DOF: 21/10/2016

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 ZEMPOALTECA TL, Subsecretario deResponsabilidades Administrativas y Contrataciones Públicas de la Secretaría de la F unción Pública en ausencia delSecretario de la Función Pública y OSVALDO ANTONIO SANTÍN QUIROZ, Jefe del Servicio de Administración Tributaria, confundamento en lo dispuesto por los artículos 17, 31 frac ción XXXIV, 34 fracción XXXIII y 37 fracciones XXII y XXIX de la LeyOrgánica de la Administración Pública Federal; 5 segundo párrafo; 2 fracción I del Reglamento de la Ley de Firma ElectrónicaAvanzada; 1, 7 fra cción XVIII y 14 fracción I de la Ley del Servicio de Administración Tributaria, en relación con el ArtículoTer cero Transitorio del Decreto por el que se reforman, adicionan y derogan diversas disposiciones contenida s en la Ley delServicio de Administración Tributaria publicado en el Diario Oficial de la Federación el 12 de junio del 2003; 5 fracción XVI delReglamento Interior de la Secretaría de Economía; 6 fracción I, 7 fracció n XII y 86 del Reglamento Interior de la Secretaría de laFunción Pública, y 8 fracción XXI del Reglamento I nterior 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 Ele ctrónica Avanzada,la cual contempla en su artículo 5, segundo párrafo, que la Secretaría de la Función Pú blica, la Secretaría de Economía y elServicio de Administración Tributaria dictarán, de manera conjunta, la s disposiciones generales para el adecuado cumplimientode la Ley mencionada;

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

Que resulta necesario determinar los requisitos, características, estándares y mecanismos tecnológico s que están obligadosa cumplir los interesados en obtener el carácter de Autoridades Certificadoras para l a emisión de los certificados digitalesprevistos en el artículo 24 de la Ley de Firma Electrónica Avanzada y la prestación de servicios relacionados; la estructura delos certificados digitales que emitan las Autoridade s Certificadoras; los requerimientos técnicos que como mínimo deberáncontener los sistemas informáticos de las dependencias y entidades de la Administración Pública Federal para estar enposibilidad de llevar a cabo el firmado de documentos electrónicos y, en su caso, mensajes de datos, así como la forma ytérmino s en que las Autoridades Certificadoras proporcionarán a las dependencias y entidades los servicios relaci onados conla 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:

Los requisitos, características, estándares y mecanismos tecnológicos que deberán cumplir las dependenci as yentidades de la Administración Pública Federal, así como los prestadores de servicios de certificación que esténinteresados en obtener el carácter de Autoridad Certificadora para la emisión de los certificados digitales previstosen la Ley de Firma Electrónica Avanzada y su Reglamento, así como la autorización par a la prestación de serviciosrelacionados con la firma electrónica avanzada;

La estructura que deberán cumplir los certificados digitales que emitan las Autoridades Certificadoras, previ stos en elTítulo Tercero, Capítulo I de la Ley de Firma Electrónica Avanzada;

Los requerimientos técnicos mínimos para que los sistemas informáticos, así como las herramientas tecnol ógicas oaplicaciones de las dependencias y entidades de la Administración Pública Federal puedan llevar a cabo el firmadode documentos electrónicos y, en su caso, mensajes de datos en la realización de los act os y actuaciones a que serefiere la Ley y su Reglamento;

La manera en que se llevará a cabo la conservación de los mensajes de datos y de los documentos electró nicos confirma electrónica avanzada;

Las medidas y controles de seguridad que deberán adoptar las Autoridades Certificadoras para

evitar la falsificación, alteración o uso indebido de Certificados Digitales;

El destino de los registros y archivos generados por las Autoridades Certificadoras que hayan sido suspen didas orevocadas de tal carácter;

La forma y términos en que las Autoridades Certificadoras proporcionarán a las dependencias y entidades de laAdministración Pública Federal, el servicio de consulta sobre el estado de validez, de los certificados digitales queemitan, y

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 R eglamento, paraefectos de las presentes Disposiciones Generales, se entenderá por:

AC: Autoridad Certificadora;

Claves criptográficas: la clave pública y la clave privada;

