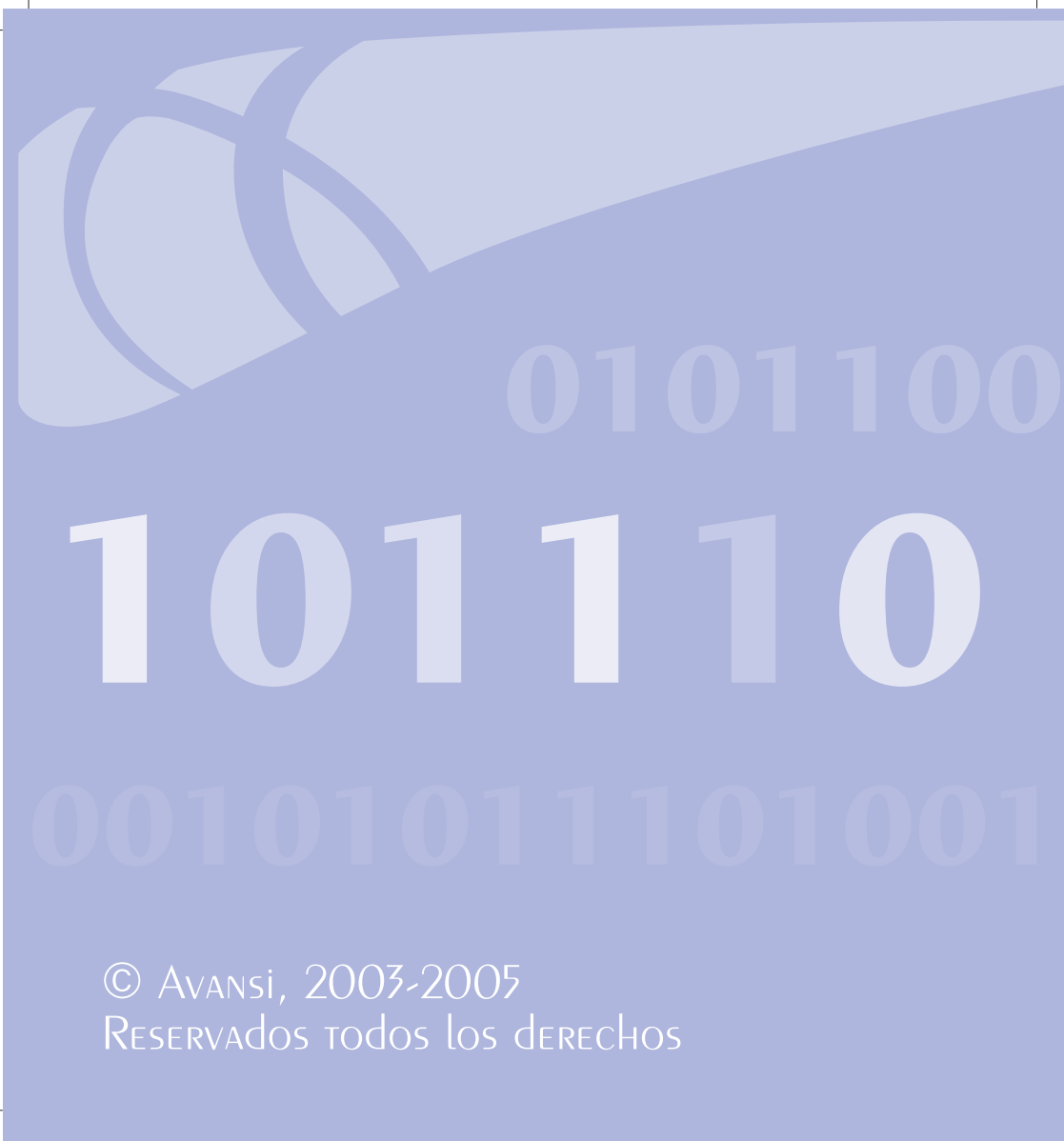


# CERTIFICACIÓN digital



CONCEPTOS

BÁSICOS



0101100

101110

00101011101001

© AVANSI, 2003-2005  
RESERVADOS TODOS LOS DERECHOS

# INTRODUCCIÓN

ACTUALMENTE NUESTRA SOCIEDAD ESTÁ VIVIENDO UNA ETAPA DE TRANSICIÓN QUE LO ESTÁ TRANSFORMANDO TODO DE UN MODO EXTRAORDINARIAMENTE ACCELERADO. ESTAMOS SIENDO LOS PROTAGONISTAS DEL PASO DE LA SOCIEDAD INDUSTRIAL A LA SOCIEDAD DE LA INFORMACIÓN Y DEL CONOCIMIENTO.

