

**POLÍTICAS DE CONTROL Y MONITOREO ENTRE LA ENTIDAD
CERTIFICADORA PÚBLICA (ECP) Y LAS AGENCIAS DE
REGISTRO (AR)**

ADSIB-FD-POLT-06

Unidad de Gestión de Servicios

	ELABORADO POR:	REVISADO POR:	APROBADO POR:
Nombre:	Jhonny Medina	Reynaldo Vera	Jannett Ibañez
Cargo:	Consultor de Línea – Monitoreo de servicios seguimiento y control de calidad de procesos y	Jefe de la Unidad de Gestión de Servicios	Directora Ejecutiva de la ADSIB
Firma:			
Fecha:			



**POLÍTICAS DE CONTROL Y MONITOREO ENTRE LA ENTIDAD CERTIFICADORA
PUBLICA (ECP) Y LAS AGENCIAS DE REGISTRO (AR)**

Índice

<u>Introducción.....</u>	<u>2</u>
<u>1. Gestión del ciclo de vida de un certificado digital de una AR.....</u>	<u>2</u>
<u>2. Criterios.....</u>	<u>2</u>
<u>3. Controles Ilustrativos.....</u>	<u>2</u>
<u>3.1. Registros de una AR.....</u>	<u>2</u>
<u>3.1.1. La ECP autentica las solicitudes de certificados de la AR.....</u>	<u>2</u>
<u>3.1.2. La ECP lleva a cabo una evaluación del cumplimiento de los requisitos del certificado digital del solicitante con los requisitos antes de aprobar una solicitud de certificado.....</u>	<u>3</u>
<u>3.2. Distribución de certificados de la AR.....</u>	<u>3</u>
<u>3.2.1. La ECP firma certificados digitales de acuerdo a las solicitudes de la AR.....</u>	<u>3</u>
<u>3.2.2. La ECP verifica la identidad y la autoridad de la AR que solicita la revocación de un certificado.....</u>	<u>4</u>
<u>3.2.3. La ECP actualiza la lista de revocación de certificados (CRL) y otros mecanismos de estado de certificados sobre la revocación del certificado.....</u>	<u>4</u>
<u>3.2.4. La ECP hace que la información de estado de los certificados digitales solicitados por la AR se encuentren disponibles para las Partes que Confían usando un mecanismo establecido.....</u>	<u>5</u>
<u>4. VERSIONES:.....</u>	<u>5</u>



POLÍTICAS DE CONTROL Y MONITOREO ENTRE LA ENTIDAD CERTIFICADORA PÚBLICA (ECP) Y LAS AGENCIAS DE REGISTRO (AR)

Introducción

La ECP - ADSIB mantiene controles efectivos para proporcionar la seguridad necesaria para que las solicitudes de certificados digitales de sus Agencias de Registro sean exactas, autenticadas y autorizadas.

1. Gestión del ciclo de vida de un certificado digital de una AR

El ciclo de vida de un certificado digital así como los controles establecidos por la AR y la ECP en cada paso de todo el procedimiento se detallan en el punto “4. Ciclo de vida de los certificados” del documento “Declaración de Prácticas de Certificación”.

2. Criterios

La ECP - ADSIB mantiene controles para proporcionar una seguridad razonable de que:

Las solicitudes de certificados digitales de la AR son exactas y los datos son autenticados y autorizados a través de servicios de interoperabilidad entre la ECP y la AR.

Las solicitudes de renovación de certificados digitales de la AR son exactos, autorizados y completos a través de servicios de interoperabilidad entre la ECP y la AR.

Las solicitudes nuevas y renovaciones de certificados digitales de la AR se generan y se emiten de conformidad en la ECP de acuerdo a las políticas de certificación y declaración de prácticas.

La información al signatario del estado de certificados es oportuna, completa, exacta y se pone a disposición de cualquier entidad, de acuerdo con las prácticas divulgadas de la ECP. Los servicios y la frecuencia de actualización se detallan en el punto “2.2. Publicación” y el punto “2.3. Frecuencia de actualización” del documento “Declaración de Prácticas de Certificación”.

3. Controles Ilustrativos

3.1. Registros de una AR

3.1.1. La ECP autentica las solicitudes de certificados de la AR



En el punto “4.4. Proceso de solicitud de certificado digital” del documento “Declaración de Prácticas de Certificación” se especifica que el envío de la solicitud de firma de certificado a la ECP debe ir firmada digitalmente por la AR:

La Agencia de Registro debe realizar un proceso de validación de la identidad del solicitante a través de servicios de interoperabilidad con el SEGIP y el SERECI, además de la verificación de cumplimiento de requisitos y verificación del pago correspondiente.

