



POLÍTICA
CERTIFICACIÓN DE FIRMA ELECTRÓNICA AVANZADA
FUNCIONARIO PÚBLICO

MPR-GIT-TIG-AEB-003-V1

SAR
SERVICIO DE ADMINISTRACIÓN DE RENTAS

SECRETARÍA GENERAL

Diciembre 2021



**POLÍTICA DE CERTIFICACIÓN DE FIRMA ELECTRÓNICA
AVANZADA FUNCIONARIO PÚBLICO**

Código:
MPR-GIT-TIG-AEB-003-V1

SECRETARÍA GENERAL

Fecha de vigencia:
Diciembre - 2021

FECHA VIGENCIA: Diciembre - 2021	CÓDIGO: MPR-GIT-TIG-AEB-003-V1	VERSIÓN 1.0	Nº PÁGINAS 43
--------------------------------------------	------------------------------------------	-----------------------	-------------------------

**POLÍTICA DE CERTIFICACIÓN DE FIRMA ELECTRÓNICA
AVANZADA FUNCIONARIO PÚBLICO**

RUBRO	CARGO	FIRMA
APROBADO POR:	Abg. Miriam Estela Guzmán Bonilla Directora Ejecutiva	
	Abg. Ángela Madrid Sub Directora Ejecutiva	
REVISADO POR:	Abog. Carmen Alejandra Suarez Secretaria General	
	Abg. Cristian Erazo Director Nacional Jurídico	
	Ing. Diana Orestila Cárcamo Rodriguez Directora Nacional de Tecnología	
	Abg. Rosa Peña Jefe Departamento de Asesoría Legal	
	Ing. Nathaly Nuñez Jefe Gestión de Procesos	
ELABORADO POR:	Abg. Carlos Antonio Garcia Garcia Especialista de Secretaria General	
	Ing. Francisco Rafael Dominguez Analista de Gestión de Procesos	

Nota:

El responsable de aprobar es sujeto de cambio siempre que exista una delegación formal de tal atribución emitida por la máxima autoridad. Los responsables de revisar serán siempre las jefaturas y direcciones responsables del proceso según el catálogo vigente a la fecha. Pueden constar como revisores jefaturas y direcciones vinculadas con el proceso.

Este documento institucional no puede ser reproducido, transmitido o almacenado por ningún medio telemático o físico sin autorización por escrito de la Administración tributaria.



Tabla de contenido

1.	Control del documento	5
2.	Objetivo estratégico vinculado al documento	5
3.	Documento Relacionado	5
4.	Área o departamento relacionado para este documento	6
5.	Identificación del proceso	6
6.	Objetivo	7
7.	Alcance	7
8.	Exclusiones	7
9.	Marco legal	8
10.	Marco técnico	8
11.	Normas y disposiciones	9
12.	Narrativa	9
12.1	Proceso I: Solicitud de Habilitación de certificado de Firma Electrónica avanzada	11
12.2	Proceso II: Firma de Documentos Electrónicos	12
12.3	Proceso III: Gestión de Suspensión de Certificado Electrónico	13
12.4	Proceso IV: Gestión de Reactivación de Certificado Electrónico	13
12.5	Proceso V: Gestión de Revocación de Certificado Electrónico	14
13.	Caracterización	15
13.1	Diagrama de flujo proceso I: Solicitud de HABILITACIÓN de Firma Electrónica Avanzada	16
13.1.1	Cuadro de Descripción Proceso I: Solicitud de HABILITACIÓN DE Certificado de Firma Electrónica Avanzada	17
13.1.2	Documentos (D) / Sistemas (S) / Correos Electrónicos (CE)	22
13.2	Diagrama de flujo proceso II: Firma de Documentos Electrónicos	23
13.2.1	Cuadro de Descripción Proceso II: Firma de Documentos Electrónicos	24
13.2.1	Documentos (D) / Sistemas (S) / Correos Electrónicos (CE)	26
13.3	Diagrama de flujo proceso III: Gestión de Suspensión de Certificado Electrónico	27



**POLÍTICA DE CERTIFICACIÓN DE FIRMA ELECTRÓNICA
AVANZADA FUNCIONARIO PÚBLICO**

SECRETARÍA GENERAL

Código:
MPR-GIT-TIG-AEB-003-V1

Fecha de vigencia:
Diciembre - 2021

13.3.1 Cuadro de Descripción Proceso III: Gestión de Suspensión de Certificado Electrónico	28
13.3.2 Documentos (D) / Sistemas (S) / Correos Electrónicos (CE)	30
13.4 Diagrama de flujo proceso IV: Gestión de Reactivación de Certificado Electrónico	31
13.4.1 Cuadro de Descripción Proceso IV: Gestión de Reactivación de Certificado Electrónico	32
13.4.2 Documentos (D) / Sistemas (S) / Correos Electrónicos (CE)	34
13.5 Diagrama de flujo proceso V: Gestión de Revocación de Certificado Electrónico	35
13.5.1 Cuadro de Descripción Proceso V: Gestión de Revocación de Certificado Electrónico	36
13.5.2 Documentos (D) / Sistemas (S) / Correos Electrónicos (CE)	38
14. Glosario de Términos	39
15. Matriz de Riesgos de Procesos	42
16. Matriz de Indicadores de Procesos	43



1. CONTROL DEL DOCUMENTO

Versión	Motivo	Fecha de vigencia	Documentos que elimina
1.0	Creación	Diciembre – 2021	N/A

2. OBJETIVO ESTRATÉGICO VINCULADO AL DOCUMENTO

OBJETIVO ESTRATÉGICO

Objetivo Estratégico 2: Reducir los costos del cumplimiento a través de la estandarización de procesos y el uso de tecnologías de la información y comunicaciones.

3. DOCUMENTO RELACIONADO

Nombre del Documento Relacionado	Código o número de acuerdo o del Documento Relacionado
Política Declaración de Prácticas de Certificación de Infraestructura de Clave Pública.	N/A



4. ÁREA O DEPARTAMENTO RELACIONADO PARA ESTE DOCUMENTO

Dirección	Departamento	Unidad Coordinación
Secretaría General	N/A	Archivo
		Acceso a la Información Pública
Dirección de Talento Humano	Departamento de Planificación y Desarrollo del Talento Humano	N/A
	Departamento de Gestión del Talento Humano	N/A
Dirección Nacional de Tecnología	Departamento de Gestión Aplicaciones	N/A
	Departamento de Infraestructura y Redes	N/A

5. IDENTIFICACIÓN DEL PROCESO

MACROPROCESO	4.- Gestión de la Información
PROCESO A PRIMER NIVEL:	4.1. Gestión del Gobierno de la Información 4.3 Gestión de la Seguridad de la Información
PROCESO A SEGUNDO NIVEL:	N/A
RESPONSABLE DEL PROCESO:	Secretaría General



6. OBJETIVO

El presente manual de procedimiento tiene por objeto recoger los procesos de firma electrónica avanzada, las que estarán regidos por el funcionamiento y la operatividad del servicio de Infraestructura de clave pública del Servicio de Administración de Rentas SAR-PKI.

Asimismo, definir las actividades en las cuales debe basarse el servicio de firma electrónica avanzada, su naturaleza, estructura y organización, de igual manera establecer los criterios y procedimientos que debe tomarse en consideración al momento de prestar el servicio de firma para las solicitudes de certificados, generación de claves, emisión, distribución, uso, revocación, suspensión y renovación de los certificados digitales.

7. ALCANCE

Que los certificados emitidos por El Servicio de Administración de Rentas SAR-PKI, cumplan con los estándares X.509 de la versión 3, y de esta manera hacer posible la adición de extensión para los certificados de atributos.

En base a lo establecido en el Acuerdo SAR-002-2017, El Servicio de Administración de Rentas crea la Secretaría General que será la encargada de regular todo lo concerniente a la Firma Electrónica, teniendo como fin poner a disposición de los funcionarios públicos los procedimientos y sistemas necesarios permitiendo garantizar la seguridad de la comunicación en la base digital.

Los documentos firmados mediante firma electrónica no excluyen la obligatoriedad de registrar las actividades en el módulo SOFIA.

8. EXCLUSIONES

En este Manual de Procedimiento se contemplan únicamente los procesos correspondientes a Firma Electrónica Avanzada de funcionarios públicos que forman parte del Servicio de Administración de Rentas.



**POLÍTICA DE CERTIFICACIÓN DE FIRMA ELECTRÓNICA
AVANZADA FUNCIONARIO PÚBLICO**

SECRETARÍA GENERAL

Código:
MPR-GIT-TIG-AEB-003-V1

Fecha de vigencia:
Diciembre - 2021

9. MARCO LEGAL

Identificación de norma (Resolución o Acuerdo)	Fecha de vigencia	Referencia específica
<ul style="list-style-type: none">Decreto Legislativo 170-2016, contenido del Código Tributario, publicado en el Diario Oficial La Gaceta No. 34,224 del 28 de diciembre del 2016 y sus reformas.	Enero 2017	Artículo, 82 y 83
<ul style="list-style-type: none">Ley de Firma Electrónica, Decreto No.149 -2013 y sus reformas	2013	Toda la Ley
<ul style="list-style-type: none">Reglamento de Firma Electrónica, Acuerdo Ejecutivo No.41-2014	2014	Todo el Reglamento
<ul style="list-style-type: none">Autorización al SAR para operar como Autoridad Certificadora o Prestadora de Servicios de Certificación PSC	2017	Resolución No. 002-2017
<ul style="list-style-type: none">Creación de Comité de Firma Electrónica	2018	Acuerdo SAR 374-2018

10. MARCO TÉCNICO

Documentos de Referencia	Fecha de vigencia
Versión 3 del estándar X.509	2008
Recomendaciones del RFC 7382	2015



11. NORMAS Y DISPOSICIONES

- a. Las normas y disposiciones señaladas en este documento son de aplicación obligatoria para todos los funcionarios y empleados del Servicio de Administración de Rentas (SAR) a nivel nacional. Los incumplimientos podrán ser sancionados conforme a lo establecido en el Régimen de Carrera de Empleados y Funcionarios en el Servicio de Administración de Rentas y las leyes vigentes de la República de Honduras que sean aplicables en la materia.
- b. Los aspectos que no se encuentren normados de forma expresa en este documento deberán ser complementados o suplidos por las disposiciones legales que apliquen.
- c. Los cambios y/o modificaciones que experimente el marco normativo nacional, prevalecerán sobre las disposiciones contenidas en el presente documento hasta su actualización.
- d. Los documentos firmados mediante firma electrónica no excluyen la obligatoriedad de registrar las actividades en el módulo SOFIA.