DENTRO DE LA NUEVA SOCIEDAD DE INFORMACIÓN, ES INDUDABLE EL PAPEL QUE JUEGA LA RED MUNDIAL DE INFORMACIÓN: INTERNET, NO SÓLO VEHÍCULO SINO PLATAFORMA FUNDAMENTAL DEL FUTURO DE LOS NEGOCIOS.

JUNTO CON LA POPULARIDAD DE INTERNET Y LA EXPLOSIÓN DE USUARIOS EN TODO EL MUNDO, HA VENIDO UNA CRECIENTE AMENAZA DE ATAQUES HACIA LOS SISTEMAS Y LA INFORMACIÓN DE LAS ORGANIZACIONES PÚBLICAS Y PRIVADAS.

## AMENAZAS Y ATAQUES

**Suplantación de identidad:** el intruso se hace pasar por una entidad diferente. Por ejemplo, ordenar una transferencia en nombre de la persona suplantada.

**Reactuación:** uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado. Por ejemplo, ingresar dinero repetidas veces en una cuenta bancaria.

**Modificación de mensajes:** una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado. Por ejemplo, "Ingreso de 50 € en cuenta A" por "Ingreso de 500 € en cuenta B".

**Degradación fraudulenta del servicio:** impide o inhibe el uso normal de los sistemas informáticos. Por ejemplo, enviar un número excesivo de mensajes hasta bloquear la cuenta de correo electrónico.

## SERVICIOS DE SEGURIDAD

### ■ AUTENTICACIÓN

¿Cómo puedo garantizar que soy quien digo ser?

### ■ INTEGRIDAD

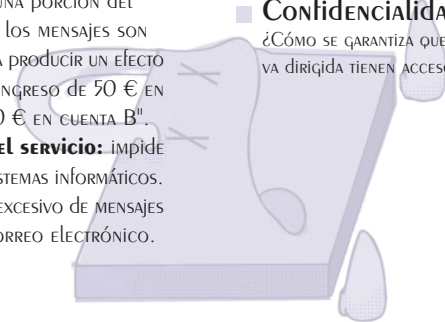
¿Cómo puedo saber que la información no ha sido manipulada?

### ■ No repudio

¿Cómo me aseguro que las partes que intervienen en una transacción no nieguen haberlo hecho?

### ■ Confidencialidad

¿Cómo se garantiza que sólo aquellos a los que va dirigida tienen acceso a la información?

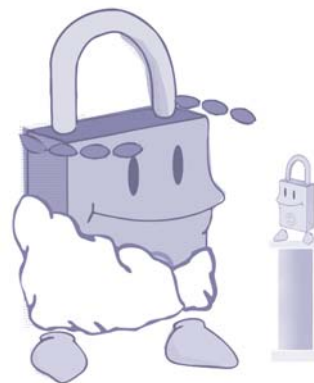


# Cifrado Digital

## Criptografía

SEGÚN EL DICCIONARIO DE LA REAL ACADEMIA, LA PALABRA Criptografía proviene del griego 'kriptos' que significa escondido, y 'graphos' que significa escritura, y su definición es 'escritura escondida'.

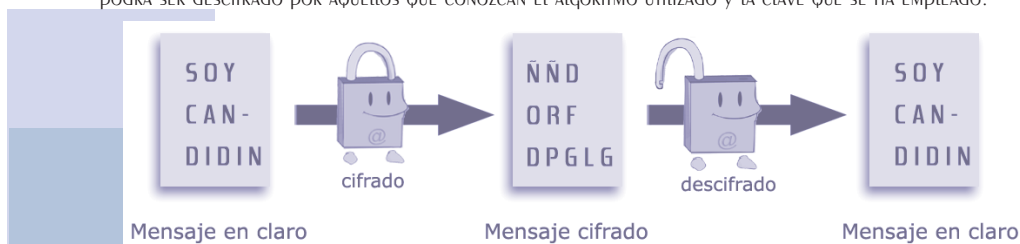
Desde la antigüedad hasta nuestros días se han mandado mensajes secretos. La necesidad de comunicarse secretamente ha ocurrido en la diplomacia y entre militares. Con la llegada de Internet el interés por mantener mensajes ininteligibles por todos, salvo el receptor, no ha hecho sino aumentar.



## Cifrado

Posiblemente el primer sistema de cifrado tuvo su origen con el Emperador Julio Cesar. Consistía simplemente en desplazar cada letra del alfabeto un número determinado de posiciones. Por ejemplo, la letra "A" podría ser codificada como "D", la "B" como "E", y así sucesivamente. En este caso, el mensaje "Me llamo Candidin" se transformaría en "oh ññdor Fdpqlqø".

