FIRMA DIGITAL

INTRODUCCIÓN A LA NORMATIVA VIGENTE

Importancia :

- ✓PRESENCIA FÍSICA DE LAS PERSONAS
- ✓PAPEL: LUGAR Y CONSERVACIÓN
- ✓SEGURIDAD Y CALIGRAFÍA
- ✓CONTROL Y VELOCIDAD DE TRÁMITE

Costos adaptativos:

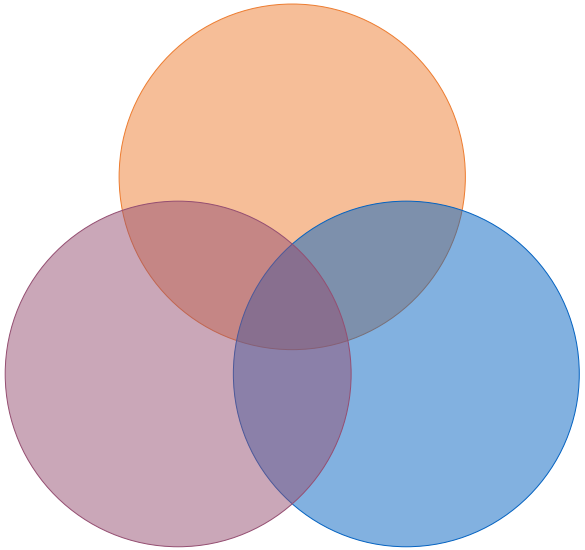
- Mayor productividad
- Mayores y nuevas demandas
- El servicio público como demanda social
- Desempleo, empleo distinto, empleo más cómodo, empleo de menor costo, nuevos empleos
- Costo de capacitación e infraestructura

- Despapelización
  - ❑administración pública
    estatal y no estatal
  - ❑administración privada y
    doméstica e individual

- Tecnologías informáticas ajenas a la firma digital involucradas en la despapelización (qué cosas no son firma digital y equivocadamente pueden atribuirse a este concepto?)

Nuevas Tecnologías

Tecnologías informáticas



Tecnologías en nuevos materiales

Biotecnologías

Tecnologías informáticas

1 Cibernética

2 Computación

3 Informática

4 Inteligencia artificial y sistemas expertos

5 Robótica

6 Realidad virtual

7 Criptografía

8 Redes

9 Teoría Gral. de Sistemas

10 Sistemas de Procesamiento de la Información como modelos racionales descriptivos del proceso sistémico (input, proceso y output)

algo de métodos o sistemas de Criptografía:

Arte y técnica de escribir con procedimientos o claves secretas o de un modo enigmático, de tal forma que lo escrito solamente sea inteligible para quien sepa descifrarlo.

Criptografía, clases:

SIMÉTRICA o de clave privada

- Una misma clave

❖**Inconvenientes relativos a los fines de la utilización sustitutiva de la firma ológrafa**