12. NARRATIVA

En el presente manual se explican 5 procesos que se tienen contemplados para la Firma electrónica y son:

1. Habilitación de certificado: En este procedimiento se explica de manera detallada los pasos a llevar a cabo para realizar la habilitación del certificado de firma electrónica el cual se hará conjuntamente a la notificación del acuerdo con los que se delegue las facultades de firma.
2. Firma de Documentos Electrónicos: En este procedimiento se explica la manera de estampar la firma electrónica en un documento, los requisitos del documento y las validaciones que realiza la herramienta tecnológica.
3. Gestión de Suspensión de Certificado Electrónico: La suspensión es el procedimiento mediante el cual se invalida de manera temporal un certificado



**POLÍTICA DE CERTIFICACIÓN DE FIRMA ELECTRÓNICA
AVANZADA FUNCIONARIO PÚBLICO**

SECRETARÍA GENERAL

Código:
MPR-GIT-TIG-AEB-003-V1

Fecha de vigencia:
Diciembre - 2021

de firma electrónica por los motivos establecidos en la "Política Declaración de Prácticas de Certificación de Infraestructura de Clave Pública"

4. *Gestión de Reactivación de Certificado Electrónico*: Es la Acción mediante la cual da validez a un certificado que anteriormente había sido suspendido, una vez que los motivos que provocaron su suspensión hayan cesado.
5. *Gestión de Revocación de Certificado Electrónico*: Es la Acción mediante la cual se invalida un certificado antes de su fecha de caducidad de manera definitiva por las causales establecidas en la Ley Sobre Firmas Electrónicas y las "Política Declaración de Prácticas de Certificación de Infraestructura de Clave Pública".

Para los procesos de cambio de estado de los Certificados de Firma Electrónica sea suspensión, reactivación o revocación se debe tener presente los movimientos de personal de los Funcionarios Públicos, actuando de oficio o previa solicitud en los casos que corresponda según las siguientes reglas:

1. **Suspensión de colaborador**: Dará lugar de oficio a la suspensión del Certificado de Firma, iniciando el proceso una vez que la Secretaría General sea informada por parte de la DNTH.
2. **Vacaciones**: Puede dar lugar a la suspensión del Certificado de Firma Electrónica a criterio del jefe normativo u operativo previa solicitud de éste a Secretaria General con el visto bueno de su respectivo Director, en este caso no será de oficio, dicha solicitud de suspensión del certificado de Firma Electrónica del colaborador que gozará de vacaciones se hará una vez que la notificación de vacaciones haya sido realizada por parte de la DNTH al colaborador.
3. **Cancelación**: Dará lugar de oficio a la revocación del Certificado de Firma Electrónica, se iniciará el proceso una vez que la Secretaría General sea informada por parte de la DNTH de la cancelación del colaborador.
4. **Licencia no remunerada**: Cuando la licencia sea de 6 meses o más tiempo dará lugar de oficio a la revocación del Certificado de Firma Electrónica, cuando sea menor de 6 meses procede de oficio la suspensión; queda a criterio del jefe normativo u operativo con el visto bueno de su respectivo Director, solicitar en este caso la revocación o la reactivación del certificado suspendido, el proceso de oficio iniciará una vez que la Secretaria General sea informada por parte de la DNTH de la autorización de la licencia.
5. **Licencia Remunerada**: Puede dar lugar a la suspensión o revocación del Certificado de Firma Electrónica a criterio del jefe normativo u operativo con el visto bueno de su respectivo Director, según el análisis del caso concreto una vez que la Secretaria General sea informada por parte de la DNTH de la autorización de la licencia.



6. **Incapacidad:** Queda a criterio del jefe normativo u operativo del colaborador involucrado con el visto bueno del respectivo Director el solicitar la suspensión del certificado de Firma Electrónica el cual debe hacerlo inmediatamente tenga conocimiento de la incapacidad y el tiempo en que el colaborador estará ausente según el análisis del caso concreto.
7. **Traslado Permanente:** Dará lugar de oficio a la revocación del Certificado de Firma Electrónica, el proceso de oficio iniciará una vez que la Secretaría General sea informada por parte de la DNTH del traslado del colaborador.
8. **Traslado Temporal:** Puede dar lugar a la suspensión o revocación del Certificado de Firma Electrónica a criterio del jefe normativo u operativo previa solicitud de este a Secretaría General con el visto bueno de su respectivo Director.
9. **Reincorporación:** La reincorporación de un colaborador que estuvo ausente de su cargo y esta ausencia generó la suspensión del Certificado de Firma de oficio, dará lugar a la Reactivación de su Certificado de oficio si este no ha caducado.

Luego de proceder con la actualización de estado del certificado, sea suspendido, reactivado o revocado, la herramienta de gestión de firma electrónica avanzada actualizará la lista de certificados revocados y notificará al custodio del certificado a través de correo electrónico el cambio de estado del certificado solicitado.

El certificado revocado, suspendido o vencido no es posible usarlo para firma de documentos en virtud que cada vez que se intenta firmar un documento el sistema validará la vigencia de este y al encontrarlo en el listado de certificados revocados, suspendidos o vencidos no estampará la firma impidiendo su uso.

12.1 PROCESO I: SOLICITUD DE HABILITACIÓN DE CERTIFICADO DE FIRMA ELECTRÓNICA AVANZADA

En este proceso se realiza la habilitación del Certificado de Firma Electrónica en donde el jefe normativo o jefe inmediato según corresponda con el visto bueno del Director correspondiente, presentará la petición de delegación de firma a Secretaría General, donde se elaborará el acuerdo que corresponda e instruirá al Encargado de Firma Electrónica para proceder con la emisión del certificado. Al cumplir con todos los requisitos el Encargado de Firma Electrónica registra la información del funcionario en la herramienta tecnológica para generar el certificado electrónico.

En el caso que el certificado que se emitió con la delegación de firma expire o haya sido revocado, el jefe del custodio de la firma solicitará la emisión de un nuevo certificado a Secretaría General la cual validará que el colaborador siga activo en la Administración Tributaria realizando la consulta a la Dirección Nacional de Talento Humano.



En caso de ser una solicitud de actualización de estado de certificado ya sea suspensión, reactivación o revocación de certificado se debe iniciar por el respectivo proceso según sea el caso.

El Encargado debe proporcionar al custodio los "TÉRMINOS Y CONDICIONES DE USO PARA LOS CERTIFICADOS DE FIRMA ELECTRONICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS" este último deberá leerlos, firmar y estampar su huella digital del dedo índice de la mano derecha como requisito previo para poder emitirle el certificado de firma electrónica correspondiente.

Una vez realizado el paso anterior, se procederá a iniciar el registro de los datos en la Herramienta de Gestión de Firma Electrónica Avanzada; previo a finalizar el Encargado solicitará al custodio que ingrese su clave privada, luego la Herramienta de Gestión de Firma Electrónica Avanzada hará la notificación y remisión del certificado al correo electrónico del custodio; éste debe realizar la validación que dicho correo fue recibido e informar al Encargado.

Se iniciará de oficio con la generación del certificado de Firma Electrónica a los funcionarios que ya tienen delegación de firma.

12.2 PROCESO II: FIRMA DE DOCUMENTOS ELECTRÓNICOS

Todo funcionario público del Servicio de Administración de Rentas debe validar el formato digital del documento que será firmado. Si no cuenta con un formato válido, lo debe convertir. En el caso de que el contenido del documento deba ser modificado previo a ser firmado y la autoría de este no pertenezca al firmante, se debe remitir el documento al autor para que realice su modificación.

Una vez validado el formato digital y el contenido del documento se procede a realizar la firma, en la parte derecha de la pantalla se busca la opción de "Mas Herramientas", se selecciona la opción de "Certificados" y se abre un panel en la parte superior, se selecciona la opción "Firmar digitalmente" de ese panel y el cursor cambia de forma para permitir seleccionar el espacio donde se firmará, se procede a parametrizar el certificado digital.

Dar clic en la opción "Configurar el ID digital", seleccionar la opción "Utilizar un ID digital de un archivo" y dar clic en continuar, luego pide que se busque el archivo de certificado en el directorio donde esta guardado, requiere que se escriba la contraseña a utilizar para la firma con el certificado de firma, clic en continuar (ver video de firma de documentos que fue remitido en el curso de firma electrónica que se llevó a cabo, mismo que será nuevamente enviado al correo institucional de todos los colaboradores).

La Herramienta Tecnológica verificará el estado del certificado, en caso de que el estado sea inválido por suspensión, revocación o vencimiento del certificado,



mostrará un mensaje que impide estampar la firma; en caso de que el certificado sea válido, la Herramienta estampa la firma en el certificado y lo encripta para que posteriormente pueda ser remitido al destino que el firmante seleccione.

En la pantalla emergente debe seleccionar la ubicación en donde se guardará el documento firmado, selecciona la opción "Guardar".

12.3 PROCESO III: GESTIÓN DE SUSPENSIÓN DE CERTIFICADO ELECTRÓNICO

El proceso de suspensión de certificado electrónico puede iniciar de oficio o por petición del jefe inmediato o normativo del Funcionario con el visto bueno del respectivo Director. En caso de ser mediante solicitud, la petición de suspensión de Certificado Electrónico debe ser presentada ante la Secretaría General.

La Secretaría General o la persona que esta designe luego de revisar que la solicitud provenga de la jefatura normativa u operativa correspondiente con el visto bueno de su respectivo Director, así como que la documentación venga firmada y que no tiene omisiones de cualquier otra información que vulnere la seguridad del proceso, e instruirá al Encargado de Firma Electrónica para que proceda iniciar la suspensión del certificado.

En el caso que el proceso sea de oficio este iniciará con la notificación que haga la DNTH a Secretaría General del movimiento de personal según está establecido en el numeral 12 de este documento; la Secretaría General o la persona que ésta designe una vez recibida la notificación instruirá al Encargado de Firma Electrónica para que proceda iniciar la suspensión del certificado.

Se debe revisar la vigencia del certificado y en caso de que no sea vigente el certificado, se debe dar respuesta al solicitante indicando que el certificado ya expiró por lo que no es posible suspenderlo.

En caso de que sea válida la vigencia del certificado, proceder con la suspensión en la herramienta de Gestión de Firma Electrónica.

12.4 PROCESO IV: GESTIÓN DE REACTIVACIÓN DE CERTIFICADO ELECTRÓNICO

El proceso de Reactivación de certificado electrónico puede iniciar de oficio o por petición del jefe inmediato o normativo del Servidor Público con el visto bueno del respectivo Director. En caso de ser mediante solicitud, la petición de Reactivación de Certificado Electrónico debe ser presentada ante la Secretaría General.

