

1 OBJETIVO

Definir la adecuada gestión del ciclo de vida de las llaves criptográficas dentro de la ADRES, mediante la asignación de los diferentes responsables en cada una de las actividades de gestión, con el propósito de ser un articulador de los procedimientos de las diferentes dependencias de la Entidad.

2 ALCANCE

Inicia desde la entrega de la llave criptográfica, continua, con la asignación del responsable de custodia y uso de esta y finaliza con la entrega de esta al tercero proveedor.

3 LÍDER DEL PROCEDIMIENTO

Director(a) de Gestión de Tecnología de Información y comunicaciones.

4 POLÍTICAS DE OPERACIÓN

- ✓ Para el entendimiento de este procedimiento se definen dos tipos de llaves criptográficas.
 - a. Llave criptográfica de firma digital. Mecanismo físico o en software que se usa para el proceso de firmar documentos de manera manual o a través de Sistemas de Información.
 - b. Token para acceso a portales de terceros.
- ✓ Dentro del presente procedimiento se entiende como Custodio y responsable del manejo del Token el Servidor Público o Contratista que se sea designado para guardar y gestionar el token de firma digital.
- ✓ La custodia de la llave criptográfica deberá estar dada bajo las siguientes medidas de seguridad física:
 - a. Debe encontrarse bajo llave siempre y cuando no se esté utilizando.
 - b. No debe ser compartida a Servidores públicos o contratistas que no hayan sido delegados por parte del director o jefe de dependencia a quien le ha sido entregada la llave.
 - c. Todas las demás que el grupo interno de Gestión Administrativa y Documental defina.
- ✓ Para el caso de llaves criptográficas de firma digital, solo se procederá a firmar los documentos o archivos que sean referenciados por parte de los diferentes directores y jefes de oficina que se encuentren dentro del archivo de control que maneje el Custodio y responsable del manejo del Token físico.
- ✓ El presente procedimiento está alineado con los siguientes objetivos de controles ISO 27000:
 - A10.1.1- Controles criptográficos. Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
 - A10.1.2 - Gestión de llaves. Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.

5 REQUISITOS LEGALES Ver Normograma

6 DEFINICIONES Ver Glosario General

7 DESARROLLO DEL PROCEDIMIENTO

No	Actividad	Descripción de la Actividad	Responsable	Registro
1	Informar a la DGTIC la existencia de una nueva llave criptográfica y delegar custodia y responsabilidad de uso	<p>Como insumo a esta actividad, se tienen dos fuentes de información:</p> <ul style="list-style-type: none"> • Un tercero remite a la ADRES una llave criptográfica la cual será entregada al director o jefe de dependencia a quien ha sido asignada. • Un Custodio y responsable del manejo de un token presenta la novedad de renuncia al cargo o contrato que tiene frente a la ADRES. <p>Mediante correo electrónico le comunica al director de Gestión de Tecnología de Información y Comunicaciones y al gestor de operaciones de la DGTIC que cumple las funciones de líder de Seguridad de la Información la novedad indicando:</p> <ul style="list-style-type: none"> • Fecha de vigencia de la llave criptográfica • Uso previsto para la llave criptográfica. • Tipo de llave: Física o Software. • Custodio y responsable del manejo de este. <p>Paralelamente, el director o jefe de dependencia mediante correo electrónico le informará al responsable de la custodia y uso de la llave criptográfica la designación que tiene; a su vez, le entregará cuando corresponda el token físico o los medios de instalación del software.</p>	Director o jefe de dependencia	Correo electrónico
2	Actualizar inventario de llaves criptográficas	El gestor de operaciones de la DGTIC que cumple las funciones de líder de Seguridad, una vez sea informado de la existencia de la nueva llave criptográfica, con el propósito de mantener actualizado el control de llaves, registra dentro del formato "Inventario de llaves criptográficas" la novedad reportada.	Gestor de operaciones de la DGTIC	OSTI-FR07 Inventario de llaves de cifrado
3	Definir y o actualizar solicitantes para firma de documentos de firma digital	El custodio y responsable del manejo de las llaves criptográficas tipo "Firma digital", una vez sea notificado de la asignación, solicita a los directores y jefes de oficina que le informen que tipos de documentos deben ser firmados con dicho token, para esto deberá solicitar la siguiente información: <ul style="list-style-type: none"> • Tipo de documento a firmar • Frecuencia de firma 	Custodio y responsable del manejo del Token	OSTI-FR06 Listado de documentos a firmar

