

SECRETARÍA DE LA FUNCIÓN PÚBLICA

ACUERDO por el que se reforman, adicionan y derogan diversas disposiciones del diverso por el que se dan a conocer los formatos que deberán utilizarse para presentar las declaraciones de situación patrimonial.

JAVIER VARGAS ZEMPOALTECATL, Subsecretario de Responsabilidades Administrativas y Contrataciones Públicas, en ausencia del Secretario de la Función Pública, con fundamento en lo dispuesto por los artículos 18 y 37, fracciones XVI y XXII, de la Ley Orgánica de la Administración Pública Federal; 1, fracciones I, II y V, 3, fracción III, 8, fracción XV, 36, 37, 38, párrafos primero y tercero, y 40 de la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos; 6, fracción I, 7, fracción XII y 86 del Reglamento Interior de la Secretaría de la Función Pública, y

CONSIDERANDO

Que en términos de los artículos 8, fracción XV, 36 y 38 de la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos, los servidores públicos tienen la obligación de presentar con oportunidad y veracidad las declaraciones de situación patrimonial a través de medios remotos de comunicación electrónica que estarán a cargo de la Secretaría de la Función Pública, para los cuales se deberán de expedir las normas y formatos electrónicos; así como los manuales e instructivos bajo los cuales los servidores públicos cumplan con la obligación de declarar su situación patrimonial.

Que en ese sentido y con la finalidad de orientar respecto del cumplimiento de la obligación a que se hizo referencia, simplificándoles a los servidores públicos el conocimiento de aquellas declaraciones que tienen obligación de presentar, así como poner a disposición para su consulta e impresión, la versión íntegra de las declaraciones de situación patrimonial y de posible conflicto de interés que han presentado ante la Secretaría de la Función Pública; así como los acuses de recibo electrónico correspondientes, esta Secretaría de Estado ha implementado una nueva versión del sistema DeclaraNet^{plus}.

Que para facilitar los procedimientos y en aprovechamiento de las tecnologías innovadoras, la nueva versión del sistema DeclaraNet^{plus}, como parte de sus ventajas, permite que los servidores públicos presenten su declaración de situación patrimonial y de posible conflicto de interés desde cualquier dispositivo electrónico, ya sea computadora personal, tableta electrónica o Smartphone, siguiendo mecanismos simplificados que agilizan y optimizan el servicio a los usuarios.

Que derivado de las adecuaciones realizadas al sistema DeclaraNet^{plus}, y con el ánimo de que éste resulte más amigable para los usuarios, es necesario modificar los apartados a requisitar en el sistema, ello con la finalidad de adecuar los rubros y apartados con los que cuenta actualmente el nuevo sistema y lograr mayor eficiencia en la presentación de las declaraciones de situación patrimonial y de posible conflicto de interés de los servidores públicos.

Que en virtud de lo expuesto y en ejercicio de las facultades y atribuciones que en materia de registro de situación patrimonial de los servidores públicos de la Administración Pública Federal, le fueron conferidas a esta Secretaría de la Función Pública, he tenido a bien expedir el siguiente:

ACUERDO POR EL QUE SE REFORMAN, ADICIONAN Y DEROGAN DIVERSAS DISPOSICIONES DEL DIVERSO POR EL QUE SE DAN A CONOCER LOS FORMATOS QUE DEBERÁN UTILIZARSE PARA PRESENTAR LAS DECLARACIONES DE SITUACIÓN PATRIMONIAL

ARTÍCULO PRIMERO.- Se **REFORMA** el artículo PRIMERO, párrafo primero, del Acuerdo por el que se dan a conocer los formatos que deberán utilizarse para presentar las declaraciones de situación patrimonial, y **se DEROGA** el párrafo segundo del artículo PRIMERO, del Acuerdo por el que se dan a conocer los formatos que deberán utilizarse para presentar las declaraciones de situación patrimonial, para quedar como sigue:

“PRIMERO.- El presente Acuerdo tiene por objeto dar a conocer los formatos que deberán utilizarse para presentar las declaraciones de situación patrimonial y de posible conflicto de interés como se establece en el instructivo para su llenado, que como anexo forma parte de este Acuerdo.”

ARTÍCULO SEGUNDO.- Se **REFORMA** el INSTRUCTIVO PARA EL LLENADO DE LA DECLARACIÓN DE SITUACIÓN PATRIMONIAL: su denominación; apartado de Introducción, párrafos primero, tercero viñeta primera, y párrafos quinto y sexto; numeral 1; numeral 2, inciso a); numeral 3.1; numeral 3.2; numeral 3.4.1, párrafo segundo, incisos b), c), d), e), f) y g); numeral 3.4.2, párrafo segundo, viñetas 4 y 7, y párrafo tercero; numeral 3.4.3.1; numeral 3.4.3.2, párrafos sexto y séptimo; numeral 3.6, párrafo quinto, viñeta 3, y párrafos décimo octavo y décimo noveno; numeral 3.7; numeral 3.7.1; numeral 3.7.2, inciso c), fracción I en su párrafo

segundo, y párrafos segundo, tercero y cuarto; numeral 3.7.3, párrafo segundo; numeral 3.7.4, último párrafo; numeral 3.8, quinto párrafo; numeral 3.8.1, párrafo tercero viñetas 1, 2, 5, párrafo cuarto viñetas 1, 2, 3 y 4, párrafo quinto viñetas 4 y 7, y párrafos noveno, décimo y décimo primero; numeral 3.8.2; numeral 3.8.3; numeral 3.8.4; numeral 3.9.1; numeral 3.9.2; numeral 3.9.3; numeral 3.9.4; numeral 3.10.1, párrafo octavo viñetas 4 a 6, y párrafos décimo primero, décimo segundo y décimo tercero; numeral 3.10.2; numeral 3.10.3; numeral 3.11.1, párrafos segundo, quinto, sexto y séptimo; numeral 3.11.2; numeral 3.11.3; numeral 3.12, párrafos primero, segundo, octavo, noveno y décimo; numeral 3.12.1, párrafos tercero, sexto, séptimo y octavo; numeral 3.12.2, párrafos segundo, tercero, cuarto, vigésimo, vigésimo primero y vigésimo segundo; numeral 3.12.3, párrafos primero, segundo, tercero, cuarto, sexto, séptimo y octavo; numeral 3.12.4; numeral 3.13; y numeral 3.15, párrafo primero; así como **se ADICIONA** la viñeta 2 del párrafo primero del numeral 3.3, recorriéndose en su orden las viñetas restantes; los incisos h), i), j) del numeral 3.4.1; el numeral 3.7.1.1; quinto párrafo del numeral 3.12.2 y el numeral 3.14, y **se DEROGA** el último párrafo del numeral 3.7.3; para quedar como sigue:

“INSTRUCTIVO PARA EL LLENADO DE LA DECLARACIÓN DE SITUACIÓN PATRIMONIAL Y DE POSIBLE CONFLICTO DE INTERÉS

Introducción.

El presente instructivo tiene por objeto orientar y facilitar a los sujetos obligados a la presentación de la declaración de situación patrimonial y de posible conflicto de interés, a través del sistema DeclaraNet^{plus}, el cual integra los formatos de las declaraciones en sus modalidades de inicio, modificación y conclusión del encargo.

...

El sistema DeclaraNet^{plus}, permite, entre otros puntos, lo siguiente:

- Efectuar de forma simple y sencilla toda la captura de la declaración de situación patrimonial y de posible conflicto de interés, para lo cual, sólo se requiere de una computadora con conexión a internet y mediante la utilización de un navegador acceder a www.declaranet.gob.mx, y elegir en el menú principal la opción "Declarar en línea".

...

Cabe señalar que en la declaración de modificación patrimonial a presentar, se deberá actualizar la información relacionada con la adquisición de bienes inmuebles, vehículos y muebles, siempre que se mantenga en el patrimonio objeto de la declaración.

Asimismo, deberá requisitar el apartado denominado "Declaración de Posible Conflicto de Interés". Esta declaración deberá hacerse al ingresar a cargos públicos federales, actualizarse anualmente o en cualquier momento en que un servidor público considere que pudiera ocurrir un posible conflicto de interés en su responsabilidad.

...

1. Requerimientos técnicos

Para presentar la declaración se requiere de un equipo de cómputo que tenga acceso a internet, con Sistema operativo Windows 7 o superior, Mac OS 10.4 o superior; navegadores web Internet Explorer ver. 9 o superior, Microsoft Edge, Google Chrome versión 28 o superior, Mozilla Firefox versión 25 o superior o Safari.

De manera adicional, los equipos de cómputo deberán contar con el visor de documentos Acrobat Reader y en caso de requerir firmar con Firma Electrónica Avanzada también se deberá contar con la máquina virtual de Java (Java Runtime Environment 1.5 update o posterior).

Asimismo se podrá presentar la declaración mediante una tableta (Tablet) que tenga acceso a internet, con Sistema operativo Android 6.0 o superior, IOS 9 o superior, Windows 8 o superior; navegadores web Microsoft Edge, Google Chrome, Mozilla Firefox o Safari. En estos dispositivos sólo se podrá firmar la declaración por medio del RFC y contraseña con el que el usuario ingresa a su declaración patrimonial.

Para iniciar la captura de la declaración patrimonial se debe ingresar a la siguiente página electrónica www.declaranet.gob.mx en la opción "Declarar en Línea".

Para ingresar al formato que se utilizará para presentar la declaración patrimonial, se debe proporcionar el RFC con homoclave y la contraseña que se registró en la cuenta y que se utilizó para presentar la declaración anterior.

Una vez capturada y revisada toda la información para el envío de la declaración de situación patrimonial, se tienen las siguientes opciones:

a) Utilizar la Firma Electrónica Avanzada (FIEL), expedida por autoridad certificadora Servicio de Administración Tributaria.

b) En caso de no contar con la FIEL, se podrá firmar la declaración patrimonial con el Registro Federal de Contribuyentes con homoclave y Contraseña, que se utiliza para ingresar al sistema DeclaraNet^{plus}.

Para lo cual, previamente se debe haber aceptado las condiciones de uso que se contienen en el formato que al efecto se encuentra disponible en dicho sistema, mismo que se deberá entregar firmado autógrafamente al Órgano Interno de Control en la dependencia o entidad en la que se preste o se haya prestado el servicio, dentro de los 15 días hábiles siguientes a la presentación de la declaración correspondiente, acompañado de una copia del acuse de recibo electrónico generado por el sistema.

2. Información necesaria

...

a) Cédula de identificación fiscal expedida por la Secretaría de Hacienda y Crédito Público o cualquier documento que contenga el Registro Federal de Contribuyentes (RFC), con homoclave.

b) a i) ...

3.1. Registro de usuario nuevo.

Antes de iniciar la captura de la declaración se debe registrar como "Nuevo usuario", para lo cual se debe elegir la opción "¿Nuevo usuario? Regístrate aquí" de la pantalla de inicio del sistema DeclaraNet^{plus} y posteriormente registrarse.

Al seleccionar esta opción, se presentará un apartado de Términos y Condiciones que deberá aceptar, se le pide proporcionar de manera obligatoria los siguientes datos para su validación:

RFC: En cuanto al Registro Federal de Contribuyentes, escriba en la primera sección, los 10 caracteres básicos y en la segunda, los 3 caracteres de la homoclave, como la emitió el Servicio de Administración Tributaria. Si no se cuenta con él, ingresar a la página electrónica: <https://rfc.siat.sat.gob.mx/PTSC/RFC/menu/index.jsp?opcion=2>, para verificar los requisitos y pasos a seguir para obtener dicho documento.

CURP: Escriba los 18 caracteres de la Clave Única de Registro de Población, como la emitió la Secretaría de Gobernación. Si no se dispone de ella, pero ya se tramitó se puede consultar en la página electrónica: <http://www.renapo.gob.mx/swb/swb/RENAPO/consultacurp>.

Si nunca se ha solicitado, imprimir el certificado de "No existencia", y acudir al módulo más cercano. Para mayor información, consultar la página electrónica: <https://consultas.curp.gob.mx/CurpSP/>.

Una vez, validados su RFC y CURP, aparecerá otra pantalla donde deberá ingresar para su registro inicial los siguientes campos obligatorios:

a) Nombre y Apellidos: Escribir el nombre o nombres completos. Así como los apellidos completos, sin abreviaturas y preferentemente sin acentos ni signos especiales (' * ^ ` " / % \ ' & " ! | ~).

Si se tiene un solo apellido colocarlo en el espacio del primer apellido y dejar el espacio del segundo apellido en blanco.

b) Los datos correspondientes a RFC con homoclave y la CURP, aparecerán precargados en la plantilla de acuerdo a la información que proporcionó para verificar sus datos.

c) Número de celular: Proporcione su número de celular (este dato no es obligatorio).

d) Email laboral: Escribir las direcciones de los correos electrónicos a los cuales se enviarán las notificaciones que sean necesarias, tales como confirmación de registro al sistema DeclaraNet^{plus}, la recuperación de contraseña, etc. Es indispensable que se escriban correctamente los correos electrónicos, ya que de lo contrario no se podrán recibir los comunicados o contraseña.

e) Email personal: Señalar otra dirección de correo a la cual se enviarán los comunicados en caso de que en la dirección primaria no pueda recibirlos.

f) Contraseña: Escribir la contraseña que le servirá para ingresar al sistema DeclaraNet^{plus}, ésta debe estar conformada por al menos 6 caracteres alfanuméricos.

Si se presentó anteriormente alguna declaración patrimonial ante la Secretaría de la Función Pública, a través de DeclaraNet^{Plus}, es necesario que se proporcione la contraseña de acceso de la última declaración enviada para que al momento de ingresar al sistema se recupere la información de la última declaración enviada, facilitando la presentación de esta nueva declaración ya que sólo se deberán actualizar los datos que hayan cambiado desde entonces a la fecha. En caso contrario, se deberá capturar nuevamente la declaración en su totalidad.

Al terminar de llenar el formato de registro de "Nuevo usuario", verificar la información capturada y oprimir el botón "Registrar", y si es necesario corregirla, podrá hacerse, posicionándose en la parte que se desea corregir y escribir los datos correctos.

Una vez que se haya llenado el formato de registro de "Nuevo usuario", oprimir el botón "Registrar" para que la información sea enviada a la Secretaría de la Función Pública y se permita el inicio de sesión para la presentación de la declaración patrimonial.

3.2 Tipo de declaración.

Después de registrarse como nuevo usuario, ingresar al sistema DeclaraNet^{Plus} y proporcionar la Contraseña, se deberá elegir la opción "Presentar" del apartado Declaración en blanco.

Si se elige "Presentar" indicar el tipo de declaración que se va a presentar, para lo cual deberá seleccionar del recuadro que aparecerá una de las siguientes opciones:

- INICIAL
- CONCLUSIÓN
- MODIFICACIÓN PATRIMONIAL

Habiendo seleccionado el tipo de declaración deberá escoger el año que corresponda, y deberá de dar clic en el botón de "Presentar".

3.3. Pantalla de acceso a los apartados de información que se debe capturar.

- ...
- Datos curriculares del Declarante.
- ...
- ...
- ...
- ...
- ...
- ...
- ...
- ...
- ...
- ...

...

3.4.1. Datos generales

...

Proporcionar o verificar los siguientes datos obligatorios:

a)

...

b) CURP: Escribe los 18 caracteres de la Clave Única de Registro de Población, como la emitió la Secretaría de Gobernación. Si no se dispone de ella, pero ya se tramitó se puede consultar en la página electrónica:

<https://consultas.curp.gob.mx/CurpSP/>

Si nunca se ha solicitado imprimir el certificado de "No existencia" en la página citada y acudir al módulo más cercano. Para mayor información consultar la página electrónica:

<https://consultas.curp.gob.mx/CurpSP/>

- c) RFC/Homoclave: En cuanto al Registro Federal de Contribuyentes, escribe en la primera sección, los 10 caracteres básicos y en la segunda, los 3 caracteres de la homoclave, como la emitió el Servicio de Administración Tributaria. Si no se cuenta con él, ingresar a la página electrónica: <https://rfc.siat.sat.gob.mx/PTSC/RFC/menu/index.jsp?opcion=2>, para verificar los requisitos y pasos a seguir para obtener dicho documento.
- d) Correo electrónico institucional o laboral: Escribir las direcciones de los correos electrónicos a los cuales se enviarán las notificaciones que sean necesarias, tales como confirmación de registro al sistema DeclaraNet^{plus}, la recuperación de contraseña.
- e) Correo electrónico alterno: Señalar otra dirección de correo a la cual se enviarán los comunicados en caso de que la dirección primaria no pueda recibirlos.
- f) Estado civil: Seleccionar en el catálogo el estado civil: casado(a), divorciado(a), soltero(a), unión libre o viudo(a). En el supuesto de seleccionar casado (a) se debe especificar el régimen matrimonial, si es el de sociedad conyugal o el de separación de bienes.

Si el declarante se encuentra casado bajo el régimen de sociedad conyugal, deberá declarar los bienes del cónyuge, y si es bajo el régimen de separación de bienes sólo aquellos que hayan sido adquiridos total o parcialmente con ingresos del declarante. Asimismo, en su caso, los bienes de la concubina o concubinario y/o dependientes económicos y los que, estando a nombre de otra persona, hayan sido adquiridos total o parcialmente con ingresos del declarante, según lo establecido en el artículo 44 de la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos.

- g) País donde nació: Aparecerá de manera predeterminada México, en caso necesario se podrá modificar seleccionando del catálogo el país donde nació el declarante.
- h) Nacionalidad: Aparecerá predeterminada mexicana, en caso necesario se podrá modificar seleccionando del catálogo la nacionalidad.
- i) Entidad donde nació el declarante: Elegir del catálogo la entidad federativa donde nació el declarante.
- j) Número celular (este dato no es obligatorio).

...

3.4.2. Domicilio del declarante.

...

Proporcionar o verificar los siguientes datos obligatorios:

- ...
- ...
- ...
- Número interior: Proporcionar el número interior. En el supuesto que el inmueble no cuenta con número interior, dicho campo puede dejarse en blanco.
- ...
- ...
- Municipio o alcaldía: Proporcionar el nombre del municipio o alcaldía política donde se encuentra el domicilio. Si se selecciona extranjero, indicar el Estado o provincia.
- ...
- ...

...

Si se requiere eliminar la información proporcionada presionar el botón "Cancelar" y aparecerá la pantalla nuevamente en blanco para el requisitado de los campos.

3.4.3.1 Escolaridad.

Dar un clic en "Escolaridad" y se mostrará la lista con la información previamente proporcionada si se está leyendo una declaración anterior, o en blanco si se está capturando una declaración nueva.

Para incorporar información oprimir el botón "Agregar".

Seleccionar el Nivel de estudios del menú que se despliega al dar clic en la flecha del lado derecho de este espacio (primaria, secundaria, bachillerato, carrera técnica o comercial, licenciatura, diplomado, maestría o doctorado, etc.), así como proporcionar o verificar los siguientes datos:

- Lugar donde se ubica la institución educativa: México o extranjero.
- Entidad federativa: Seleccionar la opción del menú que se despliega al seleccionar la flecha del lado izquierdo de este espacio. Si se eligió extranjero señalar país y ciudad.
- Municipio o alcaldía: Seleccionar la opción del menú que se despliega al dar clic en la flecha del lado derecho de este espacio.
- Institución educativa: Escribir el nombre de la institución donde se realizaron los estudios.
- Carrera o área de conocimiento: Seleccionar el nombre de la carrera o de los estudios realizados.
- Estatus: Seleccionar la opción del menú que se despliega al dar clic en la flecha del lado izquierdo de este espacio (finalizado, cursando o trunco). Si se elige la opción "cursando", se deberá proporcionar el dato de "periodos cursados".
- Periodos cursados: En caso de que se siga cursando el nivel seleccionado, proporcionar los periodos cursados y qué tipo de periodo."
- Documento obtenido: Seleccionar la opción que corresponda. Si selecciona "Título", aparecerá de igual manera un campo donde deberá escribir el número de cédula profesional, que expide la Secretaría de Educación Pública. Para mayor información sobre este documento consultar la página electrónica: <http://www.cedulaprofesional.sep.gob.mx/cedula/indexAvanzada.action>.

Al concluir el llenado del formato presionar el botón "Aceptar" y se volverá al listado para registrar otros estudios.

Para incorporar datos de otros estudios, presionar el botón "Agregar" y repetir el procedimiento.

Para verificar y/o modificar la información de algún registro dar un clic en la palabra "Validar" y se desplegará la información del registro. En caso de que haya realizado modificaciones, al terminar las correcciones presionar el botón "Aceptar".

Si se desea eliminar la información proporcionada presionar el botón "X" que se encuentra a la derecha del registro que se desea borrar y se eliminará el registro completo, una vez eliminado un registro no se podrá recuperar.