La Secretaría General o la persona que esta designe luego de revisar que la solicitud provenga de la jefatura normativa u operativa correspondiente con el visto



bueno de su respectivo Director, así como que la documentación venga firmada y que no tiene omisiones de cualquier otra información que vulnere la seguridad del proceso, e instruirá al Encargado de Firma Electrónica para que proceda iniciar la Reactivación del certificado.

En el caso que el proceso sea de oficio este iniciará con la notificación que haga la DNTH a Secretaria General del movimiento de personal según está establecido en el numeral 12 de este documento; la Secretaria General o la persona que ésta designe una vez recibida la notificación instruirá al Encargado de Firma Electrónica para que proceda iniciar la Reactivación del certificado.

Se debe revisar la vigencia del certificado y en caso de que no sea vigente el certificado, se debe iniciar el procedimiento para solicitar un nuevo certificado mediante la **Solicitud habilitación de Certificado de Firma Electrónica Avanzada**.

En caso de que sea vigente el certificado, reactivar el certificado en la herramienta de Gestión de Firma Electrónica y se le informará al solicitante del acto.

12.5 PROCESO V: GESTIÓN DE REVOCACIÓN DE CERTIFICADO ELECTRÓNICO

El proceso de revocación de certificado electrónico puede iniciar de oficio o por petición del jefe inmediato o normativo del Servidor Público con el visto bueno del respectivo Director. En caso de ser mediante solicitud, la petición de revocación de Certificado Electrónico debe ser presentada ante la Secretaria General.

La Secretaria General o la persona que ésta designe luego de revisar que la solicitud provenga de la jefatura normativa u operativa correspondiente con el visto bueno de su respectivo Director, así como que la documentación venga firmada y que no tiene omisiones de cualquier otra información que vulnere la seguridad del proceso, se instruirá al Encargado de Firma Electrónica para que proceda iniciar la revocación del certificado

En el caso que el proceso sea de oficio éste iniciará con la notificación que haga la DNTH a Secretaria General del movimiento de personal según está establecido en el numeral 12 de este documento; la Secretaria General o la persona que esta designe una vez recibida la notificación instruirá al Encargado de Firma Electrónica para que proceda iniciar la revocación del certificado.

Se debe revisar la vigencia del certificado y en caso de que no sea vigente, se debe dar respuesta al solicitante indicando que el certificado ya expiró por lo que no es posible revocarlo.

En caso de que sea válida la vigencia del certificado, se debe proceder con la revocación en la herramienta de Gestión de Firma Electrónica.