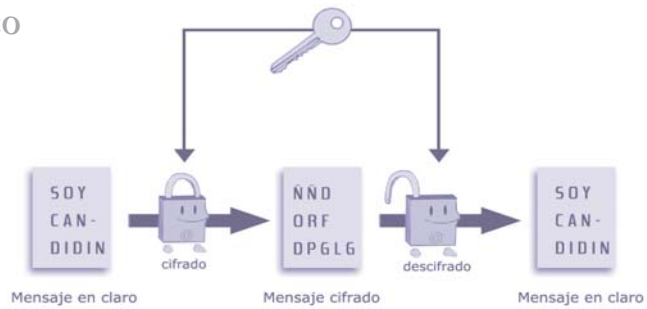
El cifrado transforma, mediante un algoritmo de cifrado, un texto **en claro** en un texto **cifrado** que sólo podrá ser descifrado por aquellos que conozcan el algoritmo utilizado y la clave que se ha empleado.



4

GARANTIZA QUE LA INFORMACIÓN NO ES INTELIGIBLE PARA OTROS (**confidencialidad**).

## Cifrado SIMÉTRICO



- Sólo existe una clave.
- La misma clave se utiliza tanto para el cifrado como para el descifrado.
- Ventaja: es un algoritmo sencillo y rápido.
- Inconveniente: la distribución de la clave es inmanejable en una red pública como Internet.

## Cifrado ASIMÉTRICO



- Existe una pareja de claves (pública y privada)
- La información cifrada mediante la clave pública sólo puede recuperarse con la clave privada y viceversa
- Ventaja: no es necesario el envío de la clave, siendo un sistema más seguro
- Inconveniente: es un procedimiento lento

### CLAVE PÚBLICA O DE CIFRADO

- se difunde al resto de los usuarios
- es utilizada por el resto de los usuarios para cifrar los mensajes que le quieren enviar protegidos

### CLAVE PRIVADA O DE DESCIFRADO

- se mantiene en secreto
- es utilizada por el usuario para descifrar los mensajes cifrados enviados por otros usuarios

# FIRMA DIGITAL

LA FIRMA DIGITAL ES UN BLOQUE DE CARACTERES QUE ACOMPAÑA A UN DOCUMENTO (O FICHERO) ACREDITANDO QUIÉN ES SU AUTOR (**AUTENTICACIÓN**) Y QUE NO HA EXISTIDO NINGUNA MANIPULACIÓN POSTERIOR DE LOS DATOS (**INTEGRIDAD**).

PARA FIRMAR UN DOCUMENTO DIGITAL, SU AUTOR UTILIZA SU PROPIA CLAVE PRIVADA (SISTEMA CRIPTOGRÁFICO ASIMÉTRICO), A LA QUE SÓLO ÉL TIENE ACCESO, LO QUE IMPIDE QUE PUEDA DESPUÉS NEGAR SU AUTORÍA (**NO REPUDIO EN ORIGEN**). DE ESTA FORMA, EL AUTOR QUEDA VINCULADO AL DOCUMENTO DE LA FIRMA. POR ÚLTIMO LA VALIDEZ DE DICHA FIRMA PODRÁ SER COMPROBADA POR CUALQUIER PERSONA QUE DISPONGA DE LA CLAVE PÚBLICA DEL AUTOR.



LA FIRMA DE UN DOCUMENTO NO IMPLICA QUE EL MENSAJE ESTÉ CIFRADO, POR LO TANTO NO GARANTIZA SU CONFIDENCIALIDAD.

NO OBSTANTE, DADO QUE LOS SISTEMAS DE CLAVE PÚBLICA SON MUY LENTOS, EN VEZ DE FIRMAR DIGITALMENTE EL MENSAJE COMPLETO, ÉSTA SE REALIZARÁ SOBRE UN RESUMEN O HASH DE LOS DATOS ORIGINALES.

