



UNIVERSIDAD DE
COSTA RICA

EDUFI

Escuela de
Educación Física
y Deportes

La Firma Digital

Aspectos legales

Seguridad

Ejemplos comunes

Solución al proceso de firmado digital



Walter Brenes F.

Aspectos legales

LA FIRMA FÍSICA O PLASMADA

Conjunto de gestos o trazos que componen grafos habituales elegidos libremente por la persona, en donde se plasma una estilización, que representa la auto imagen e identidad de algún individuo legalmente por voluntad propia con su propia mano.



LA RÚBRICA

Responde a una decoración o elemento utilizado para evitar la falsificación de la firma física, puede ser plasmada física o digitalmente, posee peso identificativo y jurídico, puede ir sola o acompañada de la firma más no define su emisor.



LA FIRMA DIGITAL

La firma digital es una herramienta tecnológica que permite garantizar la autoría e integridad de los documentos digitales, posibilitando que éstos gocen de una característica que únicamente era propia de los documentos en papel.

De acuerdo a la Ley 8454 la firma digital emitida por una autoridad certificadora registrada tiene la equivalencia jurídica de una firma manuscrita.



Seguridad

Proceso de firma

La firma digital funciona utilizando complejos procedimientos matemáticos que relacionan el documento firmado con información propia del firmante, y permiten que terceras partes puedan reconocer la identidad del firmante y asegurarse de que los contenidos no han sido modificados. Sistema Nacional de Certificación Digital-MICITT.
<http://www.firmadigital.go.cr/preguntas.html>



Seguridad

Certificados

Información encriptada en certificados



JERARQUÍA SHA2



Certificado de la CA Raíz

Hash para verificar la autenticidad del certificado de CA RAIZ NACIONAL - COSTA RICA:
Thumbprint = 68 a2 4d 2b 2c b5 c4 ce 9f e3 00 e3 b6 fc d1 df ee b9 c3 11

Número de serie del certificado de CA RAIZ NACIONAL - COSTA RICA
Serial Number= 74 b8 cf 63 8f ab 72 bc 46 c1 d2 ba cd 00 05 0c



Certificado de la CA de Políticas de Persona Física

Hash para verificar la autenticidad del certificado de CA POLITICA PERSONA FISICA - COSTA RICA: Thumbprint = b0 48 39 ce cf c7 3d 5f b0 db 8d a4 d0 61 3d 69 0f 60 4c b7

Número de serie del certificado de CA POLITICA PERSONA FISICA - COSTA RICA
Serial Number= 4e 00 00 00 02 73 8d e6 77 fe 8e 68 40 00 00 00 00 02



Certificado de la CA de Políticas de Persona Jurídica

Hash para verificar la autenticidad del certificado de CA POLITICA PERSONA JURIDICA - COSTA RICA: Thumbprint = c1 c2 ca 72 d1 30 20 0d ad 91 53 af e7 99 90 84 9c 07 b5 3b

Número de serie del certificado de CA POLITICA PERSONA JURIDICA - COSTA RICA
Serial Number= 4e 00 00 00 03 de f1 a1 6e 0f c7 ef 05 00 00 00 00 03



Certificado de la CA de Políticas de Sellado de Tiempo

Hash para verificar la autenticidad del certificado de CA POLITICA SELLADO DE TIEMPO - COSTA RICA: Thumbprint = 6f 05 59 99 b2 de b6 a2 fe 38 47 1f 4e f6 34 e8 13 a8 8a c8

Número de serie del certificado de CA POLITICA SELLADO DE TIEMPO - COSTA RICA
Serial Number= 4e 00 00 00 04 98 39 1f f8 03 b8 5b dc 00 00 00 00 04



2020



CA RAIZ NACIONAL - COSTA RICA v2



CA RAIZ NACIONAL COSTA RICA



CA RAIZ NACIONAL - COSTA RICA v2



CA RAIZ NACIONAL COSTA RICA



2021



loading...

Seguridad

Estructura o formato de firma

CADES (CMS Avanzado).

Es la evolución del primer formato de firma estandarizado. Es apropiado para firmar ficheros grandes, especialmente si la firma contiene el documento original porque optimiza el espacio de la información.

XAdES (XML Avanzado).

