

Manual de Usuario Cliente

Ares Cloud 3.0



Versión
001

Fecha
01-11-21

Código
POP-MN-14

Tabla de Contenido

ARES CLOUD 3.0	1
1 INICIO DE SESIÓN	4
2 DASHBOARD DE ARES CLOUD 3.0	6
3 ENTIDAD DE CERTIFICACIÓN DIGITAL (ECD)	7
4.1 ADMINISTRACIÓN DE LA ENTIDAD DE CERTIFICACIÓN DIGITAL DE CONFIANZA	8
4.2 REGISTRO DEL PUNTO DE DISTRIBUCIÓN DE LA CRL.....	9
5 INTEGRACIÓN MEDIANTE SERVICIOS WEB	10
5.1 SERV-007-001	11
INPUT.....	11
OUTPUT.....	13
5.1.1 EXCEPCIONES	14
CREDENCIALES DE ACCESO INCORRECTAS	14
FORMATO DE PROCESAMIENTO DE INFORMACIÓN INCORRECTO	15
5.1.2 INTEGRIDAD DE LA FIRMA DIGITAL	15
5.1.3 CONFIANZA DEL EMISOR DE LA FIRMA	16
5.1.4 ESTADO DE REVOCACIÓN DE LA FIRMA.....	16
5.1.5 CADUCIDAD DEL CERTIFICADO DIGITAL DE FIRMA.....	17
5.1.6 EJEMPLOS DE USO	17
PETICIÓN.....	17
RESPUESTA	18
5.2 SERV-007-002	19
INPUT.....	19
OUTPUT.....	20
5.2.1 EXCEPCIONES	20
CREDENCIALES DE ACCESO INCORRECTAS	20
EVIDENCIA NO ENCONTRADA.....	20
5.2.2 EJEMPLOS DE USO	21
PETICIÓN.....	21
RESPUESTA	21
5.3 SERV-007-003	21
INPUT.....	22
OUTPUT.....	23
5.3.1 EXCEPCIONES	23
CREDENCIALES DE ACCESO INCORRECTAS	23
EVIDENCIA NO ENCONTRADA.....	24
5.3.2 EJEMPLOS DE USO	24
PETICIÓN.....	24

RESPUESTA	25
5.4 SERV-007-004	25
INPUT.....	26
OUTPUT.....	27
5.4.1 EXCEPCIONES	28
CREDENCIALES DE ACCESO INCORRECTAS	28
EVIDENCIA NO ENCONTRADA.....	28
5.4.2 EJEMPLOS DE USO	29
PETICIÓN.....	29
RESPUESTA	30

Introducción

Bienvenido al instructivo de Ares sobre las funciones del Rol Cliente Gse.

Este instructivo esta realizado con el propósito de proveer una vista general de las opciones y funciones dentro de la aplicación de Ares, así como el alcance de la misma. Teniendo en cuenta todos los pasos previos dentro del ciclo, como la interfaz y sus funciones disponibles, el proceso de registro y los campos requeridos para completar la operación.

Ares Cloud 3.0 es una plataforma de servicios PKI que provee un conjunto de Servicios Web con las siguientes características:

- Validar información firmada digitalmente en formato PKCS / CMS attached y detached.
- Validar información firmada digitalmente en formato Cades / Pades / Xades / XML Signature enveloped.
- Validar información firmada digitalmente en formato PDF/A.
- Firmar documentos y mensajes de datos en formato PKCS / CMS attached con un certificado de persona jurídica.
- Cifrar información con algoritmos AES y 3DES.
- Cifrar información con llaves simétricas y asimétricas.
- Gestionar la verificación de firma digital en modo LTV.
- Verificar estampas cronológicas bajo el estándar RFC 3161.
- Generar estampas cronológicas bajo el estándar RFC 3161.
- Reportar información de uso de la plataforma.
- Almacenamiento y validación de documentos firmados desde los equipos de los usuarios corporativos.

1 Inicio de sesión

El Inicio de sesión se hará con un usuario y contraseña, así mismo los campos "Usuario" y "Clave" serán de carácter obligatorio.



Imagen 1: Panel inicial para el login

Imagen 2: Campos obligatorios para el login

Los campos "Usuario" y "Clave" se tendrán que digitar en el formato correcto, de lo contrario aparecerá un mensaje de error.

Imagen 3: Advertencia campos "Usuario" y "Clave"

Una vez se digiten los campos correctamente, el sistema le indicará al usuario que actualice la contraseña la cual debe contener mínimo 12 caracteres que incluya: mayúscula, minúscula, número y carácter especial

Imagen 4: Campos obligatorios para el cambio de contraseña

Se debe digitar la nueva contraseña en el formato correcto, de lo contrario aparecerá un mensaje de error.



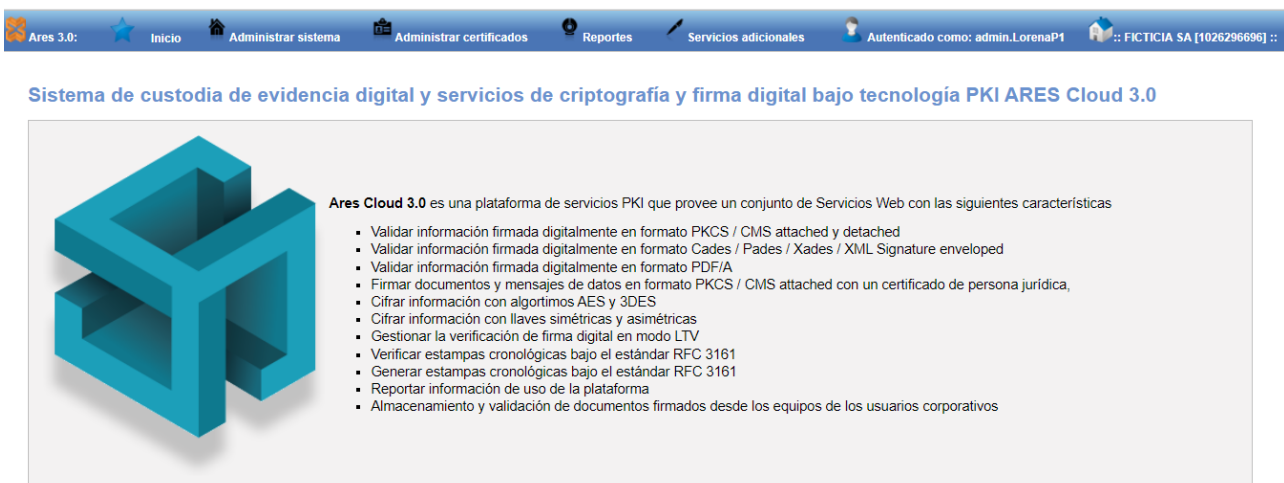
Imagen 5: Campos obligatorios para el login

Una vez se digitan los campos correctamente, el sistema permitirá el inicio de sesión y direccionará El usuario al dashboard de Ares.