Para salir de este rubro presionar el botón "Aceptar".

3.4.3.2. Experiencia laboral.

...
...
...
...
...

Para incorporar datos de otro empleo, oprimir "Agregar" y repetir el procedimiento. Para verificar y/o modificar la información de algún registro dar clic en la palabra "Validar" y se desplegará la información total del registro. En caso de que haya realizado modificaciones, al terminar las correcciones deberá presionar el botón "Aceptar".

Si se desea eliminar la información proporcionada presionar el botón "X" que se encuentra a la derecha del registro que se desea borrar y se eliminará el registro completo, una vez eliminado un registro no se podrá recuperar.

...

3.6 Datos del cónyuge, concubina o concubinario, y/o dependiente(s) económico(s).

...
...
...
...

Proporcionar o verificar los siguientes datos obligatorios:

-
-
- Segundo apellido: Proporcione el segundo apellido del cónyuge, concubina o concubinario y/o dependientes económicos. Si sólo cuenta con un apellido, deje el campo en blanco. (Este campo no es obligatorio).

...

...

...

...

...

...

...

...

...

...

...

...

Para modificar algún dato deberá dar clic en el botón "Validar". Posteriormente aparecerá la plantilla con los datos registrados, por lo que deberá modificar o corregir sin ningún problema la información. Al terminar las correcciones presionar el botón "Aceptar" para regresar a la pantalla anterior y oprimir el botón guardar.

Si se desea eliminar la información proporcionada presionar el botón "X" que se encuentra a la derecha del registro que se desea borrar y se eliminará el registro completo, una vez eliminado un registro NO se podrá recuperar.

...

3.7. Datos del encargo.

Dar un clic en el texto "Datos del encargo (que inicia, actual o que concluye)", en función del tipo de declaración que vaya a presentar. Se mostrará la pantalla que le permitirá ir a las 4 secciones de este apartado: "Datos del encargo" (inicia, actual o que concluye), "Domicilio del encargo", "Ingresos" (mensuales, del año en curso, anuales) y "¿si te desempeñaste como servidor público federal obligado a presentar declaración de situación patrimonial en el año inmediato anterior?"

3.7.1. Datos del encargo (que inicia, actual o que concluye).

Dar un clic en "Datos del encargo" y se mostrará la lista con la información previamente proporcionada si se está leyendo una declaración anterior, o en blanco si se está capturando una declaración nueva.

Para proporcionar la información de algunos rubros, es necesario que se cuente con el recibo de pago.

Proporcionar o verificar los datos que se solicitan:

- Dependencia o entidad: Dar un clic en la flecha ubicada del lado derecho de este espacio y seleccionar del catálogo que se despliega la dependencia o entidad que te corresponda.
- Nombre del encargo o puesto: Seleccionar del catálogo el nombre del encargo o puesto que desempeña, esto en función del tipo de declaración que se vaya a presentar.
- Si está contratado(a) por honorarios Seleccionar "Sí" o "No", según corresponda.
- Nivel del encargo (o clave presupuestal): Es el que aparece en el recibo o talón de pago, si no se cuenta con él se puede consultar en su coordinación administrativa o área de recursos humanos.
- Área de adscripción: Especificar el nombre de la unidad administrativa de su adscripción.

- Fecha de (inicio, conclusión o modificación) del encargo: Dicha información podrá obtenerse y corroborarse a través del área de Recursos Humanos de la dependencia y/o entidad a la que pertenece.

Si se trata de una declaración de inicio o de modificación proporcionar la fecha que se inicia el encargo o si es de conclusión, proporcionar la fecha de retiro del encargo.

Indicar la fecha con el siguiente formato dd/mm/aaaa.

- Funciones principales: Seleccionar las funciones principales que realiza, dando un clic dentro de la casilla.

Se puede señalar más de una opción.

Si las funciones no se encuentran entre las opciones enlistadas, seleccionar "Otro" para especificarlas.

3.7.1.1 Domicilio del encargo.

Dar clic en el apartado que dice "Domicilio del encargo" y capturar o verificar los siguientes datos obligatorios:

- Lugar donde se ubica: Marca la casilla que corresponda al lugar donde se ubica la dependencia o entidad: México o Extranjero.
- Calle: Proporcionar el nombre de la calle.
- Número exterior: Proporcionar el número exterior.
- Número interior: Proporcionar el número interior. En el supuesto que el inmueble no cuente con número interior, dicho campo puede dejarse en blanco al no ser un dato obligatorio.
- Localidad o colonia: Proporcionar el nombre de la localidad o de la colonia, donde se encuentra el domicilio de la dependencia o entidad.
- Entidad federativa: Proporcionar la entidad federativa donde se localiza el domicilio de la dependencia o entidad. Si se seleccionó extranjero, indicar el país o ciudad.
- Municipio o alcaldía: Proporcionar el municipio o alcaldía, donde se encuentra el domicilio de la dependencia o entidad. Si seleccionaste extranjero, indica la provincia o localidad.
- Código Postal: Proporcionar el código postal.
- Teléfono de la oficina: Proporcionar el teléfono de tu oficina directo.
- Extensión.

Presionar "Aceptar" y se regresará a la pantalla de datos del encargo.

Oprimir nuevamente "Aceptar" para ir al rubro de los ingresos.

3.7.2. Ingresos.

...

a) a b) ...

c) Conclusión.- Remuneración neta del declarante en el año en curso por su cargo público que concluye.

Para calcular este importe, debe considerar el ingreso neto recibido a partir del 1o. de enero y hasta la fecha en que concluye su cargo. Se integra por la suma del sueldo u honorarios, compensaciones, bonos u otras prestaciones, menos los impuestos correspondientes (ISR y aportaciones por concepto de seguridad social). Tomar como referencia la señalada en la hoja única de servicios que expide la dependencia o entidad a la que estuvo adscrito el servidor público, tomando en consideración el monto total de percepciones netas mensuales de acuerdo a su nivel de rango."

...

I. ...

Proporciona los ingresos netos recibidos por tu encargo público. (Anuales o mensuales según corresponda al tipo de declaración), considera ingresos por concepto de sueldo, honorarios, compensaciones, bonos, aguinaldos y otras prestaciones.

II. ...

II.1 a II.4...

A. a C. ...

Si los ingresos percibidos fueron en el extranjero, las cifras se anotarán en pesos mexicanos, mencionando en el apartado de observaciones el tipo de moneda que corresponda y la fecha que se utilizó para el tipo de cambio. Para ello deberá considerar lo dispuesto en el Diario Oficial de la Federación, consultable en la página de la Secretaría de Gobernación a través de la siguiente liga electrónica: <http://dof.gob.mx/indicadores.php>

Al terminar de llenar presione "Aceptar" para continuar con el llenado de su declaración.

3.7.3. ¿Te desempeñaste como servidor público federal obligado a presentar declaración de situación patrimonial en el año inmediato anterior?

...

Al seleccionar "SI", se presentarán las casillas para que indique el periodo en el cual se desempeñó como servidor público federal, el formato es dd/mm/aaaa e indique de qué fecha a qué fecha lo hizo.

...

...

3.7.4. ¿Ha presentado declaración de situación patrimonial con anterioridad? Sólo en el caso de declaración de conclusión.

...

...

...

...

...

...

Una vez que proporcione toda la información de este apartado presione el botón "Aceptar", para volver al menú principal nuevamente de clic en botón "Aceptar" y no se olvide de Guardar su información (botón superior derecho).

3.8. Bienes inmuebles.

...

...

...

...

Por lo que se refiere a este apartado, en la declaración de modificación patrimonial a presentar en el mes de mayo, se deberá actualizar la información relacionada con el vendedor o enajenante en la adquisición de bienes inmuebles, referida a la fecha en que se realizó la operación, siempre que al 31 de diciembre del año inmediato anterior, se mantenga el inmueble en el patrimonio objeto de la declaración.

3.8.1. Agregar un inmueble.

...

Proporcionar los siguientes datos obligatorios:

- Tipo de operación: Deberá seleccionar la opción: INCORPORACIÓN.
- Tipo de bien: Elegir del catálogo la opción (edificio, casa, departamento, local, terreno, palco, bodega, etc).
- ...
- ...
- Forma de adquisición: Seleccionar del catálogo la forma de adquisición (cesión, contado, crédito, donación, herencia, permuta, rifa o sorteo, traspaso).
- ...

Tratándose de adquisición de un inmueble por enajenación, señalar el nombre del vendedor o enajenante. En la declaración de modificación patrimonial a presentar en el mes de mayo, se deberá actualizar esta información referida a la fecha en que se realizó la operación, siempre que al 31 de diciembre del año inmediato anterior, se mantenga el inmueble en el patrimonio objeto de la declaración.

- Relación del autor de la enajenación con el titular: Indicar aquí la relación existente entre el autor de la enajenación y el titular.
- Valor del inmueble conforme a escritura pública o contrato: Proporcionar el monto de la operación conforme a escritura pública o contrato y seleccionar el tipo de moneda. No actualizar a valor presente.
- Fecha de adquisición: Indicar la fecha en que se efectuó la operación, en formato dd/mm/aaaa.
- Datos del Registro Público de la Propiedad: Indicar aquí el número de folio real con el que se inscribió el inmueble, que se encuentra en la propia escritura pública u otro dato que permita la identificación del mismo.
- ...
- ...

Para ello dar un clic en el botón que dice "Debes indicar aquí la ubicación del inmueble", para ir a la ventana de captura de la información, proporcione los siguientes datos:

- ...
- ...
- ...
- Número interior: Proporcionar el número interior. En el supuesto que el inmueble no cuente con número interior, dicho campo puede dejarse en blanco.
- ...
- ...
- Municipio o alcaldía: Proporcionar el municipio o alcaldía, donde se encuentra el domicilio del bien inmueble. Si seleccionó extranjero, indique la provincia o localidad.
- ...
- ...
- ...

Para verificar y/o modificar la información de algún registro de un clic en la palabra "Validar" y se desplegará la información total del registro, por lo que deberá modificar y hacer las correcciones necesarias. Al terminar las correcciones presionar el botón "Aceptar" para continuar con la presentación de su declaración de situación patrimonial.

Si desea eliminar totalmente la información proporcionada de un registro, presionar el botón "X" que se encuentra a la derecha del registro y se eliminará por completo, una vez eliminado un registro no podrá recuperarlo.

Habiendo concluido la captura de los bienes inmuebles totalmente presionar el botón "Aceptar". No olvide guardar la información (botón superior derecho).

3.8.2. Obra.

Si se realizó una construcción, ampliación o remodelación en un inmueble seleccionar el botón "Validar" del registro del inmueble a reportar en caso de que ya se hubiere registrado con anterioridad, si corresponde a un registro nuevo dar clic en el botón "Agregar" y posteriormente seleccionar el Tipo de operación: OBRA.

Si la obra de ampliación, construcción o remodelación abarca varios años, en la declaración de modificación patrimonial, se deberán manifestar erogaciones realizadas en el año inmediato anterior y mencionar en el rubro de observaciones que se trata de una obra de varios años.

Si corresponde a un bien inmueble registrado con anterioridad aparecerá el formato prellenado del mismo, en caso de que sea una incorporación deberá proporcionar los siguientes datos obligatorios:

- Tipo de bien: Elegir del catálogo la opción (edificio, casa, departamento, local, terreno, palco, bodega, etc).
- Tipo de Obra: Elegir del catálogo la opción (ampliación, construcción o remodelación).
- Superficie de (ampliación, construcción o remodelación).
- Superficie en metros cuadrados.
- Forma de adquisición: Seleccionar del menú que se despliega la opción (cesión, compra-venta, contado, crédito, donación, herencia, permuta, rifa o sorteo, traspaso).
- Nombre o razón social del vendedor o enajenante, autor de la donación, autor de la herencia o cesionario, según sea el caso.
- Tipo de relación del vendedor o enajenante, autor de la donación, autor de la herencia o cesionario con el titular.
- Valor del inmueble conforme a escritura pública: Proporcionar el monto de la operación conforme a escritura pública y seleccionar el tipo de moneda. No actualizar a valor presente.
- Fecha de adquisición: Indique la fecha de operación en formato dd/mm/aaaa.
- Datos del Registro Público de la Propiedad: Indicar aquí el número de folio real con el que se inscribió el inmueble, que se encuentra en la propia escritura pública u otro dato que permita la identificación del mismo.
- Titular: Seleccionar del catálogo si el bien corresponde al declarante, cónyuge, declarante y cónyuge, concubina o concubinario y/o dependientes económicos.

Posteriormente deberá ingresar los Datos de la Operación:

- Inversión en obra: Importe de la operación (ampliación, construcción o remodelación): Proporcionar el monto pagado por la obra. En caso de no haber concluido la obra, proporcionar el monto erogado a la fecha que corresponda a tu declaración.
- Fecha de la obra: Indique la fecha de la última obra realizada al inmueble en formato dd/mm/aaaa.
- Indicar la ubicación del inmueble, seleccionando con un clic en el botón que dice "Debes indicar la ubicación del inmueble" y proporcione o verifique los datos del domicilio.
- Lugar donde se ubica: Marca la casilla que corresponda al lugar donde se ubica: México o extranjero.
- Calle: Proporcionar el nombre de la calle.
- Número exterior: Proporcionar el número exterior.
- Número interior: Proporcione el número interior. En el supuesto que el inmueble no cuente con número interior, dicho campo puede dejarse en blanco.
- Localidad o colonia: Proporcionar el nombre de la localidad o de la colonia.
- Entidad federativa: Proporcionar la entidad federativa donde se localiza el bien. Si seleccionó extranjero, indique el país y ciudad.
- Municipio o alcaldía: Proporcionar el municipio o alcaldía política, donde se encuentra el domicilio del bien inmueble. Si se seleccionó extranjero, indicar la provincia o localidad.
- Código Postal: Proporcionar el código postal.

Una vez terminado de llenar el formato presione el botón "Aceptar" para regresar a la pantalla de "Obra del inmueble".

Habiendo concluido la captura de los datos de la obra totalmente presionar el botón "Aceptar". No olvide guardar la información (botón superior derecho).

En la columna "Estatus" se indicará "OBRA", que significa que se efectuó una remodelación, ampliación o construcción en el inmueble señalado.

Para indicar datos de otra obra, repetir el mismo procedimiento.

Al terminar las correcciones presione el botón "Aceptar" para regresar al menú anterior.

Para verificar y/o modificar la información de algún registro de un clic en la palabra "Validar" se desplegará la información total del registro, por lo que deberá modificar y hacer las correcciones necesarias. Al terminar las correcciones presionar el botón "Aceptar" para regresar al menú anterior.

Si desea eliminar totalmente la información proporcionada de un registro, presionar el botón "X" que se encuentra a la derecha del registro que desea borrar y se elimina el registro completo, una vez eliminado un registro no podrá recuperarlo.

Habiendo concluido la captura presionar el botón "Aceptar". No olvide guardar la información (botón superior derecho).

3.8.3. Venta de Inmuebles.

Si vendió un inmueble seleccionar el botón "Validar" del registro del inmueble a reportar en caso de que ya se hubiere registrado con anterioridad, si corresponde a un registro nuevo dar clic en el botón "Agregar" y posteriormente deberá seleccionar el tipo de operación: VENTA.

Es importante mencionar el importe de la venta y la fecha de dicha operación que se encuentran en el contrato privado que ampara la venta o en la escritura pública.

Si corresponde a un bien inmueble registrado con anterioridad aparecerá el formato prellenado del mismo.

En caso de que manifieste la venta de un inmueble no reportado con anterioridad, deberá proporcionar los siguientes datos obligatorios:

- Tipo de bien: Elija del catálogo si el bien corresponde a: casa, departamento, local, terreno.
- Superficie del terreno o indiviso: Proporcionar la superficie en metros cuadrados.
- Superficie de construcción: Proporcionar la superficie en metros cuadrados. Este campo no se desplegará en el caso de que haya elegido terreno.
- Forma de adquisición: Seleccionar del catálogo la forma de adquisición: cesión, contado, crédito, donación, herencia, permuta, rifa o sorteo, traspaso.
- Proporcionar el nombre o razón social del vendedor o enajenante, autor de la donación, autor de la herencia o cesionario, según sea el caso.
- Seleccionar el tipo de relación del vendedor o enajenante, autor de la donación, autor de la herencia o cesionario con el titular.
- Valor del inmueble: Proporciona el monto que recibió y selecciona el tipo de moneda. No actualice a valor presente.
- Fecha de adquisición: Indique la fecha de adquisición en formato dd/mm/aaaa.
- Datos del Registro Público de la Propiedad: Indique el número correspondiente a la escritura de la propiedad o cualquier dato de identificación con que se cuente.
- Titular: Seleccione del catálogo si el bien corresponde al declarante, cónyuge, declarante y cónyuge, concubina o concubinario y/o dependientes económicos.

Posteriormente deberá ingresar los Datos de la Operación:

- Forma de operación: Seleccionar del catálogo: cesión, contado, crédito, donación, herencia, permuta, rifa o sorteo, traspaso.
- Valor de la operación: Proporcionar el monto de la operación conforme a escritura pública y seleccionar el tipo de moneda. No actualizar valor presente.
- Fecha de la operación: Indique la fecha de operación en formato dd/mm/aaaa.
- Indicar la ubicación del inmueble, seleccionando con un clic en el botón que dice "Debes indicar la ubicación del inmueble" y proporcionar o verificar los datos del domicilio.
- Lugar donde se ubica: Marcar la casilla que corresponda al lugar donde se ubica: México o extranjero.
- Calle: Proporcionar el nombre de la calle.
- Número exterior: Proporcionar el número exterior.
- Número interior: Proporcionar el número interior. En el supuesto que el inmueble no cuente con número interior, dicho campo puede dejarse en blanco.

- Localidad o colonia: Proporcionar el nombre de la localidad o de la colonia.
- Entidad federativa: Proporcionar la entidad federativa donde se localiza el bien. Si seleccionaste extranjero, indica el país y ciudad.
- Municipio o alcaldía: Proporcionar el municipio o alcaldía, donde se encuentra el domicilio del bien inmueble. Si seleccionaste extranjero, indica la provincia o localidad.
- Código Postal: Proporcionar el código postal.

Una vez terminado de llenar el formato presione el botón "Aceptar" para regresar al menú de Venta del inmueble.

Habiendo concluido la captura de los datos de la "venta" presionar el botón "Aceptar". No olvide guardar la información (botón superior derecho).

En la columna Estatus se indicará "VENTA", que significa que es un bien inmueble que ya no forma parte de tu patrimonio.

Para incorporar datos de otra "Venta", repita el procedimiento.

Para verificar y/o modificar la información de algún registro dé un clic en la palabra "Validar" y se desplegará la información total del registro, por lo que deberá modificar y hacer las correcciones necesarias. Al terminar las correcciones presionar el botón Aceptar para regresar al menú anterior.

Si desea eliminar totalmente la información proporcionada de un registro, presionar el botón "X" que se encuentra a la derecha del registro y se eliminará por completo, una vez eliminado un registro no podrá recuperarlo.

Habiendo concluido la captura presionar el botón "Aceptar". No olvide guardar la información (botón superior derecho).

3.8.4 Inmuebles sin modificación.

Si los bienes de una declaración anterior que aparecen en la lista, no fueron desincorporados de su patrimonio, oprimir el botón "Validar" y después dar clic en "Aceptar".

En la columna Estatus se indicará "SIN CAMBIO", que significa que aún cuentas con el inmueble.

Es muy importante verificar que se encuentre toda la información correcta y que no se eliminen registros, para no perder el inventario y se pueda aprovechar para futuras declaraciones.

Una vez que indique la situación de todos los bienes inmuebles, oprimir "Aceptar" para ir al menú principal y seguir con la presentación de la Declaración.

3.9.1 Incorporar un vehículo.

Para incorporar información de un vehículo oprimir el botón "Agregar".

En el llenado de esta información, deberá contar con la tarjeta de circulación, con factura del (os) vehículo (s) automotores, aeronaves o embarcaciones, o de cualquier otro tipo, y en su caso, de la carta responsiva.

El dato de "Tipo", también aparece en la tarjeta de circulación o factura como submarca o línea.

Tipo de operación: Deberá seleccionar la opción INCORPORACIÓN y proporcionar los siguientes datos obligatorios:

- Marca: Seleccione del catálogo la marca del vehículo.
- Tipo: Proporcione el tipo de vehículo.
- Modelo: Indica el año del modelo.
- Número de serie: Proporciona el número de serie.
- Lugar de registro: Indicar dando un clic en la casilla que corresponda al lugar donde fue registrado: "México" o "Extranjero".
- Entidad federativa: Del catálogo, elegir la entidad federativa. En caso de que haya elegido "Extranjero" proporcionar el país y ciudad.
- Forma de adquisición: Seleccionar del catálogo la forma de adquisición: cesión, contado, crédito, donación, herencia, permuta, rifa, sorteo o traspaso.
- En caso de que haya seleccionado, cesión, herencia o donación deberá referir el nombre o razón social del autor de la cesión, donación o de la herencia.