No	Actividad	Descripción de la Actividad	Responsable	Registro
		<ul style="list-style-type: none"> Dirección oficina solicitante Destinatario Personal autorizado para solicitar la firma desde la dependencia solicitante <p>Dicha información deberá ser diligenciada en OSTI-FR06 Listado de documentos a firmar, el cual deberá quedar almacenado dentro de las herramientas colaborativas definidas por la DGTIC</p>		
4	Realizar solicitud de firma de documentos	<p>Con el propósito de cumplir con lo definido dentro de los diferentes procedimientos y conforme al archivo de control que se tenga para la llave criptográfica tipo "Firma digital", los solicitantes permitidos realizarán el requerimiento de firma de documentos al Custodio y responsable del manejo del Token, dicha solicitud la llevarán a cabo mediante correo electrónico, indicando si es necesario donde se encuentra la información a ser firmada o adjuntando el (los) documento(s) que requieren la firma.</p>	Solicitantes permitidos conforme al archivo de control	Correo electrónico
5	Validar si se cuenta con la autorización de solicitud de firma de documentos	<p>El Custodio y responsable del manejo del Token, una vez reciba la solicitud y con el propósito de firmar el(los) documento(s) de acuerdo con lo definido dentro del archivo de control, valida:</p> <ul style="list-style-type: none"> La solicitud es realizada por el personal autorizado. El o los documentos a firmar corresponden a la solicitud <p>¿Las validaciones son satisfactorias?</p> <p>SI: Se continua con la actividad siguiente</p> <p>NO: Se informa al solicitante las inconsistencias encontradas y se requiere que sean verificadas. Retornando a la actividad anterior. Para lo cual, la respuesta de la solicitud se llevará acabo vía correo electrónico.</p>	Custodio y responsable del manejo del Token	Correo electrónico
6	Realizar proceso de firma de documentos	<p>Una vez validada la solicitud, El Custodio y responsable del manejo del Token realiza el proceso de firma digital de los documentos. Posteriormente a la firma, responderá vía correo electrónico al solicitante que la acción ya se ha llevado a cabo indicando adicionalmente la ubicación en la cual se ha dispuesto la información firmada o adjuntándola dentro del cuerpo del mensaje.</p>	Custodio y responsable del manejo del Token	Correo electrónico
7	Informar novedades frente al token físico.	<p>El Custodio y responsable del manejo del Token cuando se presente una novedad frente a la gestión de este deberá informar al director o jefe que le delego la</p>	Custodio y responsable del manejo del Token	Correo electrónico

No	Actividad	Descripción de la Actividad	Responsable	Registro
		<p>responsabilidad de manejo de este. Las novedades por reportar serán:</p> <ul style="list-style-type: none"> • Retiro del Custodio y responsable del manejo del Token • Vencimiento del Token • Daño o deterioro del Token • Finalización de la relación comercial con el tercero proveedor del token <p>Dichas novedades deberán ser informadas vía correo electrónico</p>		
8 PC	Validar novedad frente al token físico.	<p>El director o jefe de dependencia, una vez conocida la novedad reportada y con el propósito de determinar la acción a seguir, valida la novedad informada, identificando la razón de esta.</p> <p>De donde: ¿Es retiro del Custodio y responsable del manejo del Token? SI: Asignará un nuevo responsable, por lo cual el procedimiento retornará a la actividad número 1 del presente procedimiento.</p> <p>NO: Teniendo en cuenta que la novedad podrá ser por:</p> <ul style="list-style-type: none"> • Vencimiento del Token • Daño o deterioro del Token • Finalización de la relación comercial con el tercero proveedor del token <p>Informará vía correo electrónico al director de Gestión de Tecnología de Información y Comunicaciones y al gestor de operaciones de la DGTIC que cumple las funciones de líder de Seguridad de la Información dicha novedad, continuando así con la siguiente actividad.</p>	Director o jefe de dependencia	Correo electrónico
	Retirar token del inventario de llaves criptográficas	El gestor de operaciones de la DGTIC que cumple las funciones de líder de Seguridad de la Información una vez sea notificado de la novedad, con el propósito de mantener actualizado el archivo de control realizará la novedad de retiro dentro este. Indicando adicionalmente, fecha y responsable de la novedad de retiro	Gestor de operaciones de la DGTIC que cumple las funciones de líder de Seguridad de la Información	OSTI-FR07 Inventario de llaves de cifrado
9	Entregar medio físico a tercero	Una vez se haya notificado al director de Gestión de Tecnología de Información y Comunicaciones y al gestor de operaciones de la DGTIC que cumple las funciones de líder de Seguridad de la Información, que se puede retirar del inventario la llave criptográfica, mediante los canales	Director o jefe de dependencia	Oficio donde se relaciona entrega del token.

	PROCEDIMIENTO GESTIÓN DE LLAVES CRIPTOGRÁFICAS	Código:	OSTI-PR13
		Versión:	01
		Fecha:	18/03/2020
		Página:	Página 5 de 5

No	Actividad	Descripción de la Actividad	Responsable	Registro
		definidos por el tercero proveedor del token, realizará la entrega de este, dejando como evidencia el oficio enviado al tercero. FIN DEL PROCEDIMIENTO		

8 CONTROL DE CAMBIOS

Versión	Fecha	Descripción del cambio	Asesor del proceso
01	<i>18 de marzo de 2020</i>	Emisión y Publicación inicial	Olga Marcela Vargas Valenzuela Asesor OAPCR
01	<i>9 de julio de 2020</i>	Actualización código por cambio de nombre del proceso de GSTE a OSTI. No se genera nueva versión debido a que no se modifica contenido del procedimiento y por lo tanto no requiere aprobación por parte del líder del proceso.	Olga Marcela Vargas Valenzuela Asesor OAPCR

9 ELABORACIÓN, REVISIÓN Y APROBACIÓN

Elaborado por:	Revisado por:	Aprobado por:
Juan Carlos Escobar Baquero Gestor de Operaciones	Carlos Andrés Ruiz Romero Gestor de Operaciones	Sergio Andrés Soler Rosas. Director de Gestión de Tecnologías de Información y Comunicaciones