

Guía para verificar documentos firmados digitalmente.

DIRECCIÓN DE CERTIFICADORES DE FIRMA DIGITAL

Versión 1.0

Fecha	Versión	Autor(es)	Aprobado	Descripción
14-12-2012	1.0	Mario Alvarez C.	Alexander Barquero, Director DCFD	Se presenta la versión 1.0 de la guía para su análisis y aprobación.

TABLA DE CONTENIDO

1.	DESCRIPCIÓN	- 4
2.	VERIFICACIÓN DE LA FIRMA DIGITAL EN MICROSOFT WORD 2010	5
3.	VERIFICACIÓN DE LA FIRMA DIGITAL EN ADOBE READER 11	- 11
	3.1. Validación manual	- 11
	3.2. Validación automática	- 13
	3.3. Verificar la validez de la Firma Digital a largo plazo en un documento PDF	- 15
	3.4. Configurar Adobe Reader para que Confíe en el Certificado Raíz	- 18
4.	INSTALAR LOS CERTIFICADOS DE LA CA RAÍZ NACIONAL	22
5.	INFORMACIÓN Y SOPORTE	- 26

1. DESCRIPCIÓN

Esta guía describe el proceso que debe seguir un usuario para verificar la validez de una Firma Digital en un documento electrónico utilizando las aplicaciones Microsoft Word 2010 y Adobe Reader 11, esta última de descarga gratuita.

Cada aplicación o sistema informático implementa de forma diferente la operación con Firma Digital, tanto el firmado como la verificación, algunos pueden ser similares pero siempre existirán características propias de cada una, el propósito de esta guía es que los usuarios cuenten con la información necesaria para verificar la legalidad de un documento firmado digitalmente.

La Firma Digital ya está siendo utilizada tanto a nivel público como privado, por lo tanto un usuario esta expuesto a recibir un documento de este tipo en cualquier momento, éste no puede ser rechazado porque ya la Ley lo obliga a darle el respectivo trámite. Esperamos que con esta guía esa persona tenga claro que hacer con un documento que contiene una Firma Digital.

Es importante tener en cuenta que si la computadora donde se va realizar el proceso de verificación nunca se ha utilizado con firma digital, se deben de instalar los certificados de la Jerarquía Nacional de Certificación Digital, esto se hace siguiendo el punto 4 de esta guía.

2. VERIFICACIÓN DE LA FIRMA DIGITAL EN MICROSOFT WORD 2010

Microsoft Word 2010 permite el firmado de documentos electrónicos y su respectiva verificación, además permite identificar si el formato de Firma Digital utilizado garantiza la validez de esa firma en el tiempo con todos elementos necesarios, esto último lo que se conoce como Formato Avanzado XADES XL.

XADES o firma electrónica avanzada XML (XML Advanced Electronic Signatures) es un conjunto de extensiones a las recomendaciones XML-DSig haciéndolas adecuadas para la firma electrónica avanzada que garantiza que los documentos firmados electrónicamente puedan seguir siendo válidos durante largos períodos, incluso en el caso de que los algoritmos criptográficos subyacentes hayan sido rotos. Existen diferentes niveles de XADES, pero esta guía describe la configuración para el nivel más robusto y seguro, **XADES XL**.

XADES XL (extended long-term), añade los propios certificados digitales y la información de revocación a los documentos firmados digitalmente para permitir la verificación en el futuro incluso si las fuentes originales (de consulta de certificados o de las listas de revocación) no estuvieran ya disponibles, garantizando la validez legal del documento y de la firma digital en el tiempo.

Cuando se recibe un documento de Microsoft Word y queremos identificar si efectivamente se encuentra firmado digitalmente, existen diferentes formas de saberlo. Importante saber que un mismo documento puede contener más de una Firma Digital.

A continuación se describen los pasos para verificar la Firma Digital de un documento de Microsoft Word 2010:

- 1. Abrir el documento de Word.
- 2. Verificar si en la parte inferior del mismo aparece el símbolo Regional que indica que este documento cuenta con Firmas Digitales, tal como lo muestra la imagen siguiente.



