

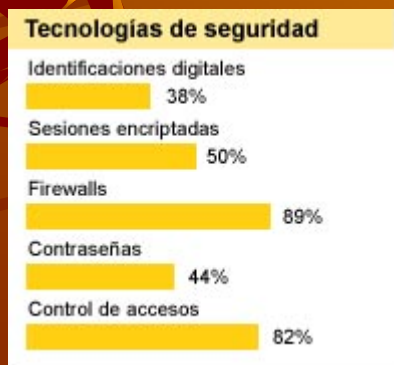
Firmas Digitales idSegura



Razones para asegurar la información que viaja a través de correo electrónico

- ◆ Internet está diseñado sobre un esquema abierto que facilita el anonimato y la divulgación de la información.
- ◆ La comunicación a través de e-mail está muy difundida y se utiliza cada vez más para enviar información de carácter confidencial.
- ◆ Facilita la realización de negocios a través de Internet al permitirle al usuario identificarse.
- ◆ Ataca todas las deficiencias del correo electrónico tradicional.

Datos estadísticos acerca del robo de información



Formas de asegurar la información que viaja por correo electrónico

La seguridad en Internet se obtiene a través de "llaves" privadas y/o públicas que permiten "cerrar" y/o "abrir" mensajes de correo electrónico.

- **Simétrica:**
Es la más antigua se basa en la distribución de la llave privada entre las personas con las que se mantiene comunicación a través de correo electrónico. Su deficiencia radica justamente en la distribución secreta de esta llave.
- **Asimétrica:**
Es la más moderna y resuelve todos los inconvenientes de seguridad planteados por la comunicación a través de correo electrónico. Se basa en un par de llaves, una privada y una pública. La privada es secreta y la tiene solo el emisor, la pública se puede distribuir libremente. Este esquema permite la creación de Firmas Digitales. En términos generales la pública cifra el mensaje y la privada es la única capaz de descifrarlo.

¿Que son las Firmas Digitales?

Una Firma Digital es la combinación del resumen Hash de un mensaje de correo electrónico y el certificado digital del emisor del mensaje. El resumen Hash se logra con la aplicación de un algoritmo matemático que crea el equivalente a la huella digital de un mensaje. El certificado digital es provisto por una Entidad Certificadora y permite conocer con certeza datos personales del emisor, como nombres, empresa en la que trabaja, dirección, teléfonos, etc.

Características de las Firmas Digitales

- ✦ **Confidencialidad:**
El mensaje podrá ser leído únicamente por el destinatario del mismo.
- ✦ **Integridad:**
El mensaje no puede ser modificado en su viaje por Internet y luego ser reenviado al destinatario.
- ✦ **Autenticidad:**
Se puede comprobar que el mensaje fue originado por el emisor y no por un intruso que se apoderó de su cuenta de correo electrónico.
- ✦ **No repudio:**
El emisor del mensaje no podrá negar que el mensaje fue escrito por él.

¿Como funcionan las Firmas Digitales?

Supongamos que en una oficina Ana quiere enviar un mensaje firmado electrónicamente a Bernardo. Para hacerlo Ana deberá realizar las siguientes actividades:

1. Ana escribe el mensaje.
2. Ana crea un resumen del mensaje y lo cifra con su llave privada, firmando así digitalmente el mensaje.
3. Ana cifra el mensaje con una llave de sesión creada de forma aleatoria y cifra esta llave con la llave pública de Bernardo, asegurándose que él va a ser el único que va a poder descifrar el mensaje.
4. Ana envía el mensaje.

Para que Bernardo pueda leer el mensaje deberá seguir los siguientes pasos:

1. Bernardo utiliza su llave privada para descifrar la llave de sesión que le envió Ana (Confidencialidad).
2. Con la llave de sesión descifra el mensaje original y crea un resumen Hash del mensaje.
3. Con la llave pública de Ana descifra la Firma Digital y compara el resumen creado por él con el de Ana, sino se alteró en su viaje por Internet estos deben ser exactos (Integridad).
4. Como Bernardo utilizó la llave pública de Ana para descifrar su Firma Digital, Ana es la única que pudo haber enviado el mensaje (Autenticidad).
5. Debido a que Ana es la única que pudo haber firmado el mensaje pues es la única que posee la llave privada, ella no puede negar que lo envió (No repudio).

Entidades Certificadoras e identidad del emisor

Una Entidad Certificadora es una organización avalada internacionalmente y por las Leyes del Ecuador para ofrecer productos que permiten habilitar legalmente a los usuarios de Internet y ofrecerles una identidad comprobable.