HTTP: Protocolo utilizado para el intercambio de información en Internet (*Hyper Text Transfer Protocol,* HT TP por sussiglas en inglés);

HTTPS: Protocolo seguro para el intercambio de información en Internet (*Hyper Text Transfer Protocol Se cure*,HTTPS por sus siglas en inglés);

MAAGTICSI: Manual Administrativo de Aplicación General en las materias de Tecnologías de la Informaci ón yComunicaciones y de Seguridad de la Información, emitido por la Secretaría y la Secretaría de Gobern ación comoanexo único del Acuerdo que tiene por objeto emitir las políticas y disposiciones para la Estrate gia Digital Nacional,en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así comoestablecer el Manual Administrativo de Aplicación General en dichas materias;

OCSP: Protocolo utilizado para obtener en tiempo real el estado actual de un certificado digital (OCSP, *Onl ineCertificate Status Protocol*, por sus siglas en inglés);

OID: es el número que se asigna para identificar un objeto sin ambigüedad, el cual se conforma de acuerd o alestándar del Instituto Nacional Estadounidense de Estándares (ANSI *American National Standards Inst itute)* (OID,*Object Identifier*, por sus siglas en inglés);

SAT: el Servicio de Administración Tributaria, y

SE: la Secretaría de Economía.

Disposiciones

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

Número de Serie: incorporará un número entero positivo;

AC que lo emitió: identificará a la AC con un nombre distintivo (DN Distinguished Name) de tipo "Name" d el estándarX.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 razónsocial
organizationalUnitName (OU)	PrintableString o UTF8String	64	Nombre de la unidad dentro de laorganizaci ón
EmailAddress (E)	IA5String	128	Correo electrónico de laorganización

StreetAddress	PrintableString o UTF8String	128	Calle, número y colonia de laorganización
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

Algoritmo de firma: contendrá el identificador del algoritmo criptográfico utilizado por la AC para firmar el certificadodigital.

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

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);

Nombre del titular del certificado digital: identificará al titular del certificado digital con un nombre distintivo (*DNDistinguished 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 deltitular del certificado digital
EmailAddress (E)	IA5String	128	Correo electrónico del titular delcertificado digital

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 de4096 bits para certificados digitales de las AC, y

Requisitos adicionales:

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

Extensiones: contendrá la siguiente información:

ATRIBUTOS	TIPO	DESCRIPCIÓN
authorityKeyIdentifier	No crítica	Permite identificar la clave pública correspondiente a laclave privada que la AC utilizó para firmar el certificadodigital. Usar sólo el campo KeyIdentifier, el cual debe contenerlos 256 bits del SHA-2 del valor subjectPublicKey delcertificado digital de la AC.

subjectKeyIdentifier	No crítica	Asigna un identificador de la clave pública del titular delcertificado digital. Debe contener los 256 bits del SHA-2 del valorsubjectPublicKey.
keyUsage	Crítica	Usos del certificado digital 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.
cRLDistributionPoint	No crítica	Indica cómo puede ser obtenida la Lista deCertificados Revocados.
authorityInfoAccess	No crítica	Indica cómo acceder a la información de la AC ysus servicios, aquí debe indicarse como mínimo ladirección electrónica de consulta de la AC.
certificatePolicies	Crítica	OID asignado por la Secretaría, quien deberá llevarun registro de los mismos.

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

Modelo Operacional de la AC;

El solicitante de acreditación deberá definir su Modelo Operacional de la AC conforme al cual operará ypre stará sus servicios al fungir como AC a efecto de lograr confiabilidad e interoperabilidad, para lo cualdesarr ollará los apartados siguientes:

Cuáles son los servicios prestados;

Cómo se interrelacionan los diferentes servicios;

En qué lugares se operará;

Qué tipos de certificados se entregarán;

Cuáles son los certificados generados con diferentes niveles de seguridad;

Cuáles son las políticas y procedimientos de cada tipo de certificado, y

Cómo se protegerán los activos.

El Modelo Operacional de la AC deberá contener un resumen que incluya:

Contenido del documento, y

Relaciones comerciales con proveedores de insumos o servicios para sus operaciones.