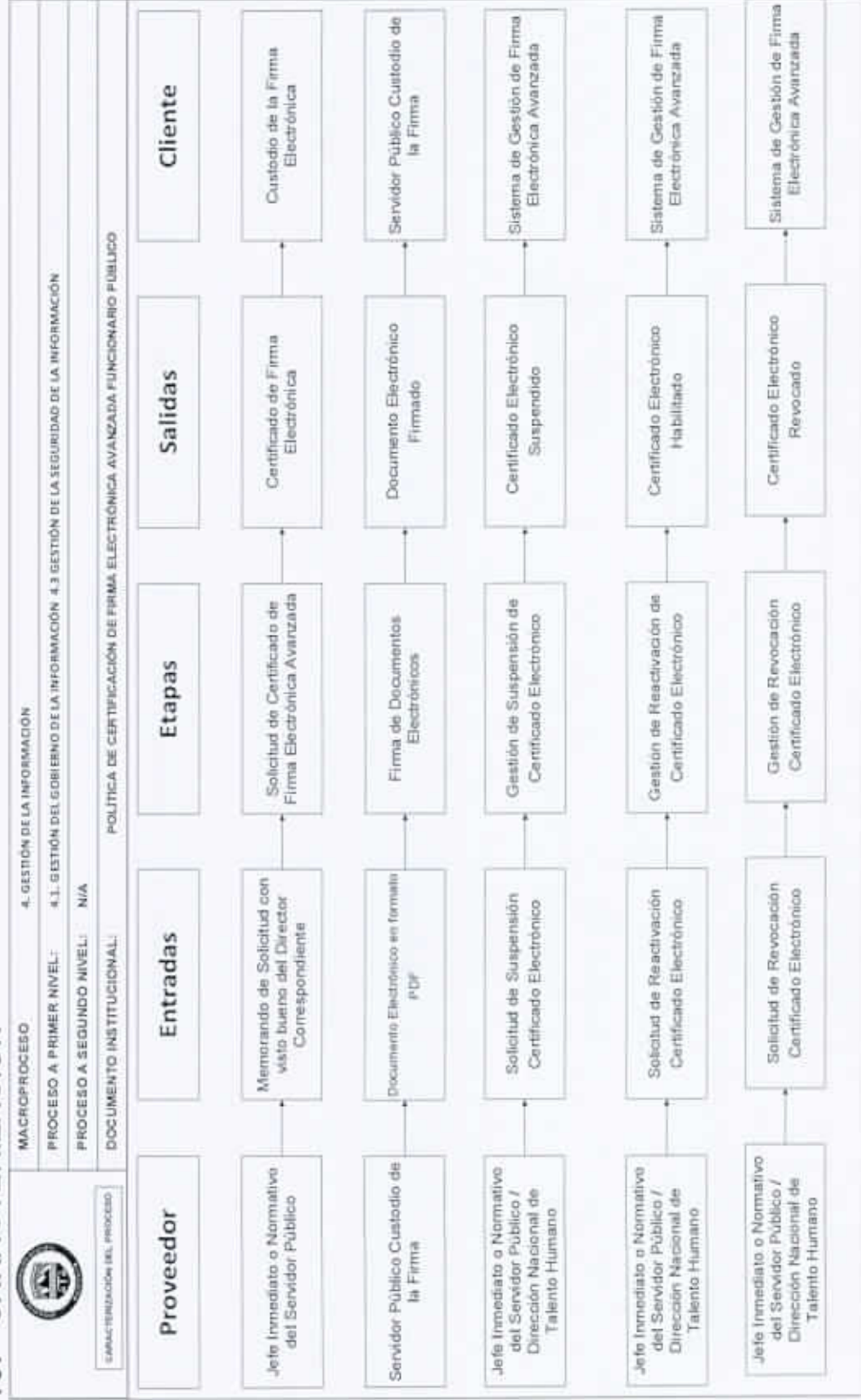
**POLÍTICA DE CERTIFICACIÓN DE FIRMA ELECTRÓNICA AVANZADA
FUNCIONARIO PÚBLICO**

SECRETARÍA GENERAL

Código:
MPR-GIT-TIG-AEB-003-V1

Fecha de vigencia:
Diciembre - 2021

13. CARACTERIZACIÓN





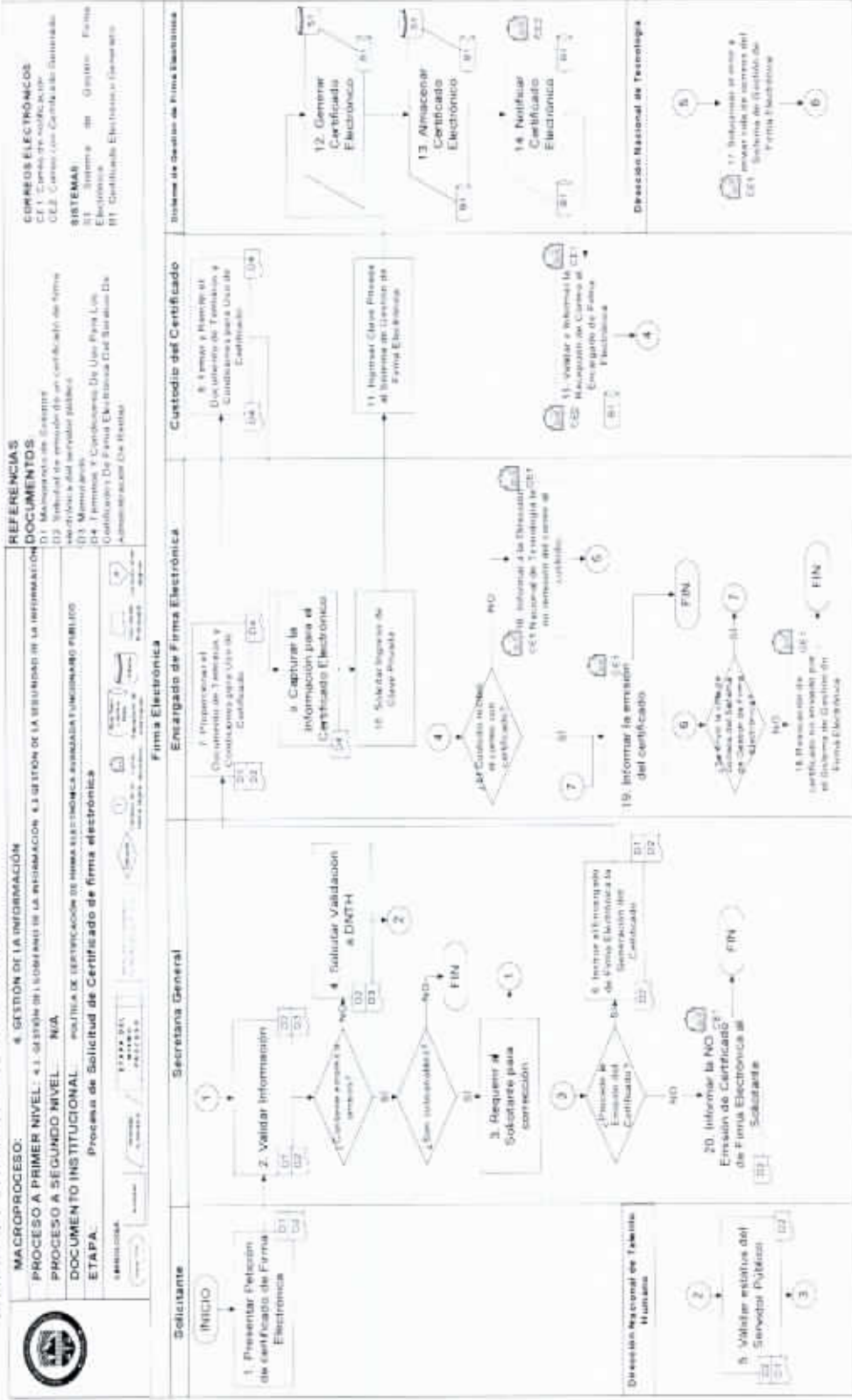
**POLÍTICA DE CERTIFICACIÓN DE FIRMA ELECTRÓNICA AVANZADA
FUNCIONARIO PÚBLICO**

SECRETARÍA GENERAL

Código:
MPR-GIT-TIG-AEB-003-V1

Fecha de vigencia:
Diciembre - 2021

13.1 DIAGRAMA DE FLUJO PROCESO I: SOLICITUD DE HABILITACIÓN DE FIRMA ELECTRÓNICA AVANZADA





13.1.1 CUADRO DE DESCRIPCIÓN PROCESO I: SOLICITUD DE
HABILITACIÓN DE CERTIFICADO DE FIRMA ELECTRÓNICA
AVANZADA.

N°	Actividad	Descripción de la Actividad	Responsable
1	Habilitación de certificado por emisión de acuerdo de delegación	Con esta actividad inicia la emisión del certificado de oficio en conjunto con la delegación de firma correspondiente. En este caso pasar a la actividad número 7.	Secretaría general
2	Solicitud de nuevo certificado por vencimiento.	Cuando este certificado expire la generación de un nuevo certificado será a solicitud del jefe del custodio con visto bueno del respectivo Director, dicha generación de nuevo certificado se hará en un tiempo máximo de 10 días hábiles.	Jefe de custodio
3	Validar información	Revisar que la solicitud provenga de la jefatura correspondiente con el visto bueno de su respectivo Director, que la documentación venga firmada, que las máximas autoridades autoricen el acuerdo y verificar que no tiene omisiones de cualquier otra información que vulnere la seguridad del proceso.	Secretaría General
4	Requerir al solicitante	En caso de que la solicitud contenga errores u omisos de los mencionados en el párrafo anterior, se requerirá al solicitante para que subsane la solicitud cuando no sean subsanables, se rechazará indicándole que debe realizarla nuevamente. En este último caso finaliza el proceso.	Secretaría General



POLÍTICA DE CERTIFICACIÓN DE FIRMA ELECTRÓNICA
AVANZADA FUNCIONARIO PÚBLICO

Código:
MPR-GIT-TIG-AEB-003-V1

Fecha de vigencia:
Diciembre - 2021

SECRETARÍA GENERAL

5	Solicitar validación a la Dirección Nacional de Talento Humano	La Secretaría General o la persona designada, firmará la solicitud y lo remitirá junto con el memorando de estatus del colaborador a la Dirección Nacional de Talento Humano para validar el estatus del funcionario público para quien se solicita la emisión de certificado de firma electrónica; si él mismo está vinculado, desvinculado o suspendido en el SAR.	Secretaría General
6	Validar el estatus del Servidor Público	La Dirección Nacional de Talento Humano informará por el mismo medio, dicho estatus, devolviendo toda la documentación remitida. (El cual debe dar respuesta en el término de un día hábil)	Dirección Nacional de Talento Humano
7	Instruir al encargado de firma electrónica la generación del certificado.	La Secretaría General o la persona designada, recibirá de Talento Humano el Informe del estatus del colaborador e instruirá al encargado que proceda a generar el certificado, si éste se encuentra vinculado al SAR. En caso de que el estatus del colaborador sea "desvinculado" o cuando existan motivo para no emitir el certificado pasar a la actividad número 21.	Secretaría General
8	Proporcionar los términos y condiciones de uso para los certificados de funcionarios públicos.	Proporcionar los términos y condiciones de uso para el certificado de funcionario público del Servicio de Administración de Rentas al custodio del certificado.	Encargado de Firma Electrónica
9	Firma de términos y condiciones de uso para los	Firmar y remitir el documento denominado "Términos y condiciones de uso para los certificados de firma electrónica	Custodio de Certificado



**POLÍTICA DE CERTIFICACIÓN DE FIRMA ELECTRÓNICA
AVANZADA FUNCIONARIO PÚBLICO**

Código:
MPR-GIT-TIG-AEB-003-V1

Fecha de vigencia:
Diciembre - 2021

SECRETARÍA GENERAL

	certificados de funcionarios público del Servicio de Administración de Rentas.	del Servicio de Administración de Rentas” al encargado de firma electrónica.	
10	Capturar la Información para el Certificado Electrónico	Ingresar al Sistema de Gestión Firma Electrónica. Transcribir los datos plasmados en el formulario de petición de firma electrónica.	Encargado de firma electrónica.
11	Solicitar ingreso clave privada	Solicitar al custodio del certificado que ingrese su clave privada al momento de generación del certificado de firma electrónica al servidor público, facilitando el teclado y pantalla para que pueda ingresar su clave privada. En caso de que el Servidor Público este asignado a una oficina cuya dirección física se encuentre fuera de Tegucigalpa, el ingreso de la clave se realizará de manera remota.	Encargado de Firma Electrónica
12	Ingresar Clave Privada al Sistema de Gestión Firma Electrónica	Ingresar Clave Privada del Certificado la cual debe ser diferente a la de su correo o cuenta institucional.	Custodio de Certificado
13	Generar el Certificado Electrónico	Encriptar los datos proporcionados en el formulario de suscripción con la clave privada del solicitante.	Sistema de Gestión de Firma Electrónica
14	Almacenar Certificado Electrónico	Almacenar el Certificado Electrónico dentro del directorio seguro.	Sistema de Gestión de Firma Electrónica



**POLÍTICA DE CERTIFICACIÓN DE FIRMA ELECTRÓNICA
AVANZADA FUNCIONARIO PÚBLICO**

Código:
MPR-GIT-TIG-AEB-003-V1

Fecha de vigencia:
Diciembre - 2021

SECRETARÍA GENERAL

15	Notificar Certificado Electrónico	Remitir a través de correo electrónico institucional el certificado de firma electrónica.	Sistema de Gestión de Firma Electrónica
16	Validar e Informar la Recepción de Correo Encargado de Firma Electrónica	En el momento de terminar la generación, el custodio debe ingresar a su correo electrónico institucional para validar la recepción del correo del Sistema de Gestión de Firma Electrónica que contiene el certificado e informar mediante correo electrónico adjuntando captura de pantalla de la recepción del correo en un plazo de 24 horas, en caso de que no lo reciba deberá informarlo mediante correo electrónico y si no notifica se dará como recibido y se validará mediante la herramienta de trazabilidad que se tenga disponible.	Custodio de Certificado
17	Informar a la Dirección Nacional de Tecnología de la no remisión del correo al custodio.	Si no recibió el correo electrónico con el certificado generado, el encargado de firma electrónica debe dejar constancia del acto e informar a la Dirección Nacional de Tecnología de tal situación.	Encargado de Firma Electrónica
18	Solucionar el error y enviar cola de correos del sistema de gestión de firma electrónica.	La Dirección Nacional de tecnología debe analizar el caso concreto y dar solución en un plazo no mayor a 3 días hábiles, e informar al encargado el resultado de su intervención, indicando si fue posible o no el envío del certificado mediante Sistema de Gestión de Firma Electrónica.	Dirección Nacional de Tecnología



**POLÍTICA DE CERTIFICACIÓN DE FIRMA ELECTRÓNICA
AVANZADA FUNCIONARIO PÚBLICO**

Código:
MPR-GIT-TIG-AEB-003-V1

Fecha de vigencia:
Diciembre - 2021

SECRETARÍA GENERAL

19	Revocación de certificado no enviado por el Sistema de Gestión de Firma Electrónica	En caso de que el certificado no fue enviado pese a la intervención de la Dirección Nacional de Tecnología y esta informó que atendió la gestión por el cual no se envió inicialmente el correo con el certificado se procederá a revocar el certificado que se generó y se notificará al solicitante que debe iniciar nuevamente el proceso. Fin del proceso.	Encargado de Firma Electrónica
20	Informar la emisión del certificado	La Secretaria General o la persona designada informará mediante correo al solicitante que el proceso de generación de firma electrónica se realizó exitosamente. Fin del proceso.	Secretaria General
21	Informar la no emisión de certificado de firma electrónica	Si en el informe de la Dirección Nacional de Talento Humano indica que el colaborador tiene estatus "desvinculado", "Suspendido" o que estando "vinculado" existan motivos para no emitir el certificado, la Secretaria General o la persona designada informará al solicitante que no procede la petición indicándole los motivos y haciéndole saber; que, cuando las circunstancias que impidieron la emisión del certificado cambien, proceda a realizar la solicitud nuevamente. Fin del proceso.	Secretaria General



**POLÍTICA DE CERTIFICACIÓN DE FIRMA ELECTRÓNICA
AVANZADA FUNCIONARIO PÚBLICO**

SECRETARÍA GENERAL

Código:
MPR-GIT-TIG-AEB-003-V1

Fecha de vigencia:
Diciembre - 2021

**13.1.2 DOCUMENTOS (D) / SISTEMAS (S) / CORREOS ELECTRÓNICOS
(CE)**

Documentos (D) / Sistemas(S) / Correos Electrónicos (CE)		Responsable de Generarlo y/o Presentarlo
D1	Memorando de la solicitud de emisión.	Jefe normativo u operativo según corresponda.
D2	Solicitud de emisión de un certificado de firma electrónica del servidor público.	Jefe normativo u operativo según corresponda.
D3	Memorando Remitiendo la solicitud	Secretaria General
D4	Memorando de remisión de estatus de colaborador	DNTH
D5	Términos Y Condiciones De Uso Para Los Certificados De Firma Electrónica Del Servicio De Administración De Rentas.	Encargado de Firma Electrónica
S1	Sistema de Gestión Firma Electrónica Avanzada	N/A
B1	Certificado Electrónico Generado	Sistema de Gestión de Firma Electrónica Avanzada
CE1	Correo de notificación.	Custodio de firma electrónica / encargado de firma electrónica.
CE2	Correo con Certificado Generado	Sistema de Gestión de Firma Electrónica Avanzada