El Oficial de Registro una vez verificada la solicitud, envía la misma firmada digitalmente a la Entidad Certificadora Pública – ADSIB.

3.1.2. La ECP lleva a cabo una evaluación del cumplimiento de los requisitos del certificado digital del solicitante con los requisitos antes de aprobar una solicitud de certificado

En el punto “4.5. Emisión del certificado” del documento “Declaración de Prácticas de Certificación” indica que la ECP realizará la evaluación de cada solicitud recibida antes de aprobarla para la respectiva emisión del certificado digital:

La Entidad Certificadora Pública – ADSIB realizará la evaluación de requisitos presentados a través de un control cruzado de los documentos antes de aprobar la solicitud de certificado. Si en la evaluación se comprueba que no se han cumplido los requisitos, la ECA procederá a la devolución inmediata de la solicitud a la Agencia de Registro para su respectiva corrección.

3.2. Distribución de certificados de la AR

3.2.1. La ECP firma certificados digitales de acuerdo a las solicitudes de la AR

En el punto “4.5. Emisión del certificado” del documento “Declaración de Prácticas de Certificación” indica que la ECP procede a la firma de certificados que hayan sido enviados por cualquier AR:

La Entidad Certificadora Pública – ADSIB una vez que recibe la solicitud CSR firmada, y se haya realizado la evaluación de los requisitos, estará en condiciones de emitir el certificado, para ello dispone de procedimientos internos que incluyen una ceremonia de Firma Digital de los certificados que garantizan la seguridad, confidencialidad e integridad de los datos.



3.2.2. La ECP verifica la identidad y la autoridad de la AR que solicita la revocación de un certificado

En el punto “4.10. Revocación del certificado” del documento “Declaración de Prácticas de Certificación” se detalla los procesos de validación de identidad que realiza la AR antes de enviar la solicitud de revocación a la ECP:

La revocación se realizará de acuerdo con los procedimientos internos con los que la ECA-ADSIB trabaja y a solicitud del usuario o autoridad competente.

Revocación Presencial: Al realizar una solicitud de revocación de manera presencial en alguna Agencia de Registro autorizada, el Oficial de Registro debe realizar la validación a través de la presentación de un documento que verifique la identidad del usuario titular.

Revocación telefónica: La solicitud de revocación vía telefónica estará pendiente, hasta realizada la validación mediante una nueva llamada telefónica al número registrado en los datos del usuario titular. La verificación se realizará solicitando la siguiente información: número de documento de identidad, nombre completo y fecha de nacimiento del usuario titular. La ECA tiene implementados los controles de validación correspondiente respecto a llamadas telefónicas.

Revocación en línea a través del Sistema de AR: La Entidad Certificadora Pública considera que la autenticación a través del sistema es prueba suficiente para verificar la identidad del usuario titular, por lo que se efectivizará la revocación del certificado de manera inmediata.

3.2.3. La ECP actualiza la lista de revocación de certificados (CRL) y otros mecanismos de estado de certificados sobre la revocación del certificado

En el punto “4.10. Revocación del certificado” del documento “Declaración de Prácticas de Certificación”, se detalla la actualización del CRL::

Una vez revocado el certificado, la Entidad Certificadora Pública lo incluye en la Lista de Certificados Revocados (CRL) con el fin de notificar a terceros que un certificado ha sido revocado. Los certificados que sean revocados no podrán por ninguna circunstancia volver al estado activo, siendo esta una acción definitiva.



3.2.4. La ECP hace que la información de estado de los certificados digitales solicitados por la AR se encuentren disponibles para las Partes que Confían usando un mecanismo establecido

En el punto “2.2. Publicación” del documento “Declaración de Prácticas de Certificación” se detalla el acceso a los servicios que proporcionan información sobre el estado de los certificados:

La ADSIB proporciona acceso público a las siguientes informaciones:

La Lista de Certificados Revocados (CRL) y los servicios de validación de certificados en línea (OCSP).

Además, en el punto “2.3. Frecuencia de actualización” del documento “Declaración de Prácticas de Certificación” se detalla:

La ADSIB realiza una constante actualización de los repositorios públicos. Por otra parte, y por ser una información crítica, la actualización del repositorio CRL se realiza cada 15 minutos y el servicio OCSP se mantiene en línea.

4. VERSIONES:

Versión	Fecha de Revisión	Descripción del cambio	Revisado por	Aprobado por	RES. ADM.	Fecha de aprobación
1	8/11/2018	• Elaboración del documento	Reynaldo Vera			