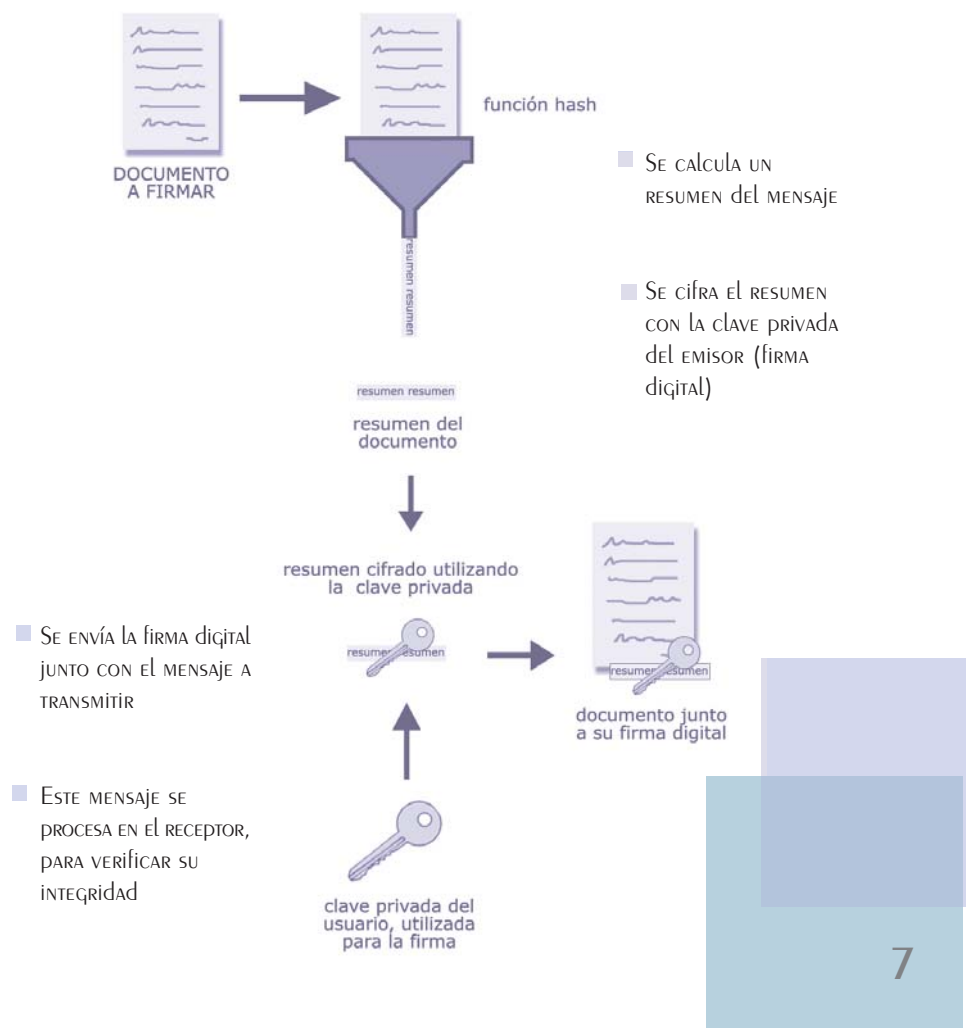
## LEGISLACIÓN

EXISTE UN MARCO REGULADOR PARA EL USO DE LA FIRMA DIGITAL:

- **REAL DECRETO LEY 14/1999 DE 17 DE SEPTIEMBRE SOBRE FIRMA ELECTRÓNICA (B.O.E. 18/9/1999).** ESTABLECE EL MARCO PARA EL USO DE LA FIRMA DIGITAL CON EL MISMO VALOR QUE LA MANUSCRITA, ASÍ COMO LA BASE PARA LAS POLÍTICAS DE CERTIFICACIÓN Y EL FUNCIONAMIENTO DE LOS PROVEEDORES DE SERVICIOS DE CERTIFICACIÓN (PSC).
- **ORDEN DE 21 DE FEBRERO DE 2000,** QUE REGULA LA ACREDITACIÓN DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN Y ESTABLECE UN REGISTRO DE P.S.C. Y LAS ENTIDADES CON CAPACIDAD DE ACREDITACIÓN DE DICHO P.S.C.
- **DIRECTIVA EUROPEA 1999/93/EC DE 13 DE DICIEMBRE DE 1999.** ESTA NORMATIVA ESTABLECE UNAS BASES COMUNES QUE DEBEN CUMPLIR TODOS LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN DENTRO DE LA UNIÓN EUROPEA.



# PROCESO DE FIRMA



# CERTIFICADO DIGITAL

ES MUY IMPORTANTE ESTAR REALMENTE SEGUROS DE QUE LA CLAVE PÚBLICA QUE MANEJAMOS PARA VERIFICAR UNA FIRMA O CÍFRAR UN TEXTO, PERTENECE REALMENTE A QUIÉN CREEMOS QUE PERTENECE.

UN CERTIFICADO ES UN DOCUMENTO EMITIDO Y FIRMADO POR UNA AUTORIDAD DE CERTIFICACIÓN QUE IDENTIFICA UNA CLAVE PÚBLICA CON SU PROPIETARIO.

UN CERTIFICADO DIGITAL CONTIENE UNA **clave pública** y una **firma digital**.