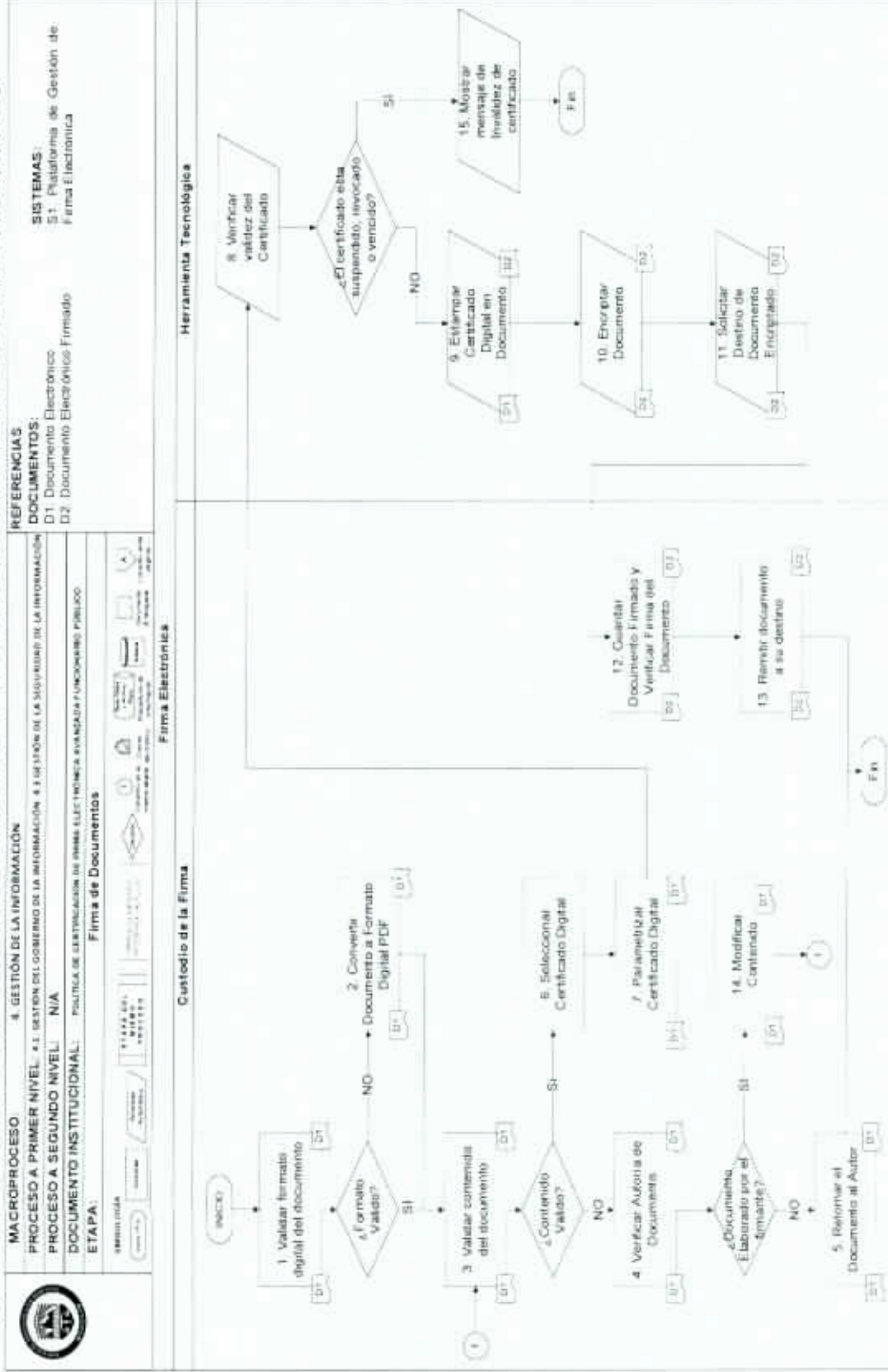
**POLÍTICA DE CERTIFICACIÓN DE FIRMA ELECTRÓNICA AVANZADA
FUNCIONARIO PÚBLICO**

SECRETARÍA GENERAL

Código:
MPR-GIT-TIG-AEB-003-V1

Fecha de vigencia:
Diciembre - 2021

13.2 DIAGRAMA DE FLUJO PROCESO II: FIRMA DE DOCUMENTOS ELECTRÓNICOS





13.2.1 CUADRO DE DESCRIPCIÓN PROCESO II: FIRMA DE DOCUMENTOS ELECTRÓNICOS

Nº	Actividad	Descripción de la Actividad	Responsable
1	Validar formato digital del documento	Abrir el documento, asegurándose que sea un formato PDF. En caso de que no sea el formato correcto, proceder a Convertir Documento a Formato Digital PDF.	Custodio de la Firma
2	Convertir Documento a Formato Digital PDF	Abrir el documento, ir a la sección de Archivo, seleccionar la opción de "Guardar Como", elegir un nombre y directorio para el archivo y cambiar la opción de formato a .pdf.	Custodio de la Firma
3	Validar contenido del documento	Validar que el contenido sea correcto. Si esta correcto, <i>Seleccionar Certificado Digital (Actividad 6).</i> En caso de que el documento seleccionado no sea válido se debe <i>Verificar la Autoría del Documento (Actividad 4)</i>	Custodio de la Firma
4	Verificar Autoría del Documento	Al momento de verificar la autoría del documento, si el documento no fue elaborado por el firmante se debe <i>Retornar el documento al Autor (Actividad 5).</i> En caso de que el documento si fue elaborado por el firmante, se debe <i>Modificar el Contenido (Actividad 14).</i>	Custodio de la Firma
5	Retornar el Documento al Autor	Remitir el documento al Autor de este.	Custodio de la Firma



**POLÍTICA DE CERTIFICACIÓN DE FIRMA ELECTRÓNICA
AVANZADA FUNCIONARIO PÚBLICO**

Código:
MPR-GIT-TIG-AEB-003-V1

Fecha de vigencia:
Diciembre - 2021

SECRETARÍA GENERAL

6	Seleccionar Certificado Digital	Seleccionar la opción de "Mas herramientas" luego la opción Certificados, abrir, en la parte superior del archivo se habilita las opciones de Certificados, elegir "Firmar digitalmente", damos clic en Aceptar al mensaje emergente que muestra.	Custodio de la Firma
7	Parametrizar Certificado Digital	Dar clic en la opción Configurar el ID digital, seleccionar la opción Utilizar un ID digital de un archivo y damos clic en continuar, requiere que escribamos la contraseña que utilizamos para la generación del certificado, luego nos pide que busquemos el archivo de certificado en el directorio donde lo tenemos guardado, clic en abrir, luego clic en continuar. En la pantalla emergente seleccionar la opción Crear de la parte superior derecha, y seleccionar que campos deseamos que se visualicen en la firma. Clic en guardar, luego dar clic en firmar	Custodio de la Firma
8	Verificar validez del Certificado	La herramienta validará el estado del certificado en caso de que el mismo sea "Suspendido, Revocado o esté vencido mostrará un mensaje y finalizará el proceso sin estampar la firma.	Herramienta Tecnológica
9	Estampar Certificado Digital en Documento	Acción interna de la herramienta.	Herramienta Tecnológica
10	Encriptar Documento	Acción interna de la herramienta.	Herramienta Tecnológica



**POLÍTICA DE CERTIFICACIÓN DE FIRMA ELECTRÓNICA
AVANZADA FUNCIONARIO PÚBLICO**

Código:
MPR-GIT-TIG-AEB-003-V1

Fecha de vigencia:
Diciembre - 2021

SECRETARÍA GENERAL

11	Solicitar Destino de Documento Encriptado	La Herramienta solicita donde se guardara el documento encriptado con la firma digital del custodio.	Herramienta Tecnológica
12	Guardar Documento Firmado y Verificar Firma del Documento	Guardar el documento y verificar la firma contenida en el documento	Custodio de la Firma
13	Remitir documento a su destino	Una vez se haya verificado que la firma está bien, se remite el documento al destino correspondiente.	Custodio de la Firma
14	Modificar Contenido	Si el contenido del documento no es correcto se debe modificar, luego se retorna a la <i>Actividad 3</i> para volver a validar el contenido del documento.	Custodio de la Firma
15	Mostrar mensaje de Invalidez de certificado	Al momento de validar el estado del certificado y si este es invalido, mostrará un mensaje que impedirá estampar la firma. Fin del Proceso	Herramienta Tecnológica

13.2.1 DOCUMENTOS (D) / SISTEMAS (S) / CORREOS ELECTRÓNICOS (CE)

Documentos (D) / Sistemas(S) / Correos Electrónicos (CE)		Responsable de Generarlo y/o Presentarlo
D1	Documento Electrónico	Custodio de la Firma
D2	Documento Electrónico Firmado	Custodio de la Firma
S1	Sistema de Gestión de Firma Electrónica	N/A