- 3. Otra forma de saber que el documento se encuentra firmado digitalmente es intentando editar o agregar algo al mismo, esto sería imposible, ya que Word bloquea el documento, incluso las opciones de formato se deshabilitan.
- 4. Ahora que ya conocemos que el documento se encuentra firmado digitalmente vamos a verificar la validez de dicha firma, para esto hacemos click en el símbolo de Firma Digital del documento a, con esto se debe abrir un panel al lado derecho de la pantalla que muestra las Firma Digitales válidas o inválidas de dicho documento. En la parte inferior de este panel se muestra una leyenda que indica: **"Este documento está firmado, cualquier modificación realizada en este documento invalidará las firmas digitales".** La imagen siguiente muestra el Panel de Firma de Word, así como la leyenda ya mencionada.



5. Si la Firma Digital es válida debe aparecer esa indicación en el panel tal como lo muestra la siguiente imagen:



6. En el mismo panel podemos ver con detalle toda la información relacionada con esa Firma Digital, para ellos debemos colocarnos sobre el nombre de la persona que firmo y hacer click derecho ó un click en una

pequeña flecha ^{2/2} que aparece y en ese momento elegimos la opción **Detalles de la Firma,** tal como lo muestra la siguiente imagen:



7. A continuación se abre una ventana donde se detallan las propiedades de la Firma Digital contenida en el documento, en la misma se puede ver la validez de dicha firma, así como el tipo de firma utilizado, la persona que realizó la firma y la Autoridad Certificadora (CA) que emitió el certificado digital de la persona.

Detalles de la firma
Firma válida: la firma y el contenido firmado no se han modificado desde que se aplicó la firma.
Tipo de firma: XAdES-X-L
Razón para firmar este documento:
Firmar como: MARIO ALONSO ALVAREZ CORDOBA (FIRMA) Emitido por: CA SINPE - PERSONA FISICA
Consultar la información de firma adicional que se recopiló

- 8. Una vez revisado la información de la Firma Digital se puede verificar con más detalle la información del certificado digital de la persona que firmó, esto presionado el botón **Ver** ubicado al lado derecho del nombre.
- 9. Con esto se abre la ventana de **Certificado**, esta cuenta con tres pestañas, La primera es **General**, en esta se puede visualizar información general del certificado, para quien fue emitido, cual fu la Autoridad Certificadora que lo emitió y el periodo de validez del mismo. Ver la imagen siguiente.

	Información	del certificado
Est	 Protege los mer 2. 16. 188. 1. 1.1 	stinado a los siguientes propósitos: isajes de correo electrónico .1.2
	Emitido para: Emitido por:	MARIO ALONSO ALVAREZ CORDOBA (FIRMA) CA SINPE - PERSONA FISICA
	Válido desde	19/ 03/ 2012 hasta 19/ 03/ 2014
	Tiene una dave p	rivada correspondiente a este certificado.
Obten	er más información a	Declaración del emigor acerca de <u>tertificados</u>

10. En la segunda pestaña se visualiza información más detallada de la Firma Digital del documento y del certificado digital, tal como la versión del certificado, número de serie o ID del mismo, algoritmo de firma utilizado, información del **Sujeto** que muestra nombre completo y número de cédula de la persona que firmó el documento, así como información de los sitios de verificación del estado del certificado digital. La siguiente imagen muestra la pestaña ya mencionada.

Certificado	cán .								
Mostrar: <todos></todos>									
Campo Versión Número de serie Algoritmo de firma Emisor Válido desde Válido hasta Suietn	Valor Image: Constraint of the second s								
Editar propiedades Copiar en archivo Más información acerca de los <u>detalles del certificado</u>									
	Aceptar								

11. La tercer pestaña de Ruta de Certificación muestra la cadena de certificados de la jerarquía nacional de Costa Rica, donde se valida que el certificado digital utilizado para firmar el documento pertenece a esa jerarquía y no es falso. Para todas las personas físicas la cadena de certificados inicia el certificado de la CA RAIZ NACIONAL – COSTA RICA, debajo de esta se encuentra el certificado de la CA POLITICA PERSONA FISICA – COSTA RICA, a continuación debe aparecer el certificado de la autoridad certificadora emisora en este caso CA SINPE - PERSONA FISICA y por último el certificado digital de la persona que emitió la Firma Digital. En caso que no apareciera toda la cadena tal como se indicó o como se muestra en la siguiente imagen podrían existir problemas con la Firma Digital del documento, por lo que se recomienda contactarse con el centro de soporte mencionado al inicio de esta guía. Para volver al documento se debe elegir la opción Aceptar y luego Cerrar.