**VERSIÓN** - identifica el formato del certificado

**Nº de serie** - cada certificado es único dentro de la Autoridad Certificadora

**ALGORITMO** - se pueden utilizar múltiples algoritmos para firmar el certificado

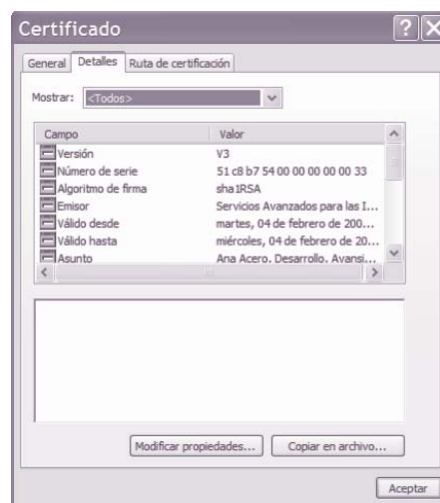
**Autoridad Emisora** - nombre de la Autoridad de Certificación que emite el certificado

**Periodo de validez** - desde / hasta

**Nombre del usuario**

**Clave Pública del usuario** - junto con el algoritmo usado y los parámetros necesarios

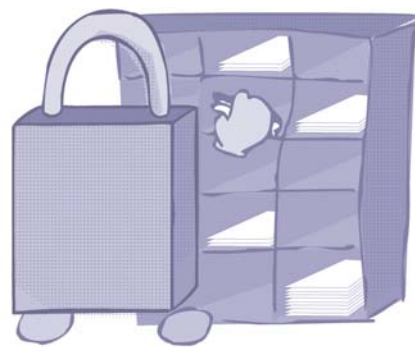
**Firma de la Autoridad de Certificación**



# AUTORIDAD DE CERTIFICACIÓN

LA VALIDEZ DE UN CERTIFICADO ES LA CONFIANZA QUE SE PUEDE TENER EN QUE LA CLAVE PÚBLICA CONTENIDA EN EL CERTIFICADO PERTENECE AL USUARIO INDICADO EN EL PROPIO CERTIFICADO. LA MANERA EN QUE SE PUEDE CONFIAR EN EL CERTIFICADO DE UN USUARIO CON EL QUE NUNCA HEMOS TENIDO RELACIÓN ES MEDIANTE LA CONFIANZA EN "TERCERAS PARTES".

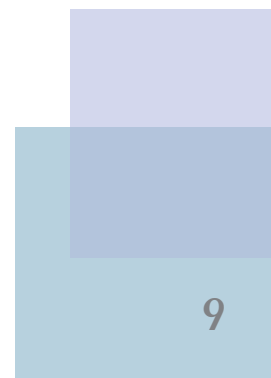
LA AUTORIDAD CERTIFICADORA ES UNA **TERCERA PARTE de Confianza** (TTP, TRUSTED THIRD PARTY) QUE ACREDITA LA IDENTIDAD DE LOS USUARIOS DE LOS CERTIFICADOS DIGITALES.



POSEE SU PROPIO PAR DE CLAVES Y FIRMA DIGITALMENTE LOS CERTIFICADOS CON SU CLAVE PRIVADA. CONFIANDO EN LA FIRMA DIGITAL DE LA AUTORIDAD CERTIFICADORA, PUEDE CONFIARSE EN CUALQUIER CERTIFICADO GENERADO POR LA MISMA.

## SERVICIOS

- GESTIÓN DE CERTIFICADOS (EMISIÓN/REVOCACIÓN/RENOVACIÓN)
- DIRECTORIO DE CERTIFICADOS
- AUTORIDAD DE REGISTRO
- FECHADO DIGITAL
- CUSTODIA DE DOCUMENTOS
- NOTIFICACIÓN ELECTRÓNICA
- RECUPERACIÓN DE CLAVES



# SEGURIDAD DE LOS NAVEGADORES

El protocolo **Secure Socket Layer** (SSL) fue desarrollado por Netscape y puesto en dominio público para la definición de canales seguros sobre TCP, el protocolo de transporte punto a punto de Internet. Su objetivo es la realización de conexiones seguras entre los servidores web y los clientes (navegadores).

SSL proporciona servicios de seguridad cifrando los datos intercambiados entre el servidor y el navegador con un algoritmo de cifrado simétrico, y cifrando la clave simétrica utilizada, denominada "clave de sesión", que se genera de manera aleatoria, mediante un algoritmo de cifrado asimétrico.