2 Dashboard de Ares Cloud 3.0

Se presenta el panel principal del dashboard de Ares, según los actores autorizados para el ingreso a la interfaz de administración Web de Ares y para el consumo de los servicios de registro y consulta de evidencia digital.

Admin Cliente: Administrador local de un cliente, encargado principalmente de disponer las políticas de organización de su evidencia digital y definir las características y atributos de las autoridades de certificación en las cuales confía.



Sistema de custodia de evidencia digital y servicios de criptografía y firma digital bajo tecnología PKI ARES Cloud 3.0

Ares Cloud 3.0 es una plataforma de servicios PKI que provee un conjunto de Servicios Web con las siguientes características

- Validar información firmada digitalmente en formato PKCS / CMS attached y detached
- Validar información firmada digitalmente en formato Cades / Pades / Xades / XML Signature enveloped
- Validar información firmada digitalmente en formato PDF/A
- Firmar documentos y mensajes de datos en formato PKCS / CMS attached con un certificado de persona jurídica,
- Cifrar información con algoritmos AES y 3DES
- Cifrar información con llaves simétricas y asimétricas
- Gestionar la verificación de firma digital en modo LTV
- Verificar estampas cronológicas bajo el estándar RFC 3161
- Generar estampas cronológicas bajo el estándar RFC 3161
- Reportar información de uso de la plataforma
- Almacenamiento y validación de documentos firmados desde los equipos de los usuarios corporativos

Imagen 6: Interfaz principal del Dashboard de Ares Cloud 3.0 perfil Admin Cliente

User: Usuario asociado a un cliente específico al cual se le han dado únicamente los permisos de exploración de evidencia digital.

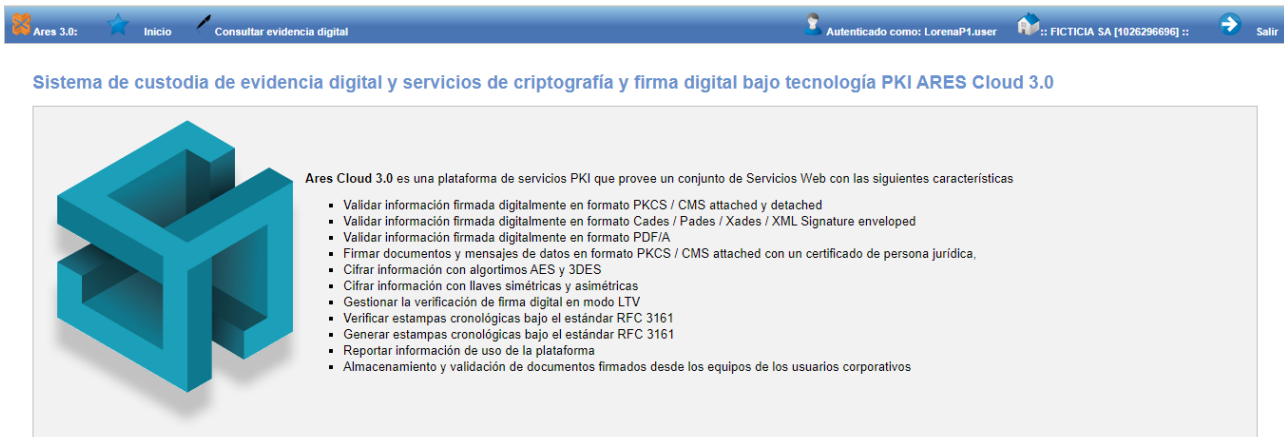


Imagen 7: Interfaz principal del Dashboard de Ares Cloud 3.0 perfil User

WS: Permite cargar la evidencia mediante la conexión con Firmaya Driver a aplicativo Ares Cloud.

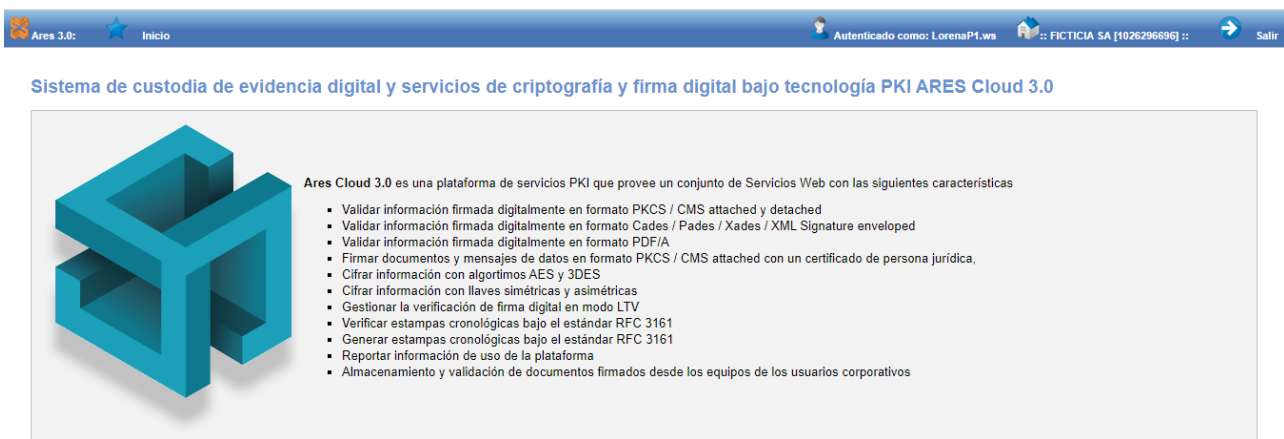


Imagen 8: Interfaz principal del Dashboard de Ares Cloud 3.0 perfil WS

3 Entidad de Certificación Digital (ECD)

Una Entidad Certificación Digital autorizada representa una persona natural o jurídica, que para un proceso de negocio específico deberá enviar evidencia firmada digitalmente. Ares verificará que todos los firmantes de la evidencia digital pertenezcan a la Entidad Certificación Digital; siempre y cuando la autoridad de certificación de confianza y el punto de distribución de la CRL se encuentre configurado.