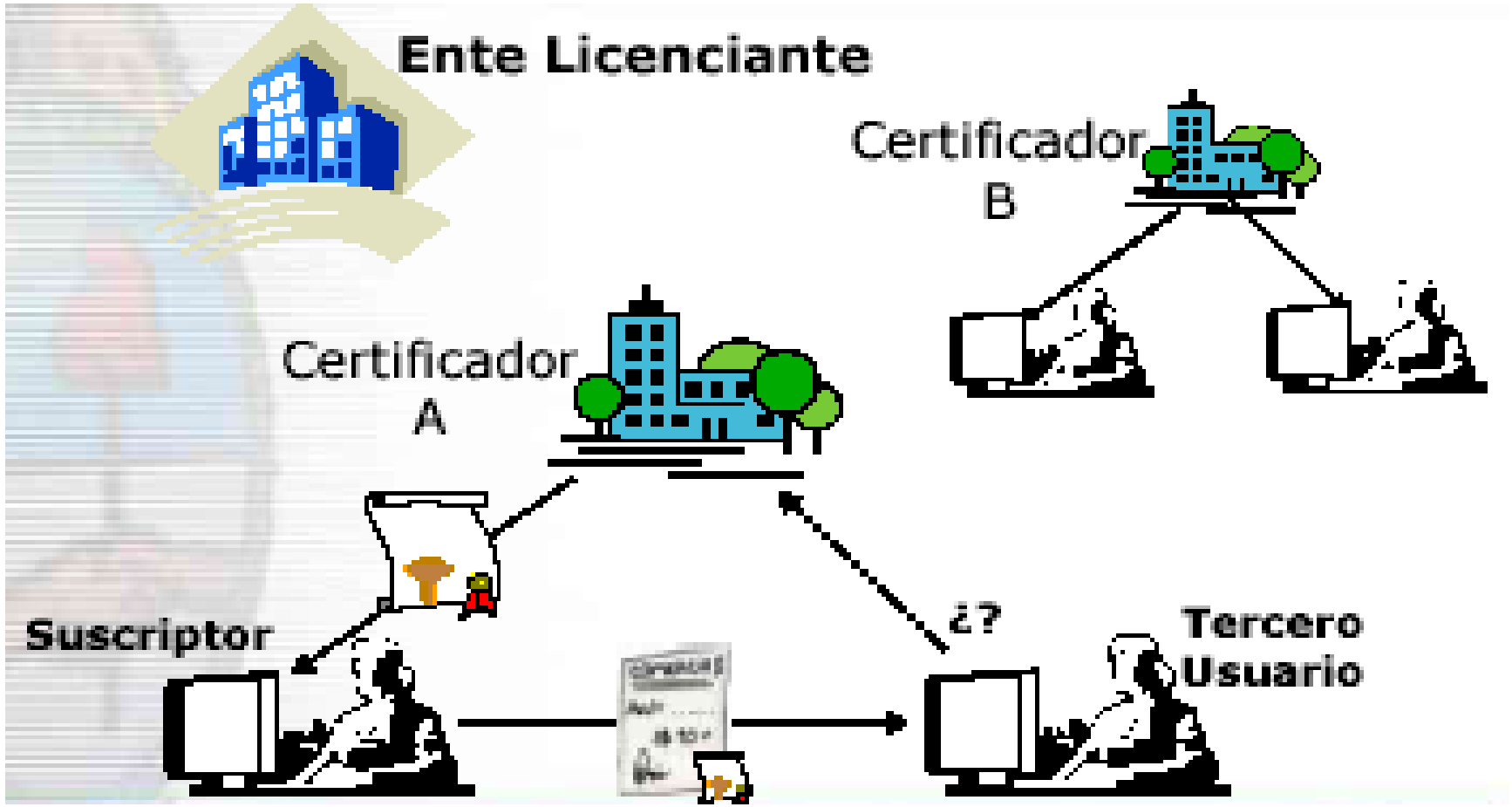
ASIMETRICA o de clave pública

- Par de claves: pública y privada

❖***Aptitud para los fines de reemplazo de la firma ológrafa***

Beneficios de la criptografía asimétrica:

- Confidencialidad o ilegibilidad
- Autenticidad o identidad
- Integridad o intangibilidad
- Certeza de recepción o de atribución al conocimiento de las partes
- Acceso restringido (privacidad)
- Accesibilidad o verificabilidad


Ente Licenciante
Certificador
B
Certificador
A
Suscriptor
¿?
Tercero
Usuario

FIRMA DIGITAL EN LA LEY 25506 (modificación por Ley 27446).

ARTICULO 2º - Firma Digital. Se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma.
Los procedimientos de firma y verificación a ser utilizados para tales fines serán los determinados por la Autoridad de Aplicación en consonancia con estándares tecnológicos internacionales vigentes.