Asimismo, deberá seleccionar del catálogo la relación del autor de la cesión, donación o de la herencia con el titular.

- Valor del vehículo al momento de la adquisición: Proporcionar el monto y seleccionar el tipo de moneda.
- Fecha de adquisición: Indicar la fecha de operación en formato dd/mm/aaaa.
- Titular: Seleccionar del catálogo si el bien corresponde al declarante, cónyuge, declarante y cónyuge, concubina o concubinario y/o dependientes económicos.

Presionar "Aceptar" y regresará al menú anterior, donde aparecerá el vehículo incorporado en la lista. En la columna Estatus se indicará INCORPORACIÓN, que significa que es un vehículo que incorporó a su patrimonio.

Para incorporar datos de otro vehículo, presionar el botón "Agregar" y repite el procedimiento.

Para verificar y/o modificar la información de algún registro dar un clic en la palabra "validar", se desplegará la información total del registro para que modifique algún dato o pueda hacer las correcciones necesarias. Al terminar las correcciones presionar el botón Aceptar para regresar al menú anterior.

Si desea eliminar totalmente la información proporcionada de un registro, presionar el botón "X" que se encuentra a la derecha del registro que desea borrar y se eliminará el registro por completo, una vez eliminado no podrá recuperarlo.

Habiendo concluido la captura presionar el botón "Aceptar". No olvide guardar la información (botón superior derecho).

3.9.2. Venta de vehículos.

Si se vendió un vehículo, oprimir el botón "Validar" del registro del vehículo a reportar, si corresponde a un registro nuevo dar clic en el botón "Agregar" y posteriormente deberá seleccionar el tipo de operación: VENTA.

Es importante mencionar el importe de la venta y la fecha de dicha operación, datos contenidos en el contrato y/o documentos que amparen la venta.

Si corresponde a un vehículo registrado con anterioridad aparecerá el formato prellenado del mismo, en caso de que sea una incorporación, deberá proporcionar los siguientes datos obligatorios:

- Marca: Seleccionar del catálogo la marca del vehículo.
- Tipo: Proporcionar el tipo de vehículo.
- Modelo: Indicar el año del modelo.
- Número de serie: Indicar el número de serie del vehículo que desees desincorporar.
- Registro: Seleccionar dando un clic en la casilla que corresponda, "México" o "Extranjero".
- Entidad Federativa del catálogo: Elegir la entidad federativa. En el caso de que se haya elegido "Extranjero" proporcionar el país y ciudad.
- Forma de adquisición: Seleccionar del catálogo la forma de adquisición: cesión, contado, crédito, donación, permuta, traspaso. En el caso de cesión o donación especificar el nombre o razón social del beneficiario.
- Valor del vehículo al momento de la adquisición: Proporcionar el monto y selecciona el tipo de moneda.
- Fecha de adquisición: Indica la fecha de adquisición en formato día/mes/año.
- Titular: Seleccionar del catálogo si el bien corresponde al declarante, cónyuge, declarante y cónyuge, concubina o concubinario y/o dependientes económicos.

Posteriormente deberá ingresar los Datos de la Operación:

- Forma de Operación: Seleccionar del catálogo: cesión, contado, crédito, donación, herencia, permuta, rifa o sorteo, traspaso.
- Valor de la Operación: Proporcionar el monto que recibió por la venta y seleccionar el tipo de moneda. No actualice a valor presente.
- Fecha de la Operación: Indicar la fecha de operación en formato dd/mm/aaaa.

Una vez que termine de capturar los datos presionar el botón "Aceptar" para regresar al menú de Vehículos.

En la columna Estatus se indicará "VENTA", que significa que es un vehículo que ya no forma parte de su patrimonio.

Para incorporar datos de otra venta, repita el procedimiento.

Para verificar y/o modificar la información de algún registro dar un clic en la palabra "Validar" de ese registro y se desplegará la información total del mismo. Para modificar algún dato deberá posicionarse en la parte que desea modificar y ahí podrá sin problemas hacer las correcciones necesarias. Al terminar las correcciones presionar el botón "Aceptar" para regresar al menú anterior.

Si desea eliminar totalmente la información proporcionada de un registro, presionar el botón "X" que se encuentra a la derecha del registro que desea borrar y se eliminará el registro por completo, una vez eliminado no podrá recuperarlo.

Habiendo concluido el llenado del rubro totalmente, presionar el botón "Aceptar" para regresar al menú principal.

3.9.3. Vehículo sin modificación.

Si los vehículos de una declaración anterior que aparecen en la lista, no fueron desincorporados de su patrimonio o no sufrieron algún cambio, oprima el botón "Validar" y posteriormente "Aceptar".

En la columna Estatus se indicará SIN CAMBIO, que significa que aun cuentas con el vehículo.

Es muy importante que se verifique la información y no se eliminen registros, para no perder su inventario y que lo pueda aprovechar para futuras declaraciones.

Si desea eliminar totalmente la información proporcionada de un registro, presionar el botón "Borrar" que se encuentra a la derecha del registro que desea borrar y se eliminará el registro por completo, una vez eliminado no podrá recuperarlo.

Habiendo concluido la captura presionar el botón "Aceptar". No olvide guardar la información (botón superior derecho).

Una vez que indique la situación de todos los vehículos, oprima "Aceptar" para continuar.

3.9.4. Vehículo con siniestro.

Si el (los) vehículo (s) que tiene registrado (s), sufrió algún siniestro y fue pérdida total o robo, y está asegurado, deberá contar con la documentación proporcionada por la aseguradora para obtener la fecha del siniestro y el monto que cubrió la aseguradora.

Oprimir el botón "Validar" del registro del vehículo con siniestro a reportar, si corresponde a un registro nuevo dar clic en el botón "Agregar" y posteriormente deberá seleccionar el tipo de operación: VENTA. Si corresponde a un vehículo registrado con anterioridad aparecerá el formato prellenado del mismo, en caso de que sea una incorporación deberá proporcionar los siguientes datos obligatorios:

- Marca: Seleccionar del catálogo la marca del vehículo.
- Tipo: Proporcionar el tipo de vehículo.
- Modelo: Indicar el año del modelo.
- Número de serie: Indicar el número de serie del vehículo que deseas desincorporar.
- Lugar de registro: Seleccionar la casilla que corresponda, "México" o "Extranjero"
- Entidad Federativa del catálogo: Elija la entidad federativa. En el caso de que haya elegido Extranjero proporcione el país y ciudad.

Validar a continuación los datos siguientes:

- Forma de adquisición: Seleccionar del catálogo la forma de adquisición: cesión, contado, crédito, donación, permuta, traspaso. En el caso de cesión o donación especificar el nombre o razón social del beneficiario.
- Valor del vehículo al momento de la adquisición: Proporcionar el monto y seleccionar el tipo de moneda.
- Fecha de adquisición: Indicar la fecha de adquisición en formato dd/mm/aaaa.
- Titular: Seleccionar del catálogo si el bien corresponde al declarante, cónyuge, declarante y cónyuge, concubina o concubinario y/o dependientes económicos.

Posteriormente deberá ingresar los datos de siniestro:

- Tipo de siniestro: Seleccionar del catálogo el tipo de siniestro, alud, colisión, explosión, granizo, huracán, incendio, inundación, robo, terremoto, tornado o volcán.
- Aseguradora: Seleccionar del catálogo la aseguradora.
- Fecha del siniestro: Indicar la fecha del siniestro, en formato dd/mm/aaaa.
- Valor de la operación: Proporcionar el monto que le pagó la aseguradora, seleccionar el tipo de moneda.

Si el vehículo no se encontraba asegurado indicarlo en observaciones y aclaraciones.

Una vez que termine de capturar los datos presionar el botón "Aceptar" para regresar al menú donde tienes toda la información de "Vehículos", oprimir el botón "Aceptar" nuevamente y regresarás al menú principal, para que pueda guardar la información.

3.10.1. Incorporar un bien inmueble.

...
...
...
...
...
...
...
...

Tipo de operación: Deberá seleccionar la opción INCORPORACIÓN y proporcionar los siguientes datos obligatorios:

- ...
- ...
- ...
- Relación del autor de la cesión, donación o herencia con el titular: Selecciona del catálogo.
- Fecha de adquisición.
- Valor de la operación: Proporcione el monto del bien y seleccione el tipo de moneda.

...
...

Para verificar y/o modificar la información de algún registro dar un clic en la palabra que "validar" de ese registro y se desplegará la información total del registro. Para modificar algún dato deberás posicionarte en la parte que deseas modificar y ahí podrá sin problemas hacer las correcciones necesarias. Al terminar las correcciones presione el botón "Aceptar" para regresar al menú anterior.

Si desea eliminar totalmente la información proporcionada de un registro, presione el botón "X" que se encuentra a la derecha del registro que deseas borrar y se eliminará el registro por completo, una vez eliminado un registro no podrá recuperarlo.

Habiendo concluido la captura presionar el botón "Aceptar". No olvide guardar la información (botón superior derecho).

3.10.2. Venta de bienes muebles.

Si vendió, cedió, traspasó, donó o desincorporó de su patrimonio un bien mueble, oprimir el botón "Validar" del registro del bien mueble a reportar, si corresponde a un registro nuevo dar clic en el botón "Agregar" y posteriormente deberá seleccionar el tipo de operación: VENTA.

Para el llenado de este rubro, deberá contar con el contrato y/o documentos que amparen la venta.

Si corresponde a un bien mueble registrado con anterioridad aparecerá el formato prellenado del mismo, en caso de que sea una incorporación deberá proporcionar los siguientes datos obligatorios:

- Tipo de bien: Seleccionar del catálogo (joyas, obras de arte, menaje de casa, colecciones, semovientes.)
- Descripción del bien: Especificar el bien a desincorporar.

En la columna Estatus se indicará VENTA, que significa que ya no forma parte de su patrimonio.

Para incorporar datos de otra venta, repetir el procedimiento.

Para verificar y/o modificar la información de algún registro dar un clic en la palabra "Validar" y se desplegará la información total del registro. Para modificar algún dato deberá posicionarse en la parte que quiera modificar y ahí podrá sin problemas hacer las correcciones necesarias. Al terminar las correcciones presionar el botón Aceptar para regresar pantalla menú a anterior.

Si desea eliminar totalmente la información proporcionada de un registro presionar el botón "X" que se encuentra a la derecha del registro que desea borrar y se eliminará por completo.

Habiendo concluido la captura presionar el botón "Aceptar". No olvide guardar la información (botón superior derecho).

3.11.3. Saldos en cuenta o inversión.

Si las cuentas bancarias o de inversión de la declaración anterior que aparecen en la lista, no fueron desincorporadas de su patrimonio, sólo se debe de actualizar el saldo de las mismas, para lo cual deberá oprimir el botón "Validar" del registro de la cuenta o inversión a reportar, y posteriormente deberá seleccionar el tipo de operación: SALDO.

Si corresponde a cuentas o inversiones registradas con anterioridad aparecerá el formato prellenado del mismo, por lo que sólo se deberá corroborar la información y requisitar el rubro de saldo: Proporcione el monto y seleccione el tipo de moneda.

En caso de que no realice actualización o modificación en el aumento o disminución del monto de los adeudos manifestados con anterioridad, deberá oprimir el botón "Validar" del adeudo correspondiente, y posteriormente deberá seleccionar el tipo de operación: SIN CAMBIO.

Es muy importante que se verifiquen los datos registrados y no se eliminen registros de cuentas vigentes, para no perder el inventario y que se pueda aprovechar para futuras declaraciones.

Para verificar y/o modificar la información de algún registro dar clic en la palabra "Validar" y se desplegará toda la información del registro. Para modificar algún dato deberá posicionarse en la parte que desea modificar y ahí podrá sin problemas hacer las correcciones necesarias. Al terminar las correcciones presionar el botón "Aceptar" para regresar al menú anterior.

Si desea eliminar totalmente la información proporcionada de un registro presionar el botón "X" que se encuentra a la derecha del registro que desea borrar y se eliminará por completo.

Habiendo concluido la captura presionar el botón "Aceptar". No olvide guardar la información (botón superior derecho).

3.12. Adeudos.

En las declaraciones de tipo Inicial proporcionar los datos de los adeudos que posee a la fecha de toma de posesión del encargo; en la de conclusión capture la información correspondiente a la fecha de término del mismo. En la de modificación patrimonial, reporte el saldo de los adeudos al 31 de diciembre del año anterior.

Para declarar la situación de sus adeudos dar clic en "Adeudos"

...

...

...

...

...

Para verificar y/o modificar la información de algún registro dar clic en la palabra "Validar" y se desplegará toda la información del registro. Para modificar algún dato deberá posicionarse en la parte que desea modificar y ahí podrá sin problemas hacer las correcciones necesarias. Al terminar las correcciones presionar el botón "Aceptar" para regresar al menú anterior.

Si desea eliminar totalmente la información proporcionada de un registro presionar el botón "X" que se encuentra a la derecha del registro que desea borrar y se eliminará por completo.

Habiendo concluido la captura presionar el botón "Aceptar". No olvide guardar la información (botón superior derecho).

3.12.1. Incorporar un adeudo.

...

...

Tipo de operación: Deberá seleccionar la opción INCORPORACIÓN y proporcionar los siguientes datos obligatorios:

- ...
- ...
- ...
- ...
- ...
- ...
- ...
- ...
- ...

...

...

Para verificar y/o modificar la información de algún registro dar clic en la palabra "Validar" y se desplegará toda la información del registro. Para modificar algún dato deberá posicionarse en la parte que desea modificar y ahí podrá, sin problemas, hacer las correcciones necesarias. Al terminar las correcciones presionar el botón "Aceptar" para regresar al menú anterior.

Si desea eliminar totalmente la información proporcionada de un registro presionar el botón "X" que se encuentra a la derecha del registro que desea borrar y se eliminará por completo.

Habiendo concluido la captura presionar el botón "Aceptar". No olvide guardar la información (botón superior derecho).

3.12.2. Actualizar montos de adeudos.

...

Para actualizar la información deberá oprimir el botón "Validar" del registro de la cuenta o inversión correspondiente, y posteriormente deberá seleccionar el tipo de operación: SALDO.

Si corresponde a información de adeudos registrada con anterioridad aparecerá el formato prellenado de la misma, por lo que sólo se deberá corroborar los datos proporcionados y requisitar el rubro de saldo: Proporcione el monto y seleccione el tipo de moneda.

En caso que considere necesario modificar los datos proporcionados, deberá actualizar los campos que sean necesarios de la información que se despliega:

Especificar el tipo: Seleccionar del catálogo según corresponda: créditos hipotecarios, préstamos personales, compras a crédito, tarjetas de crédito, compra de vehículo.

...

...

...

...

...

...

...

...

...

Para verificar y/o modificar la información de algún registro da un clic en la palabra "Validar" y se desplegará toda la información del registro. Para modificar algún dato deberá posicionarse en la parte que desea modificar y ahí podrá sin problemas hacer las correcciones necesarias. Al terminar las correcciones presionar el botón "Aceptar" para regresar al menú anterior.

Si deseas eliminar totalmente la información proporcionada de un registro presionar el botón "X" que se encuentra a la derecha del registro que desea borrar y se eliminará por completo.

Habiendo concluido la captura presionar el botón "Aceptar". No olvide guardar la información (botón superior derecho).

3.13 Declaración de posible conflicto de interés

Este apartado deberá ser llenado de manera obligatoria por todos los servidores públicos obligados a presentar declaración de situación patrimonial. Esta declaración deberá hacerse al ingresar a cargos públicos federales, actualizarse anualmente o en cualquier momento en que un servidor público considere que pudiera ocurrir un posible conflicto de interés en su responsabilidad.

Primeramente deberá seleccionar la opción "Puesto, cargo, comisión, actividades o poderes". En este apartado el declarante deberá requisitarlo conforme a los puestos, cargos, comisiones, actividades o poderes que el declarante, su cónyuge, concubina o concubinario y/o dependientes económicos, desempeñen en órganos directivos o de gobierno en organizaciones con fines de lucro (empresas), o bien, en asociaciones, sociedades, consejos, actividades filantrópicas o de consultoría donde el declarante puede o no recibir remuneración por esta participación.

En caso de que el servidor público se ubique en alguno de los supuestos referidos dar clic en el botón "Agregar" y posteriormente en Tipo de operación deberá seleccionar la opción INCORPORACIÓN ingresando los siguientes datos obligatorios:

- Responsable del conflicto de interés (Cónyuge, dependiente, declarante).
- Nombre de la institución (empresa, asociación, sindicato, etc.)
- Naturaleza del vínculo: socio, colaborador u otro.
- Antigüedad del vínculo.
- Frecuencia anual: 3 ocasiones, de 4 a 7 ocasiones, de 8 a 11 ocasiones, mensualmente, ocasionalmente u otra.
- Participación en la dirección o administración, antes o durante el servicio público.
- Tipo de persona jurídica en la que participa: instituciones de derecho público, sociedades o asociaciones de derecho privado, fundación, asociación gremial, sindicato o federación de organizaciones de trabajadores, junta de vecinos u otra organización comunitaria, iglesia o entidad religiosa, u otra.
- Tipo de colaboración o aporte: cuotas, servicios profesionales, participación voluntaria, participación remunerada, otros aportes.
- Ubicación señalando la ciudad o población, entidad federativa y país.

En la parte de observaciones o aclaraciones el declarante deberá especificar aquella información complementaria que considere necesaria para evitar dudas o confusiones sobre la declaración de posible conflicto de interés.

De no encontrarse en alguno de los supuestos, deberá marcarse la casilla "Ninguno".

Asimismo, deberá dar clic sobre la opción "Participaciones económicas o financieras". Esta sección se refiere a participaciones económicas o financieras, así como aquellos convenios, contratos, compromisos o acuerdos con un valor económico presente o futuro que el declarante, su cónyuge, concubina o concubinario y/o dependientes económicos, tengan con personas físicas o morales y que podrían ser percibidos o susceptibles de un conflicto de interés y que no pueden ser incluidos en alguna de las secciones anteriores.

En caso de que el servidor público se ubique en alguno de los supuestos referidos dar clic en el botón "Agregar" y posteriormente en Tipo de operación deberá seleccionar la opción INCORPORACIÓN ingresando los siguientes datos obligatorios:

- Responsable del conflicto de interés (Cónyuge, dependiente, declarante)
- Nombre de la empresa o sociedad o persona física.
- Fecha de la constitución de la sociedad, señalando día, mes y año, en su caso.

- Inscripción en el Registro Público de la Propiedad, en su caso u otro dato que permita identificar la sociedad de que se trata.
- Sector o industria, en su caso.
- Tipo de sociedad: sociedad anónima, sociedad civil, asociación civil u otra.
- Tipo de participación o contrato: porcentaje de participación en el capital, partes sociales, trabajo, provisión de servicios o de bienes muebles o inmuebles u otra. (Especificar)
- Antigüedad en la participación en años.
- Inicio de participación o del contrato, antes o durante el servicio público.
- Ubicación señalando la ciudad o población, entidad federativa y país, en su caso.

En la parte de observaciones o aclaraciones, el declarante deberá especificar aquella información que considere relevante sobre este tema.

De no encontrarse en alguno de los supuestos, deberá marcarse la casilla "Ninguno".

Una vez que se hayan completado los rubros de este apartado de la declaración, se deberá indicar si está de acuerdo en hacer pública la información de tu posible conflicto de interés, para lo cual deberá seleccionar alguna de las opciones "SI" o "NO", que aparecen al final de la pantalla.

3.14 Ratificar o actualizar declaración de posible conflicto de interés

Si los registros de posible conflicto de interés registrados con anterioridad, no presentan variación alguna en los datos proporcionados, deberá ubicar el registro del posible conflicto de interés correspondiente y oprimir el botón "Validar", posteriormente deberá verificar la información que se encuentra precargada en la plantilla cuyos campos de escritura se encuentran inhabilitados y deberá seleccionar el tipo de operación: SIN CAMBIO. Posteriormente deberá presionar el botón "Aceptar" para regresar al menú anterior. En la columna Estatus se indicará SIN CAMBIO, que significa que aún se reporta ese supuesto y no tuvo modificación alguna.