Certificado
General Detallet Ruta de certificación
Ruta de certificación
CA RAIZ NACIONAL - COSTA RICA
<u>V</u> er certificado
Estado del certificado:
Certificado válido.
Más información acerca de las <u>rutas de certificación</u>
Aceptar

12. Si la Firma Digital del documento es **inválida** se mostrará una leyenda en el panel de Firma Digital que se abre al lado derecho de la pantalla, esta se mostrarán en color rojo con la leyenda Firmas no válidas. Un documento con una Firma Digital inválida compromete la validez de ese documento, ya que existe la posibilidad que el documento haya sido modificado o que hubo un cambio en la Firma Digital, este tipo de documentos no deberían de ser recibidos ni tramitados en ninguna entidad antes de comprobar bien por que se invalidó la Firma Digital, o también puede contactarse con el centro de soporte mencionado al inicio de esta guía. Ver la siguiente imagen que muestra una Firma no válida.



3. VERIFICACIÓN DE LA FIRMA DIGITAL EN ADOBE READER 11

Adobe Reader 11 permite el firmado de documentos electrónicos y su respectiva validación, permitiendo que el usuario pueda verificar esa validez. Además Adobe Reader permite identificar si el formato de Firma Digital utilizado garantiza la validez de esa firma en el tiempo con todos elementos necesarios, esto último lo que se conoce como Formato Avanzado PADES LTV.

PADES LTV (long-term validation), es un estándar para añadir la Firma Digital a un documento PDF utilizando formatos avanzados ya que añade los propios certificados digitales y la información de revocación a los documentos firmados digitalmente para permitir la verificación en el futuro incluso si las fuentes originales (de consulta de certificados o de las listas de revocación) no estuvieran ya disponibles, garantizando la validez legal del documento y de la firma digital en el tiempo.

Para verificar la validez de la Firma Digital en un documento de Adobe primero la herramienta tuvo que haber ejecutado el proceso de Validación de la misma. La validación de la firma digital en Adobe Reader 11 puede ser manual o automática, tal y como se describe en las siguientes secciones de este documento, pero independientemente del método empleado, es necesario, en primer lugar, instalar los certificados de la CA Raíz Nacional (Dirección de Certificadores de Firma Digital del Ministerio de Ciencia y Tecnología) y de la CA SINPE–PERSONA FISCA (Banco Central de Costa Rica), y en segundo lugar configurar la aplicación para que confíe en el certificado raíz del Sistema Nacional de Certificación Digital.

3.1. Validación manual

Para validar la firma digital de forma manual debe seguir los pasos que se indican a continuación:

- 1. Abrir el documento
- Seleccionar la ficha de firmas eligiendo del menú principal "Ver" > "Mostrar/" > "Paneles de navegación" > "Firmas".

d-ts	2 pdf - Adobe Acrobat Pro	A CONTRACT OF A	
	Rotar <u>v</u> ista <u>N</u> avegación de página		
	<u>P</u> resentación de página <u>A</u> mpliación/Reducción		
) y t	<u>H</u> erramientas <u>C</u> omentario	·	
(<u>Lornputte</u> <u>M</u> ostrar/ocultar	Paneles de <u>n</u> avegación 👂 💱 Ár <u>b</u> ol modelo	
	💒 Modo l <u>e</u> ctura 🔲 M <u>o</u> do Pantalla completa	+H Earra de menús F9 Archivos adjuntos	
	Rastreador	Reglas y cuadrículas Coordenadas del curgor	
	<u>C</u> omparar documentos	Destinos	
		C Linnas <u>Hercedores</u> ∭ Ministuras de página	
		Mostrar panel de nayegación Restablecer paneles	 [

3. También se puede hacer seleccionando la ficha "Firmas" que se muestra en la parte izquierda del documento.



4. A continuación se muestran las firmas del documento si la misma no se ha validado aún se mostrará el





5. Una vez seleccionada la firma, pulsar el botón derecho del ratón y elegir la opción "Validar firma".

u	
	Ir al campo de firma
	Borrar firma
9	V <u>a</u> lidar firma
	<u>V</u> er versión firmada
	Comparar versión firmada con la versión actual
	Agregar información de verificación
	Mostrar <u>p</u> ropiedades de firma