El resultado es un fichero de texto XML. Los documentos obtenidos suelen ser más grandes que en el caso de CAdES, por eso no es adecuado cuando el fichero original es muy grande.

PAdES (PDF Avanzado).

Este es el formato más adecuado cuando el documento original es un pdf. El destinatario de la Firma puede comprobar fácilmente la firma y el documento firmado. Con los formatos anteriores esto no es posible si no se utilizan herramientas externas.

OOXML y ODF.

Son los formatos de firma que utilizan Microsoft Office y Open Office, respectivamente.

Ejemplos Comunes

Documento con dos firmas correctas

Resumen:

-  Garantía de integridad y autenticidad
-  Garantía de validez en el tiempo

Firmantes:

Firmante	Fecha oficial de la firma	Garantía de integridad y autenticidad	Garantía de validez en el tiempo
Evelio Arguedas Olsen Cédula: 01-0586 0130	18/05/2021 03:49:48 p.m.		
ALON SO UREÑA UREÑA Cédula: 6-0456-789	24/05/2021 04:07:24 p.m.		

Detalle de la Firma Digital:

Firma Digital #1:

 La firma es válida hoy 08/06/2021 08:07:33 p.m.

Autoría del firmante garantizada
Nombre: **Evelio Arguedas Olsen**
Identificación: 01-0586 0130

Resumen:

-  Garantía de integridad y autenticidad
-  Garantía de validez en el tiempo

Detalle:

-  **Jerarquía de confianza:** El documento fue firmado con un certificado oficial. Certificados de la jerarquía contenidos en el documento.
-  **Integridad:** El contenido del documento no ha sido modificado después de realizada la firma.
-  **Vigencia:** El certificado digital estaba vigente al momento de la firma.
-  **Tipo de certificado:** El tipo de certificado utilizado es válido para firmar.
-  **Revocación:** El certificado no estaba revocado en el momento de la firma. La información de revocación está contenida en el documento.
-  **Fecha oficial de la firma:** El documento cuenta con una estampa de tiempo en el momento de la firma.
 - Fecha de la estampa de tiempo: 18/05/2021 03:49:48 p.m.

Firma Digital #2:

 La firma es válida hoy 08/06/2021 08:07:33 p.m.

Autoría del firmante garantizada
Nombre: **ALON SO UREÑA UREÑA**
Identificación: 6-0456-789

Resumen:

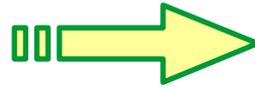
-  Garantía de integridad y autenticidad
-  Garantía de validez en el tiempo

Detalle:

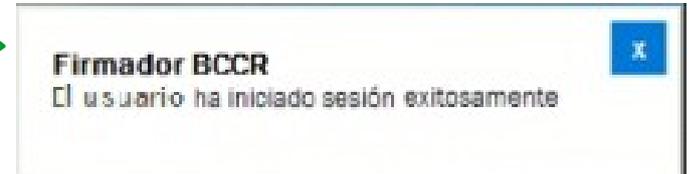
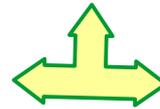
-  **Jerarquía de confianza:** El documento fue firmado con un certificado oficial. Certificados de la jerarquía contenidos en el documento.
-  **Integridad:** El contenido del documento no ha sido modificado después de realizada la firma.
-  **Vigencia:** El certificado digital estaba vigente al momento de la firma.
-  **Tipo de certificado:** El tipo de certificado utilizado es válido para firmar.
-  **Revocación:** El certificado no estaba revocado en el momento de la firma. La información de revocación está contenida en el documento.
-  **Fecha oficial de la firma:** El documento cuenta con una estampa de tiempo en el momento de la firma.
 - Fecha de la estampa de tiempo: 24/05/2021 04:07:24 p.m.