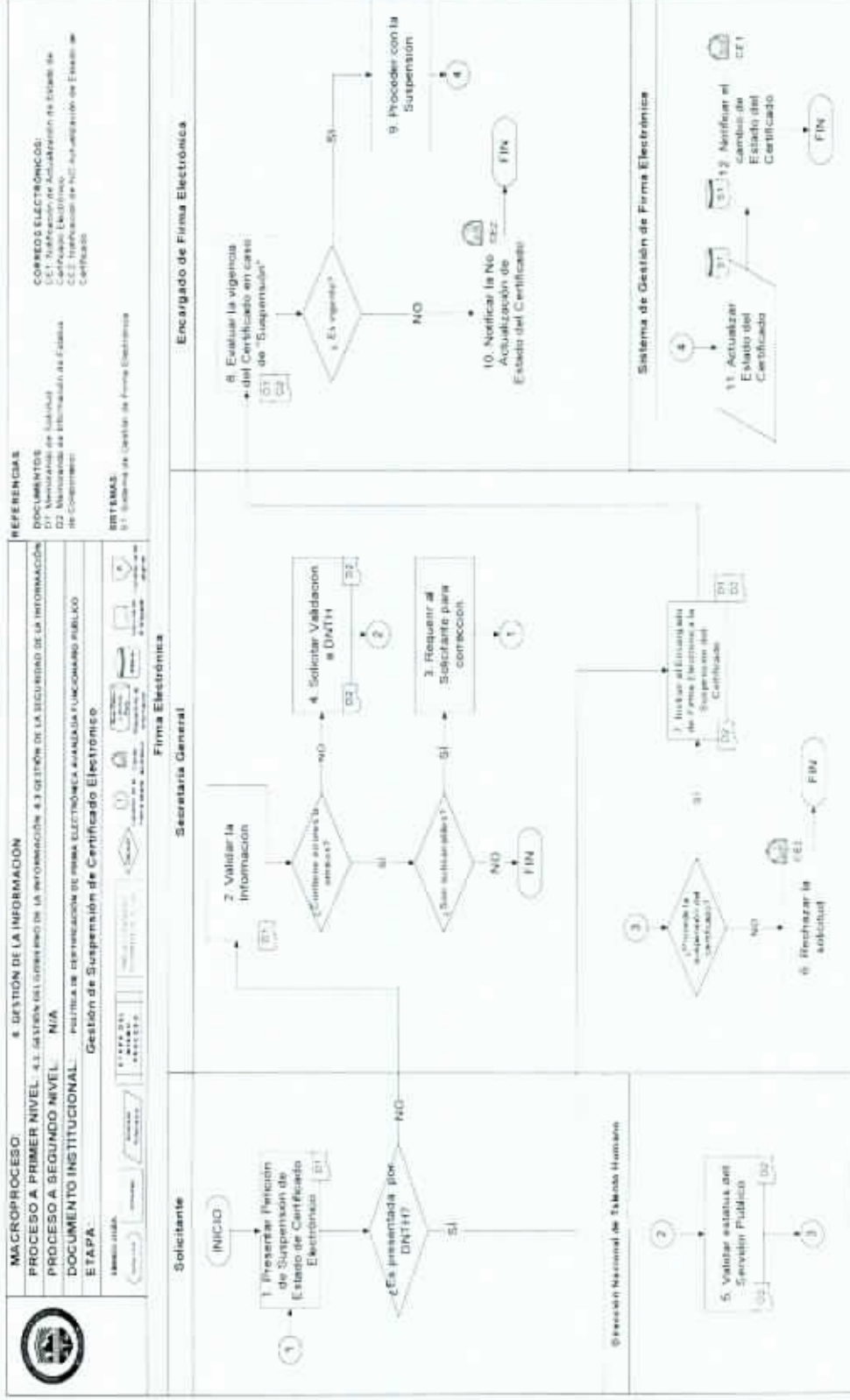
**POLÍTICA DE CERTIFICACIÓN DE FIRMA ELECTRÓNICA AVANZADA
FUNCIONARIO PÚBLICO**

SECRETARÍA GENERAL

Código:
MPR-GIT-TIG-AEB-003-V1

Fecha de vigencia:
Diciembre - 2021

13.3 DIAGRAMA DE FLUJO PROCESO III: GESTIÓN DE SUSPENSIÓN DE CERTIFICADO ELECTRÓNICO





POLÍTICA DE CERTIFICACIÓN DE FIRMA ELECTRÓNICA
AVANZADA FUNCIONARIO PÚBLICO

SECRETARÍA GENERAL

Código:
MPR-GIT-TIG-AEB-003-V1

Fecha de vigencia:
Diciembre - 2021

13.3.1 CUADRO DE DESCRIPCIÓN PROCESO III: GESTIÓN DE
SUSPENSIÓN DE CERTIFICADO ELECTRÓNICO

N°	Actividad	Descripción de la Actividad	Responsable
1	Remisión de notificación de movimiento de personal.	Remitir a la Secretaria General la notificación de movimiento de personal para que esta inicie de oficio el cambio de estado de Certificado de Firma según corresponda. Avanzar a la actividad 3.	DNTH.
2	Presentación de solicitud de suspensión de certificado de Firma Electrónica.	Presentar ante Secretaria General el memorando de solicitud de suspensión de Certificado Electrónico. Avanzar a la actividad 3.	Jefe normativo u operativo según corresponda.
3	Validar información	En caso de que la notificación de movimiento de personal sea lo que dé inicio al proceso, se debe validar que la suspensión de certificado sea la acción que corresponde según el tipo de movimiento de personal que se realizó y lo indicado en el numeral 12 de la presente Políticas de Certificación. Avanzar a la actividad 5. Revisar que la solicitud provenga de la jefatura normativa u operativa correspondiente con el visto bueno de su respectivo Director; revisar que la documentación venga firmada y verificar que no tiene omisiones de cualquier otra información que vulnere la seguridad del proceso. Avanzar a la actividad 4.	Secretaria General.
4	Requerir al solicitante	En caso de que la solicitud contenga errores y omisos de los mencionados en el párrafo anterior, se requerirá al solicitante para que proceda a corregir los errores de la solicitud en caso de	Secretaría General.



**POLÍTICA DE CERTIFICACIÓN DE FIRMA ELECTRÓNICA
AVANZADA FUNCIONARIO PÚBLICO**

SECRETARÍA GENERAL

Código:
MPR-GIT-TIG-AEB-003-V1

Fecha de vigencia:
Diciembre - 2021

		ser subsanables, cuando no sea subsanable se rechazará la solicitud indicándole que debe realizarla nuevamente. Fin del proceso	
5	Instruir al Encargado de Firma Electrónica que proceda con la suspensión de certificado electrónico	Una vez revisado el tipo de movimiento de personal que la notificación de DNTH indica que se realizó y ya se ha determinado que lo correspondiente de oficio es la suspensión del Certificado según esta Política de Certificación o habiendo concluido que la solicitud procede, se instruirá al encargado de firma electrónica que realice la suspensión del certificado de firma electrónica.	Secretaría General.
6	Evaluar la vigencia del Certificado	Se debe revisar la vigencia del certificado del custodio. Si no es vigente el certificado se debe dar respuesta al solicitante indicando que el certificado ya expiró por lo que no es posible suspenderlo. Avanzar a la actividad 8.	Encargado de firma electrónica.
7	Proceder con la Suspensión	En caso de que sea válida la vigencia del certificado, proceder con la suspensión en la herramienta de Gestión de Firma Electrónica.	Encargado de firma electrónica
8	Notificar la No Actualización de Estado del Certificado	Notificar al Custodio de Firma a la dirección de correo registrada la no actualización de estado del certificado solicitado. Fin del Proceso.	Encargado de Firma Electrónica
9	Actualizar Estado del Certificado	Luego de proceder con la suspensión, actualizar la lista de certificados suspendidos.	Sistema de Gestión de Firma Electrónica Avanzada



**POLÍTICA DE CERTIFICACIÓN DE FIRMA ELECTRÓNICA
AVANZADA FUNCIONARIO PÚBLICO**

Código:
MPR-GIT-TIG-AEB-003-V1

SECRETARÍA GENERAL

Fecha de vigencia:
Diciembre - 2021

10	Notificar el cambio de estado del Certificado	Notificar a través de correo electrónico al Custodio de Firma a la dirección de correo registrada el cambio de estado del certificado solicitado. Fin del Proceso.	Sistema de Gestión de Firma Electrónica Avanzada
----	-----------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------

13.3.2 DOCUMENTOS (D) / SISTEMAS (S) / CORREOS ELECTRÓNICOS (CE)

Documentos (D) / Sistemas(S) / Correos Electrónicos (CE)		Responsable de Generarlo y/o Presentarlo
D1	Memorando de solicitud.	Jefe normativo u operativo según corresponda
D2	Notificación de Movimiento de personal.	DNTH
CE1	Notificación de Actualización de Estado de Certificado Electrónico	Sistema de Gestión de Firma Electrónica Avanzada
CE2	Notificación de NO Actualización de Estado de Certificado	Encargado de Firma Electrónica
S1	Herramienta de Gestión de Firma Electrónica	N/A