El Modelo Operacional de la AC deberá comprender los siguientes aspectos:

Interfaces con las Autoridades Registradoras;

Implementación de elementos de seguridad;

Procesos de administración;

Sistema de directorios para los certificados;

Procesos de auditoría y respaldo, y

Bases de Datos a utilizar.

El Modelo Operacional de la AC deberá considerar la Política de Certificados, la Declaración de Prácticas d eCertificación, la Política de Seguridad de la Información y el Plan de Seguridad de Sistemas por lo que se refiere a la generación de claves.

El Modelo Operacional de la AC deberá incluir los requerimientos de seguridad física del personal, de lasin stalaciones y del módulo criptográfico.

Modelo Operacional de la Autoridad Registradora.

El solicitante de acreditación deberá definir su Modelo Operacional de Autoridad Registradora conforme alc ual operará y prestará sus servicios como autoridad registradora a efecto de lograr confiabilidad einteroper abilidad, para lo cual desarrollará los apartados siguientes:

Cuáles son los servicios de registro que se prestarán;

En qué lugares se ofrecerán dichos servicios, y

Qué tipos de certificados generados por la AC se entregarán.

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 e lgrado de fiabilidad de los mecanismos y dispositivos utilizados.

El Modelo Operacional de la Autoridad Registradora deberá comprender los siguientes aspectos:

Interfaces con AC;

Implementación de dispositivos de seguridad;

Procesos de administración;

Procesos de auditoría y respaldo;

Bases de Datos a utilizar;

Privacidad de datos, y

Descripción de la seguridad física de las instalaciones.

El Modelo Operacional de la Autoridad Registradora deberá establecer el método para proveer de unaident ificación unívoca del usuario y el procedimiento de uso de los Datos de Creación de la Firma ElectrónicaAv anzada.

Plan de Administración de Claves.

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:

Claves de la AC;

Almacenamiento, respaldo, recuperación y uso de los Datos de Creación de Firma Electrónica de laAC del Prestador de Servicios de Certificación;

Distribución del certificado de la AC;

Administración del ciclo de vida del hardware criptográfico que utilice la AC, y

Dispositivos seguros para los usuarios.

Los procedimientos implantados de acuerdo al Plan de Administración de Claves, deberán garantizar laseg uridad de las claves en todo momento, aun en caso de cambios de personal, componentes tecnológicos, y demás que señalan las presentes Reglas Generales.

El Plan de Administración de Claves deberá establecer como requerimiento mínimo el utilizar aquellas conl ongitud de 2048 bits para los usuarios y de 4096 bits para los Prestadores de Servicios de Certificación.

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-140nivel 3 en sus elementos de seguridad e implantación de los algoritmos, criptográficos estándares, o el que lesustituya.

El Plan de Administración de Claves tendrá que ser compatible por lo menos con el estándar ETSI TS 102 042sección 7.2 -
Generación de la clave de la AC, Almacenamiento, Respaldo y Recuperación de la clave de laAC, Distribu ción de la clave pública de la AC, uso de clave de la AC, fin del ciclo de vida de la clave de la AC yAdminis tración 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 o btengan el carácterde AC.

QUINTA.- Las dependencias y entidades que requieran utilizar la Firma Electrónica Avanzada, primero deben celebrar unconvenio de colaboración o coordinación con la AC que provee el servicio de OCSP y c ontar con los siguientes requerimientostécnicos mínimos en sus sistemas informáticos, así como en las he rramientas tecnológicas o aplicaciones:

Contar con la Infraestructura de comunicación necesaria (equipos de cómputo, conexión a internet).

Contar con aplicaciones que empleen el algoritmo de firmado SHA256 con RSA para certificados con una l ongitud de1024, 2048 bits o superior.

Contar con software capaz de validar los certificados mediante un servicio de consulta basado en el protoc olo decomunicación OCSP que permita a los usuarios consultar el estado que guarda un Certificado Digita l.

Proporcionar a la AC la dirección IP y la URL desde la cual se realizarán las consultas al servicio (consider ando la IPdel firewall).