Cuentan con información acerca de los datos personales de sus clientes.

Una de las obligaciones de las Entidades Certificadoras es comprobar que la información suministrada por sus clientes sea verdadera. Se logra esto mediante la comprobación en el Registro Civil y otras Instituciones Gubernamentales de los documentos proporcionados por el cliente como parte de los requerimientos necesarios para la obtención de una Firma Digital. De esa manera se hace imposible que una persona adquiera una Firma Digital a título de otra.

Valor Legal y Judicial

- ✦ Las Firmas Digitales proveídas por idSegura están avaladas por el CONATEL, por lo tanto, cumplen con la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos del Ecuador.
- ✦ Todo mensaje o documento Firmado Digitalmente tiene el mismo valor de uno firmado convencionalmente.

Dispositivos para almacenamiento de Llaves Privadas

- ◆ Existen algunos dispositivos donde se puede guardar la llave privada de una Firma Digital:
 - Disco Duro computador
 - Tokens
 - SmartCards
 - Dispositivos biométricos



Token



The image shows a blue USB security token with a callout circle highlighting a chip on its top surface. The token is connected to a USB port, and its cap is shown separately below it. The background of the white box contains faint, illegible text.

- SU ACCESO A REDES PRIVADAS VIRTUALES (VPN).**
- SU ACCESO A REDES LOCALES (LAN).**
- SU ACCESO A LA WEB.**
- SU ACCESO A E-MAIL SEGURO & CONFIDENCIAL.**
- SU PROTECCION PARA INICIO DE PC Y ARCHIVOS.**
- SU ALMACENAMIENTO SEGURO DE CLAVES.**
- SU ALMACENAMIENTO SEGURO DE CERTIFICADOS.**
- SU ALMACENAMIENTO SEGURO DE PASSWORDS.**
- SU GENERADOR ON BOARD DE CLAVES PRIVADAS.**

Smartcards



Dispositivos Biométricos



Biocert y Macroseguridad

- ✦ idSegura es representante exclusivo para Ecuador de Biocert y Macroseguridad, líderes a nivel mundial y latinoamericano, respectivamente, en la provisión de Hardware de seguridad e identificación biométrica.

idSegura

- idSegura provee de soluciones de certificación y seguridad para Internet a través de su marca idSegura, desde cuyo portal se puede comprar toda la gama de productos que comprende, como Tokens, Certificados y Firmas Digitales, etc.

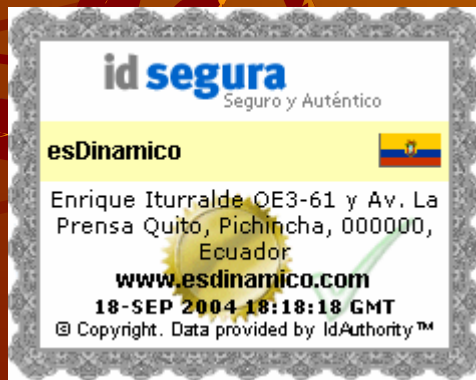


idSegura

- ◆ Para más información o comprar productos de certificación y/o seguridad para Internet visite:
www.idsegura.com

id segura

Proveedor Oficial de Certificados Digitales



Solicite gratis una Firma Digital para pruebas

- ◆ Gracias al auspicio de idSegura y su marca de certificación y seguridad para Internet, **idSegura**, usted podrá adquirir una Firma Digital gratuita solicitándola a la dirección seguridad@idsegura.com



Aplicaciones de Firmas Digitales

- ◆ Correo Seguro
- ◆ Certificación de documentos
- ◆ Contratos comerciales electrónicos
- ◆ Factura Electrónica
- ◆ Desmaterialización de documentos
- ◆ Transacciones comerciales electrónicas
- ◆ Invitación electrónica
- ◆ Dinero electrónico
- ◆ Notificaciones judiciales electrónicas
- ◆ Voto electrónico
- ◆ Decretos ejecutivos (gobierno)
- ◆ Créditos de seguridad social
- ◆ Contratación pública
- ◆ Sellado de tiempo

Algunas entidades que utilizan esta tecnología

◆ Internacional

- Ministerio de Defensa EEUU
- Servicios de impuestos en Europa, EEUU
- Cámaras de comercio Colombia

◆ Ecuador:

- Policía Nacional (Área Peritos)
- Corporación Aduanera Ecuatoriana
- SRI