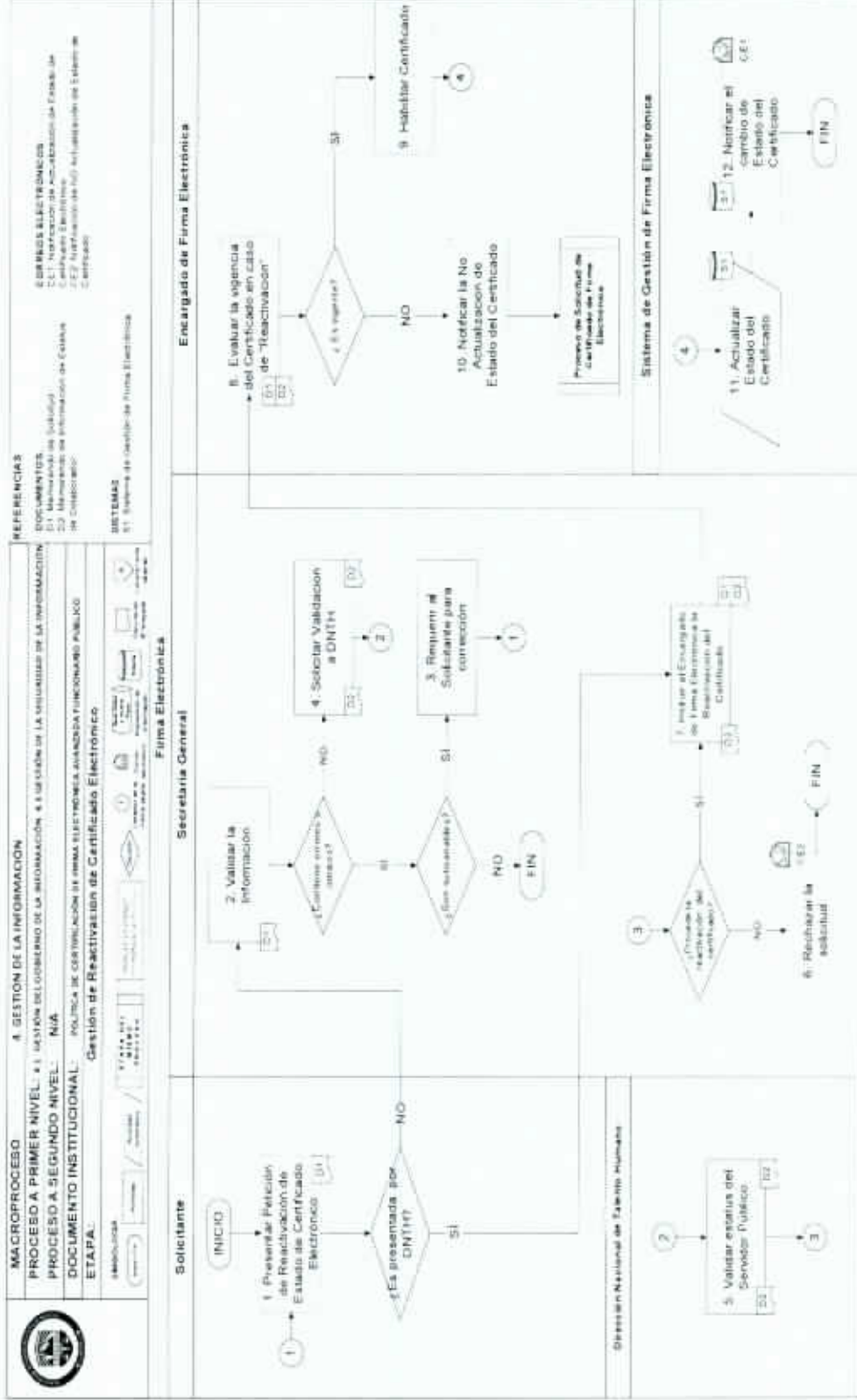
**POLÍTICA DE CERTIFICACIÓN DE FIRMA ELECTRÓNICA AVANZADA
FUNCIONARIO PÚBLICO**

SECRETARÍA GENERAL

Código:
MPR-GIT-TIG-AEB-003-V1

Fecha de vigencia:
Diciembre - 2021

13.4 DIAGRAMA DE FLUJO PROCESO IV: GESTIÓN DE REACTIVACIÓN DE CERTIFICADO ELECTRÓNICO





13.4.1 CUADRO DE DESCRIPCIÓN PROCESO IV: GESTIÓN DE
REACTIVACIÓN DE CERTIFICADO ELECTRÓNICO

Nº	Actividad	Descripción de la Actividad	Responsable
1	Remisión de notificación de movimiento de personal.	Remitir a la Secretaría General la notificación de movimiento de personal para que ésta inicie de oficio el cambio de estado de Certificado de Firma según corresponda. Avanzar a la actividad 3.	DNTH
2	Presentación de solicitud de Reactivación de certificado de Firma Electrónica.	Presentar ante Secretaria General el memorando de solicitud de Reactivación de Certificado Electrónico. Avanzar a la actividad 3.	Jefe normativo u operativo según corresponda.
3	Validar información	En caso de que la notificación de movimiento de personal sea lo que dé inicio al proceso, se debe validar que la Reactivación de certificado sea la acción que corresponde según el tipo de movimiento de personal que se realizó y lo indicado en el numeral 12 de esta Políticas de Certificación. Avanzar a la actividad 5. Revisar que la solicitud provenga de la jefatura normativa u operativa correspondiente con el visto bueno de su respectivo Director; revisar que la documentación venga firmada y verificar que no tiene omisiones de cualquier otra información que vulnere la seguridad del proceso. Avanzar a la actividad 4.	Secretaria General
4	Requerir solicitante al	En caso de que la solicitud contenga errores y omisos de los mencionados en el párrafo anterior, se requerirá al solicitante para que proceda a corregir los errores de la solicitud en caso de ser subsanables, cuando no sea	Secretaria General



**POLÍTICA DE CERTIFICACIÓN DE FIRMA ELECTRÓNICA
AVANZADA FUNCIONARIO PÚBLICO**

SECRETARÍA GENERAL

Código:
MPR-GIT-TIG-AEB-003-V1

Fecha de vigencia:
Diciembre - 2021

		subsana se rechazará la solicitud indicándole que debe realizarla nuevamente. Fin del proceso	
5	Instruir al Encargado de Firma Electrónica que proceda con la Reactivación de certificado electrónico	Una vez revisado el tipo de movimiento de personal que la notificación de DNTH indica que se realizó y ya se ha determinado que lo correspondiente de oficio es la Reactivación del Certificado según esta Políticas de Certificación o habiendo concluido que la solicitud procede, se instruirá al encargado de firma electrónica que realice la reactivación del certificado de firma electrónica.	Secretaria General
6	Evaluar la vigencia del Certificado.	Se debe revisar la vigencia del certificado del custodio. Si no es vigente el certificado se debe dar respuesta al solicitante indicando que el certificado ya expiró por lo que no es posible reactivarlo. Avanzar a la actividad 8.	Encargado de firma electrónica
7	Proceder con la Reactivación.	En caso de que sea válida la vigencia del certificado, proceder con la reactivación en la herramienta de Gestión de Firma Electrónica.	Encargado de Firma Electrónica
8	Notificar la Actualización de Estado del Certificado	Notificar al Custodio de Firma a la dirección de correo registrada la no actualización de estado del certificado solicitado. Fin del Proceso.	Sistema de Gestión de Firma Electrónica Avanzada
9	Actualizar Estado del Certificado	Luego de proceder con la reactivación, actualizar la lista de certificados reactivados.	Sistema de Gestión de Firma Electrónica Avanzada



**POLÍTICA DE CERTIFICACIÓN DE FIRMA ELECTRÓNICA
AVANZADA FUNCIONARIO PÚBLICO**

SECRETARÍA GENERAL

Código:
MPR-GIT-TIG-AEB-003-V1

Fecha de vigencia:
Diciembre - 2021

10	Notificar el cambio de Estado del Certificado	Notificar a través de correo electrónico al Custodio de Firma a la dirección de correo registrada el cambio de estado del certificado solicitado. Fin del Proceso.	Sistema de Gestión de Firma Electrónica Avanzada
----	-----------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------

13.4.2 DOCUMENTOS (D) / SISTEMAS (S) / CORREOS ELECTRÓNICOS (CE)

Documentos (D) / Sistemas(S) / Correos Electrónicos (CE)		Responsable de Generarlo y/o Presentarlo
D1	Memorando de solicitud.	Jefe normativo u operativo según corresponda o la Dirección Nacional de Talento Humano.
D2	Notificación de Movimiento de personal.	DNTH
CE1	Notificación de Actualización de Estado de Certificado Electrónico	Sistema de Gestión de Firma Electrónica Avanzada
CE2	Notificación de NO Actualización de Estado de Certificado	Encargado de Firma Electrónica
S1	Herramienta de Gestión de Firma Electrónica	N/A



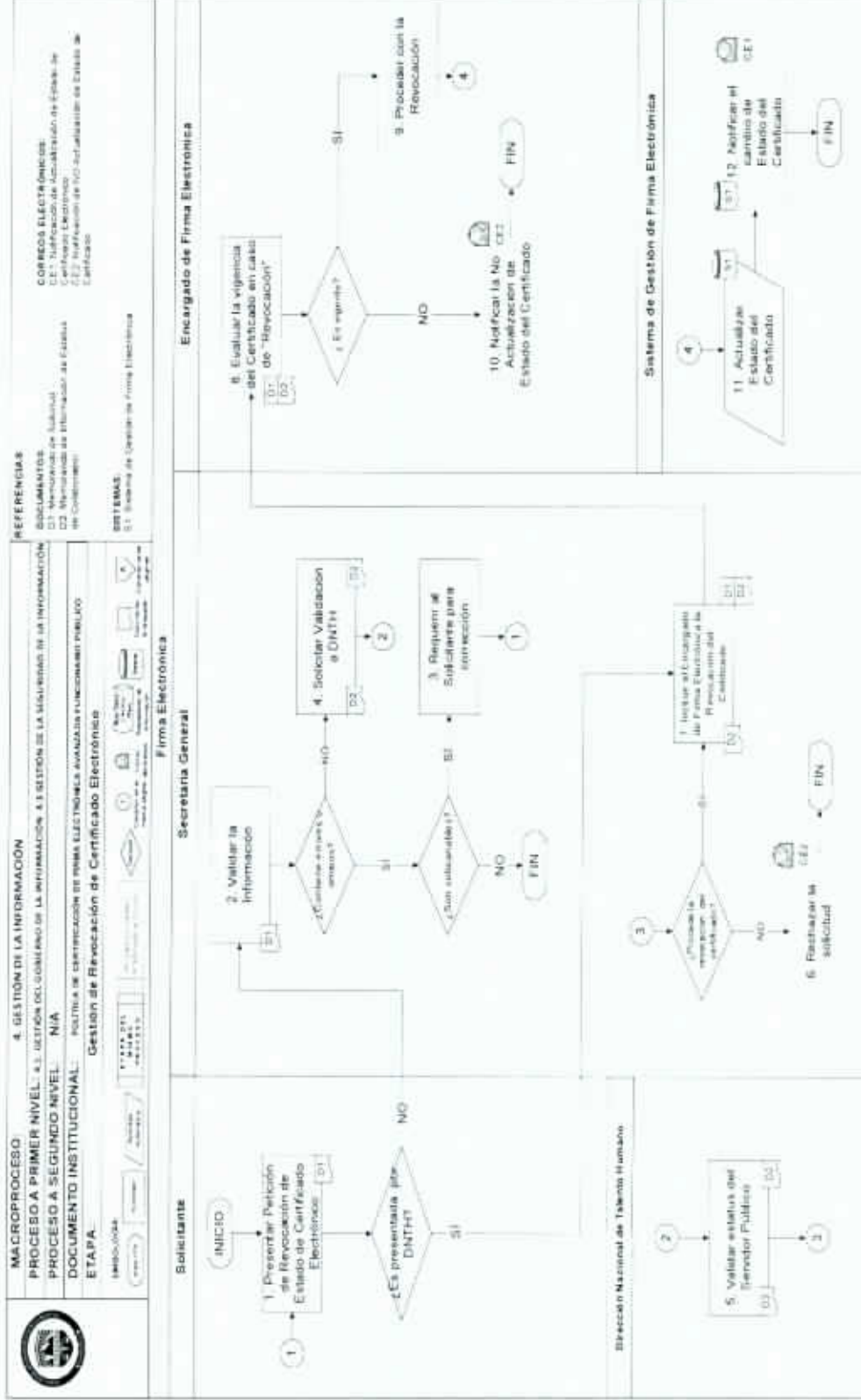
**POLÍTICA DE CERTIFICACIÓN DE FIRMA ELECTRÓNICA AVANZADA
FUNCIONARIO PÚBLICO**

SECRETARÍA GENERAL

Código:
MPR-GIT-TIG-AEB-003-V1

Fecha de vigencia:
Diciembre - 2021

13.5 DIAGRAMA DE FLUJO PROCESO V: GESTIÓN DE REVOCACIÓN DE CERTIFICADO ELECTRÓNICO





13.5.1 CUADRO DE DESCRIPCIÓN PROCESO V: GESTIÓN DE
REVOCACIÓN DE CERTIFICADO ELECTRÓNICO

N°	Actividad	Descripción de la Actividad	Responsable
1	Remisión de notificación de movimiento de personal.	Remitir a la Secretaría General la notificación de movimiento de personal para que esta inicie de oficio el cambio de estado de Certificado de Firma según corresponda. Avanzar a la actividad 3.	DNTH
2	Presentación de solicitud de revocación de certificado de Firma Electrónica.	Presentar ante Secretaria General el memorando de solicitud de revocación de Certificado Electrónico. Avanzar a la actividad 3.	Jefe normativo u operativo según corresponda.
3	Validar información	En caso de que la notificación de movimiento de personal sea lo que dé inicio al proceso, se debe validar que la revocación de certificado sea la acción que corresponde según el tipo de movimiento de personal que se realizó y lo indicado en el numeral 12 de esta Políticas de Certificación. Avanzar a la actividad 5. Revisar que la solicitud provenga de la jefatura normativa u operativa correspondiente con el visto bueno de su respectivo Director; revisar que la documentación venga firmada y verificar que no tiene omisiones de cualquier otra información que vulnere la seguridad del proceso. Avanzar a la actividad 4.	Secretaria General
4	Requerir al solicitante	En caso de que la solicitud contenga errores y omisos de los mencionados en el párrafo anterior, se requerirá al solicitante para que proceda a corregir	Secretaria General