Para actualizar la información de algún registro de posible conflicto de interés, deberá dar un clic en la palabra "Validar" y se desplegará toda la información del registro. Para modificar algún dato deberá posicionarse en la parte que desea modificar y ahí podrá sin problemas hacer las correcciones necesarias. Al terminar las correcciones se habilitará un cuadro de texto, para que se manifiesten las razones de su modificación. No se podrá registrar la modificación hasta que se hayan aclarado los motivos de la misma. Posteriormente deberá presionar el botón "Aceptar" para regresar al menú anterior. En la columna Estatus se indicará MODIFICADO, que significa que actualizó los datos de ese registro de posible conflicto de interés.

Para ratificar o modificar los datos de otro registro de posible conflicto de interés, repite el procedimiento.

Si desea eliminar totalmente la información proporcionada de un registro presionar el botón "X" que se encuentra a la derecha del registro que deseas borrar. Una vez seleccionado el botón "X" se habilitará un cuadro de texto, para que se manifiesten las razones de su eliminación. No se podrá eliminar totalmente el registro hasta que se hayan registrado los motivos de la eliminación.

Habiendo concluido el llenado del formato totalmente presiona el botón "Aceptar". No olvide guardar la información (botón superior derecho).

3.15 Observaciones y aclaraciones

Si no tiene observaciones, seleccione la casilla "Ninguno", en caso contrario dar un clic en "Observaciones y Aclaraciones", asimismo en todos los rubros se incluyó el botón de "Aclaraciones".

...

..."

TRANSITORIO

Único.- El presente Acuerdo entrará en vigor el día siguiente al de su publicación en el Diario Oficial de la Federación.

Ciudad de México, a los diecinueve días del mes de octubre de dos mil dieciséis.- El Subsecretario de Responsabilidades Administrativas y Contrataciones Públicas de la Secretaría de la Función Pública, **Javier Vargas Zempoaltecatl**.- Rúbrica.

DISPOSICIONES Generales de la Ley de Firma Electrónica Avanzada.

Al margen un sello con el Escudo Nacional, que dice: Estados Unidos Mexicanos.- Secretaría de Economía.- Secretaría de la Función Pública.- Servicio de Administración Tributaria.

ILDEFONSO GUAJARDO VILLARREAL, Secretario de Economía; JAVIER VARGAS ZEMPOALTECATL, Subsecretario de Responsabilidades Administrativas y Contrataciones Públicas de la Secretaría de la Función Pública en ausencia del Secretario de la Función Pública y OSVALDO ANTONIO SANTÍN QUIROZ, Jefe del Servicio de Administración Tributaria, con fundamento en lo dispuesto por los artículos 17, 31 fracción XXXIV, 34 fracción XXXIII y 37 fracciones XXII y XXIX de la Ley Orgánica de la Administración Pública Federal; 5 segundo párrafo; 2 fracción I del Reglamento de la Ley de Firma Electrónica Avanzada; 1, 7 fracción XVIII y 14 fracción I de la Ley del Servicio de Administración Tributaria, en relación con el Artículo Tercero Transitorio del Decreto por el que se reforman, adicionan y derogan diversas disposiciones contenidas en la Ley del Servicio de Administración Tributaria publicado en el Diario Oficial de la Federación el 12 de junio del 2003; 5 fracción XVI del Reglamento Interior de la Secretaría de Economía; 6 fracción I, 7 fracción XII y 86 del Reglamento Interior de la Secretaría de la Función Pública, y 8 fracción XXI del Reglamento Interior del Servicio de Administración Tributaria, y

CONSIDERANDO

Que con fecha 11 de enero de 2012 se publicó en el Diario Oficial de la Federación la Ley de Firma Electrónica Avanzada, la cual contempla en su artículo 5, segundo párrafo, que la Secretaría de la Función Pública, la Secretaría de Economía y el Servicio de Administración Tributaria dictarán, de manera conjunta, las disposiciones generales para el adecuado cumplimiento de la Ley mencionada;

Que con fecha 21 de marzo de 2014 se publicó en el Diario Oficial de la Federación el Reglamento de la Ley de Firma Electrónica Avanzada, el cual refiere en su artículo 2, fracción I, a las Disposiciones Generales como aquellas que se emitan en términos del artículo 5 de la Ley de Firma Electrónica Avanzada;

Que resulta necesario determinar los requisitos, características, estándares y mecanismos tecnológicos que están obligados a cumplir los interesados en obtener el carácter de Autoridades Certificadoras para la emisión de los certificados digitales previstos en el artículo 24 de la Ley de Firma Electrónica Avanzada y la prestación de servicios relacionados; la estructura de los certificados digitales que emitan las Autoridades Certificadoras; los requerimientos técnicos que como mínimo deberán contener los sistemas informáticos de las dependencias y entidades de la Administración Pública Federal para estar en posibilidad de llevar a cabo el firmado de documentos electrónicos y, en su caso, mensajes de datos, así como la forma y términos en que las Autoridades Certificadoras proporcionarán a las dependencias y entidades los servicios relacionados con la firma electrónica avanzada, por lo que hemos tenido a bien emitir las siguientes

DISPOSICIONES GENERALES DE LA LEY DE FIRMA ELECTRÓNICA AVANZADA**Objeto**

PRIMERA.- Las presentes Disposiciones Generales tienen por objeto establecer:

- I. Los requisitos, características, estándares y mecanismos tecnológicos que deberán cumplir las dependencias y entidades de la Administración Pública Federal, así como los prestadores de servicios de certificación que estén interesados en obtener el carácter de Autoridad Certificadora para la emisión de los certificados digitales previstos en la Ley de Firma Electrónica Avanzada y su Reglamento, así como la autorización para la prestación de servicios relacionados con la firma electrónica avanzada;
- II. La estructura que deberán cumplir los certificados digitales que emitan las Autoridades Certificadoras, previstos en el Título Tercero, Capítulo I de la Ley de Firma Electrónica Avanzada;
- III. Los requerimientos técnicos mínimos para que los sistemas informáticos, así como las herramientas tecnológicas o aplicaciones de las dependencias y entidades de la Administración Pública Federal puedan llevar a cabo el firmado de documentos electrónicos y, en su caso, mensajes de datos en la realización de los actos y actuaciones a que se refiere la Ley y su Reglamento;
- IV. La manera en que se llevará a cabo la conservación de los mensajes de datos y de los documentos electrónicos con firma electrónica avanzada;
- V. Las medidas y controles de seguridad que deberán adoptar las Autoridades Certificadoras para evitar la falsificación, alteración o uso indebido de Certificados Digitales;

- VI. El destino de los registros y archivos generados por las Autoridades Certificadoras que hayan sido suspendidas o revocadas de tal carácter;
- VII. La forma y términos en que las Autoridades Certificadoras proporcionarán a las dependencias y entidades de la Administración Pública Federal, el servicio de consulta sobre el estado de validez, de los certificados digitales que emitan, y
- VIII. Cualquier otro servicio relacionado con la Firma Electrónica Avanzada.

Definiciones y acrónimos

SEGUNDA.- En adición a las definiciones previstas en la Ley de Firma Electrónica Avanzada y en su Reglamento, para efectos de las presentes Disposiciones Generales, se entenderá por:

- I. **AC:** Autoridad Certificadora;
- II. **Claves criptográficas:** la clave pública y la clave privada;
- III. **HTTP:** Protocolo utilizado para el intercambio de información en Internet (*Hyper Text Transfer Protocol*, HTTP por sus siglas en inglés);
- IV. **HTTPS:** Protocolo seguro para el intercambio de información en Internet (*Hyper Text Transfer Protocol Secure*, HTTPS por sus siglas en inglés);
- V. **MAAGTICSI:** Manual Administrativo de Aplicación General en las materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información, emitido por la Secretaría y la Secretaría de Gobernación como anexo único del Acuerdo que tiene por objeto emitir las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así como establecer el Manual Administrativo de Aplicación General en dichas materias;
- VI. **OCSP:** Protocolo utilizado para obtener en tiempo real el estado actual de un certificado digital (*OCSP, Online Certificate Status Protocol*, por sus siglas en inglés);
- VII. **OID:** es el número que se asigna para identificar un objeto sin ambigüedad, el cual se conforma de acuerdo al estándar del Instituto Nacional Estadounidense de Estándares (*ANSI American National Standards Institute*) (*OID, Object Identifier*, por sus siglas en inglés);
- VIII. **SAT:** el Servicio de Administración Tributaria, y
- IX. **SE:** la Secretaría de Economía.

Disposiciones

TERCERA.- La estructura de los certificados digitales que emitan las AC debe considerar los estándares internacionales ISO/IEC 9594-8:2014 "*The Directory: Public-key and attribute certificate frameworks*" y RFC 5280 "*Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*" actualizado con el RFC 6818 y contendrá, cuando menos, los campos que a continuación se indican:

- I. **Número de Serie:** incorporará un número entero positivo;
- II. **AC que lo emitió:** identificará a la AC con un nombre distintivo (DN Distinguished Name) de tipo "Name" del estándar X.509 con los atributos siguientes:

ATRIBUTOS	TIPO	LONGITUD	DESCRIPCIÓN
commonName (CN)	PrintableString o UTF8String	64	Nombre de la AC
organizationName (O)	PrintableString o UTF8String	64	Nombre de la organización o razón social
organizationalUnitName (OU)	PrintableString o UTF8String	64	Nombre de la unidad dentro de la organización
EmailAddress (E)	IA5String	128	Correo electrónico de la organización
StreetAddress	PrintableString o UTF8String	128	Calle, número y colonia de la organización
PostalCode	PrintableString o UTF8String	40	Código postal de la organización
CountryName (C)	PrintableString	2	País
State (S)	PrintableString o UTF8String	128	Entidad federativa
LocalityName (L)	PrintableString o UTF8String	128	Municipio o delegación

- III. **Algoritmo de firma:** contendrá el identificador del algoritmo criptográfico utilizado por la AC para firmar el certificado digital.

El algoritmo utilizado para firmar el certificado digital deberá ser SHA256 con RSA o el estándar que en su momento la Secretaría, la SE y el SAT determinen y publiquen a través de sus portales institucionales, mismo que se deberá usar tanto para la firma de la AC como para la del particular, a fin de proveer un nivel adecuado de seguridad;

- IV. **Vigencia:** contendrá la fecha de inicio y la de término del periodo de validez del certificado digital.

Las AC deben utilizar el formato UTCTime (YYMMDDHHMMSSZ);

- V. **Nombre del titular del certificado digital:** identificará al titular del certificado digital con un nombre distintivo (*DN Distinguished Name*) de tipo "Name" del estándar X.509, con los siguientes atributos y valores:

ATRIBUTOS	TIPO	LONGITUD	DESCRIPCIÓN
commonName (CN)	UTF8String	64	Nombre del titular del certificado digital
serialNumber (SN)	PrintableString	64	CURP del titular del certificado digital
CountryName (C)	PrintableString	2	País
X500uniqueIdentifier (2.5.4.45)	BIT STRING		Opcional Registro Federal de Contribuyentes del titular del certificado digital
EmailAddress (E)	IA5String	128	Correo electrónico del titular del certificado digital

- VI. **Clave pública:** contendrá la clave pública y el identificador de algoritmo (contenido en el campo algoritmo de firma), deberá tener un tamaño mínimo de 2048 bits para certificados digitales emitidos a particulares, y por lo menos de 4096 bits para certificados digitales de las AC, y

- VII. **Requisitos adicionales:**

a) **Versión:** deberá contener la "Versión 3 del estándar X.509" y

b) **Extensiones:** contendrá la siguiente información:

ATRIBUTOS	TIPO	DESCRIPCIÓN																														
authorityKeyIdentifier	No crítica	Permite identificar la clave pública correspondiente a la clave privada que la AC utilizó para firmar el certificado digital. Usar sólo el campo KeyIdentifier, el cual debe contener los 256 bits del SHA-2 del valor subjectPublicKey del certificado digital de la AC.																														
subjectKeyIdentifier	No crítica	Asigna un identificador de la clave pública del titular del certificado digital. Debe contener los 256 bits del SHA-2 del valor subjectPublicKey.																														
keyUsage	Crítica	Usos del certificado digital <table border="1"> <thead> <tr> <th>Bit</th> <th>AC</th> <th>Titular</th> </tr> </thead> <tbody> <tr> <td>DigitalSignature</td> <td>S</td> <td>S</td> </tr> <tr> <td>nonrepudiation</td> <td>S</td> <td>S</td> </tr> <tr> <td>keyEncipherment</td> <td>N</td> <td>N</td> </tr> <tr> <td>dataEncipherment</td> <td>S</td> <td>S</td> </tr> <tr> <td>keyAgreement</td> <td>S</td> <td>S</td> </tr> <tr> <td>keyCertSign</td> <td>S</td> <td>N</td> </tr> <tr> <td>cRLSign</td> <td>S</td> <td>N</td> </tr> <tr> <td>encipherOnly</td> <td>N</td> <td>N</td> </tr> <tr> <td>decipherOnly</td> <td>N</td> <td>N</td> </tr> </tbody> </table>	Bit	AC	Titular	DigitalSignature	S	S	nonrepudiation	S	S	keyEncipherment	N	N	dataEncipherment	S	S	keyAgreement	S	S	keyCertSign	S	N	cRLSign	S	N	encipherOnly	N	N	decipherOnly	N	N
Bit	AC	Titular																														
DigitalSignature	S	S																														
nonrepudiation	S	S																														
keyEncipherment	N	N																														
dataEncipherment	S	S																														
keyAgreement	S	S																														
keyCertSign	S	N																														
cRLSign	S	N																														
encipherOnly	N	N																														
decipherOnly	N	N																														
basicConstraints	Crítica	Identifica si el titular del certificado digital es una AC.																														
extendedKeyUsage	No crítica	Indica uno o más propósitos de uso.																														

ATRIBUTOS	TIPO	DESCRIPCIÓN
cRLDistributionPoint	No crítica	Indica cómo puede ser obtenida la Lista de Certificados Revocados.
authorityInfoAccess	No crítica	Indica cómo acceder a la información de la AC y sus servicios, aquí debe indicarse como mínimo la dirección electrónica de consulta de la AC.
certificatePolicies	Crítica	OID asignado por la Secretaría, quien deberá llevar un registro de los mismos.

CUARTA.- Los requisitos para adquirir el carácter de AC serán:

1. Modelo Operacional de la AC;
 - 1.1. El solicitante de acreditación deberá definir su Modelo Operacional de la AC conforme al cual operará y prestará sus servicios al fungir como AC a efecto de lograr confiabilidad e interoperabilidad, para lo cual desarrollará los apartados siguientes:
 - 1.1.1. Cuáles son los servicios prestados;
 - 1.1.2. Cómo se interrelacionan los diferentes servicios;
 - 1.1.3. En qué lugares se operará;
 - 1.1.4. Qué tipos de certificados se entregarán;
 - 1.1.5. Cuáles son los certificados generados con diferentes niveles de seguridad;
 - 1.1.6. Cuáles son las políticas y procedimientos de cada tipo de certificado, y
 - 1.1.7. Cómo se protegerán los activos.
 - 1.2. El Modelo Operacional de la AC deberá contener un resumen que incluya:
 - 1.2.1. Contenido del documento, y
 - 1.2.2. Relaciones comerciales con proveedores de insumos o servicios para sus operaciones.
 - 1.3. El Modelo Operacional de la AC deberá comprender los siguientes aspectos:
 - 1.3.1. Interfaces con las Autoridades Registradoras;
 - 1.3.2. Implementación de elementos de seguridad;
 - 1.3.3. Procesos de administración;
 - 1.3.4. Sistema de directorios para los certificados;
 - 1.3.5. Procesos de auditoría y respaldo, y
 - 1.3.6. Bases de Datos a utilizar.
 - 1.4. El Modelo Operacional de la AC deberá considerar la Política de Certificados, la Declaración de Prácticas de Certificación, la Política de Seguridad de la Información y el Plan de Seguridad de Sistemas por lo que se refiere a la generación de claves.
 - 1.5. El Modelo Operacional de la AC deberá incluir los requerimientos de seguridad física del personal, de las instalaciones y del módulo criptográfico.
2. Modelo Operacional de la Autoridad Registradora.
 - 2.1 El solicitante de acreditación deberá definir su Modelo Operacional de Autoridad Registradora conforme al cual operará y prestará sus servicios como autoridad registradora a efecto de lograr confiabilidad e interoperabilidad, para lo cual desarrollará los apartados siguientes:
 - 2.1.1 Cuáles son los servicios de registro que se prestarán;
 - 2.1.2 En qué lugares se ofrecerán dichos servicios, y
 - 2.1.3 Qué tipos de certificados generados por la AC se entregarán.
 - 2.2 El solicitante de acreditación deberá ofrecer los mecanismos para que el propio usuario genere en forma privada y segura sus Datos de Creación de Firma Electrónica. Deberá indicar al usuario el grado de fiabilidad de los mecanismos y dispositivos utilizados.

- 2.3 El Modelo Operacional de la Autoridad Registradora deberá comprender los siguientes aspectos:
 - 2.3.1 Interfaces con AC;
 - 2.3.2 Implementación de dispositivos de seguridad;
 - 2.3.3 Procesos de administración;
 - 2.3.4 Procesos de auditoría y respaldo;
 - 2.3.5 Bases de Datos a utilizar;
 - 2.3.6 Privacidad de datos, y
 - 2.3.7 Descripción de la seguridad física de las instalaciones.
 - 2.4 El Modelo Operacional de la Autoridad Registradora deberá establecer el método para proveer de una identificación unívoca del usuario y el procedimiento de uso de los Datos de Creación de la Firma Electrónica Avanzada.
3. Plan de Administración de Claves.
- 3.1 El solicitante de acreditación deberá definir su Plan de Administración de Claves conforme al cual generará, protegerá y administrará sus claves criptográficas, respecto de los apartados siguientes:
 - 3.1.1 Claves de la AC;
 - 3.1.2 Almacenamiento, respaldo, recuperación y uso de los Datos de Creación de Firma Electrónica de la AC del Prestador de Servicios de Certificación;
 - 3.1.3 Distribución del certificado de la AC;
 - 3.1.4 Administración del ciclo de vida del hardware criptográfico que utilice la AC, y
 - 3.1.5 Dispositivos seguros para los usuarios.
 - 3.2 Los procedimientos implantados de acuerdo al Plan de Administración de Claves, deberán garantizar la seguridad de las claves en todo momento, aun en caso de cambios de personal, componentes tecnológicos, y demás que señalan las presentes Reglas Generales.
 - 3.3 El Plan de Administración de Claves deberá establecer como requerimiento mínimo el utilizar aquellas con longitud de 2048 bits para los usuarios y de 4096 bits para los Prestadores de Servicios de Certificación.
 - 3.4 El solicitante de acreditación, su autoridad certificadora y registradoras, utilizarán dispositivos seguros para almacenar sus Datos de Creación de Firma Electrónica, compatibles como mínimo con el estándar FIPS-140 nivel 3 en sus elementos de seguridad e implantación de los algoritmos, criptográficos estándares, o el que le sustituya.
 - 3.5 El Plan de Administración de Claves tendrá que ser compatible por lo menos con el estándar ETSI TS 102 042 sección 7.2 -Generación de la clave de la AC, Almacenamiento, Respaldo y Recuperación de la clave de la AC, Distribución de la clave pública de la AC, uso de clave de la AC, fin del ciclo de vida de la clave de la AC y Administración del ciclo de vida del Hardware criptográfico-, o el que le sustituya.

Los anteriores requisitos deberán continuar cumpliéndose una vez que los aspirantes de acreditación obtengan el carácter de AC.

QUINTA.- Las dependencias y entidades que requieran utilizar la Firma Electrónica Avanzada, primero deben celebrar un convenio de colaboración o coordinación con la AC que provee el servicio de OCSP y contar con los siguientes requerimientos técnicos mínimos en sus sistemas informáticos, así como en las herramientas tecnológicas o aplicaciones:

1. Contar con la Infraestructura de comunicación necesaria (equipos de cómputo, conexión a internet).
2. Contar con aplicaciones que empleen el algoritmo de firmado SHA256 con RSA para certificados con una longitud de 1024, 2048 bits o superior.
3. Contar con software capaz de validar los certificados mediante un servicio de consulta basado en el protocolo de comunicación OCSP que permita a los usuarios consultar el estado que guarda un Certificado Digital.

4. Proporcionar a la AC la dirección IP y la URL desde la cual se realizarán las consultas al servicio (considerando la IP del firewall).
5. Configurar sus servicios de comunicación de acuerdo al estándar RFC 6960 – X.509 *Internet Public Key Infrastructure Online Certificate Status Protocol* – OCSP.

