Instructivo General

Validación de Firma Digital









Validación de Firma Digital

Los requisitos para verificar la firma digital de un documento son:

- Tener instalada la última versión de Java. Para corroborar la versión ver la sección Verificación de Java (pág. 8)
- Tener el documento firmado en formato digital (pdf, word)
- En caso de un documento Word, se debe tener el digesto firmado (archivo .pki) guardado en la misma carpeta que el documento original

Los **pasos** que se deben seguir para validar un documento firmado digitalmente son:

1. Ingresar al portal de PKI (http://www.pki.sanluis.gov.ar) y seleccionar la opción *"Servicios"*. Luego hacer clic en *"Validación de documentos firmados digitalmente"*.

fir		TITUTO DE FIRMA DIGITAL LA PROVINCIA DE SAN LUIS		San Luis, Jueves 23	3 de Octubre de 2014
INICIO	REGISTRO DE PROVEEDORES	INSTITUTO DE FIRMA DIGITAL	MARCO LEGAL	DESCARGA DE CERTIFICADOS	SOPORTE SERVICIOS
Consulta Certificad Agentes o Cambiar de Solicitar un Renovar un Renovar un Lista de Ce Certificados Certificados Mis tramaes	as y Trámites lo de Firma Digital para del Estado Provincial Política Certificado Digital O Certificado Digital O Certificado Digital O Certificado Digital O Certificado S Revocados S Migentes	Servicios Seleccione el servicio que desea utilizar: <u>Firma de Documentos Digitales</u> • Esta herramienta le permitirá firmar dig única acción de firma. Obteniendo como com ubicación de origen de cada archivo. Excepto archivo que firmó, sin posibilidad de eliminant, • Asimismo le permite firmar más de una pretendidas, obtendrá como consecuencia de el ubicación original de cada archivo Recuerde tener conectado el dispositivo seleccionado el archivo o los archivos selección del Carthicad y el ingreso de estimado en firmar un archivo varia en m <u>Encriptar Documentos Digitales</u> • Esta herramienta le permitirá encriotar l	pitalmente uno o varios secuencia de ello el dige los archivos ".pdf, los c a después de firmado vez los archivos que de ello el digesto firmado d criptográfico donde se desde su ordenador, i su clave o contraseña, elación al tamaño del ar os documentos dioitales	archivos de cualquier extensión a través esto firmado de cada uno de los archivo usales generan la firma incrustada en el e cada firma de cada uno de los archivo encuentra almacenada su firma, una v presione firmar, el sistema le pedirá al terminar presione finalizar El tiem chivo	Firma de documentos digitales Validación de documentos firmados digitalme Encriptar Documentos Digitales Desencriptar Documentos Digitales
Autoridades	s de Registro	 Esta herramienta le permitirà encriptar los documentos digitales para conservar su privacidad, su contenido solo podrá ser visto por quien posea la clave privada para desencriptar este archivo. <u>Desencriptar Documentos Digitales</u> 			
Requisitos certificado	: para implementar s	Esta herramienta le permitirá desencrip los mismos con su clave privada. <u>Validar Documentos Firmados Digitalmen</u> Esta herramienta le permitirá a través de ur pública con los que se firmó ese documen documento	tar los documentos digit <u>te</u> na única acción: verificar ito, asimismo podrá u	ales que haya recibido, solo podrá dese la validez de uno o varios certificados c na vez validada una firma, firmar el	encriptar de clave mismo

2. La primera vez que se usa la aplicación, aparecerá un mensaje de seguridad, en el cual se debe hacer clic en la opción *"Ejecutar"*. Para que no aparezca más el mensaje, se debe tildar la opción *"No volver a mostrar esto otra vez para aplicaciones del publicador y ubicación anteriores"*.









3. Posteriormente, comenzará a cargarse la aplicación:

	TITUTO DE FIRMA DIGITAL LA PROVINCIA DE SAN LUIS	San Luis, Viernes 24 de Octubre de 2014
INICIO REGISTRO DE PROVEEDORES	INSTITUTO DE FIRMA DIGITAL MARCO LEGAL	DESCARGA DE CERTIFICADOS SOPORTE SERVICIOS
Consultas y Trámites Certificado de Firma Digital para Agentes del Estado Provincial	Validar documentos firmados digitalmente	Firma de documentos digitales Validación de documentos firmados digitalmente
Cambiar de Política Solicitar un Certificado Digital		Encriptar Documentos Digitales Desencriptar
Renovar un Certificado Digital Revocar un Certificado Digital Lista de Certificados Revocados		Documentos Digitales
Certificados Emitidos Certificados Vigentes		
Mis tramites Autoridades de Registro	Java	
Requisitos para implementar certificados		