Críticas a la definición de la ley

NO ES UN RESULTADO, *ES UN PROCEDIMIENTO ADMINISTRATIVO.*

NO SE LIMITA A LA APLICACIÓN DE UN PROCEDIMIENTO MATEMÁTICO DE EXCLUSIVO CONOCIMIENTO DEL FIRMANTE

LA CLAVE PRIVADA, NO SE ENCUENTRA SOLAMENTE BAJO EL CONTROL DEL USUARIO

Algo mas…

la tecnología de blockchain nos permite almacenar información que jamás se podrá perder, modificar o eliminar

Nuestra definición de firma digital:

La firma digital, constituye para nuestro derecho, un procedimiento administrativo, conformado por administrados/usuarios, Estado y, eventualmente, entes públicos no estatales, que con la finalidad de encriptar documentos electrónicos, mediante el uso de algoritmos de llaves asimétricas, sostienen una estructura de registro público de claves, montada sobre la base de protocolos que procuren mantener suficiente seguridad, a través de los cuales, tanto la identidad de los administrados/usuarios -remitentes y receptores- titulares de las claves, como la integridad del documento, pueden gozar de un grado de seguridad e intangibilidad a través de la tecnología de la función hash, tanto de procesos como de soportes, que permita sostener jurídicamente, la presunción de validez, salvo prueba en contrario, de su verosimilitud.-

Aspectos esenciales del procedimiento administrativo de firma digital:

- **Infraestructura de Firma Digital (Decreto 399)**
- **Estructura administrativa**
- Trámite con la obtención de un resultado
- Carácter de servicio público
- Validez pública y orden público comprometido


Ley 25.506
Certificado Digital
Política de Certificación
Manual de Procedimientos de Certificación
Resumen de la Política de Certificación y del Manual de Procedimientos de Certificación
Acuerdo con Suscriptores
Acuerdo con Terceros Usuarios
Plan de Seguridad
Plan de Contingencia
Plan de Cese de Actividades
Plataforma Tecnológica

Esquema elemental:
Qué necesitamos para estructurar el procedimiento de firma digital ?

- ✓ **Al menos dos usuarios**
- ✓ **Un ente certificante**
- ✓ **Un marco de confiabilidad adecual y legalmente admitido.**

Infraestructura de firma digital argentina

FIRMA ELECTRÓNICA Y FIRMA DIGITAL

- **ENTE LICENCIANTE MINISTERIO DE MODERNIZACIÓN MM**

Autoridad Certificante Raíz de la República Argentina (ACRAIZ)

- **CERTIFICADORES LICENCIADOS:**

ESTATALES APN, APP y CONVENIO INTERJURISDICCIONAL P. JUDICIAL.

PUBLICOS NO ESTATALES (demás reconocidos por el MM)

- **AUTORIDADES DE REGISTRO O CERTIFICADORES REGISTRADOS**

ESTATALES O NO ESTATALES

PRESTADORES DE SERVICIOS DE CONFIANZA

AUTORIDADES DE SELLO DE TIEMPO (repositorios sobre integridad f. hash)

ENTIDAD AUDITANTE SIGEN

ONTI

USUARIOS

Entes licenciantes:

- La autoridad de aplicación de la Infraestructura de Firma Digital antes mencionada es el MINISTERIO DE MODERNIZACIÓN, siendo dicho organismo y la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA, quienes entienden en las funciones de Ente Licenciante, otorgando, denegando o revocando las licencias de los certificadores licenciados y supervisando su accionar.

Certificadores licenciados a la fecha en Argentina:

- **ADMINISTRACIÓN FEDERAL DE INGRESOS PÚBLICOS AFIP**
- **ADMINISTRACIÓN NACIONALD DE LA SEGURIDAD SOCIAL ANSeS**
- **OFICINA NACIONAL DE TECNOLOGÍAS INFORMÁTICAS ONTI ACONTI**
- **ENCODE SA**
- **LAKAUT SA**
- **BOX CUSTODIA DE ARCHIVOS SA**
- **DIGILOGIX SA**
- **TECNOLOGÍA DE VALORES SA**
- **PRISMA MEDIOS DE PAGO SA**
- **SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN ADMINISTRATIVA SGMA**

Normativa básica:

Ley N° 25.506 de Firma Digital:

- ✓ ***Reconoce y establece las condiciones para el empleo de la firma electrónica y de la firma digital y su eficacia jurídica, y crea la Infraestructura de Firma Digital de la República Argentina.***

Ley Nº 27.446:

- ✓ ***Ley de simplificación y desburocratización de la administración pública nacional***

Decreto 182/2019:

- ✓ ***Aprueba la reglamentación de la Ley N° 25.506 de Firma Digital. Deroga los Decretos 2628/2002, 283/2003 y 724/2006***

Otra normativa importante:

- **Resolución Nº 399e/2016 del MINISTERIO DE MODERNIZACIÓN**

(Reemplaza la Decisión Administrativa Nº 927/2014 y la Disposición SSTG Nº 7/2015). Establece los procedimientos y condiciones que se deberán cumplir para emitir certificados digitales en el ámbito de la Infraestructura de Firma Digital de la República Argentina.

- **ANEXO I: REQUISITOS PARA EL LICENCIAMIENTO DE CERTIFICADORES**
- **ANEXO II: POLÍTICA ÚNICA DE CERTIFICACIÓN**
- **ANEXO III: PERFILES DE LOS CERTIFICADOS Y DE LAS LISTAS DE CERTIFICADOS REVOCADOS**
- **ANEXO IV: CONTENIDOS MÍNIMOS DE LOS ACUERDOS CON SUSCRIPTORES**
- **ANEXO V: CONTENIDOS MÍNIMOS DE LOS TÉRMINOS Y CONDICIONES CON TERCEROS USUARIOS**
- **ANEXO VI: MONTOS DE ARANCELES Y SEGUROS DE CAUCIÓN**
- **(Reemplazado por la Resolución MM Nº 213-E/17)**
- **ANEXO VII: CONTENIDOS MÍNIMOS DE LA POLÍTICA DE PRIVACIDAD**

Otra :

Resolución SMA Nº 37-E/16 Aprueba la POLÍTICA DE CERTIFICACIÓN DE LA AUTORIDAD CERTIFICANTE RAÍZ DE LA REPÚBLICA ARGENTINA V2.0.

- **ANEXO I: Política de Certificación v2.0 (ACR-RA)**
- **ANEXO II: Acuerdo con Suscriptores (ACR-RA)**
- **ANEXO III: Política de Privacidad del Ente Licenciante y de la ACR-RA**
- **ANEXO IV: Términos y Condiciones con Terceros Usuarios de la ACR- RA.**

Un documento digital…

- ARTICULO 6º - *Documento digital*. Se entiende por documento digital a la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo. Un documento digital también satisface el requerimiento de escritura.

Documento digital e instrumento en el CCCA.

CÓDIGO CIVIL Y COMERCIAL ARGENTINO

- **ARTICULO 287**.-Instrumentos privados y particulares no firmados. Los instrumentos particulares pueden estar firmados o no. Si lo están, se llaman instrumentos privados. **Si no lo están, se los denomina instrumentos particulares no firmados; esta categoría comprende todo escrito no firmado, entre otros, los impresos, los registros visuales o auditivos de cosas o hechos y, cualquiera que sea el medio empleado, los registros de la palabra y de información**.

DOCUMENTO ELECTRÓNICO → INSTRUMENTO PARTICULAR

INSTRUMENTO PRIVADO ELECTRÓNICO O DIGITAL (doc electrónico + firma dig o elect) → INSTRUMENTO PRIVADO

Instrumento público

- **ARTICULO 289**.-Enunciación. Son instrumentos públicos:
  a) las escrituras públicas y sus copias o testimonios;
  b) los instrumentos que extienden los escribanos o los funcionarios públicos con los requisitos que establecen las leyes;
  c) los títulos emitidos por el Estado nacional, provincial o la Ciudad Autónoma de Buenos Aires, conforme a las leyes que autorizan su emisión.

INSTRUMENTO PÚBLICO DIGITAL

=

INSTRUMENTO PUBLICO

(doc electrónico + firma dig) (electrónica???)

