MANUAL DE CONFIGURACIÓN ADOBE ACROBAT READER

Andes SCD S.A.

(2017)

Tabla de contenido

Integridad. 2

No repudio....2

Autenticidad. 2

3. REQUERIMIENTOS TÉCNICOS MÍNIMOS. 2

Permisos: 2

Hardware: 2

Software 3

Versiones de Office soportadas....3

¿Qué es un dispositivo Token? 3

Conexión a Internet: 3

4. PROCEDIMIENTO 3

Firma de documentos en Adobe Reader. 3

¿Cómo firmar?: 4

- 4.1. Firma visible: 4
- 4.2. Firma Invisible: 6

5. Configurar los certificados de Entidades de confianza el repositorio de Adobe Acrobat 6

1. ALCANCE

Este manual de usuario describe el procedimiento para configurar los certificados de Entidades de confianza el repositorio de Adobe Acrobat Reader.

Un certificado de firma digital debe ser reconocido como emitido por un prestador de servicios de certificación que cumple los requisitos establecidos en la normativa vigente, tal como dispone la ley, Los distintos programas lectores de ficheros PDF, navegadores de Internet y sistemas operativos van incorporando a Entidades de confianza en su repositorio, o realizan la validación de los certificados de

firma digital por medio de la OSCP, para inclusión de estos en Adobe Reader ,se detalla a continuación la forma de incorporar a una entidad como emisor de confianza, para que se pueda realizar el procedimiento de comprobación de la vigencia del citado certificado digital.

2. DEFINICIONES

El proceso de firma digital es equivalente en el mundo electrónico a la firma manuscrita, el propósito de esta es sustituir la exigencia del documento físico por su equivalente funcional como lo es el documento electrónico que proporciona los siguientes atributos:

Integridad.

El sistema permite verificar que un documento firmado digitalmente no ha sido modificada o alterado durante su viaje por la red.

No repudio

El autor está obligado mediante la firma digital del mensaje de datos a reconocer tanto su autoría como el contenido del mismo.

Autenticidad.

Jurídicamente un mensaje de datos firmado se constituye en plena prueba y es equivalente en el mundo digital al documento físico firmado y autenticado ante notario público.

3. REQUERIMIENTOS TÉCNICOS MÍNIMOS.

Permisos:

- Se requieren privilegios de usuario administrador para realizar la instalación de drivers correspondientes a los dispositivos token que se requieran.

Hardware:

- 5 Mb de espacio libre en disco de almacenamiento.
- 256 Mb de Memoria RAM
- Puerto USB (para dispositivos token físicos)

Software:

- Windows XP, Windows 2000, Windows ME, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10.

Versiones de Office soportadas

- Adobe Reader 8
- Adobe Reader 9
- Adobe Reader X
- Adobe Reader XI
- Adobe Reader X Standard
- Adobe Reader DC
- Adobe Acrobat Pro X

¿Qué es un dispositivo Token?

Un Token es un dispositivo criptográfico USB que permite custodiar los datos de creación de firmas digitales. El Token posee una clave de activación (PIN) que debe ser suministrada para hacer uso de las claves privadas, la clave de activación debe ser de uso exclusivo del suscriptor para garantizar que los datos de creación de firma están protegidos contra la utilización de terceros.

Conexión a Internet:

Esta es requerida para la verificación del estado del certificado utilizado para firma asegúrese que su ordenador cuneta con los recursos de red adecuados para comunicarse por internet.

4. PROCEDIMIENTO

Firma de documentos en Adobe Reader.

Una vez terminado el documento que se desea firmar digitalmente se deben tener en cuenta las siguientes premisas:

- Para iniciar el proceso de firma el documento deberá ser guardado previamente.
- Una vez firmado el documento quedará marcado como final y no debe modificarse.

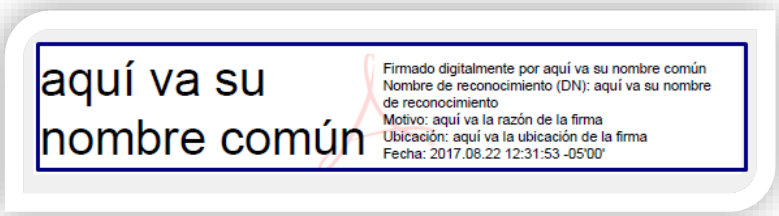
- Si se modifica el documento este perderá la marca de firma y se eliminará la firma digital.
- Este proceso se realiza de la misma manera en toda la suite de Adobe Reader.