Configurar sus servicios de comunicación de acuerdo al estándar RFC 6960 X.509 *Internet Public Key Infr astructureOnline Certificate Status Protocol* OCSP.

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

Verificar que el certificado digital presentado tenga una vigencia válida.

Enviar un mensaje para conocer el estado que guarda el certificado digital y suspende la aceptación del ce rtificadodigital hasta que la respuesta sea recibida de parte de la AC.

Obtener el mensaje de respuesta que envía el servicio de OCSP.

Contar con la capacidad de interpretar las respuestas firmadas de las consultas al servicio OCSP utilizand o elcertificado de la AC para aceptar y en su caso rechazar la solicitud si el certificado ha sido revocado y por lo tanto noes válido a pesar de su vigencia.

SEXTA.- La conservación de los mensajes de datos y de los documentos electrónicos con firma electr ónica avanzada seregirá por la naturaleza de la documentación de acuerdo con las disposiciones legales a plicables y se deberá asegurar que seha mantenido íntegra e inalterada a partir del momento en que se ge neró por primera vez en su forma definitiva y sea accesiblepara su ulterior consulta; para tales efectos deb erá observarse lo establecido en la norma oficial mexicana que para talesefectos emita la SE.

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

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

OCTAVA.- Los requisitos para obtener el carácter de AC, establecidos en las presentes disposiciones, los deberá cumplirdirectamente el solicitante de acreditación, y en su caso, la AC cuando obtenga tal carácter, por lo que dichas obligaciones nopodrán 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 decualquier 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 seannecesarias para asegurar el cumplimiento de las obligaciones establecidas en la Ley, en el Reglamento y en las demásdisposiciones aplicables. La realización de dichas visitas se ajustarán a lo previsto en el capítulo Décimo primero del TítuloTercero de la Ley Federal de Procedimiento Administrativo.

Finalmente, la AC que obtenga tal carácter, deberá cumplir todas las disposiciones aplicables para las dependencias yentidades de la Administración Pública Federal en materia de tecnologías de la información y comunicaciones, seguridad de lainformación 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 FirmaElectrónica Avanzada y 21 de su Reglamento, deberán transferir los certificados digitales, registros y archivos generados a laAC 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 3de las presentes Disposiciones Generales.

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

RFC 5958 *"PKCS#8: Private-Key Information Syntax Standard"*, para la creación de la clave privada;

RFC 2986 *"PKCS #10: Certification Request Syntax Specification Version 1.7"*, para la generación del archivo derequerimiento del certificado digital, y

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 1de las presentes Disposiciones Generales.

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

Cumplir con lo señalado en el RFC 6960 "*X.509 Internet Public Key Infrastructure Online Certificate Status ProtocolOCSP"*;

Utilizar mensajes codificados que deberán ser transmitidos sobre el protocolo HTTP o HTTPS;

Firmar la respuesta a la solicitud utilizando el certificado digital de la AC o bien, con otro certificado digital generadoespecialmente por la AC para la prestación de ese servicio;

Mantener operando el servicio con una disponibilidad del 99.95%, y

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 hayansido revocados, los cuales se integrarán en una Lista de Certificados Revocados, misma que elaborarán al menos cada 24horas y que deberá cumplir con lo siguiente:

Ser compatible con la última versión del estándar ISO/IEC 9594-8:2014 "*The Directory: Public-key and attributecertificate frameworks"* o RFC 5280 *"X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL)Profile*";

Contener fecha y hora de su emisión, y

Ser firmada por la AC que la emita.

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

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

La verificación de validez se realizará mediante consulta que formulen a la AC que expidió el certificad o digitalcorrespondiente, a través del servicio de OCSP de acuerdo a las características definidas por la A C.

DÉCIMA QUINTA.- La interpretación para efectos administrativos de las Disposiciones Generales cont enidas en el presenteAcuerdo, así como la resolución de los casos no previstos en las mismas, correspon derá a la Secretaría a través de la Unidadde Gobierno Digital.

DISPOSICIONES TRANSITORIAS

Primera.- Las presentes Disposiciones entrarán en vigor el día siguiente al de su publicación en el Diar io Oficial de laFederación.