Nota: En la página Web de Gestión De Seguridad Electronica SA podrá descargar:

- Certificado Raíz: https://certs2.gse.com.co/CA_ROOT.crt
- Certificado Subordinado: https://certs2.gse.com.co/CA_SUB01.crt
- Lista de Certificados Revocados (CRL): https://crl2.gse.com.co/CA_SUB01.crl

4.1 Administración de la Entidad de Certificación Digital de confianza

Para registrar la Entidad Certificación Digital autorizada se deberá hacer clic sobre la opción **Administrar certificados** \Rightarrow **Administrar certificado X.509 de autoridad de certificación**.

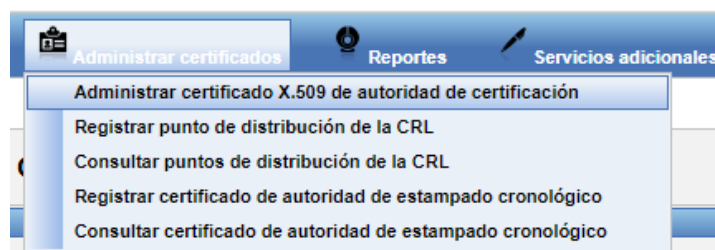


Imagen 9: Lista de opciones Administrar certificado

La acción anterior desplegará en el panel de trabajo principal la interfaz "Registrar certificado de autoridad de certificación", por lo que el usuario deberá hacer clic en el botón "Agregar" y adjuntar inicialmente el Certificado Subordinado seguidamente dar clic en "Registrar" y finalmente adjuntar el Certificado Subordinado y dar clic en "Registrar"



Imagen 10: Panel consulta Registrar certificado de autoridad de certificación

Finalizado el registro del Certificado Raíz y Subordinado usted podrá visualizar los certificados en el sistema como se muestra en la Imagen 13.

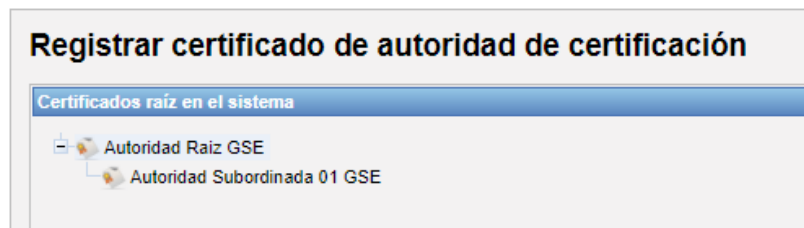


Imagen 11: Vista Certificados Raíz y Subordinando en el Sistema

4.2 Registro del punto de distribución de la CRL

Para registrar la Entidad Certificación Digital autorizada se deberá hacer clic sobre la opción **Administrar certificados** ⇒ **Registrar punto de distribución de la CRL**

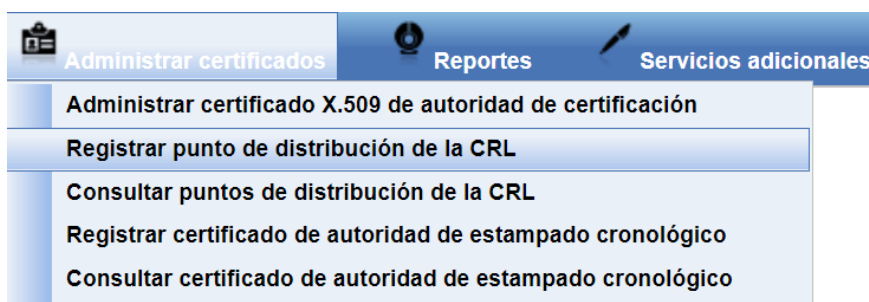


Imagen 12: Lista de opciones Administrar certificado

Una vez sea visible el formulario de Registro la URL de la CRL, prioridad 1 y Frecuencia de actualización 60 horas se deberá hacer clic en el botón "Registrar".

Imagen 13: Formulario Registrar un nuevo punto de distribución de la CRL

Para consultar los puntos de distribución de la CRL ➔ Administrar sistema, Acto seguido deberá hacer clic en el botón ➔ Consultar puntos de distribución de la CRL.

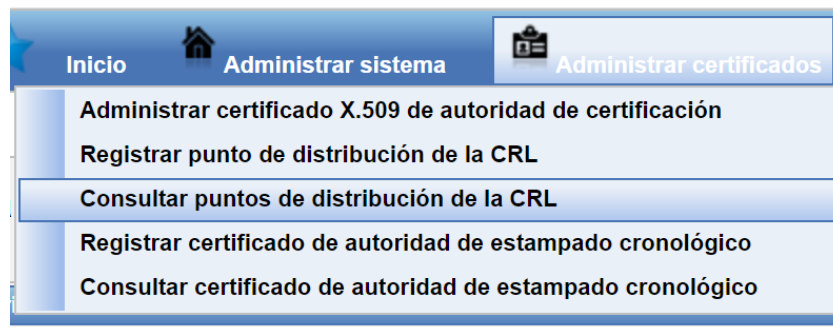


Imagen 14: Lista de opciones Administrar sistema

La acción anterior desplegará en el panel de trabajo principal la siguiente interfaz:



Imagen 15: Vista registro de la CRL en el sistema

5 Integración mediante Servicios Web

Servicios

Código	Aplicación	Transporte	Protocolo	Autenticación	Descripción
SERV-007-001	APP-007	https	Soap	Usuario y contraseña	Registrar evidencia digital
SERV-007-002	APP-007	https	Soap	Usuario y contraseña	Recupera un solo registro a partir de los filtros de consulta
SERV-007-003	APP-007	https	Soap	Usuario y contraseña	Recupera una lista (máximo 1.000 elementos) a partir de los filtros de consulta
SERV-007-004	APP-007	https	Soap	Usuario y contraseña	Retorna los firmantes de una evidencia digital consultada a partir de un conjunto de filtros de búsqueda.