6. Una vez validada la firma, si todo ha funcionado correctamente, se desplegará junto a la firma el icono



3.2. Validación automática

Se puede configurar la aplicación para que la firma digital de un documento PDF se valide automáticamente al abrirlo, pero hay que tener en cuenta que esta operación consume un pequeño lapso de tiempo cada vez que se abra el documento. Para establecer la validación automática hay que configurar las preferencias de las firmas digitales de Adobe Reader de la siguiente manera:

- 1. Abrir el documento
- 2. Seleccionar del menú principal "Edición" > "Preferencias".



- 3. Seleccionar en la ventana que se muestra la opción "Seguridad" de entre todas las que hay en el panel de la izquierda.
- 4. Marcar, si no lo está, la opción "Verificar firmas al abrir el documento".

5. Pulsar el botón "Preferencias Avanzadas" para abrir el cuadro de diálogo "Preferencias avanzadas de las firmas digitales".

Categorías:	Firmas digitales
Pantalla completa	Verificar firmer al abrie el de sumente
Presentación de página	V veniticar firmas ai abrir ei documento
3D v mutimedia	Ver documentos en el modo de vista previa de documentos al firmar
Accesibilidad	Aspecto
ctualizador	Nuevo
dministración de color	
dministrador de confianza	Editar
sistente de acciones	
uscar	Duplicar
atálogo	
onfianza en contenido multimedia (heredado)	Eliminar
Convertir a PDF	
onvertir de PDF	
ormularios	
entidad	Configuración de seguridad
ternacional	Cargar la configuración de seguridad desde un servidor
iternet E	Configuración del servidor
ivaScript	
ectura	un <u>k</u> .
1edición (2D)	La configuración debe firmarse antes del: Permitir cualquier certificado
ledición (3D)	
Aedición (Geo)	Comprobar cada: O Semana O Mes
Aultimedia (heredado)	Accontant of the
Intografia	🔿 2 semanas 👘 3 meses 📝 Preguntar antes de actualizar
astreador	
etocar	
	Servidor de normativas LiveCycle
	Bennyi informatika da munda anadada
eguridad	Borrar intormación de cuenta recordada
eguridad ogwided (mejorada)	bond information de catina recordada
eguridad ogwided (mejorada) ervicios en línea	Bonar gnormación de cacina recordada

- 6. Seleccionar la pestaña "Verificación", y en la opción "Al verificar:" marcar "Usar el método especificado en el documento. Preguntar si no está disponible".
- 7. Marcar la opción "Requerir la comprobación de revocación de certificados al comprobar firmas siempre que sea posible".
- 8. En el recuadro "Hora de verificación" seleccionar la opción "Si está disponible, hora segura (por ejemplo la marca de hora) incrustada en la firma; en caso contrario la hora actual".

Verificación Creación Integración de Wir	ndows	
Al verificar:		
<u>⊚U</u> sar el método especificado en el	documento. Preguntar si no está disponible.	
Usar el método especificado en el	documento. Usar el método predeterminado si no está disponible.	
Usar siempre el método predeterr	ninado (anula el método especificado en el documento).	
Método predeterminado para verificar fin	mas: Seguridad predet. de Adobe 🗸 🗸	
Requerir la comprohación de revocaci	ón de certificados al comprohar firmas siempre que sea posible	
Ignorar información de validación de r	documento	
Hora de verificación		
Verificar firmas mediante:		
Hora actual		
Si está disponible, hora segura	(por ejemplo la marca de hora) incrustada en la firma; en caso contrario	la hora actual
<u>H</u> ora en la que se creo la firma		
Usar marcas de hora caducada	2700	
	ur.	

- 9. Pulsar "Aceptar" para cerrar la ventana de "Preferencias avanzadas de las firmas digitales", y de nuevo en "Aceptar" para cerrar la ventana "Preferencias".
- 10. La próxima vez que se abra el documento, se validará la firma digital automáticamente.

3.3. Verificar la validez de la Firma Digital a largo plazo en un documento PDF

Una vez que la herramienta Adobe Reader 11 se ha encargado de validar las firmas contenidas en el documento, vamos a proceder a verificar esa validez y que además el formato de firma utilizado garantice que la validez se mantenga en el tiempo o lo que se conoce como PADES LTV. A continuación se describen los pasos que hacen eso.