## PROCESO

Durante el protocolo SSL, el navegador y el servidor web intercambian una serie de mensajes para negociar las mejoras de seguridad. Este protocolo sigue las siguientes fases (de manera muy resumida):

- **La fase Hola**, usada para ponerse de acuerdo sobre el conjunto de algoritmos para mantener la intimidad y para la autenticación. El navegador le informa al servidor de los algoritmos que posee disponibles. Normalmente se utilizarán los más fuertes que se puedan acordar entre las dos partes. En función de las posibilidades criptográficas del navegador, el servidor elegirá un conjunto u otro de algoritmos con una cierta longitud de claves.
- **La fase de autenticación**, en la que el servidor envía al navegador su certificado que contiene su clave pública y solicita a su vez al cliente su certificado (sólo si la aplicación exige la autenticación de cliente).
- **La fase de creación de clave de sesión**, en la que el cliente envía al servidor una clave maestra a partir de la cual se generará la clave de sesión para cifrar los datos intercambiados posteriormente haciendo uso del algoritmo de cifrado simétrico acordado en la fase 1. El navegador envía cifrada esta clave maestra usando la clave pública del servidor que extrajo de su certificado en la fase 2. Posteriormente, ambos generarán idénticas claves de sesión a partir de la clave maestra generada por el navegador.
- **La fase Fin**, en la que se verifica mutuamente la autenticidad de las partes implicadas y que el canal seguro ha sido correctamente establecido.

Una vez finalizada esta fase, SSL proporciona un canal de comunicaciones seguro entre los servidores Web y los navegadores a través del cual se intercambiará cifrada la información relevante.

# CONEXIÓN SEGURA



CUANDO INTENTE ACCEDER A UN SITIO SEGURO, SU NAVEGADOR COMPROBARÁ QUE LA DIRECCIÓN DE INTERNET ALMACENADA EN EL CERTIFICADO SEA CORRECTA. SI LA INFORMACIÓN NO ES ACTUAL NI VÁLIDA SE MOSTRará UNA ADVERTENCIA.

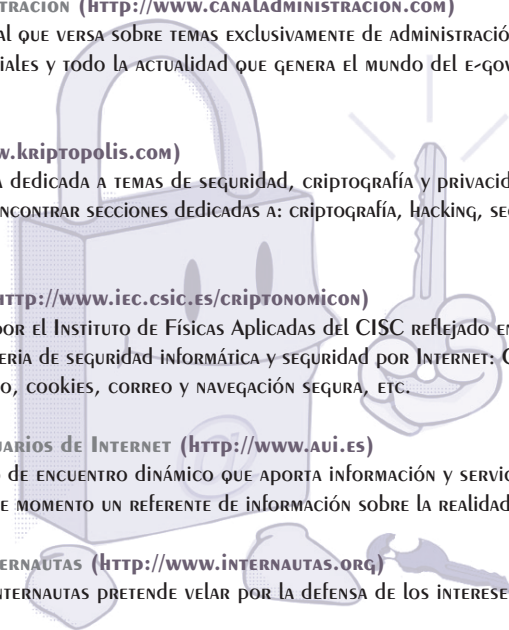


## CONSEJOS PRÁCTICOS

- CONVIENE PROTEGER LOS CERTIFICADOS CON CONTRASEÑA Y SELECCIONAR EL NIVEL DE SEGURIDAD ALTO
- ES RECOMENDABLE REALIZAR COPIAS DE SUS CERTIFICADOS CON SUS CLAVES PRIVADAS Y CONSERVARLOS EN UN SITIO SEGURO. SI LOS PIERDE O BORRA ACCIDENTALMENTE, SERÁ INCAPAZ DE LEER EL CORREO CIFRADO RECIBIDO Y NO SE PODRÁ IDENTIFICAR ANTE LOS SITIOS WEB
- ANTES DE SUMINISTRAR INFORMACIÓN CONFIDENCIAL COMPROBAR QUE ES UN SITIO SEGURO (CANDADO CERRADO O HTTPS) Y VERIFICAR EL CERTIFICADO