5.1 SERV-007-001

Operation	Input	Output
<i>registrarEvidenciaDigital</i>	<i>registrarEvidenciaDigital</i>	registrarEvidenciaDigitalResponse

Input

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ws="http://ws.evidencia.ares.softcol.com.co/">
  <soapenv:Header />
  <soapenv:Body>
    <ws:registrarEvidenciaDigital>
      <arg0>
        <login?</login>
        <password?</password>
        <format?</format>
        <digitalRecordID?</digitalRecordID>
        <path?</path>
        <!--Zero or more repetitions:-->
        <ids>
          <nombre?</nombre>
          <valor?</valor>
        </ids>
        <signature>cid:262786315164</signature>
        <!--Zero or more repetitions:-->
        <signatureMetadata>
          <nombre?</nombre>
          <valor?</valor>
        </signatureMetadata>
        <signedData>cid:742755230061</signedData>
        <!--Zero or more repetitions:-->
        <signedDataMetadata>
          <nombre?</nombre>
          <valor?</valor>
        </signedDataMetadata>
      </arg0>
    </ws:registrarEvidenciaDigital>
  </soapenv:Body>
</soapenv:Envelope>
```

Argumento	Tipo	Descripción	Opcional
<i>login</i>	String	Usuario con permisos de consumo de los Web Services	No
<i>password</i>	String	Contraseña de acceso asociada al usuario	No
<i>format</i>	String	Formato de procesamiento de la evidencia digital.	No
<i>digitalRecordID</i>	Long	Identificador del expediente digital en el cual se almacenará la evidencia	Sí
<i>path</i>	String	Ruta en donde se almacenará la evidencia digital. Folder lógico	Sí

<i>ids</i>	Object	Lista de objetos clave-valor con identificadores de búsqueda de evidencia	Sí
<i>signature</i>	byte[]	Firma digital a verificar	Sí
<i>signedData</i>	byte[]	Texto claro asociado a la firma digital (se utiliza cuando el formato de firma es PKCS7 detached)	No
<i>signatureMetadata</i>	List<Object>	Lista de objetos clave-valor con la metadata asociada a la firma digital (i.e. nombre de la evidencia, algoritmos de ciframiento, etc.)	Sí
<i>signedDataMetadata</i>	List<Object>	Lista de objetos clave-valor con la metadata asociada al texto claro (i.e. nombre de la evidencia)	No

Valor format	Descripción
<i>SIGN_ATTACHED_PDF</i>	Formato de procesamiento y validación aplicable para archivos firmados digitalmente con el estándar definido para los documentos en formato PDF
<i>SIGN_ATTACHED_CMS</i>	Formato de procesamiento y validación aplicable para archivos firmados digitalmente con el estándar CMS attached. De la misma manera, este formato de procesamiento soporta el estándar PKCS7
<i>SIGN_ATTACHED_CMS_CLEAR_TEXT</i>	Formato de procesamiento y validación aplicable para archivos firmados digitalmente con el estándar CMS attached. La lógica de negocio implementada para este formato es heredada del formato SIGN_ATTACHED_CMS. Sin embargo, en este caso, siempre se retornará el texto claro asociado a la firma digital. Por defecto ARES no retorna el texto claro asociado a las firmas digitales en formato attached por razones de eficiencia en el consumo de los Servicios Web de registro de evidencia
<i>SIGN_ATTACHED_XML_ENVELOPED</i>	Formato de procesamiento y validación aplicable para archivos XML firmados digitalmente con el estándar XML Signature Enveloped
<i>SIGN_DETACHED_CMS</i>	Formato de procesamiento y validación aplicable para archivos firmados digitalmente con el estándar CMS detached. De la misma manera, este formato de procesamiento soporta el estándar PKCS7
<i>TIME_STAMP</i>	Formato de procesamiento y validación aplicable a estampas de tiempo que respetan el estándar RFC 3161
<i>ARCHIVING</i>	Formato de almacenamiento de evidencia digital en modalidad de Trusted Archiving. Esta modalidad de almacenamiento firma digitalmente la evidencia digital antes de almacenarla. La firma ejecutada respeta el estándar CMS attached
<i>SIGN_ATTACHED_CMS_OCSP</i>	Formato de procesamiento y validación aplicable para archivos firmados digitalmente con el estándar CMS attached. La diferencia fundamental con el estándar SIGN_ATTACHED_CMS radica fundamentalmente en la estrategia utilizada para verificar el estado de revocación del certificado. Mientras SIGN_ATTACHED_CMS utiliza una estrategia basada en listas de certificados revocados, SIGN_ATTACHED_CMS_OCSP utiliza una estrategia basada en el protocolo OCSP
<i>ARCHIVING_STORE</i>	Formato de almacenamiento genérico de información. A diferencia del formato ARCHIVING este formato no ejecuta una firma digital CMS sobre la evidencia antes de almacenarla
<i>ARCHIVING_SIGN_RETURN</i>	Formato de almacenamiento de evidencia digital en modalidad de Trusted Archiving. Esta modalidad de almacenamiento firma digitalmente la evidencia digital antes de almacenarla y retorna el texto firmado digitalmente. La lógica de negocio implementada para este formato es heredada del formato ARCHIVING. Sin embargo, en este caso, siempre se retornará la firma digital de la evidencia almacenada en formato CMS / PKCS7 ATTACHED

ARCHIVING_CRYPTEDP12_CMS	<p>Formato de desciframiento de información (desciframiento sin almacenamiento en ARES). La llave asimétrica de desciframiento se encontrará almacenada en un archivo PKCS12 previamente cargado en la interfaz de ARES. Adicionalmente, los parámetros de desciframiento se cargarán a partir de las siguientes propiedades del sistema:</p> <p>P12_CIPHER_ALGORITHM (i.e. DES_EDE3_CBC)</p>
ARCHIVING_CIPHER_AND_SIGN	<p>Formato que permite llevar a cabo las siguiente operaciones en el orden aquí establecido:</p> <p>Ciframiento de información con una llave asimétrica tipo X509V3. El algoritmo de ciframiento se debe enviar en el campo <i>signatureMetadata</i> bajo una llave nombrada como ALGORITHM (i.e. DES_EDE3_CBC). El (los) certificado(s) digital(es) de ciframiento se deberán enviar en el parámetro ids en donde la llave es el nombre del destinatario y el valor es el certificado digital Base64 encoded</p> <p>Firma digital en formato CMS/PKCS7 attached. La firma digital será generada con un certificado de persona jurídica asociado al cliente que consume el web Service.</p>
ARCHIVING_XML_RETURN	Formato que permite firmar un archivo XML con el estándar XML Signature enveloped. El certificado de firma a utilizar será aquel cargado para el cliente.
ARCHIVING_PDF_RETURN	Formato que permite firmar un archivo PDF con el estándar definido por Acrobat Reader. El certificado de firma a utilizar será aquel cargado para el cliente.

Output