- 1. Abrir el documento.
- Seleccionar la ficha de firmas, eligiendo del menú principal "Ver" > "Mostrar/" > "Paneles de navegación" > "Firmas", o bien seleccionando la ficha "Firmas" que se muestra en la parte izquierda del documento.

🔁 adobe-signed-ts	2 pdf - Adobe Acrobat Pro	has not self.	A Research Towner Spectra Barriers and The
Archivo Edición	Ver Ventana Ayuda		
🗭 Crear 🔻	Rotar <u>v</u> ista		
	Navegación de página		
	Presentación de página	• 🔚 🖽	
Firmado y t	<u>A</u> mpliación/Reducción	•	
V	<u>H</u> erramientas	•	
	<u>C</u> omentario	•	
	Compartir		
	Mostrar/ocultar	Paneles de <u>n</u> avegación	🕑 🔀 Ár <u>b</u> ol modelo
	Modo lectura	Ctrl+H Elementos de la barra de herramientas	 Archivos adjuntos
	Modo Pantalla completa	Ctrl+L Barra de menús	F9 🕼 Artíc <u>u</u> los
THE	Rastreador	Reglas y cuadrículas	Capas
	Leer en voz alta	Coordenadas del cur <u>s</u> or	Contenido
	Comparar documentor		Destinos
	<u>comparar documentos</u>		Linguetas
			Eirmas
			₩ Marcadores
			L' Miniaturas de <u>p</u> ágina
			器 Ord <u>e</u> n
			Mostrar panel de navegación F4
			<u>R</u> establecer paneles

3. Se selecciona la Firma Digital que se desea verificar en la ficha de Firmas y procedemos a abrir el detalle de esa firma dando un click en el botón

obs 🛃	be-signed-	ts2.pdf	- Adob	e Re	ader						-		-	-	-	-	-	-
Archiv	o <u>E</u> dición	<u>V</u> er	Ve <u>n</u> ta	na	Ayuda													
Ģ	🔁 📝	Ŷ		0	\square		•	1 /	17		•	93,5%	•		↓	P	5	
se la companya de la	Firmado y	todas l	as firma	as so	n válidas	5.												
	Firmas											I	• •					
P	83-										Va	lidar to	das					
\sim	🕀 🦻 Re	ev. 1: F	irmado	por	MARIO	ALONS	O ALVA	REZ CO	ORDOB	A (FIR	MA)			-				
Ĭ														-				
¢Ø																		

- 4. A continuación vamos a verificar la información que nos muestra Adobe Reader 11 con la cuál garantizamos la validez de la Firma Digital contenida en el documento.
- 5. En primer lugar en la parte superior de la ficha de Firmas se va mostrar el símbolo que indica que esa Firma Digital es válida. Este mismo símbolo se muestra también al lado del nombre de la persona que firmó el documento.
- 6. Al abrir el detalle de la Firma Digital aparecen una serie de enunciados que nos confirman que la misma es válida.
 - a. Primero Adobe Reader nos indica: "La firma es válida".
 - b. También que No ha habido modificaciones en Documento desde que se firmó
 - c. Y lo más importante el documento indica: La firma está activada para LTV, esto nos garantiza que el formato de firma utilizado es PADES LTV el cuál incorpora los elementos necesarios que hacen que esa firma se mantenga válida en el tiempo sin importar cuantos años pasen.
 - d. Con estas tres características ya garantizamos la validez de la firma digital del documento en el tiempo.
 - e. Ver la siguiente imagen.



7. Cuando el documento no fue firmado utilizando el formato PADES LTV la firma digital siempre se muestra como válida, pero dicha validez caducará en un tiempo determinado. Esto sucede porque no se incluye el sellado de tiempo ni demás elementos de los formatos avanzados de Firma Digital. Podemos comprobar esto si nos muestra el enunciado "La firma no está activada para LTV y caducará después de...". Si esto ocurre se recomienda contactar al centro de soporte indicado al inicio de esta guía. Ver la siguiente imagen.