El procedimiento que deben cumplir las dependencias y entidades, para estar en condiciones de utilizar el protocolo de comunicación OCSP es el siguiente:

1. Verificar que el certificado digital presentado tenga una vigencia válida.
2. Enviar un mensaje para conocer el estado que guarda el certificado digital y suspende la aceptación del certificado digital hasta que la respuesta sea recibida de parte de la AC.
3. Obtener el mensaje de respuesta que envía el servicio de OCSP.
4. Contar con la capacidad de interpretar las respuestas firmadas de las consultas al servicio OCSP utilizando el certificado de la AC para aceptar y en su caso rechazar la solicitud si el certificado ha sido revocado y por lo tanto no es válido a pesar de su vigencia.

SEXTA.- La conservación de los mensajes de datos y de los documentos electrónicos con firma electrónica avanzada se regirá por la naturaleza de la documentación de acuerdo con las disposiciones legales aplicables y se deberá asegurar que se ha mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y sea accesible para su ulterior consulta; para tales efectos deberá observarse lo establecido en la norma oficial mexicana que para tales efectos emita la SE.

SÉPTIMA.- Los solicitantes de acreditación y las AC deben cumplir con la matriz de control descrita en el Anexo 4 "Matriz de control de seguridad para autoridades certificadoras" a fin de evitar la falsificación, alteración o uso indebido de los certificados digitales.

Asimismo, deben cumplir con generar las políticas definidas en el modelo operacional de la AC con base en la especificación del RFC 3647.

OCTAVA.- Los requisitos para obtener el carácter de AC, establecidos en las presentes disposiciones, los deberá cumplir directamente el solicitante de acreditación, y en su caso, la AC cuando obtenga tal carácter, por lo que dichas obligaciones no podrán ser cedidas, subrogadas o transferidas en favor de terceros.

Asimismo, los derechos adquiridos, una vez que se obtenga el carácter de AC, no podrán ser transferidos en favor de cualquier otra persona.

Las AC estarán sujetas a las visitas de verificación por parte de la Secretaría con el apoyo de la SE y/o del SAT, que sean necesarias para asegurar el cumplimiento de las obligaciones establecidas en la Ley, en el Reglamento y en las demás disposiciones aplicables. La realización de dichas visitas se ajustarán a lo previsto en el capítulo Décimo primero del Título Tercero de la Ley Federal de Procedimiento Administrativo.

Finalmente, la AC que obtenga tal carácter, deberá cumplir todas las disposiciones aplicables para las dependencias y entidades de la Administración Pública Federal en materia de tecnologías de la información y comunicaciones, seguridad de la información y protección de datos personales, que se encuentren vigentes.

NOVENA.- Las AC que hayan sido suspendidas o revocadas de tal carácter en términos del artículo 26 de la Ley de Firma Electrónica Avanzada y 21 de su Reglamento, deberán transferir los certificados digitales, registros y archivos generados a la AC que determine la Secretaría, los cuales serán administrados conforme a las disposiciones jurídicas aplicables.

La AC que reciba los certificados digitales debe tener un método que permita verificar en línea el estatus de los mismos.

DÉCIMA.- Para llevar a cabo el registro de datos y verificación de elementos de identificación, así como la emisión, renovación y revocación de certificados digitales, las AC deberán observar los procedimientos definidos en los anexos 1, 2 y 3 de las presentes Disposiciones Generales.

El procedimiento para la emisión de certificados digitales se formulará, tomando en cuenta los estándares internacionales que a continuación se indican:

- a. RFC 5958 "*PKCS#8: Private-Key Information Syntax Standard*", para la creación de la clave privada;
- b. RFC 2986 "*PKCS #10: Certification Request Syntax Specification Version 1.7*", para la generación del archivo de requerimiento del certificado digital, y
- c. RFC 5652 "*Cryptographic Message Syntax (CMS)*", para la descripción del formato del mensaje de datos del certificado digital.

Asimismo, el procedimiento a seguirse para llevar a cabo la captura de biométricos deberá realizarse conforme al Anexo 1 de las presentes Disposiciones Generales.

DÉCIMA PRIMERA.- Las AC proporcionarán el servicio de consulta sobre el estado de validez de los certificados digitales expedidos por las mismas, el cual deberá:

- I. Cumplir con lo señalado en el RFC 6960 “*X.509 Internet Public Key Infrastructure Online Certificate Status Protocol–OCSP*”;
- II. Utilizar mensajes codificados que deberán ser transmitidos sobre el protocolo HTTP o HTTPS;
- III. Firmar la respuesta a la solicitud utilizando el certificado digital de la AC o bien, con otro certificado digital generado especialmente por la AC para la prestación de ese servicio;
- IV. Mantener operando el servicio con una disponibilidad del 99.95%, y
- V. Contar con una dirección electrónica para llevar a cabo la consulta correspondiente, a través del protocolo OCSP.

DÉCIMA SEGUNDA.- Las AC llevarán un registro de los certificados digitales que emitan, identificando aquéllos que hayan sido revocados, los cuales se integrarán en una Lista de Certificados Revocados, misma que elaborarán al menos cada 24 horas y que deberá cumplir con lo siguiente:

- I. Ser compatible con la última versión del estándar ISO/IEC 9594-8:2014 “*The Directory: Public-key and attribute certificate frameworks*” o RFC 5280 “*X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*”;
- II. Contener fecha y hora de su emisión, y
- III. Ser firmada por la AC que la emita.

DÉCIMA TERCERA.- En caso de contingencia o no disponibilidad del servicio de consulta sobre el estado de validez de los certificados digitales a través del protocolo OCSP, las dependencias y entidades, podrán hacer uso de la última Lista de Certificados Revocados que las AC tengan disponible para su consulta en su página Web, siempre y cuando dicha Lista de Certificados Revocados refleje el estado de validez de los certificados digitales hasta 24 horas antes del caso de contingencia o no disponibilidad del servicio.

DÉCIMA CUARTA.- Las dependencias y entidades verificarán, previamente a la firma de los mensajes de datos o documentos electrónicos, el estado de validez y vigencia del certificado digital que se utilizará en el acto de que se trate.

La verificación de validez se realizará mediante consulta que formulen a la AC que expidió el certificado digital correspondiente, a través del servicio de OCSP de acuerdo a las características definidas por la AC.

DÉCIMA QUINTA.- La interpretación para efectos administrativos de las Disposiciones Generales contenidas en el presente Acuerdo, así como la resolución de los casos no previstos en las mismas, corresponderá a la Secretaría a través de la Unidad de Gobierno Digital.

DISPOSICIONES TRANSITORIAS

Primera.- Las presentes Disposiciones entrarán en vigor el día siguiente al de su publicación en el Diario Oficial de la Federación.

Segunda.- A fin de garantizar la interoperabilidad del firmado de los certificados con una longitud de 1024 bits se debe mantener el algoritmo de firmado SHA – 1 hasta el término de vigencia del certificado.

Tercera.- Las dependencias y entidades realizarán, de acuerdo con los plazos previstos en sus respectivos programas de instrumentación para el uso de la firma electrónica avanzada, los ajustes que procedan a sus sistemas informáticos, a efecto de que los mismos cumplan con lo establecido en la disposición tercera fracción III.

Ciudad de México, a 18 de octubre de 2016.- El Secretario de Economía, **Ildelfonso Guajardo Villarreal**.- Rúbrica.- En suplencia por ausencia del Secretario de la Función Pública con fundamento en lo dispuesto por los artículos 7 fracción XII y 86 del Reglamento Interior de la Secretaría de la Función Pública, el Subsecretario de Responsabilidades Administrativas y Contrataciones Públicas de la Secretaría de la Función Pública, **Javier Vargas Zempoaltecatl**.- Rúbrica.- El Jefe del Servicio de Administración Tributaria, **Oswaldo Antonio Santín Quiroz**.- Rúbrica.

Procedimiento de Emisión de los Certificados ANEXO 1

Objetivo

Dotar a las AC de políticas y procedimientos a través de los cuales ejerzan sus facultades, así como promover la estandarización de su operación a nivel nacional, con la finalidad de brindar un servicio eficaz, eficiente y de calidad.

Alcance

El presente procedimiento es de aplicación para el personal encargado de la emisión de los certificados (en lo sucesivo Agentes Certificadores) de las Autoridades Certificadoras (AC).

Políticas de Operación

Primera.- La AC debe tener disponible en su portal de Internet una sección particular para Firma Electrónica Avanzada que al menos contenga la siguiente información:

- a. Requisitos para solicitar la generación de la Firma Electrónica Avanzada, en términos del artículo 18 de la Ley de Firma Electrónica Avanzada.
- b. Dirección de las oficinas a las que debe acudir el solicitante.
- c. Horarios de atención.
- d. Canales de comunicación para la atención de los solicitantes.
- e. Esquema de atención a Quejas, Sugerencias y Reconocimientos.

Segunda.- La AC debe garantizar que el personal (Agente Certificador) cuenta con la capacitación correspondiente para llevar a cabo las actividades para la emisión de certificados, además de contar con los elementos de confiabilidad correspondientes.

Tercera.- La AC debe llevar a cabo evaluaciones de conocimiento y confiabilidad a los Agentes Certificadores en un periodo no mayor a 13 meses para garantizar el cumplimiento de la política previa.

Cuarta.- La AC debe garantizar que el personal que se separa del cargo de las actividades de certificación deje de tener acceso a los sistemas involucrados.

Quinta.- El personal relacionado con el proceso de emisión de certificados debe estar plenamente identificado a través de un gafete, en el que sea visible el nombre del personal, que debe portar durante el proceso de atención.

Sexta.- La AC debe contar con espacios destinados para la instalación y operación del Servicio de Acreditación de Identidad y Enrolamiento vigente, con la correspondiente señalización.

Séptima.- La AC debe garantizar que terceros y personal ajeno al proceso de emisión de certificados de Firma Electrónica Avanzada no tenga acceso a los sistemas relacionados con dichos procesos.

Octava.- Para efectos del presente procedimiento se entiende por acreditación de identidad: Al acto de comparecencia del ciudadano solicitante del certificado de Firma Electrónica Avanzada ante la AC y exhibir la documentación señalada en la sección de Firma Electrónica Avanzada de la página de Internet de la AC, la cual el Agente Certificador cotejará y validará contra los sistemas Institucionales, para proceder a canalizarlos a la Estación de Enrolamiento para el Servicio de Acreditación de Identidad y Enrolamiento.

Novena.- El Agente Certificador tendrá la obligación de verificar que el solicitante cuente con el archivo de requerimiento *.req y el formato de solicitud de firma electrónica avanzada.

En el supuesto de que el solicitante no cuente con los mismos, se le deberá apoyar para llenar la solicitud y realizar la generación del archivo de requerimiento *.req, al momento en que acuda a realizar el trámite.

Nota: Para efectos del llenado del formato de solicitud de firma electrónica avanzada, el solicitante que opte por llenarlo a mano, podrá utilizar tinta negra o azul, utilizando únicamente tinta azul al firmar el citado formato por ambos lados, en caso que el solicitante no cuente con pluma de tinta azul, la AC deberá proporcionársela.

Décima.- Los datos y elementos de identificación obtenidos en el trámite de Firma Electrónica Avanzada formarán parte del sistema de Registro Nacional de Población (RENAPO).

El Agente Certificador deberá recabar los datos y elementos de identificación de conformidad con el Acuerdo por el cual se dan a conocer el Procedimiento Técnico de Captura de Información y el Procedimiento Técnico de Intercambio de Información, así como sus respectivos anexos, publicado en el Diario Oficial de la Federación, por la Secretaría de Gobernación.

Dichos datos y elementos de identificación serán dados a conocer por la Secretaría, la SE y el SAT en sus portales de internet.

La acreditación de la identidad y la certificación documental del trámite de generación del certificado de Firma Electrónica Avanzada del solicitante es responsabilidad del Agente Certificador, y debe estar completa antes de que se canalice al solicitante a la estación de enrolamiento para la toma de biométricos, la digitalización de la documentación probatoria y la emisión del certificado de Firma Electrónica Avanzada.

Décima primera.- La AC debe designar un responsable del proceso de emisión de certificados de Firma Electrónica Avanzada, quién será el encargado de supervisar la adecuada captura de los datos y elementos de identificación del solicitante y de garantizar que no exista inconsistencias o duplicidades de los datos y elementos de identificación.

Décima segunda.- Cuando el Agente Certificador detecte inconsistencias o duplicidades en los datos y elementos de identificación, se deberá rechazar el trámite e informar al solicitante que acuda ante la autoridad correspondiente, para corregir la inconsistencia o duplicidad.

Décima tercera.- La AC podrá emitir certificados de Firma Electrónica Avanzada para los solicitantes que se encuentren bajo ciertos supuestos especiales, siempre y cuando acrediten tal característica, de conformidad con las disposiciones jurídicas aplicables. De manera enunciativa mas no limitativa se mencionan los certificados para los menores de edad que presten exclusivamente un servicio personal subordinado, los menores de edad emancipados y los contribuyentes con incapacidad legal declarada judicialmente.

Décima cuarta.- La AC debe llevar a cabo la toma de biométricos, registro y validación de los mismos conforme al Procedimiento Técnico de Captura de Información y el Procedimiento Técnico de Intercambio de Información, así como sus respectivos anexos publicados en el Diario Oficial de la Federación, disponibles en el portal de Internet de RENAPO.

Décima quinta.- La AC debe emitir los certificados de Firma Electrónica Avanzada de acuerdo al estándar que establecen las Disposiciones Generales.

Décima sexta.- La AC debe enviar a la Autoridad Registradora los certificados de Firma Electrónica Avanzada generados a fin de que se validen y se registren dentro de la infraestructura correspondiente para su validación.

Décima séptima.- La AC debe resguardar de forma digital toda la documentación comprobatoria que acredita la identidad del solicitante en su carácter de persona física, así como el documento mediante el cual el solicitante confirma la recepción o entrega de la Firma Electrónica Avanzada de forma segura y secreta.

Décima octava.- La AC debe contar con un expediente electrónico por cada solicitante, asimismo debe mantener una bitácora electrónica de los registros o movimientos que se efectúan en el día por cada Agente Certificador y mantenerlos bajo resguardo.

Décima novena.- La AC deberá hacer del conocimiento del solicitante los siguientes términos y condiciones, los cuales deben estar impresos en el formato de solicitud, mismos que deben ser firmados de forma autógrafa por el solicitante:

Términos:

- El suscrito, cuyos datos generales aparecen al anverso de la solicitud de Certificado Digital de Firma Electrónica Avanzada, y a quien en lo sucesivo se le denominará como "El Solicitante" para todos los efectos legales que deriven del presente documento a que haya lugar, manifiesta ante <poner aquí el nombre de la AC>, a quien en lo sucesivo se le denominará como "La Autoridad Certificadora" (AC), que es su libre voluntad contar con un Certificado Digital de Firma Electrónica Avanzada en el que conste la clave pública que se encuentra asociada a la clave privada y frase de seguridad que manifiesta haber generado previamente y en absoluto secreto, sin que persona alguna lo haya asistido durante dicho proceso.
- Asimismo manifiesta su conformidad en que "La AC" utilice el procedimiento de certificación de identidad que establece el Procedimiento Técnico de Captura de Información, publicado en el Diario Oficial de la Federación.

- “La AC” manifiesta que los datos personales recabados de “El Solicitante” durante su comparecencia serán protegidos, incorporados y tratados en el sistema <poner aquí el nombre del sistema de enrolamiento>, con fundamento en <poner aquí fundamento legal vigente>, y cuya finalidad es garantizar el vínculo que existe entre un Certificado Digital de Firma Electrónica Avanzada y su titular, el cual fue registrado en el “Listado de Sistemas de Datos Personales” ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales ifai.org.mx, y serán transmitidos al Registro Nacional de Población, para la conformación del “Sistema Integral del Registro Nacional de Población”.
- La Unidad Administrativa responsable de este sistema es <poner nombre aquí>. “El Solicitante” podrá ejercer los derechos de acceso y corrección de datos a través de <poner aquí el mecanismo o ubicación del inmueble en donde se pueden ejercer estos derechos>. Lo anterior se informa en cumplimiento del DECIMOSÉPTIMO de los “Lineamientos de Protección de Datos Personales”, publicados en el Diario Oficial de la Federación el 30 de septiembre de 2005.
- “El Solicitante” reconoce que para la emisión del referido Certificado Digital de Firma Electrónica Avanzada, “La AC” revisó la documentación que se indica en el anverso de este documento, con la cual “El Solicitante” se identificó, constatando a simple vista que los documentos corresponden a los rasgos fisonómicos y caligráficos de “El Solicitante”, por lo que este último asume la responsabilidad exclusiva respecto de la autenticidad de los datos y documentación por él proporcionada a “La AC”. De la misma forma “El Solicitante” asume la responsabilidad exclusiva del debido uso del Certificado Digital de Firma Electrónica Avanzada.
- “El Solicitante” en este acto acepta el Certificado Digital mencionado, sirviendo este documento como el acuse de recibo.
- Adicionalmente, “El Solicitante” acepta que el uso de la clave privada y frase de seguridad con base en las cuales dicho certificado fue elaborado, quedarán bajo su estricta y absoluta responsabilidad, la cual incluye en forma enunciativa, los daños y perjuicios, incluso aquéllos de carácter financiero, que pudieran causarse por su uso indebido, no pudiendo alegar que tal uso se realizó por persona no autorizada.
- “El Solicitante” conoce y acepta que la clave pública proporcionada por él y contenida en el Certificado Digital de Firma Electrónica Avanzada, así como en cualquier otro certificado digital que con posterioridad se obtenga, será de carácter público y podrá ser consultada libremente por cualquier interesado a través de los medios y formas que disponga “La AC”.
- Por lo anterior, “El Solicitante” se obliga a mantener absoluta confidencialidad respecto de las aludidas clave privada y frase de seguridad, así como a realizar los trámites necesarios para la revocación de dicho certificado ante “La AC”, mediante los mecanismos y procedimientos que el mismo establezca, en el evento de que por cualquier causa dicha información sea divulgada o se realice cualquier supuesto por el que “El Solicitante” deba solicitar su cancelación en los términos de las disposiciones jurídicas aplicables.
- Por otra parte “El Solicitante” manifiesta conocer el contenido y alcance de las disposiciones jurídicas relativas a la celebración de actos jurídicos mediante el uso de medios electrónicos, digitales o de cualquier otra tecnología, por lo que asume plena responsabilidad respecto de la información y contenido de todo documento electrónico o digital elaborado y enviado en el que se haga uso de la citada clave privada, toda vez que por ese solo hecho se considerará que el documento electrónico o digital le es atribuible.
- “El Solicitante” reconoce y acepta que “La AC” únicamente es responsable de los errores que, en su caso, llegaren a cometer bajo su responsabilidad en el proceso de generación, registro, entrega y revocación del Certificado Digital, según corresponda, así como que no será responsable por los daños y perjuicios que se pudieran causar a “El Solicitante” o a terceros, cuando por caso fortuito o fuerza mayor no puedan realizarse registros, verificaciones, revocaciones o tramitar documentos electrónicos cifrados con las claves públicas y privadas relacionadas con dicho certificado. Para efectos de lo anterior por caso fortuito o fuerza mayor se entenderá todo acontecimiento o circunstancia inevitable, más allá del control razonable de “La AC”, que le impida el cumplimiento de sus funciones con el carácter que le corresponde.
- “El Solicitante” reconoce a través de su firma autógrafa asentada en el espacio designado para ello en el anverso y reverso de este formato, al presente como prueba fehaciente de la aceptación de todo lo especificado en el mismo.

Condiciones:

- El Certificado Digital que se genere derivado de la realización de este trámite, estará disponible en <poner aquí dirección electrónica>; para que “El Solicitante” realice la descarga del mismo.
- La Firma Electrónica Avanzada asignada es personal e intransferible y el uso de la misma es responsabilidad de “El Solicitante”.
- La Firma Electrónica Avanzada tendrá los mismos alcances y efectos que la firma autógrafa.
- Con esta firma podrá hacer uso de servicios y trámites electrónicos disponibles en los cuales se reconozca el Certificado Digital de Firma Electrónica Avanzada.
- “El Solicitante” será responsable de las obligaciones derivadas del uso de su firma.
- “El Solicitante” acepta que deberá notificar oportunamente a “La AC”, la invalidación, pérdida o cualquier otra situación que pudiera implicar la reproducción o uso indebido de su clave privada.
- “El Solicitante” acepta las condiciones de operación y límites de responsabilidad de <poner aquí el nombre de la AC> en su calidad de “La AC” que se encuentran disponibles en la dirección electrónica <poner aquí la dirección electrónica> para su consulta.