```

<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
  <env:Header />
  <env:Body>
    <ws:registrarEvidenciaDigitalResponse xmlns:ws="http://ws.evidencia.ares.softcol.com.co/">
      <return>
        <mensajeValidacion?</mensajeValidacion>
        <resultadoValidacion?</resultadoValidacion>
        <textoClaro?</textoClaro>
        <idRegisteredEvidence?</idRegisteredEvidence>
        <idRegisteredEvidenceItemMain?</idRegisteredEvidenceItemMain>
        <idRegisteredEvidenceItemSecondary?</idRegisteredEvidenceItemSecondary>

        <!--Zero or more repetitions-->
        <signersCertificatesSubjects?</signersCertificatesSubjects>
        <!--Zero or more repetitions-->
        <signersCertificatesSerials?</signersCertificatesSerials>
      </return>
    </ws:registrarEvidenciaDigitalResponse>
  </env:Body>
</env:Envelope>

```

Argumento	Tipo	Descripción
<i>mensajeValidacion</i>	String	Detalles del mensaje de error si <i>resultadoValidacion</i> es False.
<i>resultadoValidacion</i>	Boolean	True si la evidencia digital fue registrada correctamente. False de lo contrario
<i>textoClaro</i>	byte[]	Resultado del procesamiento de la información de acuerdo al formato enviado
<i>idRegisteredEvidence</i>	Long	Identificador del expediente digital creado para almacenar el ítem
<i>idRegisteredEvidenceItemMain</i>	Long	Identificador del ítem de evidencia digital
<i>signersCertificatesSubjects</i>	List<String>	Lista de los asuntos de los certificados digitales asociados a la evidencia digital
<i>signersCertificatesSerials</i>	List<String>	Lista de los seriales de los certificados digitales asociados a la evidencia digital

5.1.1 Excepciones

Credenciales de acceso incorrectas

```

<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
  <env:Header />
  <env:Body>
    <ws:registrarEvidenciaDigitalResponse
      xmlns:ws="http://ws.evidencia.ares.softcol.com.co/">
      <return>
        <mensajeValidacion>
          002-El nombre de usuario empleado aún no ha sido dado de
          alta. Por favor comuníquese con el administrador del Sistema
        </mensajeValidacion>
        <resultadoValidacion>>false</resultadoValidacion>
      </return>
    </ws:registrarEvidenciaDigitalResponse>
  </env:Body>
</env:Envelope>

```

Formato de procesamiento de información incorrecto

```

<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
  <env:Header />
  <env:Body>
    <ws:registrarEvidenciaDigitalResponse xmlns:ws="http://ws.evidencia.ares.softcol.com.co/">
      <return>
        <mensajeValidacion>
          Formato no se encuentra configurado en el sistema
        </mensajeValidacion>
        <resultadoValidacion>false</resultadoValidacion>
      </return>
    </ws:registrarEvidenciaDigitalResponse>
  </env:Body>
</env:Envelope>

```

5.1.2 Integridad de la firma digital

```

<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
  <env:Header />
  <env:Body>
    <ws:registrarEvidenciaDigitalResponse
      xmlns:ws="http://ws.evidencia.ares.softcol.com.co/">
      <return>
        <idRegisteredEvidence>44014</idRegisteredEvidence>
        <idRegisteredEvidencieltemMain>63352</idRegisteredEvidencieltemMain>
        <mensajeValidacion>
          1-Error no controlado por el componente de verificación de
          firma en formato PKCS7. Descripción interna: Error no
          controlado por el componente de verificación de firma en
          formato PKCS7. Descripción interna: Se encuentra una firma
          digital incorrecta: [Subject firma incorrecta]
        </mensajeValidacion>
        <resultadoValidacion>false</resultadoValidacion>
      </return>
    </ws:registrarEvidenciaDigitalResponse>
  </env:Body>
</env:Envelope>

```

5.1.3 Confianza del emisor de la firma

```

<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
  <env:Header />
  <env:Body>
    <ws:registrarEvidenciaDigitalResponse xmlns:ws="http://ws.evidencia.ares.softcol.com.co/">
      <return>
        <idRegisteredEvidence>44014</idRegisteredEvidence>
        <idRegisteredEvidenceltemMain>63352</idRegisteredEvidenceltemMain>
        <mensajeValidacion>
          3-El certificado digital no es de confianza para el sistema. Asunto
          del certificado digital: [Subject certificado del firmante].
          Descripción interna: Problemas al tratar de determinar la cadena
          de confianza del certificado [Subject certificado del firmante].
          Descripción interna: No issuer certificate for certificate in
          certification path found.
        </mensajeValidacion>
        <resultadoValidacion>>false</resultadoValidacion>
      </return>
    </ws:registrarEvidenciaDigitalResponse>
  </env:Body>
</env:Envelope>

```

5.1.4 Estado de revocación de la firma

```

<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
  <env:Header />
  <env:Body>
    <ws:registrarEvidenciaDigitalResponse xmlns:ws="http://ws.evidencia.ares.softcol.com.co/">
      <return>
        <idRegisteredEvidence>44014</idRegisteredEvidence>
        <idRegisteredEvidenceltemMain>63352</idRegisteredEvidenceltemMain>
        <mensajeValidacion>
          4- [Subject certificado del firmante] revocado. Detalles: Error al
          momento de verificar el estado de revocación del certificado digital.
          Descripción interna: El certificado digital se encuentra revocado.
          Emisor de la revocación: [Issuer subject] Fecha de revocación:[Fecha
          de revocación en formato UTC] Serial del certificado revocado: [Serial
          del certificado revocado]
        </mensajeValidacion>
        <resultadoValidacion>>false</resultadoValidacion>
      </return>
    </ws:registrarEvidenciaDigitalResponse>
  </env:Body>
</env:Envelope>

```


5.1.5 Caducidad del certificado digital de firma