🄁 jsigr	npdf-signed.pdf - Adobe Reader	
Archiv	ro <u>E</u> dición <u>V</u> er Ve <u>n</u> tana A <u>v</u> uda	
F	Box A → A → A → A → A → A → A → A → A → A	P
E	Firmado y todas las firmas son válidas.	
C	Firmas (4) >	
	8= - Validar todas	
\sim	🗉 🚭 Rev. 1: Firmado por MARIO ALONSO ALVAREZ CORDOBA (FIRMA)	
D	La firma es válida:	
<u> </u>	No ha habido modificaciones en: Documento desde que se firmó	
4	Firmado por el usuario actual	
	La firma incluye una marca de hora incrustada, pero no se ha podido verificar.	
	La firma no está activada para LTV y caducará después de 2014/03/19 10:15:06 -06'00'	
	Detalles de la firma	
	Última comprobación: 2012.12.13 10:59:40 -06'00'	
	Campo: Signature1 en la página 1	
	Haga clic para ver esta versión	

3.4. Configurar Adobe Reader para que Confíe en el Certificado Raíz

Al abrir por primera vez un PDF firmado digitalmente se puede añadir el certificado raíz de la Jerarquía Nacional de Certificación Digital a las identidades de confianza del Adobe, de la siguiente manera:

- 1. Abrir el documento.
- Seleccionar la ficha de firmas, eligiendo del menú principal "Ver" > "Mostrar/" > "Paneles de navegación" > "Firmas", o bien seleccionando la ficha "Firmas" que se muestra en la parte izquierda del documento.

Archivo Edición	2 pdf - Adobe Acrobat Pro Ver Ventana Ayuda	the per affect	Contract Track Special Residence of the
Crear •	Rotar vista Navegación de página Presentación de página Ampliación/Reducción Herramientas <u>C</u> omentario		
F 0 9 9 0	Compartir Mostrar/ocultar Modo Igctura Ctrl+H Modo Pantalla completa Ctrl+L Rastreador Leer en vog alta Comparar documentos	Paneles de <u>n</u> avegación Elementos de la barra de herramientas <u>B</u> arra de menús <u>R</u> eglas y cuadrículas Coordenadas del curgor	 Provide Archivos adjuntos Archivos adjuntos Artículos Capaş Contegido Destinos Entretor
			 ✓ Birnas ✓ Marcadores ○ Miniaturas de gágina ☑ Ordgn ✓ Mostrar panel de navegación F4 Restablecer paneles

Seleccionar la firma (se mostrará el icono o uno similar, junto a la firma para indicar que la identidad del firmante es desconocida porque no se ha incluido en la lista de identidades de confianza y ninguno de sus certificados principales es una identidad de confianza).

🔁 BOE	-A-2008	8-174	481.	pdf -	A do
Archivo	Edición	Ver	Docu	imento	He
8	•	G	0		₽
	Está vienc	lo est	e docu	umento	en n
ľ	Firmas				•
7	٠.		Valida	ar toda	s
	± 强 ∎	tev. 1	: Firn	nado (>

4. Una vez seleccionada la firma, pulsar el botón derecho del ratón y elegir la opción "Mostrar propiedades de la firma..." del menú que se despliega. Se abrirá la ventana "Propiedades de la firma", en la que se muestran varias pestañas. Elegir la primera ("Resumen") y pulsar el botón "Mostrar certificado ..."

ropiedades	de la firma
La va	idez de la firma es DESCONOCIDA.
Resumen	ocumento Firmante Fecha y hora Legal
Eirmado po	r: DESCRIPCION SERVICIO DE FIRMA DE DIARIOS OFICIALES Mostrar certificado
M <u>o</u> tiv	0:
Fech	a: 2008/12/15 11:25:02 +01'00'
Resumer	i de validez
S No) ha habido modificaciones en: Documento desde que se firmó.
🚰 La de	i identidad del firmante es desconocida porque no se ha incluido en la lista de identidades 2 confianza y ninguno de sus certificados principales es una identidad de confianza.
🔥 Lā	rfecha y hora de la firma proceden del reloj del equipo del firmante.

 Se abrirá una nueva ventana, "Visor de certificados", en la que se muestra en el panel de la izquierda la lista de certificados que componen la ruta de certificación completa. Seleccionar el certificado raíz CA RAÍZ NACIONAL – COSTA RICA (el primero en la jerarquía).