Actividades del procedimiento y su detalle

DETALLE DE LA ACTIVIDAD	Generación de la llave privada [*key] y archivo de requerimiento [*req] para la Firma Electrónica Avanzada
--------------------------------	--

Puesto / Rol Responsable	Tarea	Descripción de la tarea	Documentos involucrados
Usuario		<ol style="list-style-type: none"> 1. Accede a la página de la AC en Internet en la sección de Firma Electrónica Avanzada y procede a bajar la aplicación para generar el requerimiento [*req] y la llave privada [*key] en su equipo de cómputo. 2. Instala en su PC la aplicación que genera el *.req y *.key. 3. Ejecuta la aplicación de generación de archivos antes mencionados, y llena los datos requeridos, conforme es instruido en el aplicativo. 4. Respalda en una unidad de memoria extraíble USB o disco compacto [CD] el archivo *.req y lo integra a la documentación que presentará en la AC. 5. Acude a la AC presentando los documentos requeridos al Agente Certificador para realizar el trámite de emisión de Certificado Digital de Firma Electrónica Avanzada. <p>Requisitos</p> <ul style="list-style-type: none"> ↳ Identificación oficial. ↳ Acta de nacimiento. ↳ Solicitud de Certificado de Firma Electrónica Avanzada, firmada de forma autógrafa. ↳ Archivo de requerimiento [USB o CD]. 	
Agente Certificador		<ol style="list-style-type: none"> 6. Verifica que la documentación presentada esté completa y determina. <p>Sí está la documentación completa Continúa en la DT 8.</p> <p>No está la documentación completa Continúa en la DT 7.</p>	

		<p>7. Informa al Usuario de los faltantes. Devuelve documentación indicando que deberá hacer una nueva cita y traer los documentos que falten.</p> <p>Concluye procedimiento</p> <p>8. Procede a validar la información de la documentación presentada que acredita la identidad del solicitante.</p> <p>Si la información es consistente continúa en la DT10.</p> <p>En caso de identificar inconsistencias, continua en la DT9.</p>	
		<p>9. Informa al solicitante que no es posible llevar a cabo el trámite, por lo que será necesario que corrija las inconsistencias reportadas.</p> <p>Concluye el procedimiento.</p>	
		<p>10. Digitaliza la documentación con la que acredita la identidad del solicitante y la integra en un expediente electrónico.</p>	
		<p>11. Canaliza al área de toma de biométricos.</p>	
		<p>12. Realiza la toma de biométricos, los valida y en su caso los registra conforme al Procedimiento Técnico de Captura de Información y el Procedimiento Técnico de Intercambio de Información.</p>	
		<p>13. Registra los biométricos en el sistema y se procede a generar el Certificado Digital de Firma Electrónica Avanzada.</p>	
		<p>14. Se solicita al usuario registrar en el sistema su clave privada a fin de generar el Certificado Digital de Firma Electrónica Avanzada y el archivo llave.</p>	
		<p>15. Se emite el "Comprobante de Inscripción para la Firma Electrónica Avanzada" para que lo firme de forma autógrafa el solicitante.</p>	
Usuario		<p>16. Recibe y procede a firmar de recibido en los dos tantos del "Comprobante de Inscripción para la Firma Electrónica Avanzada" y devuelve.</p>	
Agente Certificador		<p>17. La AC recibe y acusa de recibo con sello en los dos tantos del formato de "Solicitud de Certificado de Firma Electrónica Avanzada". La AC entrega un tanto de este al Usuario junto con un tanto del "Comprobante de Inscripción para la Firma Electrónica Avanzada", los originales de su documentación y el dispositivo externo con su archivo *.cer.</p>	
		<p>18. Anexa la documentación al o expediente del Usuario la nueva documentación recibida.</p> <p>Fin del Procedimiento</p>	

FORMATOS E INSTRUCTIVOS DE LLENADO

**Procedimiento de Revocación de Certificados Digitales de Firma Electrónica Avanzada
ANEXO 2**

Objetivo

Dotar a las Autoridades Certificadoras (AC) de políticas y procedimientos a través de los cuales ejerzan sus facultades, así como promover la estandarización de su operación a nivel nacional, con la finalidad de brindar un servicio eficaz, eficiente y de calidad.

Alcance

El presente procedimiento es de aplicación para los Agentes Certificadores de las AC.

Políticas de Operación

Primera.- La revocación de los Certificados Digitales de Firma Electrónica Avanzada se podrá realizar en la oficina de la AC.

Segunda.- El Agente Certificador deberá acreditar la identidad del solicitante, a través de la validación de las huellas dactilares.

Se deberá corroborar con el solicitante o representante legal, según sea el caso los datos de: RFC, CURP y nombre.

Tercera.- El Agente Certificador tendrá la responsabilidad de integrar al expediente electrónico correspondiente para la generación de la Firma Electrónica Avanzada, la documentación que respalda el trámite de revocación.

Cuarta.- Para efectos de lo dispuesto en el artículo 19 de la Ley de Firma Electrónica Avanzada, los motivos para la revocación de certificados digitales serán:

1. Extravío de la llave privada u olvido de la contraseña de acceso a la llave privada.
2. Cambio de nombre.
3. Cambio de Clave Única de Registro de Población.
4. Cambio de clave de Registro Federal de Contribuyentes.
5. Por suposición que su contraseña y/o llaves privadas fueron comprometidas.
6. Por haberse modificado la situación jurídica del solicitante

Quinta.- El Agente Certificador deberá requerir el escrito libre de solicitud de revocación, mismo que especificará la causa por la cual se solicita la revocación del Certificado Digital. El Agente Certificador procederá conforme a lo siguiente:

1. Se cotejará la siguiente documentación:
 - a. Original o copia certificada de la identificación oficial del solicitante.

Sexta.- El Agente Certificador orientará al solicitante para que revoque su certificado utilizando el portal de Internet de la AC.

Actividades del procedimiento y su detalle

DETALLE DE LA ACTIVIDAD	Revocación de Certificados Digitales de Firma Electrónica Avanzada	
--------------------------------	--	--

Puesto / Rol Responsable	Tarea	Descripción de la tarea	Documentos involucrados
Usuario		1. Acude a la oficina de la AC a presentar escrito de solicitud de revocación de certificados.	Escrito libre
Agente Certificador		2. Verifica que se presente la siguiente documentación: <ul style="list-style-type: none"> ⊕ Escrito libre con la solicitud de revocación. ⊕ Original o copia certificada de la identificación oficial del solicitante. 	Escrito libre Identificación oficial del solicitante
Agente Certificador		3. <i>Acredita la identidad del solicitante a través de la validación de las huellas dactilares.</i>	
Usuario		4. Accede al sistema de revocación provisto por la AC, captura número de serie del certificado a revocar y RFC y procede a revocar.	
		5. Imprime comprobante y entrega al Solicitante los dos tantos y solicita firme acuse de recibo.	Comprobante de revocación de certificado
		6. Recibe, firma acuse de recibo y devuelve.	Comprobante de revocación de certificado
Agente Certificador		7. Entrega al solicitante copia del escrito libre, el comprobante de revocación de certificado junto con el original de la identificación oficial.	Escrito libre Identificación oficial Comprobante de revocación de certificado
		8. Digitaliza la información correspondiente a la revocación y la integra al expediente electrónico del solicitante.	
		9. Integra al original del escrito libre el comprobante de revocación e integra al expediente físico.	
		Fin del Procedimiento	

FORMATOS E INSTRUCTIVOS DE LLENADO

ESCRITO LIBRE

UBICACIÓN (CIUDAD) a ____ de _____ AÑO.

AUTORIDAD CERTIFICADORA XXXXX

**ASUNTO: Revocación del Certificado Digital
de Firma Electrónica Avanzada**

Quien suscribe C. _____ con clave de R.F.C _____, y domicilio fiscal ubicado en: _____ y correo electrónico: _____

Por medio del presente y en apego al xxxxxxxxxxxxxxx solicito a esta autoridad realice la revocación del Certificado Digital de Firma Electrónica Avanzada con número de serie 00001000000 _____ por motivo de _____.

Sin más por el momento y agradeciendo su atención,

ATENTAMENTE

C.

NOMBRE DEL SOLICITANTE

**Procedimiento de Renovación de Certificados Digitales de Firma Electrónica Avanzada
ANEXO 3**

Objetivo

Dotar a las AC de políticas y procedimientos a través de los cuales ejerzan sus facultades, así como promover la estandarización de su operación a nivel nacional, con la finalidad de brindar un servicio eficaz, eficiente y de calidad.

Alcance

El presente procedimiento es de aplicación para los Agentes Certificadores de las Autoridades Certificadoras (AC).

Políticas de operación.

Primera.- La renovación de los certificados digitales se podrá realizar en la oficina de la AC.

Segunda.- El Agente Certificador deberá acreditar la identidad del solicitante, a través de la validación de las huellas dactilares.

Se deberá corroborar con el solicitante, según sea el caso los datos de: RFC, CURP y, nombre.

Tercera.- El Agente Certificador tendrá la responsabilidad de integrar al expediente electrónico correspondiente para la generación de la Firma Electrónica Avanzada, la documentación que respalda el trámite de renovación.

Cuarta.- Los motivos para la renovación de certificados digitales serán:

1. Cuando el certificado de Firma Electrónica Avanzada no está vigente.
2. Cuando la fecha de vencimiento del certificado esta próxima.

Quinta.- El Agente Certificador genera la solicitud de renovación.

Sexta.- El Agente Certificador orientará al solicitante para que renueve su certificado utilizando el portal de Internet de la AC.

Actividades del procedimiento y su detalle

DETALLE DE LA ACTIVIDAD	Renovación de Certificados Digitales de Firma electrónica Avanzada vía AC
--------------------------------	---

Puesto / Rol Responsable	Tarea	Descripción de la tarea	Documentos involucrados
Usuario		1. Acude a la AC presentando los documentos requeridos para realizar el trámite de renovación del Certificado Digital de Firma Electrónica Avanzada. Requisitos de renovación: ↳ Original o copia certificada de la identificación oficial del solicitante. ↳ Archivo de requerimiento (dispositivo o mecanismo de almacenamiento). ↳ Correo electrónico.	Identificación oficial Archivo *.req

Agente Certificador		<p>2. Verifica que la documentación esté correcta.</p> <p>3. Corroborar con el solicitante los datos de: RFC, CURP, nombre y domicilio desplegados en pantalla, también verifica que el apartado <Biométricos> señale la opción <Sí>.</p> <p>4. Acredita la identidad del solicitante, a través de la validación de las huellas dactilares.</p> <p>5. Genera e imprime en dos tantos la "solicitud de renovación" y recaba firma del solicitante.</p> <p>6. Genera y almacena el Certificado Digital de Firma Electrónica Avanzada en el dispositivo o mecanismo de almacenamiento.</p> <p>7. Imprime en dos tantos el Comprobante de Inscripción para la Firma Electrónica Avanzada y recaba firma del solicitante. Extrae dispositivo o mecanismo de almacenamiento.</p>	<p>Solicitud de renovación</p> <p>Comprobante de Inscripción para la Firma Electrónica Avanzada</p>
Usuario		<p>8. Recibe y firma de recibido en los dos tantos de la "Solicitud de renovación" y del 'Comprobante de Inscripción para la Firma Electrónica Avanzada' y devuelve.</p>	<p>Comprobante de Inscripción para la Firma Electrónica Avanzada</p>
Agente Certificador		<p>9. Recibe y acusa de recibo con sello de la AC en los dos tantos del formato de 'Solicitud de renovación, entrega un tanto de éste al solicitante junto con un tanto del 'Comprobante de Inscripción para la Firma Electrónica Avanzada' y los originales de su documentación y su dispositivo o mecanismo de almacenamiento con su Certificado Digital de Firma Electrónica Avanzada.</p> <p>10. Anexa la documentación digitalizada al expediente electrónico e integra lo correspondiente al expediente físico del solicitante la nueva documentación recibida.</p> <p>Fin del Procedimiento</p>	<p>Comprobante de Inscripción</p>

FORMATOS E INSTRUCTIVOS DE LLENADO

Comprobante de inscripción para la Firma Electrónica Avanzada

Autoridad Certificadora

Autoridad Certificadora _____

COMPROBANTE DE INSCRIPCIÓN PARA LA FIRMA ELECTRÓNICA AVANZADA

NÚMERO DE OPERACIÓN: 041100000282

Autoridad Certificadora _____ CERTIFICA QUE EL USUARIO : ANA GONZALEZ MARTINEZ

CON RFC: GOM700101884, ENTREGÓ UN ARCHIVO DE REQUERIMIENTO QUE CONTIENE LA SOLICITUD PARA LA GENERACIÓN DE SU CERTIFICADO DE FIRMA ELECTRÓNICA AVANZADA.

LLEVÓ A CABO SU ACREDITACIÓN DE IDENTIDAD, DE CONFORMIDAD CON LFEA

ASIMISMO, QUE COMO RESULTADO DEL PROCESO SE LE HACE ENTREGA DE UN ARCHIVO QUE CONTIENE SU CERTIFICADO DIGITAL CON LLAVE PÚBLICA:

21 11 15 12 11 11 11 02 07 06 12 25 72 02 77 02 11 00 12 74 31 51 21 12 31 24 06 15 01 01 12 02 01 12 02 06 16 10 26 16
01 25 12 15 21 21 22 01 24 11 24 27 00 10 01 16 20 11 27 01 32 32 17 26 32 10 17 20 21 24 02 14 26 02 22 24 20 21 72 12
20 22 12 10 26 22 26 11 73 21 22 11 22 11 11 11 07 07 02 02 01 02 15 11 21 21 10 21 01 01 22 01 21 22 26 27 21 10 17 03 12
02 24 22 12 01 04 26 14 25 11 22 11 10 26 12 12 12 11 11 11

FIRMA DE CONFORMIDAD
NOMBRE: ANA GONZALEZ MARTINEZ
RFC: GOM700101884

AUTORIDAD CERTIFICADORA A 10 DE NOVIEMBRE DE 2012

NOTA: PARA DESCARGAR POSTERIORMENTE SU CERTIFICADO DIGITAL, SI ASI LO REQUIERE, DEBERÁ ACCEDER A LA PAGINA DE INTERNET DE ESTA AUTORIDAD CERTIFICADORA

EL RESGUARDO DE LOS ARCHIVOS DE LA CLAVE PRIVADA Y DEL CERTIFICADO DIGITAL GENERADO, ASI COMO LA SELECCIÓN DEL MEDIO DE ALMACENAMIENTO DE LOS MISMOS, ES RESPONSABILIDAD DE LA PERSONA TITULAR DE LA FIRMA ELECTRÓNICA AVANZADA.

**Matriz de control de seguridad para autoridades certificadoras
ANEXO 4**

Matriz de Controles para la Revisión de Seguridad para AC						
Nota: La presente matriz estará vigente a partir de XXXXXX						
Área de Control	Sub-área de Control	ID Control	Control	Interpretación del Control	Periodicidad / Parámetro Requerido	Entrega esperada
Área de control: Postura de la Autoridad Certificadora sobre la Seguridad de la Información						
	Entendimiento del negocio	1	Contexto del negocio en donde éste pretende alcanzar sus objetivos.	Parámetros internos y externos del ambiente AC, establecer el alcance y criterios de riesgos. Se espera un documento donde se identifique el contexto donde la AC se va a desenvolver, los factores que pueden afectar, los riesgos, factores de cambio.	Al inicio de solicitud.	Documento con la descripción del contexto de negocio.
		2	Requerimientos de negocio de los distintos participantes (internos y externos)	Requerimientos de negocio de los distintos participantes involucrados en el proceso de prestación de servicios. Ej. Gobierno, INAI Solicitante, Negocio. Se espera un documento en donde se especifique qué requerimientos existen para que el negocio pueda operar.	Al inicio de solicitud.	Documento y mapa de requerimientos.
		3	Definir alcance de los objetivos y procesos de negocio.	1. Proceso documentado del negocio. 2. Alcance detallado del proceso. 3. Objetivos, indicadores claves de cumplimiento y métricas. 4. Entradas y salidas del proceso. (Diagrama) 5. Roles, responsabilidades y competencias del personal que interviene en el proceso. 6. Recursos que intervienen en la ejecución del proceso. (organigrama) 7. Tareas que se ejecutan en el proceso. 8. Indicadores y métricas que demuestren que el proceso se realiza de forma eficiente. 9. Estándares, normas o buenas prácticas a las que está alineado el proceso. 10. Monitoreo y evaluación	Al inicio de solicitud, posteriormente actualizaciones cada que existan cambios en los procesos. Deben cumplir con COBIT, TOGAF o equivalente.	* Documento con el proceso de negocio. * Documento con objetivos, indicadores claves de cumplimiento y métricas. * Documento con Entradas y salidas del proceso. * Estándares, normas o buenas prácticas a las que está alineado el proceso. * Monitoreo y evaluación del proceso.

				del proceso.		
Liderazgo de la Alta Dirección	4	Liderazgo y compromiso	<p>1. Se deben tener objetivos y una política de seguridad de la información de alto nivel compatible con la estrategia de negocio corporativa dentro del alcance de los servicios del negocio.</p> <p>2. Asegurar que los requerimientos de la seguridad de la información están integrados a los procesos organizacionales relacionados con los servicios del negocio.</p> <p>3. Asegurar que se proporcionen los recursos requeridos para mantener la seguridad de la información del negocio.</p> <p>4. Comunicar en forma efectiva la importancia de mantener los niveles adecuados de seguridad de información y se conforme con todo lo solicitado por la Secretaría, con el apoyo técnico de la Secretaría de Economía y el Servicio de Administración Tributaria, en este rubro.</p> <p>5. Asegurar que los requerimientos de seguridad de la información alcancen sus objetivos.</p> <p>6. Dirigir y liderar los roles gerenciales para contribuir a la efectividad en el cumplimiento de los requerimientos de seguridad y la mejora continua de su gestión.</p>	<p>Al inicio de solicitud, posteriormente actualizaciones cada que existan cambios en las directivas y políticas de seguridad.</p> <p>Deben cumplir con ISO27000, Risk IT o equivalente.</p>	<p>* Documento con la incorporación de la estrategia de seguridad en la del negocio.</p> <p>* Documento con los recursos asignados.</p> <p>* Documento con el programa de seguridad de la información.</p> <p>* Documento de reporte de asignación y supervisión de avance del programa de seguridad de la información.</p>	
	5	Política de seguridad de la información	<p>La AC debe contar con un documento de Política de Seguridad de la Información autorizado, el cual debe estar publicado y disponible para el personal interno y terceros que colaboren con la AC.</p>	<p>Al inicio de solicitud, posteriormente actualizaciones cada que existan cambios en las directivas y políticas de seguridad.</p> <p>Deben cumplir con ISO27000, Risk IT o equivalente.</p>	<p>Debe de implementar un Sistema de Gestión de Seguridad de la Información (SGSI), protocolizado de conformidad a ISO27000 por lo menos.</p>	
	6	Políticas específicas de seguridad de la información	<p>1. Política de seguridad de la información. - Contiene los lineamientos generales de las políticas de información.</p> <p>2. Política de la organización de la seguridad de la información. Contiene los lineamientos bajo los cuales se rige la seguridad de la información.</p> <p>3. Política para seguridad de los recursos humanos. - Políticas relacionadas a la administración del recurso humano.</p> <p>4. Política de gestión de activos. - Políticas que definirán el proceso con lo cual se gestionarán los activos.</p> <p>5. Política de control de accesos. - Política que detalla el acceso a las</p>	<p>Al inicio de solicitud, posteriormente actualizaciones cada que existan cambios en las directivas y políticas de seguridad.</p> <p>Deben cumplir con ISO27000, Risk IT o equivalente.</p> <p>*Las políticas deberán ser revisadas por lo menos una vez al año.</p>	<p>Políticas alineadas a mejores prácticas. La Autoridad Certificadora debe contar con un documento de Política de Seguridad de la Información autorizado, debe estar publicada y disponible para el personal interno y terceros que colaboren con la empresa.</p> <p>Debe de implementar un Sistema de Gestión de Seguridad de la Información (SGSI), protocolizado de conformidad a ISO27000 por lo menos.</p>	

				diferentes instalaciones.		
				<p>6. Política de criptografía. - Política de uso de criptografía en aplicaciones y servicios.</p> <p>7. Política de seguridad física y ambiental. - Políticas que rigen la seguridad física y ambiental de las distintas instalaciones.</p> <p>8. Política de seguridad en las operaciones. - Políticas con las consideraciones de seguridad para las operaciones diarias.</p> <p>9. Política de seguridad en las comunicaciones. - Políticas que rigen las comunicaciones para los activos que participan en el proceso.</p> <p>10. Política para la adquisición, desarrollo y mantenimiento de sistemas. Las políticas que tienen impacto en la operación, los nuevos sistemas y su impacto en los mismos.</p> <p>11. Política de relaciones con los proveedores. Las políticas que rigen el trato con los proveedores así como las implicaciones de seguridad que se deben considerar.</p> <p>12. Política para la gestión de incidentes de seguridad de la información Política que regirá la gestión del incidente, desde que se presenta el mismo.</p> <p>13. Política para la gestión de los aspectos de seguridad de la información en la continuidad de negocio. Política con las consideraciones que se tomarán para el desarrollo del plan de continuidad del negocio (por sus siglas en inglés BCP, Bussiness Continuity Plan).</p> <p>14. Política para el cumplimiento. - Reglas que se van a tomar en cuenta para el seguimiento y cumplimiento de las normativas de la AC.</p> <p>'15. Política de uso de contraseñas. La AC debe contar con una política de uso de contraseñas, donde se especifique la responsabilidad de los usuarios en el uso de las mismas, caducidad y</p>		

				protección de las mismas.		
				<p>16. Política de equipo desatendido. La AC debe contar con una política de equipo desatendido, donde se especifiquen los requerimientos de seguridad para el equipo cuando el usuario no está presente.</p> <p>17. Política de escritorio limpio. La AC debe contar con una política de Escritorio limpio, donde se especifiquen los requerimientos de seguridad para los puestos de trabajo.</p> <p>18. Política de control de accesos. La AC debe tener una política y procedimientos formales de Control de Accesos que apliquen por lo menos a todos los activos que dan soporte al proceso de la AC, mismos que deben ser revisados y actualizados por lo menos cada 6 meses.</p>		
	Estructura organizacional	7	Roles, responsabilidades y autoridad con respecto a la seguridad de la información.	<p>Se debe de tener una carta responsiva firmada específica para el rol y responsabilidades de cada elemento que va a participar en la prestación del servicio.</p> <p>Debe de considerar por lo menos tipo de documento, área, fecha, nombre, puesto, descripción, texto que identifique a qué información accede, responsabilidades y obligaciones, marco de referencia normativo (interno y externo), firma y fecha de aceptación y conformidad.</p>	Deben cumplir con ISO27000, Risk IT o equivalente.	<p>* Documentos con las cartas responsivas de los participantes.</p> <p>* Organigrama</p> <p>* Roles dentro del organigrama.</p>
		8	Marco de trabajo seleccionado para la gestión de riesgos de seguridad de la información.	<p>Gestión de administración del riesgo:</p> <p>1.-Diseño o elección del marco de trabajo para administrar el riesgo.</p> <p>2.-Implementar la administración de riesgos.</p> <p>3.-Monitorear y revisar el marco de trabajo.</p> <p>4.-Mejora continua del marco de trabajo.</p> <p>Lo anterior es enunciativo</p>	Deben cumplir con ISO27000, Risk IT o equivalente.	Documento con el marco de trabajo.