Servicio de Validación de Firma digital

Instituto de Firma Digital de la Provincia de San Luis

4. Una vez que se cargó la aplicación, hacer clic en el botón "Seleccionar el archivo".

	ITUTO DE FIRMA DIGITAL A PROVINCIA DE SAN LUIS	San Luis, Viernes 24	le Octubre de 2014
INICIO REGISTRO DE PROVEEDORES	INSTITUTO DE FIRMA DIGITAL MARCO LEGAL	DESCARGA DE CERTIFICADOS	SOPORTE SERVICIOS
Consultas y Trámites Certificado de Firma Digital para Agentes del Estado Provincial Cambiar de Política Solicitar un Certificado Digital Renovar un Certificado Digital Revocar un Certificado Digital Lista de Certificados Revocados Certificados Vigentes Mis tramites Autoridades de Registro	Validar documentos firmados digitalmente Seleccionar Archivo Agregar el digesto firmado Eliminar digesto Archivos	Validar y firmar Validar	Firma de documentos digitales Validación de documentos firmados digitalmente Encriptar Documentos Digitales Desencriptar Documentos Digitales

5. Luego, buscar el archivo firmado en la carpeta donde el mismo fue guardado.

🛓 Seleccionar			— X—
Buscar en:	Documentos) 📸 🖬 🕶
Elementos recientes	Chromeinstall-70 Documento para Documento para ListaRevocados	u67 a validar a validar.docx.RAMOS NATALIA BEATRIZ (FIRMA).pki	
Escritorio	🔁 Servicio Firmar o	de Documento Digital	
Mis documentos			
Equipo			
	Nombre de archivo:	Documento para validar.docx	Seleccionar
Red	Archivos de tipo:	Todos los Archivos 🗸	Cancelar







6. Al seleccionar el archivo, el mismo aparecerá en la aplicación de validación de firma. En caso de los archivos Word, el digesto .pki se incorpora automáticamente en la aplicación. Luego hacer clic en el botón "Validar".

Validación de documentos f	irmados digitalmente
Seleccionar Archivo	
Agregar el digesto firmado	Eliminar digesto
Archivos C: \Users \ULP \Documentos \Docum	ento para validar.docx.RAMOS NATALIA BEATRIZ (FIRMA).pki
	Validar y firmar Validar

En el caso de querer validar un archivo en formato .pdf, la firma queda incrustada dentro de mismo archivo PDF y NO se adjunta otro documento con extensión .pki. A continuación se muestra dicho caso:

Validación de documentos firmados digitalmente				
Seleccionar Archivo				
Servicio Firmar de Documento Digital.pdf				
Agregar el digesto firmado	Eliminar digesto			
Archivos				
	Valid	ar y firmar 🛛 Validar 🌘		







 Al momento de hacer la validación, si el documento original y/o su archivo de firma no sufrieron modificaciones, se muestra una ventana indicando que la *"Firma es válida"*. Se pueden agregar más archivos para validar.

Validación de documentos firmados digitalmente Archivo validado Documento para validar.docx Resultado de la validación de firmas:			
Firmante	Resultado	Estado del certificado	
RAMOS NATALIA BEATRIZ (FIRMA)	La firma es válida	Vigente	
			Validar más archivos

El icono permite ver información del certificado digital que firmó el documento. En la *solapa "Detalles"* se muestran los datos del certificado digital con el cual se firmó el documento.







Servicio de Validación de Firma digital Instituto de Firma Digital de la Provincia de San Luis

⁷ La firma es válida.	🧹 La firma es vá	lida.
eneral Detalles	General Detailes	
Información del certificado	Campo Version	Valor 3
	Número de serie	54 21 00 39 00 01 00 00 12 c6
ste certificado esta destinado a los siguientes propositos:	Emisor	C=AR,O=Gobierno de la provincia
[1.3.6.1.5.5.7.3.4, 2.16.32.1.3.2.1.1.1]	Valido desde Valido hasta	02/12/2013 09:51 02/12/2015 10:01 ST-San Luis O-Liniversidad de La
	Clave pública Identificador de clave entidad	30 81 9f 30 0d 06 09 2a 86 48 86 f emisora 09 55 d1 f1 0e 19 9d aa e4 a0 20 f
Enviado a: Alaniz Luis Ramiro	Punto de distribución CRL Acceso a la información de ent	Punto de distribución CRL Nombre idad [1]Acceso a información de autorid
Emitido por CA del IFDPSL como CL	ST=San Luis O=Universidad de L OU=Instituto de Fi	a Punta rma Digital de la Provincia
Válido desde 02/12/2013 09:51 hasta 02/12/2015 10:01	E= @ulp.edu.	ar
La hora de la firma procede del reloj del equipo del firmante.	C=AK SERIALNUMBER=DU CN=	
	4	m