Certificate Viewer				
This dialog allows you correspond to the sele Show all certification	to view t ected ent n paths fo	t he details of a cer t ry. bund	tificate and its entire issuance chain. The details	
	AL - CC	Summary Detai	Is Revocation Trust Policies Legal Notice	
CA SINPE - MARIO	PERSOF PERSC ALON:		CA RAIZ NACIONAL - COSTA RICA	
		Issued by		
			MICIT	
		Valid from	: 2008/11/14 18:19:55 -06'00'	
		Valid to	: 2045/11/14 18:28:21 -06'00'	
		Intended usage	Sign transaction, Sign CRL, Sign certificate (CA)	

6. Seleccionar la pestaña "Confianza" y pulsar el botón "Agregar identidades de confianza ..."

Certificate Viewer	×
This dialog allows you to view t correspond to the selected en	he details of a certificate and its entire issuance chain. The details ry.
Show all certification paths fo	ound
CA RAIZ NACIONAL - CC	Summary Details Revocation Trust Policies Legal Notice
CA SINPE - PERSC MARIO ALON:	This certificate is directly trusted in your trusted identities list.
	This certificate is set as a trust anchor, the result being that this certificate and all certificates issued beneath this certificate are trusted to: Sign documents or data
	Certify documents
	Execute dynamic content that is embedded in a certified document
	Execute high privilege JavaScripts that are embedded in a certified document
	Perform privileged system operations (networking, printing, file access, etc.)
	Revocation checking is not performed for this certificate because it is directly trusted as a trust anchor.
	Add to Trusted Identities

7. Se abre una nueva ventana, "Importar configuración de contactos", en ella, marcar en la sección
 "Confianza" la casilla "Utilizar este certificado como raíz de confianza"

rtificate	Details
ubject:	CA POLITICA PERSONA FISICA - COSTA RICA
suer: (CA RAIZ NACIONAL - COSTA RICA
sage:	Sign transaction, Sign certificate (CA), Sign CRL
piratio	n: 04/12/2025 11:10:16 p.m.
Trust]
A cer root i on or	tificate used to sign a document must be a trusted root or be issued by a trusted n order for signature validation to succeed. Revocation checking is not performed above a trusted root.
A cer root i on or	tificate used to sign a document must be a trusted root or be issued by a trusted n order for signature validation to succeed. Revocation checking is not performed above a trusted root.
A cer root i on or Us	tificate used to sign a document must be a trusted root or be issued by a trusted n order for signature validation to succeed. Revocation checking is not performed above a trusted root. This certificate as a trusted root gnature vanuation succeeds, trust this certificate for:
A cer root i on or Us	tificate used to sign a document must be a trusted root or be issued by a trusted n order for signature validation to succeed. Revocation checking is not performed above a trusted root. This certificate as a trusted root gnature vanuation succeeds, trust this certificate for: Signed documents or data Certified documents
A cer root i on or Us	tificate used to sign a document must be a trusted root or be issued by a trusted n order for signature validation to succeed. Revocation checking is not performed above a trusted root. This certificate as a trusted root gnature vanuation succeeds, trust this certificate for: Signed documents or data Certified documents
A cer root i on or Us If si	tificate used to sign a document must be a trusted root or be issued by a trusted in order for signature validation to succeed. Revocation checking is not performed above a trusted root. This certificate as a trusted root gnature vanoauon succeeds, trust this certificate for: Signed documents or data Certified documents Dynamic content Embedded high privilege JavaScript

8. Pulsar "**Aceptar**" para cerrar la ventana "Importar configuración de contactos" y de nuevo "**Aceptar**" en la ventana "Visor de certificados".

4. INSTALAR LOS CERTIFICADOS DE LA CA RAÍZ NACIONAL

Para poder utilizar y verificar correctamente la firma digital de los documentos de Word 2010, debe registrar en su computadora los certificados de la CA Raíz Nacional.

Estos certificados están disponibles en los siguientes enlaces:

- Certificado de la Autoridad Certificadora Raíz:
 http://www.firmadigital.go.cr/repositorio/CA RAIZ NACIONAL COSTA RICA.crt
- Certificado de la Autoridad Certificadora de Política de Persona Física:
 http://www.firmadigital.go.cr/repositorio/ca politica persona fisica costa rica.crt
- Certificado de la Autoridad Certificadora Intermedia SINPE Persona Física
 http://fdi.sinpe.fi.cr/repositorio/CA_SINPE PERSONA_FISICA.crt

A continuación se describen los pasos que debe seguir para instalar los certificados de la cadena de confianza de la jerarquía nacional.