				mas no limitativo.		
	Gestión de riesgos	9	Metodología para la gestión de riesgos	<p>1. Nivel de riesgo aceptable.</p> <p>2. Proceso de valoración de riesgos:</p> <p>2.1 Identificación de riesgos.</p> <p>2.2 Análisis de riesgos.</p> <p>2.3 Evaluación de riesgos.</p> <p>3. Proceso de tratamiento de riesgo:</p> <p>3.1 Selección de tipo de tratamiento con justificación.</p> <p>3.2 Declaración de aplicabilidad de los controles de seguridad de la información.</p> <p>3.2.1 Determinar la aplicación o no de los controles así como las razones para su aplicación o no aplicación.</p> <p>3.2.2 Determinar si el control está operando así como su efectividad. En caso contrario, mostrar su plan de despliegue correspondiente.</p> <p>3.3 Plan de implementación de controles.</p>	Deben cumplir con ISO27000, Risk IT o equivalente.	Documento con la metodología a seguir.
		10	Ejecución de los procesos de gestión de riesgos.	<p>1. Valoración del cálculo del nivel del riesgo.</p> <p>2. Trazabilidad de la gestión del riesgo.</p>	Deben cumplir con ISO27000, Risk IT o equivalente.	Documento con los resultados de la gestión de riesgo.
	Objetivos y competencias	11	Objetivos de seguridad de la información	<p>1. Deben estar alineados con la política de TIC.</p> <p>2. Deben de ser medibles.</p> <p>3. Deben de tomar en cuenta los requerimientos de seguridad de la información, resultados de análisis de riesgos propios y tratamientos de los riesgos.</p> <p>4. Deben de estar comunicados en la AC.</p> <p>5. Deben de estar actualizados.</p> <p>6. Deben incluir un Plan de trabajo para su cumplimiento</p> <p>6.1 ¿Qué es lo que se va a hacer?</p> <p>6.2 ¿Qué recursos son requeridos?</p> <p>6.3 ¿Quién va a ser responsable?</p> <p>6.4 ¿Cuándo se va a completar?</p> <p>6.5 ¿Cómo se van a evaluar los resultados?</p> <p>Los numerales son</p>	Deben cumplir con ISO27000, Risk IT o equivalente.	Documento y plan de trabajo con los objetivos de la seguridad de la información.

				enunciativos mas no limitativos.		
		12	Competencias	<p>1. Las personas que participan en los servicios del negocio o son encargados de la seguridad de la información deberán tener la competencia requerida para desempeñar sus funciones. (Con base a su experiencia, educación y/o entrenamiento adecuado)</p> <p>2. Plan de capacitación o entrenamiento para alcanzar o retener las competencias requeridas para desempeñar las funciones.</p>	Deben cumplir con ISO27000, Risk IT o equivalente. Presentar currículos acompañados de las certificaciones respaldo de las competencias en Seguridad de la Información.	Documento con las competencias por rol y plan de capacitación.
	Comunicación	13	Gestión de comunicación de seguridad de la información con entidades internas y externas.	<p>La AC debe de determinar las necesidades de comunicación interna y externa relevante para la administración del sistema de seguridad de la información en la cual se debe de incluir lo siguiente:</p> <p>1. ¿Qué es lo que se debe de comunicar?</p> <p>2. ¿Cuándo se debe de comunicar?</p> <p>3. ¿A quién se le debe de comunicar?</p> <p>4. ¿Quién lo debe de comunicar?</p> <p>5. Los procesos que pueden ser afectados por la comunicación.</p>	Deben cumplir con ISO27000, Risk IT o equivalente.	Documento que detalle la gestión de comunicación.
		14	Concientización	<p>El personal que este participando debe de tener conocimiento de:</p> <p>1. La política de seguridad de la información.</p> <p>2. Su participación para la efectividad de la seguridad de la información y sus beneficios.</p> <p>3. Las implicaciones de no cumplir con los requerimientos de la seguridad de la información.</p> <p>4. Las sanciones internas a las que se harían acreedores en caso de no cumplir con alguna de las políticas de seguridad de la información.</p> <p>Los puntos son enunciativos mas no limitativos.</p>	Deben cumplir con ISO27000, Risk IT o equivalente.	Plan de concientización. Listados de asistencia con fecha y firma.
Área de control: Operación de la Seguridad de la Información en la AC						
	Operación de la seguridad	15	Operación	Planear, implementar y controlar los requerimientos y objetivos de seguridad de información. Debe de considerar el control de cambios, así como plan de	Deben cumplir con ISO27000, 31000, Risk IT o equivalente.	Plan operativo de seguridad de la información, controles de cambio, controles de seguridad de la

				acción para mitigar cualquier efecto adverso.		información.
Área de control: Evaluación del rendimiento de la Seguridad de la Información en la AC						
	Monitoreo y auditoría	16	Monitoreo, medición, análisis y evaluación.	<p>La AC deberá evaluar si el desempeño y efectividad de su servicio y la seguridad se encuentran acorde a sus políticas y procesos:</p> <ol style="list-style-type: none"> 1. Determinar qué se debe de monitorear y medir. 2. Determinar qué métodos se van a utilizar para monitorear, medir, analizar y evaluar. 3. Determinar cuándo se deben de monitorear y medir. 4. Determinar quién debe de monitorear y medir. 5. Determinar cuándo se revisarán los resultados de monitoreo. 6. Quién deberá realizar el análisis y evaluación de estos resultados. 7. Quién detonará y dará seguimiento a las acciones correctivas. <p>* Se debe de considerar el servicio ofrecido al solicitante y su operación interna.</p>	Deben cumplir con ISO27000, Risk IT o equivalente.	Documento de gestión de monitoreo, reportes de operación y atención a desviaciones.
		17	Auditorías realizadas mediante personal autorizado y seguimiento	<p>La AC debe realizar auditorías internas por personal interno o externo con las credenciales adecuadas para la revisión de los controles, los auditores deberán tener independencia operativa.</p> <p>La auditoría evaluará el cumplimiento de los objetivos o requerimientos de seguridad de la información que se hayan trazado, lo efectivo y eficaz que hayan implementado los controles de seguridad de la información para gestionar los riesgos.</p> <p>Se deberá revisar el cumplimiento de la matriz presente.</p> <p>Se deberá planear, establecer e implementar un plan de auditoría, que incluya frecuencia, seguimiento del resultado de</p>	1 vez al año como mínimo.	Reporte de auditoría.

				las auditorías y responsable de las actividades.		
Clasificación de la Información		18	Acuerdos de Confidencialidad	La AC debe tener acuerdos de confidencialidad y/o acuerdos de no divulgación de información, firmados con su personal interno y externo, y deben ser revisados de manera periódica. Es importante que la responsabilidad del personal que firma se encuentre vigente durante el desempeño de sus actividades, en caso de que deje de laborar en la empresa considerar un periodo posterior en el cual tenga efecto.	Deben cumplir con ISO27000, Risk IT o equivalente.	* Acuerdos de confidencialidad. * Acuerdos de no divulgación.
		19	Contacto con las Autoridades	La AC debe contar con procedimientos formales para mantener contacto y permitir investigaciones por parte de las autoridades. Ej. Protección civil, el SAT, seguridad pública.	Cumplir con el proceso ASI del MAAGTICSI.	Documento con información como Nombres, teléfonos, correos electrónicos, teléfonos de emergencia de las autoridades relevantes.
		20	Contacto con Grupos de Interés Especial	La AC debe estar en contacto con grupos especializados en seguridad y/o asociaciones profesionales.	Cumplir con el proceso ASI del MAAGTICSI.	Certificaciones, constancias de asistencia a cursos de seguridad, suscripciones con autoridades en seguridad como en NIST, SANS, ENISA, ISO, CERT's, etc.
		21	Política de Clasificación de la Información	La AC debe contar con una política y procedimientos formales para la clasificación de la información de acuerdo a su relevancia o sensibilidad.	Como mínimo se deberá considerar lo establecido en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y el artículo 69 del Código Fiscal de la Federación.	Política con clasificación de la información en: pública, reservada y confidencial.
		22	Etiquetado y Manejo de la Información	La AC debe contar con procedimientos formales para etiquetar y manejar la información tanto en formato electrónico como en formatos físicos de acuerdo a su clasificación.	Debe cumplir con ITIL.	Política de etiquetado, manejo y resguardo de la información de acuerdo a su clasificación.
Seguridad en el Personal						
Personal Interno		23	Selección del Personal	Se debe llevar a cabo la verificación de antecedentes de todos los candidatos a puestos internos de la AC.	Cada que se contrata personal nuevo.	Cartas de antecedentes no penales de los empleados. Certificaciones correspondientes al perfil y rol del puesto. El personal deberá aprobar un examen de control de confianza, para todas las áreas: administrativas, técnicas

						y operativas, debiendo realizarlo al menos cada 2 años.
	Terminación del Empleo	24	Eliminación de Derechos de Acceso	La AC debe contar con procedimientos para llevar a cabo la eliminación de accesos lógicos y físicos al personal interno o externo que ya no labore en la empresa.	Deben cumplir con ISO27000, ISO31000, Risk IT o equivalente.	Política y procedimientos para la eliminación de accesos lógicos y físicos al personal interno o externo que ya no labore en la empresa.
		25	Devolución de Activos	La AC debe contar con un procedimiento para la devolución de los activos que el personal tuvo asignado mientras laboraba para la AC. Proceso de sanitización de la información en los equipos.	Deben cumplir con ISO27000, ISO31000, Risk IT o equivalente.	Política y procedimientos para la devolución de activos.
		26	Responsabilidades del personal dado de baja	Se deben revisar los contratos, cláusulas y acuerdos de confidencialidad para garantizar que el personal dado de baja conserva sus obligaciones con respecto a la confidencialidad de la información a la que tuvo acceso durante su estancia en la AC.	Deben cumplir con ISO27000, ISO31000, Risk IT o equivalente.	Contrato laboral y acuerdos de confidencialidad.
Gestión de los Activos						
	Gestión de los Activos	27	Inventario de Activos	Todos los activos deben estar claramente identificados. Se debe elaborar y mantener un inventario actualizado de todos los activos de la AC.	Debe cumplir con ITIL.	* Políticas y procedimientos de gestión de activos. *CMDB. * Inventario de Activos.
		28	Propiedad de los activos	Toda la información y los activos asociados con los medios de procesamiento de la información deben ser 'propiedad' (responsabilidad) de una parte designada de la AC.	Debe cumplir con ITIL.	Políticas y procedimientos de manejo de activos.
		29	Uso aceptable de activos	La AC debe contar con una política y procedimientos para identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados.	Debe cumplir con ITIL.	Políticas y procedimientos de manejo de activos.
Seguridad Física en Oficinas						
	Seguridad Física	30	Perímetro de Seguridad Física	Se deben utilizar perímetros de seguridad (barreras tales como paredes y puertas de ingreso controlado, policías o receptionistas) para proteger áreas operativas y de oficina que contienen información de la AC.	Deben cumplir con ISO27000, ISO31000, Risk IT o equivalente.	* CCTV. * Custodia de las oficinas. * Bitácora de acceso.
		31	Controles de Entrada	Se deben proteger las áreas seguras mediante controles de entrada apropiados para	Deben cumplir con ISO27000, ISO31000, Risk IT o	Política y bitácoras de acceso a las instalaciones.

				asegurar que sólo se permita acceso al personal autorizado.	equivalente.	
Procesos de Gestión de la Seguridad						
	Manejo de Incidentes y Problemas	32	Incidentes y Problemas	La AC debe contar con una política y procedimientos para la Gestión de Incidentes de Seguridad, que maneje como mínimo: <ul style="list-style-type: none"> - Identificación de Incidentes y Problemas. - Registro de Incidentes y Problemas (indicando tipo, clasificación, diagnóstico). - Notificación y Escalamiento de Incidentes y Problemas. - Seguimiento y solución de Incidentes y Problemas. 	Deben cumplir con ISO27000, ISO31000, Risk IT o equivalente.	<ul style="list-style-type: none"> * Proceso de gestión de incidentes. * Matriz de escalamiento de incidentes y problemas. * SLA vigentes. * Incidentes de seguridad, su clasificación, seguimiento, responsables y fechas compromiso de solución.
		33	Notificación a la Secretaría, o en su caso, a la SE o al SAT	La AC debe contar con procedimientos de notificación a la Secretaría, o en su caso, a la SE o al SAT, en caso de Incidentes o problemas que puedan comprometer la información de los ciudadanos.	Deben cumplir con ISO27000, ISO31000, Risk IT o equivalente.	<ul style="list-style-type: none"> * Procedimientos de notificación en caso de Incidentes. * Matriz de escalamiento de incidentes. * Directorio telefónico de contactos de la AC. * Directorio telefónico de contactos.
	Monitoreo de Seguridad	34	Definición de Eventos de Seguridad	La AC debe definir aquellos eventos de seguridad que van a monitorear, de acuerdo a su análisis de riesgos, en los cuales deben considerar como mínimo: <ul style="list-style-type: none"> - Uso de cuentas privilegiadas. - Acceso a información con clasificación alta de confidencialidad. - Comportamiento anormal de los equipos. 	Deben cumplir con ISO27000, ISO31000, Risk IT o equivalente.	<ul style="list-style-type: none"> * Proceso de respuesta a incidentes donde exista una definición clara de lo que es un incidente de seguridad y cómo se debe de tratar y escalar. * Matriz de escalamiento.
	BCP	35	Plan de Continuidad del Negocio	La AC debe contar con un BCP documentado y aprobado. El BCP debe incluir el proceso de AC, incluyendo como mínimo: <ul style="list-style-type: none"> Identificación de los activos que le dan soporte al proceso. Requerimientos de procesamiento, personal, información y todo lo necesario para garantizar la continuidad del servicio de la AC. 	Deben cumplir con ISO27031 e ISO22301.	BCP derivado de un BIA.

		36	Pruebas de BCP	La AC debe contar con un plan de ejecución de pruebas del BCP por lo menos cada 12 meses.	12 meses.	Reporte anual de los resultados de las pruebas al BCP.
	Gestión de la Capacidad	37	Capacidad Tecnológica	Se debe planear, monitorear, y ajustar el uso de recursos tecnológicos (software, equipos, comunicaciones, etc.) para asegurar el desempeño requerido por los sistemas que dan soporte al proceso de AC, por lo menos durante 12 meses. Se debe dar cumplimiento a las medidas necesarias identificadas durante la planeación y monitoreo.	12 meses.	Plan anualizado de gestión de la capacidad tecnológica.
		38	Capacidad Operativa	Se debe planear, monitorear, y ajustar el uso de recursos operativos (personal, herramientas, espacios) para asegurar el desempeño requerido por los sistemas que dan soporte al proceso de AC, por lo menos durante 12 meses. Se debe dar cumplimiento a las medidas necesarias identificadas durante la planeación y monitoreo.	12 meses.	Plan anualizado de gestión de la capacidad operativa.
Seguridad de la Plataforma Tecnológica						
	DRP	39	Plan de Recuperación de Desastres	La AC debe contar con un plan de recuperación de desastres para su centro de datos que incluya por lo menos los activos necesarios para el funcionamiento del proceso de AC.	12 meses, cumpliendo con ISO24762.	DRP derivado de un BIA.
		40	Pruebas del DRP	La empresa debe contar con un plan de pruebas del DRP.	Anual, cumpliendo con ISO24762.	Reporte anual de los resultados de las pruebas al DRP.
	Manejo de Certificados	41	Manejo de Certificados	La AC debe de contar con un proceso formal de manejo de certificados que cubra como mínimo los siguiente puntos: 1.- Proceso de identificación y autenticación de la entidad solicitante del servicio de certificación PKI. 2.- Proceso de Registro y enrolamiento. 3.- Proceso de Generación (definición técnica de algoritmos y tamaño de las llaves acorde al marco regulatorio). 4.- Proceso de Emisión y entrega del documento digital. 5.- Proceso de Publicación de los documentos digitales. 6.- Proceso de Renovación de los documentos digitales. 7.- Proceso de Suspensión de los documentos digitales. 8.- Proceso de Revocación de los documentos digitales. 9.- Proceso de Archivado y resguardo de los documentos digitales conforme a la norma NOM-151-SCFI-2002, Prácticas		

				comerciales-Requisitos que deben observarse para la conservación de mensajes de datos, o aquella que le sustituya.		
	Resguardo de Llaves digitales	42	Resguardo de Llaves digitales	<p>La AC debe de contar con un equipo específico con características de certificación FIPS_140-3 y documentación en donde se detalle la ejecución de al menos los siguientes procesos de seguridad:</p> <ol style="list-style-type: none"> 1.- Proceso inicio seguro y configuración inicial. 2.- Proceso de definición y configuración de dominios de seguridad. 3.- Proceso de inicialización de llave privada y generación del archivo *.req. 4.- Proceso de configuración de web service y/o integración del API del fabricante. 5.- Proceso de Respaldo del equipo. 6.- Proceso de configuración de alta disponibilidad del equipo. 7.- Proceso de Cambio de Llaves de acceso al equipo. 8.- Proceso de Destrucción de llaves del equipo. 9.- Proceso de revocación de llaves comprometidas. 		
	Manejo de Llaves	43	Manejo de Llaves	<p>La AC debe de contar con un proceso formal de manejo de certificados que cubra lo siguiente:</p> <ol style="list-style-type: none"> 1.- Proceso de Distribución. 2.- Proceso de Almacenamiento. 3.- Proceso de Uso. 4.- Proceso de Respaldo. 5.- Proceso de Cambio de Llaves. 6.- Proceso de Destrucción. 7.- Proceso de Llaves Comprometidas. 		
	Protocolo de verificación de estatus del certificado en línea (OCSP, por sus siglas en inglés, Online Certificate Status Protocol)	44	Servicio de OCSP	<p>La AC deberá de implementar el servicio de OCSP público para validación del estado de los Certificados Digitales de Firma Electrónica Avanzada.</p>	Debe cumplir RFC 6960.	Disponibilidad del servicio 99.999%
	Lista de certificados	45	Servicio de CRL	<p>La AC deberá de implementar el servicio de</p>	Debe cumplir RFC 5280.	Disponibilidad del servicio 99.999%,

	revocados (CRL, por sus siglas en inglés, Certificate Revocation List)			CRL público para validación de certificados revocados de firma electrónica avanzada		actualizado cada 12 horas al menos.
	Gestión de cuentas	46	Altas, Bajas y Cambios de Accesos de Usuarios	<p>La AC debe documentar procedimientos formales para las Altas, Bajas y Cambios de accesos de usuarios, que incluyan como mínimo:</p> <ul style="list-style-type: none"> - Bloqueo de las cuentas por intentos fallidos de autenticación. - Bloqueo de cuentas por periodo de inactividad. <p>Los accesos remotos sólo se deberán proporcionar bajo circunstancias de excepción y con un estricto proceso de autorizaciones y monitoreo.</p>	Deben cumplir con ISO27000 e ITIL o equivalente.	Procedimiento de gestión de cuentas.
		47	Gestión de Privilegios	<p>La AC debe contar con procedimientos formales para restringir y controlar la asignación y uso de los privilegios. Debe existir un catálogo con la descripción de privilegios y la asignación de los mismos.</p>	Deben cumplir con ISO27000 e ITIL o equivalente.	Procedimiento de gestión de cuentas con privilegios.
		48	Gestión de Contraseñas de Usuarios	<p>La AC debe contar con procedimientos formales de asignación de contraseñas, mismos que deben contar por lo menos con las siguientes reglas:</p> <ul style="list-style-type: none"> - Reglas para la creación de contraseñas (longitud mínima, histórico, caracteres permitidos, etc.). - Las contraseñas se deben encriptar en todos los activos que dan soporte al proceso de AC. 	Deben cumplir con ISO27000 e ITIL o equivalente.	Política de gestión y cifrado de contraseñas.
		49	Revisión de Permisos	<p>La AC debe realizar periódicamente (por lo menos cada 6 meses) una revisión de los usuarios existentes en los sistemas de información y activos, para verificar que sus permisos sigan siendo vigentes de acuerdo al procedimiento de altas o cambios de Accesos de Usuarios.</p>	6 meses.	Procedimiento de altas o cambios de accesos de usuarios.
	Seguridad Física	50	Ubicación del Centro de Datos	<p>El centro de datos debe estar asentado en lugares libres de altos riesgos, por lo menos a 100 m de lugares como gasolineras, gaseras, minas, acometidas de</p>	100 m	Plano de ubicación del centro de datos y sus colindancias.