```
<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
  <env:Header />
  <env:Body>
    <ws:registrarEvidenciaDigitalResponse xmlns:ws="http://ws.evidencia.ares.softcol.com.co/">
      <return>
        <idRegisteredEvidence>44014</idRegisteredEvidence>
        <idRegisteredEvidenceltemMain>63352</idRegisteredEvidenceltemMain>
        <mensajeValidacion>
          2-Error al momento de verificar la vigencia del certificado digital
          emitido a [Subject firmante]. Certificado expirado. Certificado válido
          desde:[Fecha inicio de vigencia en formato UTC].
          Certificado válido hasta:[Fecha fin de vigencia en formato UTC].
          Fecha de verificación: [Fecha verificación en formato UTC]
          Descripción interna: certificate expired on [Fecha inicio de expiración
          del certificado]
        </mensajeValidacion>
        <resultadoValidacion>>false</resultadoValidacion>
      </return>
    </ws:registrarEvidenciaDigitalResponse>
  </env:Body>
</env:Envelope>
```

5.1.6 Ejemplos de uso

Petición

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ws="http://ws.evidencia.ares.softcol.com.co/">
  <soapenv:Header />
  <soapenv:Body>
    <ws:registrarEvidenciaDigital>
      <arg0>
        <login>user.ws</login>
        <password>user.ws</password>
        <format>SIGN_ATTACHED_CMS_CLEAR_TEXT</format>
        <signature>cid:262786315164</signature>
        <!--Zero or more repetitions!-->
        <signatureMetadata>
          <nombre>FILE_NAME</nombre>
          <valor>NombreArchivo.txt.p7z</valor>
        </signatureMetadata>
      </arg0>
    </ws:registrarEvidenciaDigital>
  </soapenv:Body>
</soapenv:Envelope>
```

Respuesta

```

<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
  <env:Header />
  <env:Body>
    <ws:registrarEvidenciaDigitalResponse xmlns:ws="http://ws.evidencia.ares.softcol.com.co/">
      <return>
        <idRegisteredEvidence>53941</idRegisteredEvidence>
        <idRegisteredEvidenceltemMain>77750</idRegisteredEvidenceltemMain>
        <mensajeValidacion>OK</mensajeValidacion>
        <resultadoValidacion>>true</resultadoValidacion>
        <signersCertificatesSerials>8043151062728246399</signersCertificatesSerials>
        <signersCertificatesSerials>1231507428221841160</signersCertificatesSerials>
        <signersCertificatesSubjects>
          OID.1.3.6.1.4.1.31136.2.2.1.2.3=8999890221,
          OID.1.3.6.1.4.1.31136.2.2.1.2.2=NIT,
          OID.1.3.6.1.4.1.31136.2.2.1.2.1=Cedula Ciudadania,
          STREET=Calle 43-57-31, OID.2.5.4.13=Funcion Publica,
          OID.2.5.4.12=TECNICO ADMINISTRATIVO, CN=NOMBRE
          USUARIO FIRMANTE 1, OU=GRUPO DE TECNOLOGIA DE
          INFORMACION Y COMUNICACION, O=ORGANIZACION,
          OID.2.5.4.42=Nombres, OID.2.5.4.5=80958521, ST=BOGOTA
          D.C., L=BOGOTA, OID.2.5.4.4=Apellidos,
          OID.1.2.840.113549.1.9.1=user@email.co, C=CO
        </signersCertificatesSubjects>
        <signersCertificatesSubjects>
          OID.1.3.6.1.4.1.31136.2.2.1.2.3=8991413380,
          OID.1.3.6.1.4.1.31136.2.2.1.2.2=NIT,
          OID.1.3.6.1.4.1.31136.2.2.1.2.1=CC, STREET=AVENIDA EL
          DORADO 75-25, OID.2.5.4.13=CERTIFICADO DE FUNCION
          PUBLICA, OID.2.5.4.12=JEFE AREA ADMINISTRACION,
          CN=NOMBRE USUARIO FIRMANTE 2, OU=DIRECCION,
          O=Organización, OID.2.5.4.42=Nombres, OID.2.5.4.5=89913833,
          ST=BOGOTA D.C., L=BOGOTA D.C., OID.2.5.4.4=Apellidos,
          OID.1.2.840.113549.1.9.1=user@email.co, C=CO
        </signersCertificatesSubjects>
        <textoClaro>
          DQojaWdub3JIHRodW1ibmFpbHMgY3JlYXRIZCBieSB3aW5kb3dzD
          QpUaHVtYnMuZGINCiNJ
          Z25vcmlzZm9uVWpibGQgYnkgVmlzdWFsIFN0dWRpbw0KKi5v
          YmoNCiouZXhIDQoqLnB
          kYg0KKi51c2VyDQoqLmFwcw0KKi5wY2gNCioudnNwc2NjDQoqX2ku
          Yw0KKi9wLmMNCioubm
          NiDQoqLnN1bw0KKi50bGINCioudGxoDQoqLmJhaw0KKi5jYWN0ZQ0
          KKI5pbGsNCioubG9nDQoqLmRsbA0KKi5saWINCiouc2JyDQo=
        </textoClaro>
      </return>
    </ws:registrarEvidenciaDigitalResponse>
  </env:Body>
</env:Envelope>

```

5.2 SERV-007-002

Operation	Input	Output
obtenerEvidenciaDigital	obtenerEvidenciaDigital	obtenerEvidenciaDigitalResponse

Input

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ws="http://ws.evidencia.ares.softcol.com.co/">
  <soapenv:Header />
  <soapenv:Body>
    <ws:obtenerEvidenciaDigital>
      <arg0>
        <login?</login>
        <password?</password>
        <name?</name>
        <digitalRecordItemID?</digitalRecordItemID>
        <digitalRecordID?</digitalRecordID>
      </arg0>
    </ws:obtenerEvidenciaDigital>
  </soapenv:Body>
</soapenv:Envelope>
```

Argumento	Tipo	Descripción	Opcional
login	String	Usuario con permisos de consumo de los Web Services	No
password	String	Contraseña de acceso asociada al usuario	No
name	String	Nombre de la evidencia digital a recuperar.	Sí
digitalRecordID	Long	Identificador del expediente digital en el cual se almacenará la evidencia	Sí
digitalRecordItemID	String	Identificador de un Ítem dentro de un expediente digital	Sí

Output

```
<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
  <env:Header />
  <env:Body>
    <ws:obtenerEvidenciaDigitalResponse xmlns:ws="http://ws.evidencia.ares.softcol.com.co/">
      <return>[Evidencia codificada en Base 64]
    </return>
    </ws:obtenerEvidenciaDigitalResponse>
  </env:Body>
</env:Envelope>
```

5.2.1 Excepciones

Credenciales de acceso incorrectas

```
<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
  <env:Header />
  <env:Body>
    <ws:obtenerEvidenciaDigitalResponse xmlns:ws="http://ws.evidencia.ares.softcol.com.co/">
      <return xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:nil="1" />
    </ws:obtenerEvidenciaDigitalResponse>
  </env:Body>
</env:Envelope>
```

Evidencia no encontrada