- 1. Pulse los enlaces para cada uno de los certificados mencionados anteriormente.
- 2. Se abrirá una ventana similar a la que se muestra a continuación, preguntando si desea abrir el archivo o guardarlo en su equipo, pulse el botón "Abrir".



3. A continuación se mostrará una ventana con los datos del certificado, seleccione la pestaña "General" y pulse el botón "Instalar certificado ..."

Certificado
General Detalles Ruta de certificación
Información del certificado
Este certif. está destinado a los siguientes propósitos: • Todas las directivas de emisión • Todas las directivas de la aplicación
Emitido para: CA RAIZ NACIONAL - COSTA RICA
Emitido por: CA RAIZ NACIONAL - COSTA RICA
Válido desde 14/ 11/ 2008 hasta 14/ 11/ 2045
Instalar certificado Declaración del emigor Obtener más información acerca de <u>certificados</u>
Aceptar

4. Se abrirá una nueva ventana con el "Asistente para importación de certificados", pulse el botón "Siguiente" en este paso y en el paso posterior, y finalmente el botón "Finalizar". Tras este último paso se mostrará un mensaje indicando que la importación se realizó correctamente.

Asistente para importación de	e certificados
	Éste es el Asistente para importación de certificados Este asistente le ayuda a copiar certificados, listas de certificados de confianza y listas de revocación de certificados desde su disco a un almacén de certificados. Un certificado, que se emite por una entidad de contiene información que se una para proteger datos o para establecer conexiones de red seguras. Un almacén de certificados es el área del sistema donde se guardan los certificados.
	< <u>A</u> trás Siguiente > Cancelar

Alma	én de certificados
0	os almacenes de certificados son las áreas del sistema donde se guardan los ertificados.
V P	índows puede seleccionar automáticamente un almacén de certificados; también se uede especificar una ubicación para el certificado.
	 Seleccionar automáticamente el almacén de certificados según el tipo de certificado
	Colocar todos los certificados en el siguiente almacén
	Almacén de certificados:
	Examinar
ás in	formación acerca de los <u>almacenes de certificados</u>
	< <u>A</u> trás Siguien <u>t</u> e > Cano

Asistente para importación de c	ertificados 🗾 🔀
	Finalización del Asistente para importación de certificados
	Se importará el certificado después de hacer clic en Finalizar.
	Especinico la siguiente configuradion: Almacén de certificados seleccionado Contenido Certificado
	۲ III ا
	< <u>A</u> trás Finalizar Cancelar



5. Pulse el botón "Aceptar" de la ventana que muestra la información del certificado para cerrarla.

Certificado
General Detalles Ruta de certificación
Información del certificado
Este certif. está destinado a los siguientes propósitos:
Iodas las directivas de emisión Todas las directivas de la aplicación
Emitido para: CA RAIZ NACIONAL - COSTA RICA
Emitido por: CA RAIZ NACIONAL - COSTA RICA
Válido desde 14/ 11/ 2008 hasta 14/ 11/ 2045
Instalar certificado Declaración del emigor
Obtener más información acerca de <u>certificados</u>
Aceptar

 Pulse el enlace para los certificados: "Autoridad Certificadora de Política de Persona Física" y "Autoridad Certificadora Intermedia SINPE – Persona Física" y repita los pasos del 2 al 5 para instalar estos nuevos certificado.

Si ha optado por guardar los certificados en su disco, haciendo doble click sobre cada uno de los archivos se mostrará la ventana del paso 4, y podrá seguir con el resto de pasos hasta importar el certificado.

5. INFORMACIÓN Y SOPORTE

Si desea obtener información sobre esta guía u otras del uso de Firma Digital, así como, obtener soporte técnico se debe comunicar a:

- Ministerio de Ciencia y Tecnología
- Dirección de Certificadores de Firma Digital
- Teléfono: 2248-1515 ext. 232
- Correo electrónico: <u>firmadigital@micit.go.cr</u>
- <u>www.firmadigital.go.cr</u>
- <u>www.soportefirmadigital.com</u>