se establecen los detalles de la comunican cliente-servidor. Principalmente se define qué tipo de autenticación y cifrado conocen las dos partes (servidor y navegador) y cuáles pueden usar. Siempre que alguno de ellos no pueda soportar alguna versión se intentará con otra versión anterior, y normalmente de menor seguridad. Por ello es especialmente importante utilizar software actualizado que soporte las últimas versiones seguras de todos los protocolos.

Es necesario que el sitio web posea un certificado de clave pública válido y correctamente firmado por una Autoridad Certificadora. Es el navegador quien se encarga de comprobarlo. Una vez se ha establecido la comunicación segura, los datos se envían cifrados al servidor hasta el cierre de la conexión.

Ilustración 4: Ejemplo de conexión SSL



Fuente: INTECO

III Medidas y consejos de seguridad

Cuando se va a realizar cualquier tipo de transacción en la red, se deben observar las mismas medidas de seguridad que en el resto de acciones, añadiendo ciertas precauciones extra. Como mínimo, se deben comprobar los siguientes aspectos acerca de la página que se visita:

- Comprobar la existencia de certificados de seguridad al día. No son aceptables certificados caducados o inválidos. El navegador advertirá sobre cualquier circunstancia en este sentido. Se debe respetar la advertencia y, en la mayoría de los casos, esperar a aclarar la situación antes de acceder al sitio deseado.

Ilustración 5: Advertencia del navegador ante un certificado no válido



El certificado de seguridad del sitio no es de confianza.

Has intentado acceder a [asec.com](#), pero el servidor contiene un certificado emitido por una entidad que no es de confianza para el sistema operativo de tu ordenador. Esto puede suponer que el servidor haya generado sus propias credenciales de seguridad, en las que Google Chrome no puede confiar en relación con la información de identidad, o que un atacante haya intentado interceptar tus comunicaciones. No debes continuar, **sobre todo** si no has recibido nunca esta advertencia para este sitio.

Fuente: INTECO

- Comprobar la existencia de certificaciones válidas de sitio seguro: Trust-e, Verisign, www.confianzaonline.es.
- Comprobar la URL y confirmar que es la original del banco (www.mibanco.com), empresa o tienda online. La modificación de un único carácter puede dirigirnos a sitios web que simulen ser un banco, tienda o empresa para robar los datos y claves que se introduzcan en ellos.
- Ante la petición de datos confidenciales no usuales es necesario asegurarse de que es un sitio legítimo comprobando las medidas anteriores.
- Comprobar que es una empresa real, con sus datos de localización y fiscales a la vista y comprobables. Descartar cualquier empresa que no proporcione una dirección válida, número de teléfono o CIF.
- Si se tienen dudas o es la primera vez que se compra en una página, es recomendable comparar y buscar opiniones sobre la web o contactar directamente con los responsables. Existen páginas que permiten conocer la reputación de los comercios online, así como foros especializados en que los usuarios muestran su nivel de satisfacción con los servicios prestados.
- Comprobar la política y normativa de la web. Es conveniente leer detenidamente la "letra pequeña" para asegurarse de que no existen cobros posteriores.

Una vez finalizada la compra online

Tras cerrarse el proceso de compra se debe comprobar que todo se ha realizado correctamente y que se está preparando nuestro envío:

- Comprobar la transacción y que el importe cargado en la cuenta bancaria es el esperado.
- Verificar que se recibe un correo electrónico confirmando la compra, producto y valor.

- Nunca contestar a correos, enlaces o llamadas telefónicas donde se pidan datos personales de las cuentas. Los bancos y otras entidades legítimas contactan con sus clientes generalmente a través de correo postal. Ningún operador legítimo llamará o escribirá un email preguntando por las credenciales o contraseñas.

Otras formas y medios de pago

Existen diferentes medios de pago alternativos al ya tradicional uso de tarjetas de crédito. Su utilización supone una medida más de seguridad para evitar posibles problemas:

- Utilizar tarjetas prepago con un importe predefinido. Es posible comprarlas físicamente en las oficinas de Correos, en grandes almacenes o solicitarlas a la entidad bancaria.
- Utilizar tarjetas virtuales asociadas a la cuenta, a las que es posible asignar un saldo fijo.
- Dispositivos POS como el pago por móvil, que alertarán vía SMS o mail de la transacción, cargo e importe realizados.
- Utilizar servicios de pago por Internet a través de intermediarios. Se trata de servicios que permiten realizar transacciones sin que el destinatario final conozca los datos bancarios del cliente. Ejemplo de estos servicios son el pago mediante cuentas de Paypal, Google Checkout, o Moneybookers.
- Vigilar asiduamente los movimientos de las cuentas asociadas a las tarjetas que han sido utilizadas en estas transacciones.

Herramientas software y dispositivos

De especial relevancia son los dispositivos desde los que se realicen las transacciones, al igual que el software utilizado:

- Utilizar siempre dispositivos propios, nunca ajenos o públicos. Si el dispositivo no es fiable, cualquier medida de seguridad podría quedar invalidada. Cabe la posibilidad de que un troyano alojado en el sistema se apropie de los datos personales y credenciales o que exista una configuración que registre y almacene todas las operaciones que se realicen desde el dispositivo.
- Mantener el software, antivirus y navegadores actualizados. Es la mejor forma de evitar que problemas conocidos puedan ser explotados mediante malware que robe información.

- Como medida extra de seguridad se pueden utilizar los mencionados teclados virtuales disponibles como parte del propio sistema operativo o de algunas suites de seguridad. Proporcionan al usuario la capacidad de escribir mediante un teclado en pantalla, sin utilizar el teclado físico del ordenador, intentando evitar que un programa pueda registrar la pulsación de las teclas.



www.facebook.com/ObservaINTECO



www.twitter.com/ObservaINTECO



www.inteco.es/blog/Seguridad/Observatorio/BlogSeguridad



www.youtube.com/ObservaINTECO



www.scribd.com/ObservaINTECO



www.slideshare.net/ObservaINTECO



observatorio@inteco.es