```
<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
  <env:Header />
  <env:Body>
    <ws:obtenerEvidenciaDigitalResponse xmlns:ws="http://ws.evidencia.ares.softcol.com.co/">
      <return/>
    </ws:obtenerEvidenciaDigitalResponse>
  </env:Body>
</env:Envelope>
```

5.2.2 Ejemplos de uso

Petición

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ws="http://ws.evidencia.ares.softcol.com.co/">
  <soapenv:Header />
  <soapenv:Body>
    <ws:obtenerEvidenciaDigital>
      <arg0>
        <login>user.ws</login>
        <password>user.ws</password>
        <name>NombreArchivo.txt.p7z</name>
      </arg0>
    </ws:obtenerEvidenciaDigital>
  </soapenv:Body>
</soapenv:Envelope>
```

Respuesta

```
<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
  <env:Header />
  <env:Body>
    <ws:obtenerEvidenciaDigitalResponse xmlns:ws="http://ws.evidencia.ares.softcol.com.co/">
      <return>
        c3ludGF4OiBnbG9iDQoNCiRodW1icy5kYg0KKi5vYmoNCiouZXhIDQoqLnBkYg0K
        Ki51c2VyDQoqLmFwc
        w0KKi5wY2gNCioudnNwc2NjDQoqX2kuYw0KKi9wLmMNCioubmNiDQoqLnN1bw0
        KKi50bGINCioudGxo
        DQoqLmJhaw0KKi5jYWNoZQ0KKi5pbGsNCioubG9nDQoqLmRsbA0KKi5saWINCi
        ouc2JyDQo=
      </return>
    </ws:obtenerEvidenciaDigitalResponse>
  </env:Body>
</env:Envelope>
```

5.3 SERV-007-003

Operation	Input	Output
<i>obtenerListaEvidenciaDigital</i>	<i>obtenerListaEvidenciaDigital</i>	obtenerListaEvidenciaDigitalResponse

Input

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ws="http://ws.evidencia.ares.softcol.com.co/">
  <soapenv:Header />
  <soapenv:Body>
    <ws:obtenerListaEvidenciaDigital>
      <arg0>
        <login?</login>
        <password?</password>
        <name?</name>
        <path?</digitalRecordItemID>
      </arg0>
    </ws:obtenerListaEvidenciaDigital>
  </soapenv:Body>
</soapenv:Envelope>
```

Argumento	Tipo	Descripción	Opcional
login	String	Usuario con permisos de consumo de los Web Services	No
password	String	Contraseña de acceso asociada al usuario	No
name	String	Nombre de la evidencia digital a recuperar. Puede ser una subcadena.	No
path	Long	Nombre del folder lógico en donde se encuentra almacenada la evidencia	Sí

Output

```
<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
  <env:Header />
  <env:Body>
    <ws:obtenerListaEvidenciaDigitalResponse
      xmlns:ws="http://ws.evidencia.ares.softcol.com.co/">
      <return>
        <!--Zero or more repetitions:-->
        <evidenceFinderResponse>
          <digitalRecordItemName?</digitalRecordItemName>
          <idDigitalRecord?</idDigitalRecord>
          <idDigitalRecordItem?</idDigitalRecordItem>
          <registrationDate?</registrationDate>
          <validationResult?</validationResult>
        </evidenceFinderResponse>
        <tiempoConsulta?</tiempoConsulta>
      </return>
    </ws:obtenerListaEvidenciaDigitalResponse>
  </env:Body>
</env:Envelope>
```

Argumento	Tipo	Descripción
digitalRecordItemName	String	Nombre de la evidencia digital
idDigitalRecord	Long	Identificador del expediente
idDigitalRecordItem	Long	Identificador de ítem
registrationDate	String	Fecha de registro de la evidencia digital en formato YYYY-MM-DDTHH:mm:ss.S
validationResult	Boolean	True si la validación de la evidencia digital fue exitosa. False de lo contrario
tiempoConsulta	Long	Tiempo en milisegundos empleado para llevar a cabo la consulta.

5.3.1 Excepciones

Credenciales de acceso incorrectas

```
<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
  <env:Header />
  <env:Body>
    <ws:obtenerListaEvidenciaDigitalResponse xmlns:ws="http://ws.evidencia.ares.softcol.com.co/">
      <return xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:nil="1" />
    </ws:obtenerListaEvidenciaDigitalResponse>
  </env:Body>
</env:Envelope>
```

Evidencia no encontrada

```
<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
  <env:Header />
  <env:Body>
    <ws:obtenerListaEvidenciaDigitalResponse xmlns:ws="http://ws.evidencia.ares.softcol.com.co/">
      <return>
        <tiempoConsulta>76</tiempoConsulta>
      </return>
    </ws:obtenerListaEvidenciaDigitalResponse>
  </env:Body>
</env:Envelope>
```

5.3.2 Ejemplos de uso

Petición

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ws="http://ws.evidencia.ares.softcol.com.co/">
  <soapenv:Header />
  <soapenv:Body>
    <ws:obtenerListaEvidenciaDigital>
      <arg0>
        <login>user.ws</login>
        <password>user.ws</password>
        <name>NombreArchivo</name>
      </arg0>
    </ws:obtenerListaEvidenciaDigital>
  </soapenv:Body>
</soapenv:Envelope>
```


Respuesta

```

<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
  <env:Header />
  <env:Body>
    <ws:obtenerListaEvidenciaDigitalResponse xmlns:ws="http://ws.evidencia.ares.softcol.com.co/">
      <return>
        <evidenceFinderResponse>
          <digitalRecordItemName>NombreArchivo.txt.p7z</digitalRecordItemName>
          <idDigitalRecord>53941</idDigitalRecord>
          <idDigitalRecordItem>77750</idDigitalRecordItem>
          <registrationDate>2020-01-03T21:22:45.133Z</registrationDate>
          <validationResult>true</validationResult>
        </evidenceFinderResponse>
        <evidenceFinderResponse>
          <digitalRecordItemName>NombreArchivo.txt.p7z</digitalRecordItemName>
          <idDigitalRecord>53936</idDigitalRecord>
          <idDigitalRecordItem>77745</idDigitalRecordItem>
          <registrationDate>2020-01-03T21:13:30.625Z</registrationDate>
          <validationResult>true</validationResult>
        </evidenceFinderResponse>
        <tiempoConsulta>74</tiempoConsulta>
      </return>
    </ws:obtenerListaEvidenciaDigitalResponse>
  </env:Body>
</env:Envelope>

```

5.4 SERV-007-004

Operation	Input	Output
<i>listarFirmantes</i>	<i>listarFirmantes</i>	listarFirmantesResponse