¿Cómo firmar?:

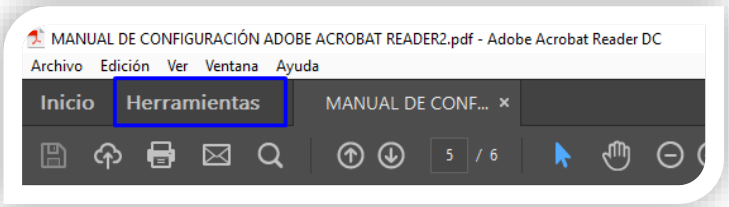
Para realizar el proceso de firma de documentos en Adobe Reader se puede elegir entre dos métodos que permiten tener una apariencia diferente en la presentación del documento.

- 4.1. Firma visible:

Es un método que permite mostrar una imagen asociada a la firma, por ejemplo:



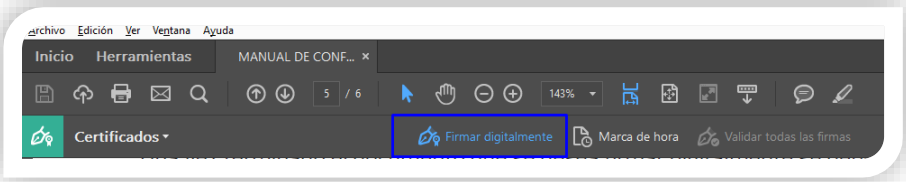
En la parte superior izquierda encontrara la pestaña de herramientas



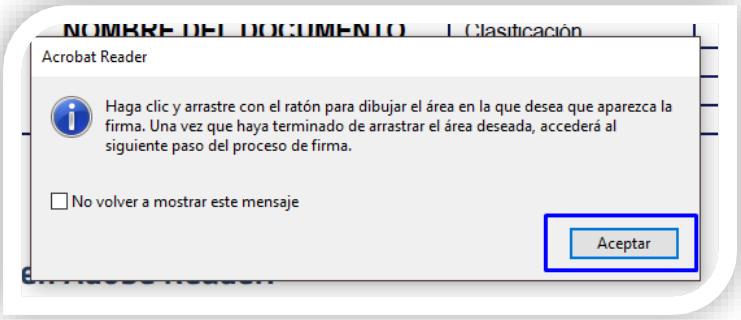
En esta sección se encuentra el icono de certificados, de clic sobre ella.



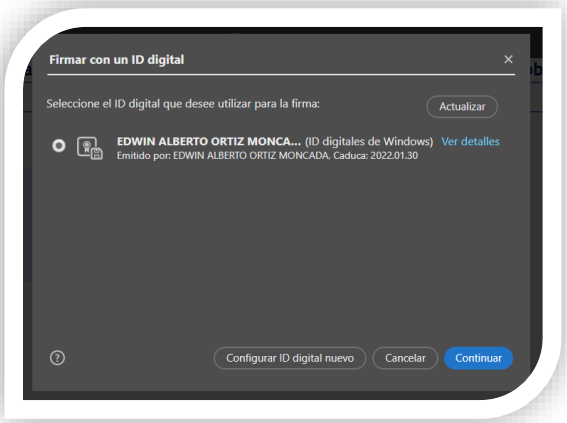
En la barra de herramientas aparece habilitada una sección llamada certificados en la que encuentra tres herramientas, seleccionamos, firmar digitalmente.

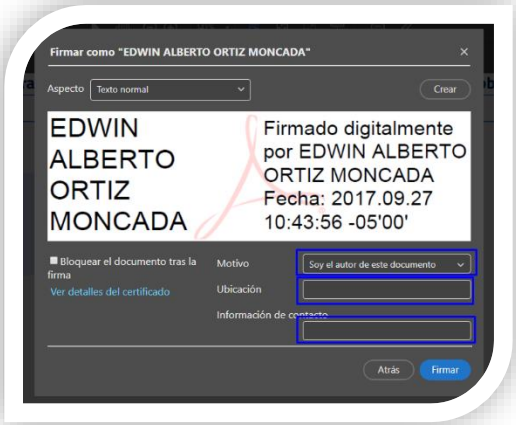


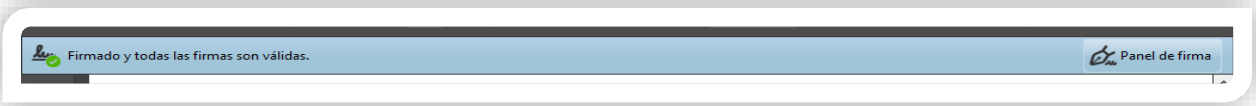
Se habilita un cuadro de dialogo donde le indica que debe realizar un cuadro con el mouse en el lugar que desea que aparezca la firma.