Segunda.- A fin de garantizar la interoperabilidad del firmado de los certificados con una longitud de 1 024 bits se debemantener 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 respec tivos programas deinstrumentación para el uso de la firma electrónica avanzada, los ajustes que procedan a sus sistemas informáticos, a efecto deque los mismos cumplan con lo establecido en la disposición terce ra fracción III.

Ciudad de México, a 18 de octubre de 2016.- El Secretario de Economía, **Ildefonso Guajardo Villarre al**.- Rúbrica.- Ensuplencia por ausencia del Secretario de la Función Pública con fundamento en lo dispues to por los artículos 7 fracción XII y 86del Reglamento Interior de la Secretaría de la Función Pública, el Sub secretario de Responsabilidades Administrativas yContrataciones Públicas de la Secretaría de la Función Pública, **Javier Vargas Zempoaltecatl**.- Rúbrica.- El Jefe del Serviciode Administración Tributaria, **Osvald o 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 pr omover laestandarización de su operación a nivel nacional, con la finalidad de brindar un servicio eficaz, ef iciente y de calidad.

Alcance

El presente procedimiento es de aplicación para el personal encargado de la emisión de los certificado s (en lo sucesivoAgentes 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 Electr ónica Avanzada queal menos contenga la siguiente información:

Requisitos para solicitar la generación de la Firma Electrónica Avanzada, en términos del artículo 18 de la Ley deFirma Electrónica Avanzada.

Dirección de las oficinas a las que debe acudir el solicitante.

Horarios de atención.

Canales de comunicación para la atención de los solicitantes.

Esquema de atención a Quejas, Sugerencias y Reconocimientos.

Segunda.- La AC debe garantizar que el personal (Agente Certificador) cuenta con la capacitación corr espondiente parallevar a cabo las actividades para la emisión de certificados, además de contar con los el ementos de confiabilidadcorrespondientes.

Tercera.- La AC debe llevar a cabo evaluaciones de conocimiento y confiabilidad a los Agentes Certific adores en un periodono 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 certifica ción deje de teneracceso a los sistemas involucrados.

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

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

Séptima.- La AC debe garantizar que terceros y personal ajeno al proceso de emisión de certificados d e Firma ElectrónicaAvanzada 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 delciudadano solicitante del certificado de Firma Electrónica Avanzada ante la AC y exhibi r la documentación señalada en lasección de Firma Electrónica Avanzada de la página de Internet de la A C, la cual el Agente Certificador cotejará y validarácontra los sistemas Institucionales, para proceder a can alizarlos a la Estación de Enrolamiento para el Servicio de Acreditaciónde 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 solicit ud y realizar lageneración del archivo de requerimiento *.req, al momento en que acuda a realizar el trámit e.

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 porambos lados, en caso que el solicitante no cuente con pluma de tinta azul, la AC deberá propo rcionársela.

Décima.- Los datos y elementos de identificación obtenidos en el trámite de Firma Electrónica Avanzad a formarán parte delsistema de Registro Nacional de Población (RENAPO).

El Agente Certificador deberá recabar los datos y elementos de identificación de conformidad con el Ac uerdo por el cual sedan 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 deinternet.

La acreditación de la identidad y la certificación documental del trámite de generación del certificado de Firma ElectrónicaAvanzada del solicitante es responsabilidad del Agente Certificador, y debe estar compl eta antes de que se canalice alsolicitante a la estación de enrolamiento para la toma de biométricos, la digi talización de la documentación probatoria y laemisión del certificado de Firma Electrónica Avanzada.

Décima primera.- La AC debe designar un responsable del proceso de emisión de certificados de Firm a ElectrónicaAvanzada, quién será el encargado de supervisar la adecuada captura de los datos y element os de identificación del solicitantey 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 deidentificación, se deberá rechazar el trámite e informar al solicitante que acuda ante la autori dad correspondiente, para corregirla inconsistencia o duplicidad.

Décima tercera.- La AC podrá emitir certificados de Firma Electrónica Avanzada para los solicitantes q ue se encuentren bajociertos supuestos especiales, siempre y cuando acrediten tal característica, de conf ormidad con las disposiciones jurídicasaplicables. De manera enunciativa mas no limitativa se mencionan los certificados para los menores de edad que prestenexclusivamente un s

ervicio personal subordinado, los menores de edad emancipados y los contribuyentes con incapacidadlegal declarada judicialmente.