8. En caso de que la firma no sea válida, ya sea porque se modificó el documento original o porque el archivo de firma no es el correcto, se muestra una ventana indicando que la *"Firma no es válida"*.

Archivo validado Documento para validar.docx				
Resultado de la validación o	de firmas:			

IMPORTANTE: El proceso de validez de firma, por un lado aplica al documento original el algoritmo Hash, y por otro descifra el archivo firmado con la clave pública del firmante que está contenida en el archivo .pki. Luego se comparan estos resultados y si ambos coinciden se deduce que la firma es válida, caso contrario no se debe confiar en la integridad del documento original.







Verificación de Java

1. Ingresar al "Panel de Control", opción "Programas" y seleccionar "Java".



2. Presionar el botón "Acerca de" para ver la versión de Java instalada en su máquina.

	💁 Panel de Control de Java
1	General Adtualizar Java Seguridad Avanzado
	Acerca de Consulte la información sobre la versión del panel de control de Java. Configuración de Red La configuración de red se utiliza cuando se establece la conexión a Internet. Java utilizará por defecto la configuración de red del explorador web. Esta configuración sólo debe ser modificada por usuarios con conocimientos avanzados.
	Configuración de Red Archivos Temporales de Internet Los archivos utilizados en las aplicaciones de Java se guardan en una carpeta especial para acelerar su ejecución posterior. Sólo los usuarios con conocimientos avanzados deberían suprimir archivos o modificar esta configuración.
	Configuración Ver
	Aceptar Cancelar Aplicar





8



Servicio de Validación de Firma digital Instituto de Firma Digital de la Provincia de San Luis



3. En caso de tener una versión anterior a la última disponible, se debe presionar el botón *"Actualizar Ahora"* en la solapa *"Actualizar"*.

🛓 Panel de	Control de Java		
General Ad	ualizar Java Seguridad Avanzado	2	
(il)	El mecanismo de actualización de Java plataforma Java. Las opciones siguien aplicar las actualizaciones.	le garantiza que tendrá la úl tes permiten controlar la forr	tima versión de la na de obtener y
	Recibir notificación:	Antes de la descarga	
	Comprobar Actualizaciones Autor	náticamente	Avanzadas
	Java Update comprobará las actualiza las 09:00. Si se recomienda alguna ac notificaciones de la barra de tareas de el estado de la actualización.Se le noti Normalmente recibirá la notificación so su publicación. Sin embargo, si una act notificación dentro de la semana siguie	ciones al menos una vez en s tualización, aparecerá un ico I sistema. Sitúe el cursor sob ficará antes de descargar la bre las actualizaciones dentr tualización se considera crític ente a su publicación.	emana los domingo a no en el área de re el icono para ver actualización. o del mes siguiente a a, recibirá una
	Última ejecución de Java Update: 11:3	36, día 16/08/14.	Actualizar Ahora
		Aceptar Can	celar Aplicar







4. Luego comenzará la descarga correspondiente. En caso de que el icono de Java no esté visible desde el Panel de Control es porque la misma no está instalada y se deberá descargar la versión disponible desde el sitio <u>www.java.com</u>.

Una vez que se descargó el archivo, se debe hacer doble clic sobre el mismo y presionar el botón "*Ejecutar*". La aplicación comenzará su descarga.





5. A continuación hacer clic en "Siguiente".









Servicio de Validación de Firma digital Instituto de Firma Digital de la Provincia de San Luis

Configuración de Java - Restaurar peticiones de datos de seg	guridad
👙 Java [.]	ORACLE
Restaurar peticiones de datos de segurida	ad de Java
Algunas peticiones de datos de seguridad de Jav seleccionar la opción 'No volver a mostrar'. Puede de su información personal restaurando estas peti 30 días.	a se han ocultado al e mejorar la seguridad ciones de datos cada
Más Información	
Restaurar peticiones de datos de seguridad de Java	
	Siguiente >

6. Una vez que Java se instaló, se mostrará un mensaje indicando que la operación fue concretada.