**POLÍTICA DE CERTIFICACIÓN DE FIRMA ELECTRÓNICA
AVANZADA FUNCIONARIO PÚBLICO**

Código:
MPR-GIT-TIG-AEB-003-V1

Fecha de vigencia:
Diciembre - 2021

SECRETARÍA GENERAL

		los errores de la solicitud en caso de ser subsanables, cuando no sea subsanable se rechazará la solicitud indicándole que debe realizarla nuevamente. Fin del proceso	
5	Instruir al Encargado de Firma Electrónica que proceda con la revocación de certificado electrónico	Una vez revisado el tipo de movimiento de personal que la notificación de DNTH indica que se realizó y ya se ha determinado que lo correspondiente de oficio es la revocación del Certificado según esta Políticas de Certificación o habiendo concluido que la solicitud procede, se instruirá al Encargado de Firma Electrónica que realice la revocación del certificado de firma electrónica.	Secretaría General
6	Evaluar la vigencia del Certificado.	Se debe revisar la vigencia del certificado del custodio. Si no es vigente el certificado se debe dar respuesta al solicitante indicando que el certificado ya expiró por lo que no es posible revocarlo. Avanzar a la actividad 8.	Encargado de Firma Electrónica.
7	Proceder con la revocación.	En caso de que sea válida la vigencia del certificado, proceder con la revocación en la herramienta de Gestión de Firma Electrónica.	Encargado de Firma Electrónica.
8	Notificar la No Actualización de Estado del Certificado	Notificar al Custodio de Firma a la dirección de correo registrada la no actualización de estado del certificado solicitado. Fin del Proceso.	Sistema de Gestión de Firma Electrónica Avanzada
9	Actualizar Estado del Certificado	Luego de proceder con la revocación, actualizar la lista de certificados revocados.	Sistema de Gestión de Firma Electrónica Avanzada



**POLÍTICA DE CERTIFICACIÓN DE FIRMA ELECTRÓNICA
AVANZADA FUNCIONARIO PÚBLICO**

Código:
MPR-GIT-TIG-AEB-003-V1

SECRETARÍA GENERAL

Fecha de vigencia:
Diciembre - 2021

10	Notificar el cambio de Estado del Certificado	Notificar a través de correo electrónico al Custodio de Firma a la dirección de correo registrada el cambio de estado del certificado solicitado. Fin del Proceso.	Sistema de Gestión de Firma Electrónica Avanzada
----	-----------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------

13.5.2 DOCUMENTOS (D) / SISTEMAS (S) / CORREOS ELECTRÓNICOS (CE)

Documentos (D) / Sistemas(S) / Correos Electrónicos (CE)		Responsable de Generarlo y/o Presentarlo
D1	Memorando de solicitud.	Jefe normativo u operativo según corresponda o la Dirección Nacional de Talento Humano.
D2	Notificación de Movimiento de personal.	DNTH
CE1	Notificación de Actualización de Estado de Certificado Electrónico	Sistema de Gestión de Firma Electrónica Avanzada
CE2	Notificación de NO Actualización de Estado de Certificado	Encargado de Firma Electrónica
S1	Herramienta de Gestión de Firma Electrónica	N/A



14. GLOSARIO DE TÉRMINOS

- **Actualización de estado** Proceso de cambiar el status de un certificado electrónico a suspendido, reactivado o revocado.
- **Certificado electrónico:** Todo mensaje de datos proporcionado por un "Prestador de servicios de Certificación" que le atribuye certeza y validez a la firma electrónica.
- **Clave Privada:** Es una de las claves de un sistema de criptografía asimétrica que se emplea para generar una firma digital sobre un mensaje de datos y es mantenida en reserva por el titular de la Firma Electrónica.
- **Clave Pública:** Es la otra clave de un sistema de criptografía asimétrica que es usada por el destinatario de un mensaje de datos para verificar la Firma electrónica puesta en dicho mensaje. La clave publica puede ser conocida por cualquier persona
- **Custodio de firma electrónica** Persona que hace uso y mantiene bajo su cuidado del certificado de firma electrónica.
- **DPC** Declaración de Políticas de Certificación.
- **Encargado de Firma Electrónica** Persona que opera el Sistema de Gestión de Firma Electrónica Avanzada.



**POLÍTICA DE CERTIFICACIÓN DE FIRMA ELECTRÓNICA
AVANZADA FUNCIONARIO PÚBLICO**

Código:
MPR-GIT-TIG-AEB-003-V1

Fecha de vigencia:
Diciembre - 2021

SECRETARÍA GENERAL

- **Identificación:** Implica la acción y efecto de identificar, que es reconocer a un solicitante o Suscriptor de certificado en la República de Honduras.
- **Infraestructura de Clave Pública:** Una infraestructura de claves públicas (PKI) es un sistema de recursos, políticas y servicios que da soporte al uso del cifrado de claves públicas para autenticar a las partes que participan en una transacción.
- **Prestador de Servicios de Certificación:** Es la persona natural o jurídica, nacional o extranjera responsable de emitir o revocar los certificados o prestar otros servicios en relación con la firma electrónica.
- **Reactivación:** Proceso mediante el cual se revoca una suspensión de certificado de firma electrónica.
- **Revocación:** La revocación de un certificado se define por la acción mediante la cual se invalida un certificado antes de su fecha de caducidad.
- **Solicitante:** Individuo que solicita un certificado electrónico mediante los procesos provistos por la SAR-PKI.
- **Suspensión:** Proceso mediante el cual se deja en suspenso de manera temporal la validez de un certificado de firma electrónica.
- **X.509** Estándar UIT-T para infraestructuras de claves públicas (en inglés, Public Key Infrastructure o PKI).¹ X.509 especifica, entre otras cosas, formatos estándar para certificados de claves públicas y un algoritmo de validación de la ruta de certificación.



**POLÍTICA DE CERTIFICACIÓN DE FIRMA ELECTRÓNICA
AVANZADA FUNCIONARIO PÚBLICO**

SECRETARÍA GENERAL

Código:
MPR-GIT-TIG-AEB-003-V1

Fecha de vigencia:
Diciembre - 2021

- **Validación:** Proceso mediante el cual se verifica la certeza de los datos provistos por el solicitante, en el caso de certificados, corresponde a la verificación del estado de estos.



**POLÍTICA DE CERTIFICACIÓN DE FIRMA ELECTRÓNICA AVANZADA
FUNCIONARIO PÚBLICO**

Código:
MPR-GIT-TIG-AEB-003-V1

Fecha de vigencia:
Diciembre - 2021

SECRETARÍA GENERAL

15. MATRIZ DE RIESGOS DE PROCESOS

Macroproceso o	Nombre del Manual de Procedimiento	Nro. Causa del riesgo	Riesgo	Efecto	Descripción del riesgo detectado	Tipo de riesgo	Categoría de riesgo (escala nominal)	Impacto sobre los objetivos institucionales	Valor del riesgo	Ranking (escala ordinal)	Nivel de riesgo aceptado	Estrategia de respuesta	Forma de evaluación	Frecuencia de medición	Dueño de la acción de respuesta	Dueño del Riesgo
4. Gestión de la información	Manual de Procedimiento Firma Electrónica Avanzada para Funcionario Público	1	Debido a un certificado no sea emitido correctamente o exista la probabilidad que se den por aprobadas instrucciones, documentos y decisiones que no deben serlo.	Debido a un certificado no sea emitido correctamente o exista la probabilidad que se den por aprobadas instrucciones, documentos y decisiones que no deben serlo.	Debido a un certificado no sea emitido correctamente o exista la probabilidad que se den por aprobadas instrucciones, documentos y decisiones que no deben serlo, lo que provocara una mala reputación de la Administración Tributaria.	De Información	Políticos y Legales	10	70	Riesgo Alto	10	Entrar	Herramienta de Gestión de Firma Electrónica Avanzada	Trimestral	Secretaría General	Secretaría General



**POLÍTICA DE CERTIFICACIÓN DE FIRMA ELECTRÓNICA AVANZADA
FUNCIONARIO PÚBLICO**

SECRETARÍA GENERAL

Código:
MPR-GIT-TIG-AEB-003-V1

Fecha de vigencia:
Diciembre - 2021

16. MATRIZ DE INDICADORES DE PROCESOS

MACRO PROCESO	PROCESO DE PRIMER NIVEL	NOMBRE DEL INDICADOR	CONCEPTO	FORMULA	UNIDAD DE MEDIDA	PERIODICIDAD DE CARGA	PERIODICIDAD DE REVISIÓN	NIVEL DE MEDICIÓN	RESPONSABLE DE CARGA DE INFORMACIÓN	TENDENCIA	RESPONSABLE DE MEDICIÓN	FUENTE DE INFORMACIÓN
4 Gestión de la Información	4.1 Gestión del Gobierno de la Información	Porcentaje de Funcionarios Públicos del SAR que cuentan con Firma Electrónica	Porcentaje de Funcionarios Públicos del SAR que cuentan con Firma Electrónica	# número de Funcionarios del SAR que cuentan con Firma Electrónica del SAR / Cantidad de Funcionarios del SAR	%	Trimestral	Trimestral	Nacional	Secretaría General	Creciente	Secretaría General	Sistema de Gestión de Firma Electrónica Avanzada
4 Gestión de la Información	4.1 Gestión del Gobierno de la Información	Certificados Electrónicos Generados	Cantidad de Certificados Electrónicos a través del Sistema de Gestión de Firma Electrónica	# número de certificados generados	#	Trimestral	Trimestral	Nacional	Secretaría General	Creciente	Secretaría General	Sistema de Gestión de Firma Electrónica Avanzada
4 Gestión de la Información	4.1 Gestión del Gobierno de la Información	Actualizaciones de Estado de Certificado Electrónicos	Cantidad de Certificados Electrónicos con Actualización de Estado (Renovación, Suspensión, Revocación)	# número de actualizaciones de certificados electrónicos	#	Trimestral	Trimestral	Nacional	Secretaría General	Creciente	Secretaría General	Sistema de Gestión de Firma Electrónica Avanzada