Realice el recuadro del tamaño que desea y en la posición que considere adecuada, hecho esto aparecerá una ventana donde podrá elegir entre los certificados disponibles en el repositorio de Windows.





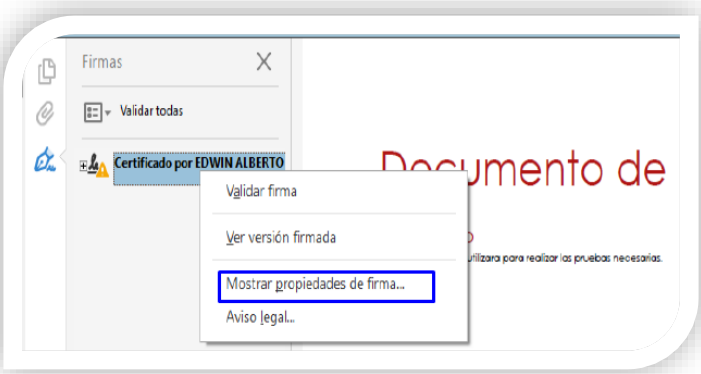


- 4.2. Firma Invisible:

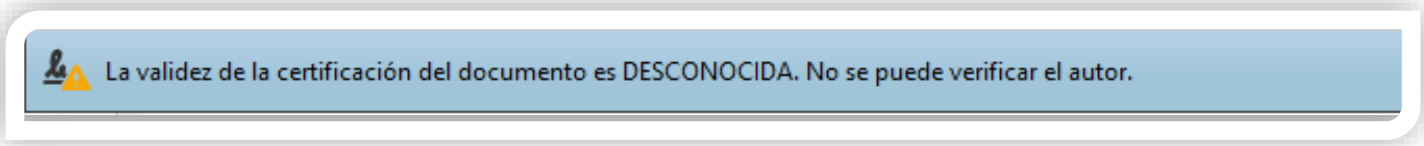
En este método no se altera la composición del documento ya que no genera marcas visibles en este; para poder realizar la utilización de este método es necesario contar con las versiones PRO de Acrobat.

Este manual de usuario describe el procedimiento para configurar los certificados de Entidades de confianza el repositorio de Adobe Acrobat Reader.

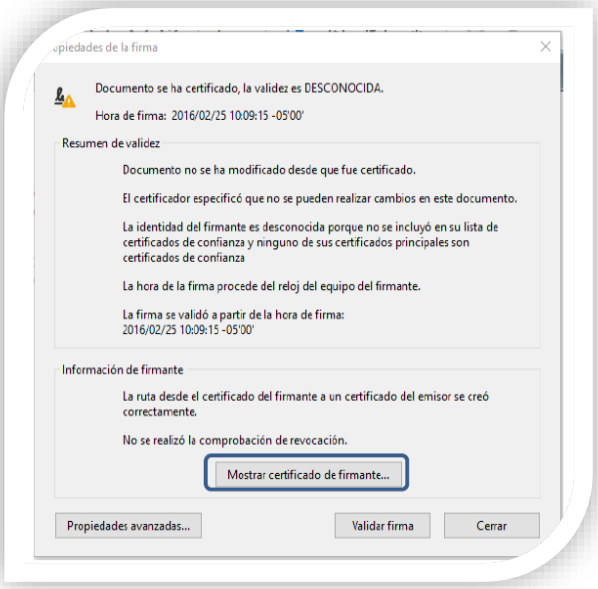
5. Configurar los certificados de Entidades de confianza el repositorio de Adobe Acrobat



Al abrir un PDF firmado, Adobe Reader nos indica "Hay al menos una firma que presenta problemas", visible en el Panel de firma y en los sellos de firma (si existen). Esto es debido a que Adobe Reader no Cene como emisor de confianza a la Autoridad de Certificación que emitió el certificado.