Ejemplos Comunes

Errores en Sesión no iniciada o sin sincronización

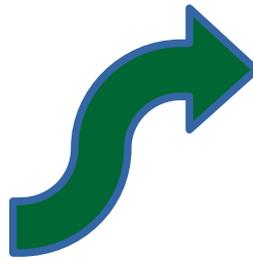


Es importante confirmar



Ejemplos Comunes

Error en estructura o formato de firma



Ejemplos Comunes

Error en la configuración de certificados

Resumen:

- ✔ **Garantía de integridad y autenticidad**
- ✔ **Garantía de validez en el tiempo**

Detalle:

- ✔ **Jerarquía de confianza:** El documento fue firmado con un certificado oficial. Certificados de la jerarquía contenidos en el documento.
- ✔ **Integridad:** El contenido del documento no ha sido modificado después de realizada la firma.
- ✔ **Vigencia:** El certificado digital estaba vigente al momento de la firma.
- ✔ **Tipo de certificado:** El tipo de certificado utilizado es válido para firmar.
- ✔ **Revocación:** El certificado no estaba revocado en el momento de la firma. La información de revocación está contenida en el documento.
- ⚠ **Fecha oficial de la firma:** El documento cuenta con una estampa de tiempo en el momento de la firma. Pero no incluye información de revocación o los certificados de la jerarquía correspondiente.
 - **Fecha de la estampa de tiempo:** 18/05/2021 10:21:37 a.m.

Ejemplos Comunes

Error general con certificado, sin LTV, sin suma de verificación

Formato: Pdf
Tamaño: 184 KB

Resumen:

-  Garantía de integridad y autenticidad
-  Garantía de validez en el tiempo

Firmantes:

Firmante	Fecha oficial de la firma	Garantía de integridad y autenticidad	Garantía de validez en el tiempo
Desconocido	Sin fecha		

Detalle de la Firma Digital:

Firma Digital #1:

 La firma no es válida hoy 08/06/2021 07:37:49 p.m.

Resumen:

-  Garantía de integridad y autenticidad
-  Garantía de validez en el tiempo

Detalle:

-  **Jerarquía de confianza:** El documento fue firmado con un certificado no oficial.

Ejemplos Comunes

¿Cómo realizar comprobación de documentos?



Firma Digital

Consulte aquí la información sobre las funcionalidades de firma digital que ofrece Central Directo.



Validación de documentos firmados digitalmente



Resumen:

- ✓ Garantía de integridad y autenticidad
- ✓ Garantía de validez en el tiempo

Firmantes:

Firma	Fecha oficial de la firma	Garantía de integridad y autenticidad	Garantía de validez en el tiempo
Evelio Arguedas Olsen Cédula: 11088-010	18/03/2021 10:48:43 p.m.	✓	✓
ALCANTARA, JESICA Identificación: 04455-719	24/03/2021 04:07:34 p.m.	✓	✓

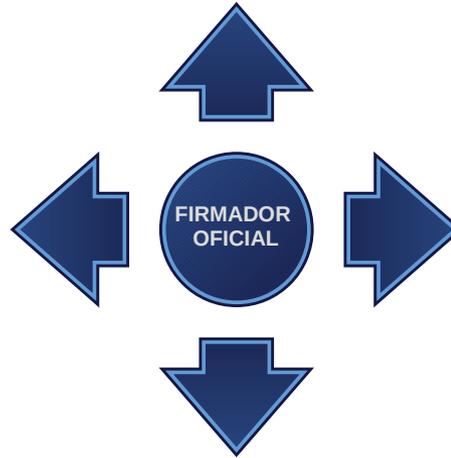
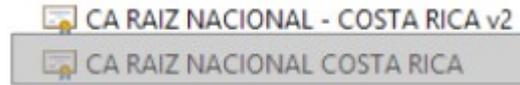
Detalle de la Firma Digital:

Firma Digital en:	Firma Digital en:
<ul style="list-style-type: none">✓ La firma es válida hoy 05/03/2021 05:07:23 p.m. <p>Judicia que firmario garantiza JUDICIAL ALCAZAR, JUDITH Identificación: 11088-010</p> <p>Resumen:</p> <ul style="list-style-type: none">✓ Garantía de integridad y autenticidad✓ Garantía de validez en el tiempo<p>Detalle:</p><ul style="list-style-type: none">✓ Garantía de confiable: El documento fue firmado con un certificado oficial. Certificado de la jerarquía correspondiente en el documento.✓ Integridad: El contenido del documento no ha sido modificado después de realizada la firma.✓ Vigencia: El certificado digital vigente al momento de la firma.✓ Tipo de certificado: El tipo de certificado utilizado es válido para firma.✓ Revocación: El certificado no estaba revocado en el momento de la firma. La información de revocación está disponible en el documento.✓ Fecha oficial de la firma: El documento cuenta con una evidencia de tiempo en el momento de la firma. - Fecha de la evidencia de tiempo: 18/03/2021 10:48:43 p.m.	<ul style="list-style-type: none">✓ La firma es válida hoy 05/03/2021 05:07:23 p.m. <p>Judicia que firmario garantiza JUDICIAL ALCAZAR, JUDITH Identificación: 04455-719</p> <p>Resumen:</p> <ul style="list-style-type: none">✓ Garantía de integridad y autenticidad✓ Garantía de validez en el tiempo<p>Detalle:</p><ul style="list-style-type: none">✓ Garantía de confiable: El documento fue firmado con un certificado oficial. Certificado de la jerarquía correspondiente en el documento.✓ Integridad: El contenido del documento no ha sido modificado después de realizada la firma.✓ Vigencia: El certificado digital vigente al momento de la firma.✓ Tipo de certificado: El tipo de certificado utilizado es válido para firma.✓ Revocación: El certificado no estaba revocado en el momento de la firma. La información de revocación está disponible en el documento.✓ Fecha oficial de la firma: El documento cuenta con una evidencia de tiempo en el momento de la firma. - Fecha de la evidencia de tiempo: 24/03/2021 04:07:34 p.m.

Solución proceso de firmado

Aplicación oficial para firmado digital

- JERARQUÍA SHA2**
- Certificado de la CA Raíz**
Hash para verificar la autenticidad del certificado de CA RAIZ NACIONAL - COSTA RICA:
Thumbprint = 68 a2 4d 2b 2c b5 c4 ce 9f e3 00 e3 b6 fc d1 df ee b9 c3 11
Número de serie del certificado de CA RAIZ NACIONAL - COSTA RICA
Serial Number= 74 b8 cf 63 8f ab 72 bc 46 c1 d2 ba cd 00 05 0c
 - Certificado de la CA de Políticas de Persona Física**
Hash para verificar la autenticidad del certificado de CA POLITICA PERSONA FISICA - COSTA RICA: Thumbprint = b0 48 39 ce cf c7 3d 5f b0 db 8d a4 d0 61 3d 69 0f 60 4c b7
Número de serie del certificado de CA POLITICA PERSONA FISICA - COSTA RICA
Serial Number= 4e 00 00 00 02 73 8d e6 77 fe 8e 68 40 00 00 00 00 02
 - Certificado de la CA de Políticas de Persona Jurídica**
Hash para verificar la autenticidad del certificado de CA POLITICA PERSONA JURIDICA - COSTA RICA: Thumbprint = c1 c2 ca 72 d1 30 20 0d ad 91 53 af e7 99 90 84 9c 07 b5 3b
Número de serie del certificado de CA POLITICA PERSONA JURIDICA - COSTA RICA
Serial Number= 4e 00 00 00 03 de f1 a1 6e 0f c7 ef 05 00 00 00 00 00 03
 - Certificado de la CA de Políticas de Sellado de Tiempo**
Hash para verificar la autenticidad del certificado de CA POLITICA SELLADO DE TIEMPO - COSTA RICA: Thumbprint = 6f 05 59 99 b2 de b6 a2 fe 38 47 1f 4e 16 34 e8 13 a8 8a c8
Número de serie del certificado de CA POLITICA SELLADO DE TIEMPO - COSTA RICA
Serial Number= 4e 00 00 00 04 98 39 1f f8 03 b8 5b dc 00 00 00 00 00 04