				cableado de electricidad y gas, etc. y deberá estar dispuesta como una instalación no evidente.		
		51	Control de Accesos Físicos	<p>El centro de datos debe estar protegido por un perímetro de acceso físico controlado, controles de acceso automatizados y procedimientos formales de control de accesos.</p> <p>El personal que acceda al centro de datos no deberá introducir medios de almacenamiento extraíbles sin autorización.</p> <p>Las bitácoras de acceso deberán resguardarse en un lugar seguro.</p>	Deben cumplir con ISO27000 e ITIL o equivalente.	Autenticación para el acceso.
		52	Vigilancia y Monitoreo	<p>El centro de datos debe contar con personal de vigilancia las 24 horas y un sistema de monitoreo de las instalaciones (CCTV, etc.).</p> <p>El sistema de monitoreo debe almacenar los videos de vigilancia con historial de por lo menos 30 días y almacenarlos en un lugar seguro, fuera de las instalaciones principales.</p> <p>El personal debe estar debidamente capacitado y contar con las herramientas necesarias para responder en caso de emergencias.</p>	30 días.	Información respecto a la seguridad física con la que cuenta la AC, considerando los controles de seguridad tales como, CCTV, bardas perimetrales, sistemas de control de acceso y autenticación al área de servidores, control y gestión de exclusas, bitácoras del personal visitante al centro de datos.
		53	Señalización	<p>Las instalaciones deben contar con señalización que indique claramente:</p> <ul style="list-style-type: none"> - Áreas de acceso restringido. - Rutas de evacuación. - Ubicación del equipo de emergencia. 	Deben cumplir con ISO27000 e ITIL o equivalente.	Instructivo de señalización de las áreas.
	Controles Ambientales	54	Medidas contra Incendios	El centro de datos debe contar con medidas de protección contra incendios.	Contar con certificación TIER-IV o equivalente.	Información de sensores de humo, aspersores, sensor de humedad, extintores o cualquier otro mecanismo de medidas contra incendios.
		55	Aire Acondicionado	El centro de datos debe contar con un sistema de aire acondicionado.	Contar con certificación TIER-IV o equivalente.	Contrato del mantenimiento de los sistemas de aire acondicionado.

		56	Medidas contra Inundaciones	El centro de datos debe contar con medidas de protección contra inundaciones.	Contar con certificación TIER-IV o equivalente.	Contrato del mantenimiento de los sistemas de flujo de agua.
	Servicios de Soporte	57	Instalación Eléctrica	El centro de datos debe contar con medidas de seguridad en el cableado y medidas de respaldo de energía de emergencia. La infraestructura eléctrica debe revisarse por lo menos cada 6 meses para garantizar su buen funcionamiento.	Contar con certificación TIER-IV o equivalente.	Contrato del mantenimiento de: a) Generadores. b) UPS. c) Baterías de respaldo. d) Acometidas de energía. e) Cableado.
		58	Planes y Contratos de Mantenimiento	El centro de datos debe contar con planes de mantenimiento y contratos vigentes con proveedores de los medios y dispositivos de controles ambientales y servicios de soporte.	Contar con certificación TIER-IV o equivalente.	Contratos de Mantenimiento.
	Comunicaciones	59	Prevención y Detección de Intrusos	Las redes dentro del centro de datos deben contar con dispositivos de prevención o detección de Intrusos.	Deben cumplir con ISO27000 e ITIL o equivalente.	Configuración, reglas y estatus del IDS/IPS.
		60	Protección Perimetral	La red debe estar protegida con dispositivos de seguridad que apliquen listas de control de acceso.	Deben cumplir con ISO27000 e ITIL o equivalente.	* Configuración de las reglas o listas de control de acceso del FW. * Proceso de gestión del FW. * Control de acceso al FW.
		61	Segmentación de Redes	Las redes deben estar segmentadas para proteger el flujo de información en redes con distintos tipos de usuarios.	Deben cumplir con ISO27000 e ITIL o equivalente.	Controles de segregación de redes.
	Líneas Base de Seguridad (Endurecimiento y Actualización)	62	Líneas Base de Seguridad	El aplicativo debe tener aplicada una línea base de seguridad que debe incluir como mínimo: - Implementación de autenticación de los usuarios (internos o clientes). - Implementación de mecanismo de no repudio de transacciones. - Protección contra inyección de código. - Inicio de sesión seguro. - Validación de datos de entrada / salida para evitar errores en el procesamiento de la información. - Manejo de errores. - Endurecer el sistema. (Hardening) Los activos (aplicativos, servidores, bases de datos, dispositivos de red, etc.) del centro de datos que dan soporte al proceso de AC deben contar con líneas base de seguridad documentadas e implementadas, que consideren como mínimo: - Protección del BIOS en arranque de los sistemas. - Deshabilitación de unidades de almacenamiento removibles. - Instalación del S.O. en	Deben cumplir con ISO27000 e ITIL o equivalente.	Documento con configuración y línea base de seguridad del aplicativo, listado de activos, versión del sistema.

				partición exclusiva. - Inhabilitación de puertos, protocolos usuarios y servicios innecesarios. - Recomendaciones de seguridad del fabricante del equipo y sistema operativo.		
	Respaldos	63	Actualizaciones	Los activos que dan soporte al proceso de AC deben contar con los últimos parches de seguridad y actualizaciones emitidas por el fabricante de los servidores y sistemas operativos que hayan pasado por un procedimiento de pruebas previas a la implementación.	Deben cumplir con ISO27000 e ITIL o equivalente.	Políticas y procedimientos de control de cambios y control de pruebas para el despliegue de nuevos parches y/o actualizaciones.
		64	Respaldos	Se deben generar respaldos de los activos y la información que dan soporte al proceso de AC, con la periodicidad definida por la AC.	Periodicidad definida por la AC.	Política y procedimientos para la generación, etiquetado y resguardo de los respaldos.
		65	Etiquetado	Los medios donde se almacene información de los solicitantes y de la AC deberán estar inventariados y etiquetados con el nivel más alto de confidencialidad definido en el proceso de clasificación de información, y se deberá dar el tratamiento de acuerdo a la clasificación.		
		66	Pruebas de Respaldos	Se debe contar con un plan de pruebas de los respaldos para verificar que son funcionales.	Deben cumplir con ISO27000 e ITIL o equivalente.	* Plan de pruebas de respaldos. * Bitácora de respaldos.
		67	Protección de Medios de Respaldo	Los medios donde se almacenan los respaldos deberán estar protegidos en un área específica para este efecto, en un sitio alternativo, en medios encriptados y con medidas de protección contra el acceso no autorizado.	Deben cumplir con ISO27000 e ITIL o equivalente.	* Cifrado de los respaldos. * Responsables que cuenten con acceso a los respaldos. * Controles de seguridad física (caja fuerte).
		68	Destrucción o Borrado	Los medios donde se almacenen respaldos o información de los solicitantes o de la AC deberán estar sujetos a un procedimiento formal de destrucción o borrado seguro que debe contener como mínimo:	Deben cumplir con ISO27000, ISO31000, Risk IT o equivalente.	Acta de destrucción, ordenes de servicio de destrucción.

				<ul style="list-style-type: none"> - Solicitud y Autorización explícitas de la destrucción o borrado. - Actas de destrucción o borrado firmadas por el personal que lo realiza. 		
	Criptografía	69	Criptografía en servicios expuestos	Los servicios del aplicativo que se encuentren expuestos para el consumo por parte de los clientes, deberán contar con mecanismos de criptografía. Se deberá de utilizar un algoritmo de cifrado.	Deben cumplir con ISO27000, ISO31000, Risk IT o equivalente.	Documento en donde se especifique el método y la criptografía usada en caso de tener servicios expuestos.
		70	Protección de Llaves y Certificados	<p>Las llaves y Certificados usados para el cifrado deben estar protegidos por un dispositivo recubierto con algún material opaco y contar con salvaguardas que impidan que sea abierto o que invaliden la información en caso de que sea forzado, además de contar por lo menos con las siguientes medidas:</p> <ul style="list-style-type: none"> - Control de Accesos Físicos y Lógicos (Sólo personal autorizado). - Registro de Hashes de Control. - Segregación de roles con acceso a los dispositivos de almacenamiento de llaves y certificados. - Instalación única de la llave provista para la operación de la AC (respaldada por un acta firmada por los responsables de su instalación y custodia). - Contexto o partición exclusiva para el almacenamiento de los certificados. 	Implementación de HSM.	Características del HSM, registro de inserción, cambios a los certificados, documento de segregación de roles, bitácoras.
	Pruebas de Seguridad	71	Pruebas de Seguridad	Se deben realizar, documentar y dar seguimiento a pruebas de seguridad en los activos que dan soporte al proceso de AC al igual que al propio aplicativo de AC.	Deben cumplir con ISO27000, ISO31000, Risk IT o equivalente.	Plan de pruebas de seguridad, reportes de las pruebas de seguridad y hallazgos.
		72	Seguimiento a hallazgos de pruebas de Seguridad	Se debe realizar un plan para atender los hallazgos detectados durante las pruebas de seguridad y reportar a la Secretaría, en su caso a la SE o al SAT, en un lapso no mayor a 24 horas, el diagnóstico y la solución pertinente.	Deben cumplir con ISO27000, ISO31000, Risk IT o equivalente.	Plan de seguimiento a los hallazgos y control de cambios de los mismos.

	Protección Contra Código Malicioso	73	Protección contra Código Malicioso	Todos los activos tecnológicos que dan soporte al proceso de AC deberán contar con una solución de protección contra código malicioso instalada y actualizada.	Deben cumplir con ISO27000, ISO31000, Risk IT o equivalente.	IPS, IDS, antivirus, programas de protección.
	Separación de Ambientes	74	Separación de Ambientes	Los ambientes de desarrollo, pruebas y producción deben estar separados física o lógicamente unos de otros y todos deben tener su propia administración de accesos.	Deben cumplir con ISO27000 e ITIL o equivalente.	Diagrama de arquitectura de hardware.
		75	Aislamiento de información	La información del proceso de AC debe estar separada física o lógicamente de la información de otros procesos o aplicativos proporcionados por la AC.	Deben cumplir con ISO27000 e ITIL o equivalente.	Diagrama de arquitectura, listado de activos, arquitectura de software, diagrama de red y reglas de red.
	Seguridad en Aplicativo	76	Documentación	El aplicativo de AC debe contar con documentación técnica completa. La documentación técnica debe incluir como mínimo: - Flujo de Datos. - Modelo y Diccionario de Datos. - Diagrama de implementación.	Deben cumplir con ISO12207 y SCRUM o SEI-CMM.	Mapa del flujo de datos, modelo y diccionario de la base de datos.
		77	Control de Cambios	El aplicativo debe contar con un proceso formal de control de cambios, que debe incluir como mínimo: - Estimación de impacto de cambios. - Pruebas. - Autorización. - Liberación de cambios. - Reversos de cambios.	Deben cumplir con ISO12207 y SCRUM o SEI-CMM.	Documento con el proceso de control de cambios, evidencia de un control de cambios, bitácoras, aprobaciones.
		78	Bitácoras	El aplicativo debe contar con bitácoras de acceso y uso, que deben contener como mínimo: - Fecha y hora. - Usuario. - IP origen. - Folio. - Detalle de la actividad (RFC y detalle como mínimo). Se debe registrar lo siguiente en la bitácora: - Registro de intentos de acceso fallidos. - Registro de accesos exitosos. - Registro de cierre de sesión ya sea por inactividad o por parte del usuario. - Registro de consulta de las propias bitácoras. - Registro de errores y/o excepciones. - Registro de actividad de los usuarios: a) Registro de Altas, Bajas y cambios. b) Registro de impresiones. c) Registro de consultas a documentos. d) Registro de documentos. Lo anterior a nivel base de datos, aplicación y sistema operativo.	12 meses en sistema y 5 años en histórico.	Bitácoras, pantallas.

				Las bitácoras están enfocadas al personal administrativo de la aplicación o servicio.		
		79	Expiración de sesión por inactividad	El aplicativo debe contar con sesiones que expiren después de máximo 10 minutos de inactividad. El reingreso deberá de solicitar de nuevo las credenciales.	Máximo 10 minutos.	Pantalla.
	Acceso a base de datos	80	Procedimiento de acceso a la base de datos	Se debe de especificar un procedimiento por medio del cual la Secretaría, o en su caso la SE o el SAT, puedan tener acceso a las bases de datos de información de la AC.	Deben cumplir con ISO27000 e ITIL o equivalente.	Documento que contenga el proceso.
	Servidor de tiempo	81	NTP	Las transacciones de timbrado del proceso de AC deben estar sincronizadas usando un servidor de NTP con GPS.	Cumpliendo con (según aplique): RFC 5905: Network Time Protocol Version 4: Protocol and Algorithms Specification. RFC 5906: Network Time Protocol Version 4: Autokey Specification. RFC 5907: Definitions of Managed Objects for Network Time Protocol Version 4 (NTPv4). RFC 5908: Network Time Protocol (NTP) Server Option for DHCPv6.	Configuración y uso de servidor de tiempo.
	Encriptación de Datos	82	Encriptación de datos del solicitante.	Debe existir una política y procedimientos formales que aseguren el manejo de la información y los datos personales de los solicitantes. Los cuales deben estar encriptados tanto en su almacenamiento, tránsito y medios que los contengan. Deberá de existir un procedimiento de resguardo de certificados apegado a las mejores prácticas. Política de cifrado de información y gestión de las llaves públicas y privadas. Se deben de contemplar por lo menos los requerimientos para la protección de datos personales en posesión de particulares, de conformidad con las disposiciones jurídicas aplicables en la materia.	Deben cumplir con ISO27000, ISO31000, Risk IT o equivalente.	Documentos, procedimiento, mejores prácticas.
		83	Implementar controles de validación de integridad de datos	Deberán de existir procesos y procedimientos para la gestión de la integridad de la información almacenada y gestionada en servicio. Implementar un proceso de monitoreo que detalle el mecanismo de control de cambios realizados sobre la información sensible de los solicitantes y los	Deben cumplir con ISO27000, ISO31000, Risk IT o equivalente.	Documento de proceso de gestión de la integridad.

				documentos digitales. Se debe de validar que la información es consistente e íntegra, que los registros no se pueden cambiar sin que se generen alertas. Se deberán de implementar medios para validar y mantener la integridad de la información.		
		84	Implementar controles de validación de seguridad de la aplicación.	Debe existir una política y procedimientos para llevar a cabo la validación de la seguridad del aplicativo. Considerando las pruebas de seguridad para al menos los siguientes rubros: A1: SQL Injection. A2: Cross-site Scripting. A3: Broken Authentication and Session Management. A4: Insecure Direct Object Reference. A5: Cross-site Request Forgery. A6: Security Misconfiguration. A7: Failure to Restrict URL Access. A8: Insufficient Transport Layer Protection. A9: Unvalidated Redirects and Forwards. A10: Ataque de negación de servicio (DDoS, por sus siglas en inglés, Distributed Denial of Service).	Deben cumplir con ISO27000, ISO31000, Risk IT o equivalente.	Documento con políticas, procedimientos y reportes.
		85	Implementar controles de validación de seguridad de datos para el flujo de la aplicación.	Debe existir una política y procedimientos para llevar a cabo la validación de los datos ingresados a la aplicación, con el fin de identificar y realizar la gestión adecuada. Se deberá considerar: Uso de catálogos. Validación de entradas. Codificación de salidas. Validación y administración de contraseñas. Administración de sesión. Prácticas de criptografía. Administración de errores y accesos. Protección de datos. Seguridad de la	Deben cumplir con ISO27000 e ITIL o equivalente.	Documento con las políticas y procedimientos para llevar a cabo la validación de los datos ingresados.

				<p>comunicación.</p> <p>Configuración del sistema.</p> <p>Seguridad en la base de datos.</p> <p>Administración de archivos.</p> <p>Mejores prácticas de codificación.</p>		
	SLAs	86	Deberán mantenerse y registrarse los niveles de servicio	<p>Se deberán registrar y reportar niveles de servicio de la aplicación. Se debe de contar con un procedimiento documentado de cómo se capturan y reportan los Niveles de Servicio.</p> <p>Se deberá generar un reporte con los Niveles de Servicio de forma mensual. El mínimo requerimiento de nivel de servicio es del 99.99% de disponibilidad mensual.</p>	Mensual.	Reporte.
	Consulta de la Secretaría	87	Implementar un medio de consulta de bitácora para la Secretaría.	Debe de existir un procedimiento para la consulta en línea de las bitácoras del aplicativo, el cual deberá de tener controles de seguridad así como implementación de mejores prácticas de seguridad.	Diario.	Procedimiento de acceso y reportes.
	Consulta de la Secretaría	88	Prevención de Pérdida de la Información	Se debe de implementar un procedimiento que registre y monitoree la actividad de cada equipo que interviene o tiene contacto con la operación del servicio, a fin de evitar el uso indebido o pérdida de la información.	Diario.	Procedimiento, pantallas, bitácoras, reglas, herramienta.
	Consulta de la Secretaría	89	Prevención de Pérdida de la Información	Se debe de implementar un procedimiento que registre y monitoree la actividad de cada equipo que interviene o tiene contacto con la operación del servicio, a fin de evitar el uso indebido o pérdida de la información.	Diario.	Procedimiento, pantallas, bitácoras, reglas, herramienta.
Cumplimiento Legal y Regulatorio	Cumplimiento con Leyes y Regulaciones Aplicables	90	Conocimiento de Leyes y Regulaciones Aplicables	<p>El representante legal de la AC debe presentar un documento donde afirme que conoce y respetará el apego a las leyes y demás instrumentos jurídicos aplicables vigentes.</p> <p>El aspirante deberá indicar que conoce su responsabilidad de verificar el cumplimiento del marco jurídico aplicable a la materia.</p> <p>El aspirante deberá indicar que exime a la Secretaría de</p>		Documento firmado por el representante legal.

				cualquier responsabilidad derivada del incumplimiento de las leyes aplicables.		
	Cumplimiento con Leyes y Regulaciones Aplicables	90	Declaración de prácticas de certificación de la AC	El representante legal de la AC debe presentar su proyecto de Declaración de prácticas de certificación de la misma.	Cumplir con el RFC 3647.	Documento con la Declaración de prácticas de certificación, mismo que deberá estar publicado en internet.