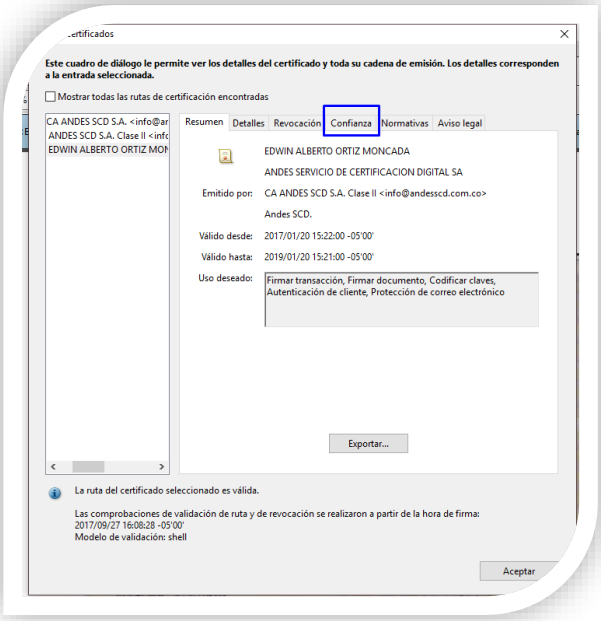


Para solucionarlo, se configura Adobe Reader para que confíe en el emisor del certificado. Pulsamos botón derecho del ratón sobre la firma, y seleccionamos "Mostrar propiedades de firma".



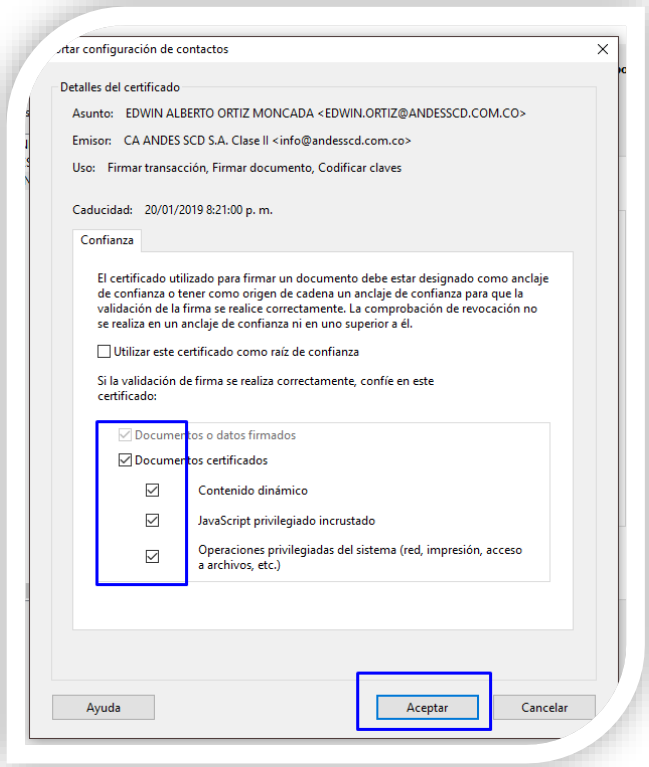
Se abre una ventana con las "Propiedades de la firma", se muestra el detalle de la información de firma. Pulsamos en el botón "Mostrar certificado del firmante".

A continuación, se abre el Visor de certificados. A la izquierda vemos el emisor del certificado y el detalle del certificado. Abrimos la pestaña "Confianza", donde vemos que "Este certificado no es de confianza" (éste es el origen del problema). Pulsamos en "Agregar a certificados de confianza".