## ENLACES DE INTERÉS

- **MINISTERIO DE CIENCIA Y TECNOLOGÍA (<http://www.mcyt.es>)**  
El MINISTERIO DE CIENCIA Y TECNOLOGÍA OFRECE EN SU PORTAL UNA INFORMACIÓN ÍNTEGRA SOBRE LAS TELECOMUNICACIONES Y LA SOCIEDAD DE LA INFORMACIÓN, POLÍTICA CIENTÍFICA Y TECNOLÓGICA TODOS LOS ORGANISMOS DE INVESTIGACIÓN. INCLUYE TODA LA NORMATIVA REFERENTE A LA ADMINISTRACIÓN ELECTRÓNICA Y LA SEGURIDAD EN LA RED, ENTRE OTROS ASPECTOS.
- **LEY DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN (<http://www.lssi.es>)**  
ESTA PÁGINA CONTIENE INFORMACIÓN GENERAL SOBRE LA LEY DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN Y DE COMERCIO ELECTRÓNICO (LSSI), QUE HA SIDO ELABORADA POR LA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES Y PARA LA SOCIEDAD DE LA INFORMACIÓN DEL MINISTERIO DE CIENCIA Y TECNOLOGÍA, EN CUMPLIMIENTO DE LO DISPUESTO EN EL ARTÍCULO 33 DE LA CITADA LEY.
- **PLAN DE ACCIÓN InfoXXI (<http://www.infoxxi.es>)**  
El PLAN DE ACCIÓN DE LA INICIATIVA Info XXI ESTÁ COMPUESTO POR UN CONJUNTO DE INICIATIVAS (MÁS DE 300 ACCIONES Y PROYECTOS) QUE RESPONDEN A LOS OBJETIVOS ESTABLECIDOS EN LA INICIATIVA E-EUROPE, APROBADA EN EL CONSEJO EXTRAORDINARIO DE LISBOA, EN MARZO DE 2000.
- **FÁBRICA NACIONAL DE MONEDA Y TIMBRE (<http://www.cert.fnmt.es>)**  
El sitio web de la FÁBRICA NACIONAL DE MONEDA Y TIMBRE OFRECE UN COMPLETO ÍNDICE CON INFORMACIÓN SOBRE LA EMISIÓN DE CERTIFICADOS DIGITALES, TARJETAS INTELIGENTES, O EL PROYECTO CERES.  
REVISTA ELECTRÓNICA DEDICADA A TEMAS DE SEGURIDAD, CRIPTOGRAFÍA Y PRIVACIDAD POR INTERNET. EN EL WEB NOS PODEMOS ENCONTRAR SECCIONES DEDICADAS A: CRIPTOGRAFÍA, HACKING, SEGURIDAD WEB, REPORTAJES E INFORMES, ETC.

- 
- **AGENCIA DE PROTECCIÓN DE DATOS ([www.agenciaprotecciondatos.org](http://www.agenciaprotecciondatos.org))**  
Sitio de la AGENCIA DE PROTECCIÓN DE DATOS. Su finalidad principal es velar por el cumplimiento de la legislación sobre protección de datos personales y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, oposición, rectificación y cancelación de datos.
  - **CANAL de Administración (<http://www.canaladministracion.com>)**  
UN PERIÓDICO DIGITAL QUE VERSA SOBRE TEMAS EXCLUSIVAMENTE DE ADMINISTRACIÓN ELECTRÓNICA. NOTICIAS, ENTREVISTAS, EDITORIALES Y TODO LA ACTUALIDAD QUE GENERA EL MUNDO DEL E-GOVERNMENT Y LA SEGURIDAD EN LA RED A DIARIO.
  - **Kriptópolis ([www.kriptopolis.com](http://www.kriptopolis.com))**  
REVISTA ELECTRÓNICA DEDICADA A TEMAS DE SEGURIDAD, CRIPTOGRAFÍA Y PRIVACIDAD POR INTERNET. EN EL WEB NOS PODEMOS ENCONTRAR SECCIONES DEDICADAS A: CRIPTOGRAFÍA, HACKING, SEGURIDAD WEB, REPORTAJES E INFORMES, ETC.
  - **CriptonómicoN (<http://www.iec.csic.es/criptonomicon>)**  
SERVICIO OFRECIDO POR EL INSTITUTO DE FÍSICAS APLICADAS DEL CSIC REFLEJADO EN UN WEB CON ABUNDANTE INFORMACIÓN EN MATERIA DE SEGURIDAD INFORMÁTICA Y SEGURIDAD POR INTERNET: CGI 's, JAVA, JAVASCRIPT, CONTROLES DE ACCESO, COOKIES, CORREO Y NAVEGACIÓN SEGURA, ETC.
  - **Asociación de usuarios de INTERNET (<http://www.aui.es>)**  
EL SITE ES UN PUNTO DE ENCUENTRO DINÁMICO QUE APORTA INFORMACIÓN Y SERVICIOS PRÁCTICOS A LOS USUARIOS. ES EN ESTE MOMENTO UN REFERENTE DE INFORMACIÓN SOBRE LA REALIDAD DE INTERNET EN ESPAÑA.
  - **Asociación de INTERNAUTAS (<http://www.internautas.org>)**  
LA ASOCIACIÓN DE INTERNAUTAS PRETENDE VELAR POR LA DEFENSA DE LOS INTERESES DE SUS SOCIOS.
  - **Hispacec ([www.hispasec.com](http://www.hispasec.com))**  
SITE DEDICADO A TEMAS DE SEGURIDAD CON DIVERSAS SECCIONES DEDICADAS A: NOTICIAS DIARIAS, VIRUS, CRIPTOGRAFÍA, LEGISLACIÓN, INTERNET, EVENTOS, COMPARATIVA DE PRODUCTOS,... INCLUYE UNA COMPLETA BASE DE DATOS ASÍ COMO LINKS A PROGRAMAS ANTIVIRUS Y DE RECUPERACIÓN DE DISCOS INFECTADOS. INCLUYEN UN BOLETÍN DIARIO: "Hispacec UNA AL DÍA", CON UNA NOTICIA DIARIA SOBRE TEMAS RELACIONADOS CON LA SEGURIDAD.