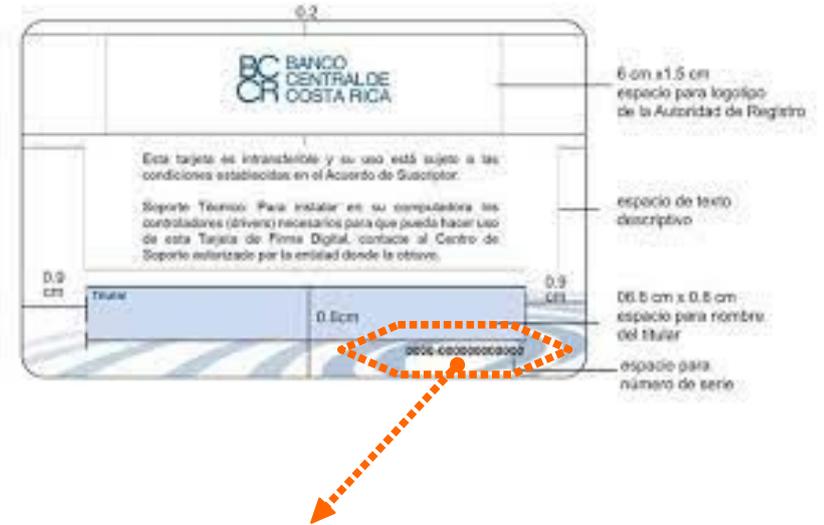


Verifica las firmas incrustadas en el documento

Solución proceso de firmado

Verificación de controladores y series de tarjetas

1



La 6.44.00 se utiliza en tarjetas que con numeración que inicien con 35-0D-0A, se puede descargar desde

https://www.soportefirmadigital.com/dd/sfd_Windows_rev57a.exe

La 7.24.01 se utiliza en tarjetas que con numeración que inicien con 8 ó 9, se encuentran en nuestra página.

El resto de las tarjetas funcionan con ambas versiones.

Solución proceso de firmado

Actualización e instalación de Java

2



The screenshot shows the Java website interface. At the top, there is a red navigation bar with the Java logo on the left, the text "Descargar" and "Ayuda" in the center, and a search box on the right labeled "Buscar". Below the navigation bar, the main heading reads "JAVA Y TÚ, DESCARGAR HOY". Underneath this heading is a prominent red button with the text "Descarga gratuita de Java". At the bottom of the page, there are two small links: "¿Qué es Java?" and "¿Necesita ayuda?".



Solución proceso de firmado

Descarga y ejecución de firmador oficial

3



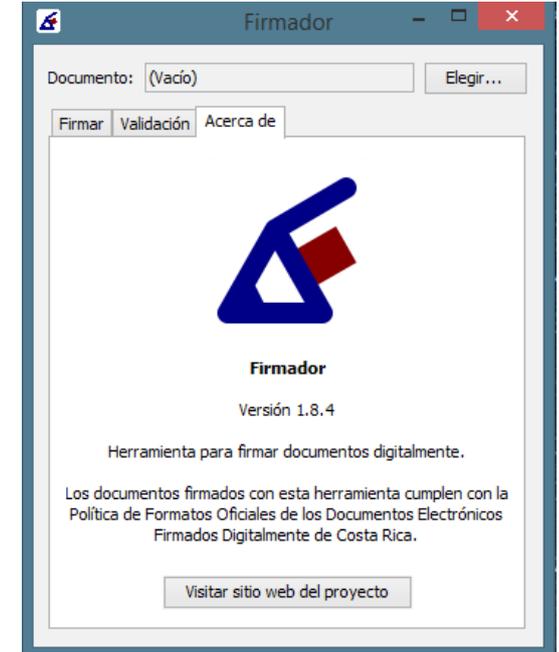
Firmador

Herramienta para firmar documentos cumpliendo con la [Política de Formatos Oficiales de los Documentos Electrónicos Firmados Digitalmente](#) de Costa Rica.

Descargar Firmador



firmador oficial



Solución proceso de firmado

Proceso de firmado para varias plataformas



https://www.soportefirmadigital.com/dd/Firmador_jar.mp4

Anexo

Vínculos de interés

<https://www.bccr.fi.cr/firma-digital>

<http://www.firmadigital.go.cr/preguntas.html>

<https://soportefirmadigital.com/web/es/guias-y-manuales.html>

<https://soportefirmadigital.com/web/es/preguntas-frecuentes.html>

<https://firmaelectronica.gob.es/Home/Ciudadanos/Formatos-Firma.html>

<https://peritoscaligrafosjudicial.es/2020/09/24/cual-es-la-diferencia-entre-firma-y-rubrica/>



UNIVERSIDAD DE
COSTA RICA

EDUFI

Escuela de
**Educación Física
y Deportes**

спасибо 谢谢
GRACIAS

THANK YOU

ありがとうございました **MERCI**

DANKE धन्यवाद

شُكراً **OBRIGADO**