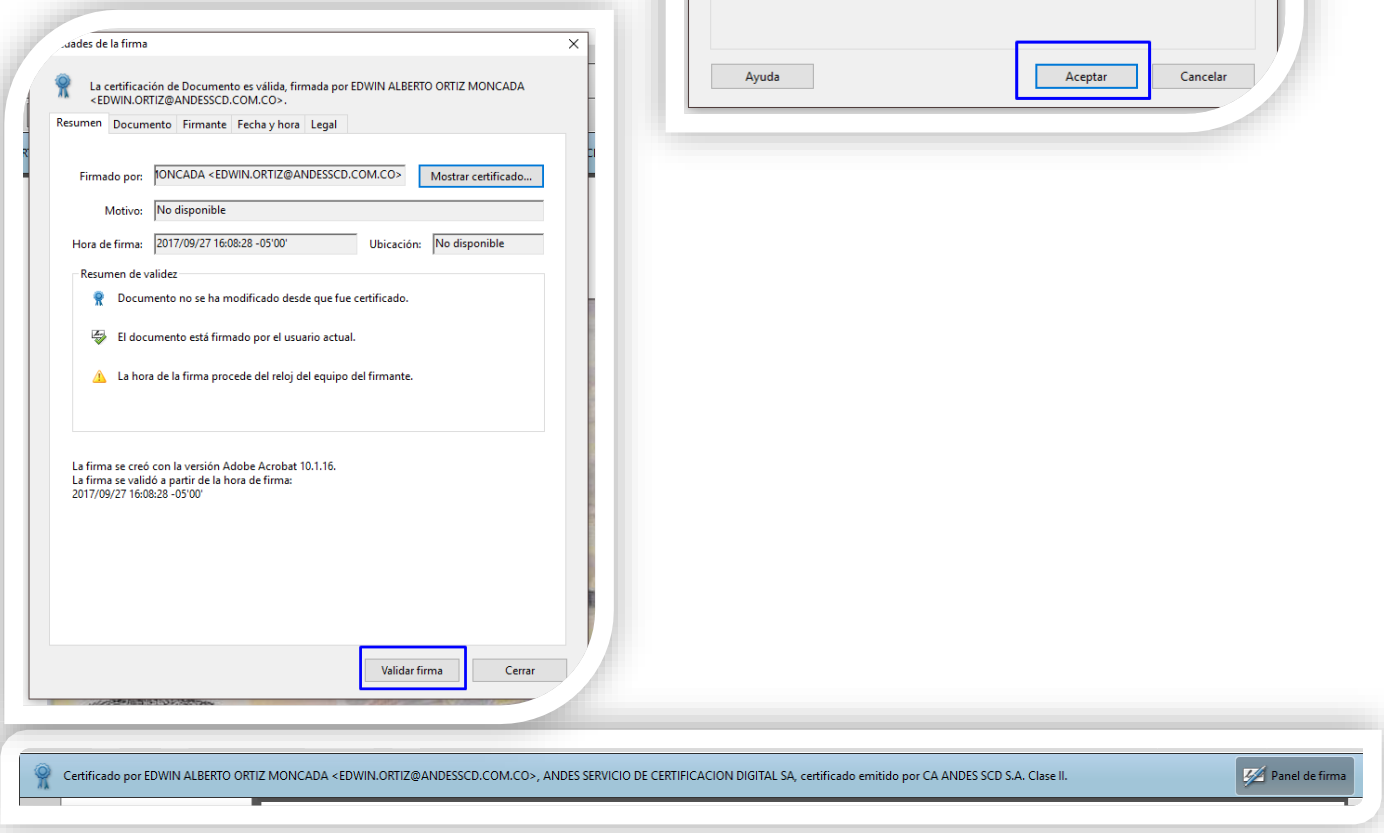
Es posible que Adobe Acrobat nos muestre un mensaje de alerta después de pulsar el botón anterior. Procedemos a pulsar en "Aceptar".

seleccionamos las casillas de verificación que aparecen en blanco y luego “Aceptar”

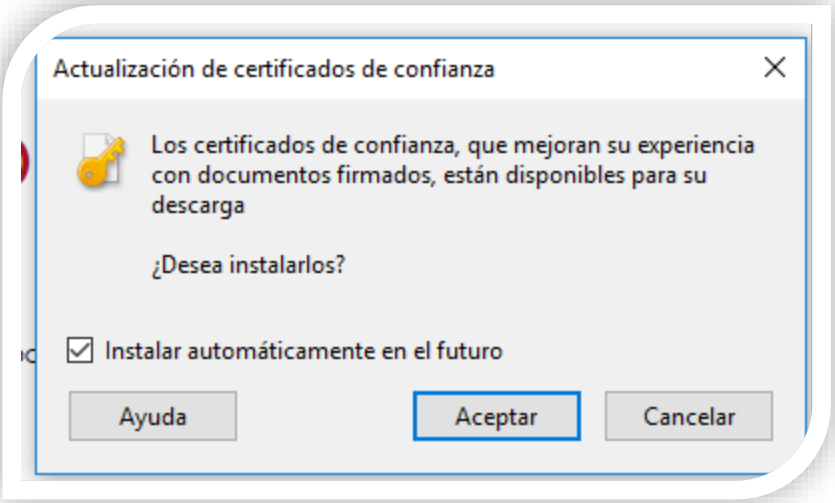


Nota: Este proceso solo se debe realizar una única vez y se debe realizar únicamente con los certificados de ROOT y CLASE II

Al validar nuevamente el certificado nos mostrara que es un certificado valido y el estado actual del documento, y nos mostrara la barra azul en la parte superior del documento