## Glosario

### B

**B2B (Business-to-Business).** Modalidad de comercio electrónico en el que las operaciones comerciales se realizan entre empresas.

**B2C (Business-to-Consumer).** Modalidad de comercio electrónico en el que las operaciones comerciales se realizan entre una empresa y sus usuarios finales.

### C

**C2C (Consumer-to-Consumer).** Relaciones de intercambio entre dos consumidores a través de Internet.

**CPS (Certification Practice Statement).** Conjunto de prácticas utilizadas por una Autoridad de Certificación en la emisión y administración de los certificados.

**CRL (Certificate Revocation List).** Lista emitida por entidades de certificación en la que se publican todos aquellos certificados que han dejado de tener validez.

**CSP (Cryptographic Service Provider).** Herramienta software o hardware que contiene implementaciones de algoritmos y estándares criptográficos.

### I

**IPSec (Internet Protocol Security).** Conjunto de protocolos que soportan IP y que introducen características de seguridad antes no contempladas.

### L

**LDAP (Lightweight Directory Access Protocol).** Protocolo de servicio de directorio que utiliza un subconjunto del estándar X.500 de directorio para proveer una forma común de identificar al usuario y la información de grupo.

**LOPD (Ley Orgánica de Protección de Datos).** Tiene por objeto garantizar y proteger en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas.

## O

**OCSP (Online Certificate Status Protocol).** PERMITE A LAS APLICACIONES DETERMINAR EL ESTADO DE REVOCACIÓN DE UN DETERMINADO CERTIFICADO.

## P

**PKCS.** FAMILIA DE ESTÁNDARES PARA CRIPTOGRAFÍA DE CLAVE PÚBLICA, QUE ENLOBAN LOS SIGUIENTES TEMAS: ENCRIPCIÓN RSA, ACUERDO MUTUO DE CLAVE Diffie-Hellman. ENCRIPCIÓN BASADA EN PASSWORD. SINTAXIS DE CERTIFICADO EXTENDIDO. SINTAXIS DE INFORMACIÓN DE CLAVE PÚBLICA. SINTAXIS DE PETICIÓN DE CERTIFICADO.

**PKI (Infraestructura de Clave Pública).** ESTRUCTURA EN LA QUE LOS CLIENTES O USUARIOS Y SERVIDORES DISPONEN DE UN PAR DE CLAVES ASIMÉTRICAS, GUARDANDO LA PRIVADA Y DISTRIBUYENDO LA PÚBLICA EN UN CERTIFICADO EMITIDO POR UNA AUTORIDAD DE CERTIFICACIÓN.

## R

**RA (Autoridad de Registro).** ES LA ENCARGADA DE RECIBIR LAS SOLICITUDES DE CERTIFICACIÓN PROVENIENTES DE LAS ENTIDADES DESTINATARIAS Y DECIDIR SU VALIDACIÓN O DENIEGO. ENTIDAD INTERMEDIA ENTRE EL USUARIO Y LA AUTORIDAD DE CERTIFICACIÓN (CA), QUE DESCARGA A LA CA DE LAS TAREAS DE IDENTIFICACIÓN Y VALIDACIÓN DE LOS SOLICITANTES DEL CERTIFICADO.

## S

**SET (Secure Electronic Transaction).** TECNOLOGÍA PARA AUTENTIFICACIÓN DE LAS PARTES INVOLUCRADAS EN UN PAGO ELECTRÓNICO. ADEMÁS SET ASEGURA EL MANTENIMIENTO DE LA CONFIDENCIALIDAD Y LA INTEGRIDAD DEL CONCEPTO DEL PAGO.

**SSL (Secure Socket Layer).** PROTOCOLO CREADO POR NETSCAPE PARA ESTABLECER COMUNICACIONES SEGURAS. UNA SESIÓN SSL ESTA SECURIZADA GRACIAS AL USO DE TÉCNICAS DE CRIPTOGRAFÍA BASADAS EN CLAVE PÚBLICA.

## X

**X509v3.** PROTOCOLO PARA LA GENERACIÓN DE CERTIFICADOS DIGITALES.

[www.avansi.com](http://www.avansi.com)



101110



**AVANSI**. Servicios Avanzados para las Instituciones S.L.

Ava. Clara Campoamor, 4 Bloque 2, planta 1ª, piso 1  
41920 - San Juan de Aznalfarache - Sevilla

T. 954 179 005 F. 954 763 828 [info@avansi.com](mailto:info@avansi.com)



SERVICIOS AVANZADOS  
PARA LAS INSTITUCIONES

A V A N S I