CONSECUENCIAS JURÍDICAS DIRECTAS DE LA FIRMA DIGITAL

- ARTICULO 3º - *Del requerimiento de firma*. Cuando la ley requiera una firma manuscrita, esa exigencia también queda satisfecha por una firma digital. Este principio es aplicable a los casos en que la ley establece la obligación de firmar o prescribe consecuencias para su ausencia.
- ARTICULO 11. - *Original*. Los documentos electrónicos firmados digitalmente y los reproducidos en formato digital firmados digitalmente a partir de originales de primera generación en cualquier otro soporte, también serán considerados originales y poseen, como consecuencia de ello, valor probatorio como tales, según los procedimientos que determine la reglamentación.
- ARTICULO 12. - *Conservación*. La exigencia legal de conservar documentos, registros o datos, también queda satisfecha con la conservación de los correspondientes documentos digitales firmados digitalmente, según los procedimientos que determine la reglamentación, siempre que sean accesibles para su posterior consulta y permitan determinar fehacientemente el origen, destino, fecha y hora de su generación, envío y/o recepción.

Presunciones de la firma digital:

- ARTICULO 7º - *Presunción de autoría*. Se presume, salvo prueba en contrario, que toda firma digital pertenece al titular del certificado digital que permite la verificación de dicha firma.
- Artículo 10: Remitente. Presunción. Cuando un documento electrónico sea firmado por un certificado de aplicación, se presumirá, salvo prueba en contrario, que el documento firmado proviene de la persona titular del certificado.
- ARTICULO 8º - *Presunción de integridad*. Si el resultado de un procedimiento de verificación de una firma digital aplicado a un documento digital es verdadero, se presume, salvo prueba en contrario, que este documento digital no ha sido modificado desde el de su firma.

Presupuestos de validez
firma digital regular

ARTICULO 9º - *Validez*. Una firma digital es válida si cumple con los siguientes requisitos:

a) Haber sido creada durante el período de vigencia del certificado digital válido del firmante;
b) Ser debidamente verificada por la referencia a los datos de verificación de firma digital indicados en dicho certificado según el procedimiento de verificación correspondiente;
c) Que dicho certificado haya sido emitido o reconocido, según el artículo 16 de la presente, por un certificador licenciado

Firma electrónica o firma digital irregular

- ARTICULO 5º - *Firma electrónica*. Se entiende por firma electrónica al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez.

Consecuencias semánticas y jurídicas

- FIRMA ELECTRÓNICA, INSTRUMENTO PRIVADO ELECTRÓNICO, EXPEDIENTE ELECTRÓNICO
- FIRMA DIGITAL, INSTRUMENTO PRIVADO DIGITAL, EXPEDIENTE DIGITAL
- LA INSTRUMENTACIÓN PUBLICA
- INFORMÁTICA DOCUMENTAL, DE GESTIÓN Y AUTOMÁTICA

Clases de firma electrónica (lato sensu)

Firma electrónica art 5 Ley Firma Digital

Firma digital art 2 Ley Firma Digital

Administración Pública Nacional

CLASES DE FIRMA DIGITAL EN LA APN EN EL SISTEMA DE GESTIÓN DOCUMENTAL ELECTRÓNICA GDE NUEVO DEC REGL 182/19

a) Firma digital remota: se utiliza para para firmar digitalmente todo tipo de documento electrónico incluyendo actos administrativos SIN TOKEN. (SALE DE LA PLATAFORMA DE FIRMA DIGITAL REMOTA DE LA RES. 121 SMA 2018 A CARGO DEL MIN MODERNIZACIÓN)

b) Firma digital con dispositivo criptográfico externo: se utiliza para firmar digitalmente todo tipo de documento electrónico incluyendo actos administrativos CON TOKEN.

c) firma digital con certificado del sistema: se utiliza para firmar documentos electrónicos, excepto actos administrativos, como dictámenes, informes, comunicaciones oficiales, etc con uso de una clave memorizada dentro y es con las computadoras dentro del sistema en el organismo