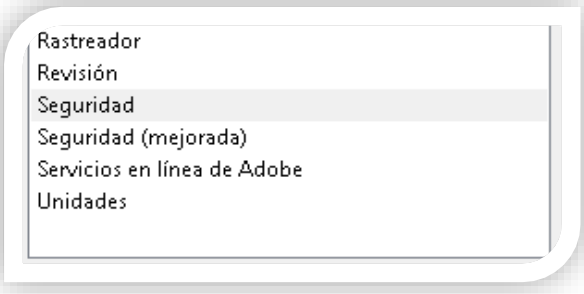


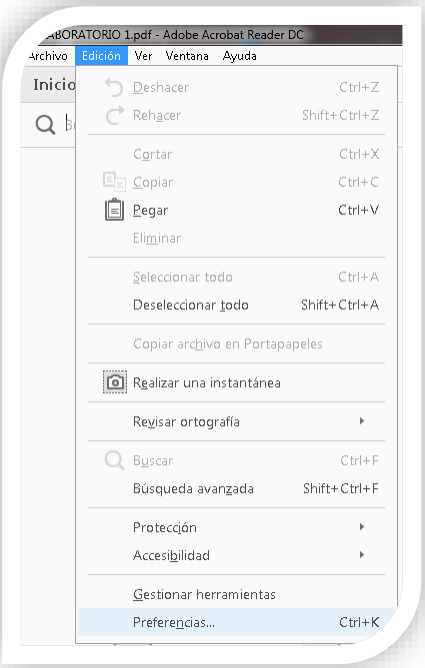
En las nuevas versiones de Acrobat en el moneto de abrir un documeto que contenga firmas digitales validas aparecerá un mensaje solicitando permisos para agregar los certificados de confianza de la entidad emisora del certificado.

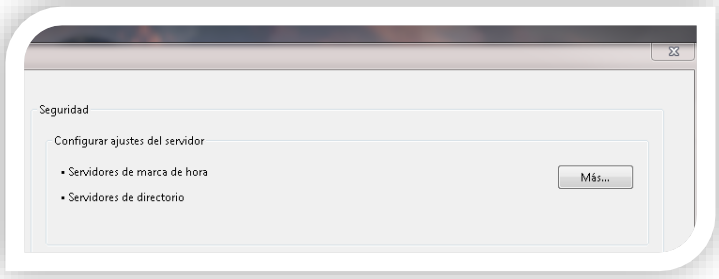


6. CONFIGURACIÓN DE ESTAMPAS DE TIEMPO

- Abra Acrobat Reader y en la barra de herramientas ingrese a menú y luego preferencias.
- En categorías encontrara la sección de seguridad, servidores de marca de tiempo, seleccione Más.

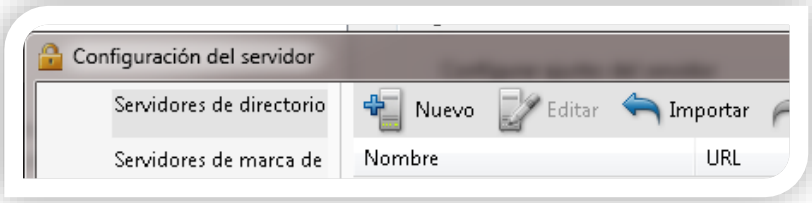


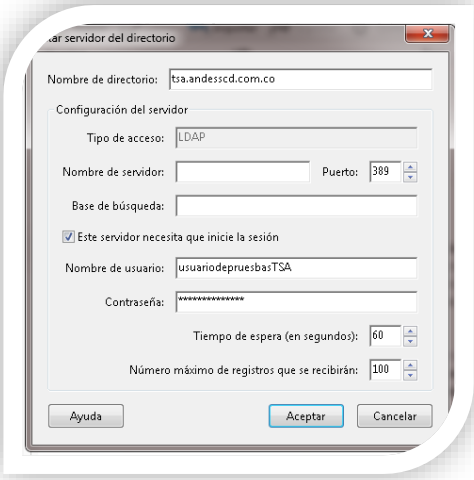




- En nuevo podrá adicionar los datos necesarios.

- Complete los datos solicitados y de aceptar





Al terminar esta configuración todos los documentos que se firmen digitalmente, quedaran también con firma de estampa de tiempo y se verá reflejado en el campo de la hora que muestra el estado del documento.

Actividad	Detalle	Responsable	Registro

Control de Cambios

Versión	Fecha	Detalle	Responsable

7. Firmas

Elaboración	Revisión	Aprobación