Input

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ws="http://ws.evidencia.ares.softcol.com.co/">
  <soapenv:Header />
  <soapenv:Body>
    <ws:listarFirmantes>
      <arg0>
        <login>?</login>
        <password>?</password>
        <nameArchive>?</nameArchive>
        <digitalRecordID>?</digitalRecordID>
        <digitalRecordItemID>?</digitalRecordItemID>
      </arg0>
    </ws:listarFirmantes>
  </soapenv:Body>
</soapenv:Envelope>
```

Argumento	Tipo	Descripción	Opcional
login	String	Usuario con permisos de consumo de los Web Services	No
password	String	Contraseña de acceso asociada al usuario	No
nameArchive	String	Nombre de la evidencia digital a recuperar. Puede ser una subcadena.	Sí
digitalRecordID	Long	Identificador del expediente digital	Sí
digitalRecordItemID	Long	Identificador de un ítem que pertenece a un expediente digital	Sí

Output

```

<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
  <env:Header />
  <env:Body>
    <ws:listarFirmantesResponse xmlns:ws="http://ws.evidencia.ares.softcol.com.co/">
      <return>
        <!--Zero or more repetitions-->
        <evidencerSignatoriesFindeResponse>
          <digitalRecordItemName?></digitalRecordItemName>
          <idDigitalRecord?></idDigitalRecord>
          <idDigitalRecordItem?></idDigitalRecordItem>
          <idX509UserCertificate?></idX509UserCertificate>
          <issuer?></issuer>
          <notAfter?></notAfter>
          <notBefore?></notBefore>
          <path?></path>
          <subject?></subject>
        </evidencerSignatoriesFindeResponse>
        <tiempoConsulta?></tiempoConsulta>
      </return>
    </ws:listarFirmantesResponse>
  </env:Body>
</env:Envelope>

```

Argumento	Tipo	Descripción
<i>digitalRecordItemName</i>	String	Nombre de la evidencia digital
<i>idDigitalRecord</i>	Long	Identificador del expediente
<i>idDigitalRecordItem</i>	Long	Identificador de ítem
<i>idX509UserCertificate</i>	Long	Identificador con el cual se ha almacenado el certificado de firma del usuario
<i>issuer</i>	String	Autoridad de certificación emisora del certificado del usuario.
<i>notAfter</i>	String	Fecha de finalización de la vigencia del certificado en formato YYYY-MM-DDTHH:mm:ss.S
<i>notBefore</i>	String	Fecha de inicio de la vigencia del certificado en formato YYYY-MM-DDTHH:mm:ss.S
<i>path</i>	String	Folder de almacenamiento lógico del expediente digital
<i>subject</i>	String	Asunto del certificado digital del firmante
<i>tiempoConsulta</i>	Long	Tiempo, en milisegundos, que tomó el sistema para llevar a cabo la consulta.

5.4.1 Excepciones

Credenciales de acceso incorrectas

```
<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
  <env:Header />
  <env:Body>
    <ws:listarFirmantesResponse xmlns:ws="http://ws.evidencia.ares.softcol.com.co/">
      <return>
        <message>Usuario incorrecto</message>
      </return>
    </ws:listarFirmantesResponse>
  </env:Body>
</env:Envelope>
```

Evidencia no encontrada

```
<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
  <env:Header />
  <env:Body>
    <ws:listarFirmantesResponse xmlns:ws="http://ws.evidencia.ares.softcol.com.co/">
      <return>
        <message>Sin resultados de búsqueda</message>
        <tiempoConsulta>446</tiempoConsulta>
      </return>
    </ws:listarFirmantesResponse>
  </env:Body>
</env:Envelope>
```

5.4.2 Ejemplos de uso

Petición

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ws="http://ws.evidencia.ares.softcol.com.co">
  <soapenv:Header />
  <soapenv:Body>
    <ws:listarFirmantes>
      <arg0>
        <login>mhcp.regalias.ws</login>
        <password>mhcp.regalias.ws</password>
        <nameArchive>NombreArchivo</nameArchive>
      </arg0>
    </ws:listarFirmantes>
  </soapenv:Body>
</soapenv:Envelope>
```

Respuesta

```

<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
  <env:Header />
  <env:Body>
    <ws:listarFirmantesResponse xmlns:ws="http://ws.evidencia.ares.softcol.com.co/">
      <return>
        <evidencerSignatoriesFindeResponse>
          <digitalRecordItemName>NombreArchivo.txt.p7z</digitalRecordItemName>
          <idDigitalRecord>53936</idDigitalRecord>
          <idDigitalRecordItem>77745</idDigitalRecordItem>
          <idX509UserCertificate>1662</idX509UserCertificate>
          <issuer>[Subject issuer]</issuer>
          <notAfter>2020-11-03T00:00:00Z</notAfter>
          <notBefore>2019-10-25T00:00:00Z</notBefore>
          <path>/home/ec2-user/Ares/company/certs/2019/10/1662.cer</path>
          <subject>[Subject signer]</subject>
        </evidencerSignatoriesFindeResponse>
        <evidencerSignatoriesFindeResponse>
          <digitalRecordItemName>NombreArchivo.txt.p7z</digitalRecordItemName>
          <idDigitalRecord>53941</idDigitalRecord>
          <idDigitalRecordItem>77750</idDigitalRecordItem>
          <idX509UserCertificate>1662</idX509UserCertificate>
          <issuer>[Subject issuer]</issuer>
          <notAfter>2020-11-03T00:00:00Z</notAfter>
          <notBefore>2019-10-25T00:00:00Z</notBefore>
          <path>/home/ec2-user/Ares/company/certs/2019/10/1662.cer</path>
          <subject>[Subject signer No. 1]</subject>
        </evidencerSignatoriesFindeResponse>
        <evidencerSignatoriesFindeResponse>
          <digitalRecordItemName>NombreArchivo.txt.p7z</digitalRecordItemName>
          <idDigitalRecord>53941</idDigitalRecord>
          <idDigitalRecordItem>77750</idDigitalRecordItem>
          <idX509UserCertificate>1763</idX509UserCertificate>
          <issuer>[Subject issuer]</issuer>
          <notAfter>2020-11-27T00:00:00Z</notAfter>
          <notBefore>2019-11-18T00:00:00Z</notBefore>
          <path>/home/ec2-user/Ares/company/certs/2020/1/1763.cer</path>
          <subject>[Subject signer No. 2]</subject>
        </evidencerSignatoriesFindeResponse>
        <tiempoConsulta>239</tiempoConsulta>
      </return>
    </ws:listarFirmantesResponse>
  </env:Body>
</env:Envelope>

```