A.P. Provincial – Ley 9003

Extranjera art 16 LFD

APNE administración pública no estatal, certificadores reconocidos no estatales

Firma Digital o Firma Electrónica de particulares p uso no profesional o estatal

Firma digital profesional y el derogado art 18

Firma digital extranjera:

- ARTICULO 16. - *Reconocimiento de certificados extranjeros*. Los certificados digitales emitidos por certificadores extranjeros podrán ser reconocidos en los mismos términos y condiciones exigidos en la ley y sus normas reglamentarias cuando:
- a) Reúnan las condiciones que establece la presente ley y la reglamentación correspondiente para los certificados emitidos por certificadores nacionales y se encuentre vigente un acuerdo de reciprocidad firmado por la República Argentina y el país de origen del certificador extranjero, o
  b) Tales certificados sean reconocidos por un certificador licenciado en el país, que garantice su validez y vigencia conforme a la presente ley. A fin de tener efectos, este reconocimiento deberá ser validado por la autoridad de aplicación.

Firma digital profesional

- Qué decía el artículo 18 antes de la reforma?

- ARTICULO 18. - *Certificados por profesión*. Las entidades que controlan la matrícula, en relación a la prestación de servicios profesionales, podrán emitir certificados digitales en lo referido a esta función, con igual validez y alcance jurídico que las firmas efectuadas en forma manuscrita. A ese efecto deberán cumplir los requisitos para ser certificador licenciado.

- Pueden los colegios o consejos profesionales ser certificadores licenciados o autoridades de registro?

- **La Infraestructura de Firma Digital de la REPÚBLICA ARGENTINA (IFD-RA) está conformada por un conjunto de componentes que interactúan entre sí, permitiendo la emisión de certificados digitales para verificar firmas en condiciones seguras, tanto desde el punto de vista técnico como legal.**

CERTIFICADORES LICENCIADOS:

- Los certificadores licenciados son entidades públicas o privadas que se encuentran habilitados por el Ente Licenciante para emitir certificados digitales, en el marco de la Ley 25.506 de Firma Digital.

AUTORIDADES DE REGISTRO O CERTIFICADORES REGISTRADOS

- Las Autoridades de Registro son entidades públicas o privadas que se encuentran habilitados por el Ente Licenciante/Autoridad Certificante para emitir certificados digitales, en el marco de la normativa vigente. Serán las encargadas de facilitar el proceso de registración de los solicitantes y suscriptores de certificados de Firma Digital Remota. Es así que, mediante las funciones delegadas por la Autoridad Certificante (AC-Modernización-PFDR), las ARs son las responsables de efectuar las funciones de validación de la identidad y otros datos de los suscriptores de certificados, de aprobación o rechazo de las solicitudes, así como también de las solicitudes de revocación de los certificados digitales.

RES.399 - ANEXO I:
Requisitos para el licenciamiento de certificadores

- ***Sección 1: Documentación que debe entregar el solicitante para obtener una licencia.***
- ***Sección 2: Pautas de control a las que será sometido el solicitante para obtener la licencia, según sea el caso.***
- ***Sección 3: Registro de eventos.***
- ***Sección 4: Controles Físicos.***

SECCIÓN 2: (Res.399)

Pautas de control a las que estará sometido el s
obtener una licencia, según sea el caso

Código de práctica para la gestión de seguridad de la información

1.- Normas que debe cumplir el Plan de Seguridad:

- El Plan de Seguridad deberá cumplir con los lineamientos
ISO/IEC 27002, **no siendo exigible la certificación,** y sus correspondientes actualizaciones o reemplazos vigentes al momento de la presentación de la solicitud de licencia, en lo referente a todos aquellos aspectos relacionados directa o indirectamente con las actividades de certificación.

2.- Documentos que componen el Plan de Seguridad

- Una política de seguridad de la información, documentada y aprobada por la máxima autoridad del certificador, en la que se indicará cuáles son las acciones que se realizarán para cumplir con sus objetivos.
- Un manual que documente detalladamente los procedimientos para ejecutar las acciones necesarias para cumplir con los objetivos de la política de seguridad.