Décima cuarta.- La AC debe llevar a cabo la toma de biométricos, registro y validación de los mismos conforme alProcedimiento Técnico de Captura de Información y el Procedimiento Técnico de Intercambio de Información, así como susrespectivos 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 establecenlas Disposiciones Generales.

Décima sexta.- La AC debe enviar a la Autoridad Registradora los certificados de Firma Electrónica Avanzada generados afin 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 identidaddel solicitante en su carácter de persona física, así como el documento mediante el cual el solicitante confirma la recepción oentrega 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 unabitácora electrónica de los registros o movimientos que se efectúan en el día por cada Agente Certificador y mantenerlos bajoresguardo.

Décima novena.- La AC deberá hacer del conocimiento del solicitante los siguientes términos y condiciones, los cualesdeben 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 ElectrónicaAvanzada, y a quien en lo sucesivo se le denominará como "El Solicitante" para todos los efectos legales que derivendel presente documento a que haya lugar, manifiesta ante <poner aquí el nombre de la AC>, a quien en lo sucesivo sele denominará como "La Autoridad Certificadora" (AC), que es su libre voluntad contar con un Certificado Digital deFirma Electrónica

Avanzada en el que conste la clave pública que se encuentra asociada a la clave privada y frase de seguridad quemanifiesta haber generado previamente y en absoluto secreto, sin que persona alguna lo haya asistido durante dichoproceso.

Asimismo manifiesta su conformidad en que "La AC" utilice el procedimiento de certificación de identidad queestablece 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 <poneraquí fundamento legal vigente>, y cuya finalidad es garantizar el vínculo que existe entre un Certificado Digital deFirma Electrónica Avanzada y su titular, el cual fue registrado en el "Listado de Sistemas de Datos Personales" ante elInstituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales **ifai**.org.mx, y seránтransmitidos al Registro Nacional de Población, para la conformación del "Sistema Integral del Registro Nacional dePoblación".

La Unidad Administrativa responsable de este sistema es <poner nombre aquí>. "El Solicitante" podrá ejercer losderechos de acceso y corrección de datos a través de <poner aquí el mecanismo o ubicación del inmueble en dondese pueden ejercer estos derechos>. Lo anterior se informa en cumplimiento del DECIMO SÉPTIMO de los"Lineamientos de Protección de Datos Personales", publicados en el Diario Oficial de la Federación el 30 deseptiembre 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 ydocumentación por él proporcionada a "La AC". De la misma forma "El Solicitante" asume la responsabilidad exclusivadel 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 derecibo.

Adicionalmente, "El Solicitante" acepta que el uso de la clave privada y frase de seguridad con base en las cualesdicho certificado fue elaborado, quedarán bajo su estricta y absoluta responsabilidad, la cual incluye en formaenunciativa, los daños y perjuicios, incluso aquéllos de carácter financiero, que pudieran causarse por su usoindebido, 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 FirmaElectrónica Avanzada, así como en cualquier otro certificado digital que con posterioridad se obtenga, será de carácterpúblico y podrá ser consultada libremente por cualquier interesado a través de los medios y formas que disponga "LaAC".

Por lo anterior, "El Solicitante" se obliga a mantener absoluta confidencialidad respecto de las aludidas clave privada yfrase 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 dichainformación sea divulgada o se realice cualquier supuesto por el que "El Solicitante" deba solicitar su cancelación enlos términos de las disposiciones jurídicas aplicables.

Por otra parte "El Solicitante" manifiesta conocer el contenido y alcance de las disposiciones jurídicas relativas a lacelebración de actos jurídicos mediante el uso de medios electrónicos, digitales o de cualquier otra tecnología, por loque asume plena responsabilidad respecto de la información y contenido de todo documento electrónico o digitalelaborado y enviado en el que se haga uso de la citada clave privada, toda vez que por ese solo hecho se consideraráque 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 acometer 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 "ElSolicitante" 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 anteriorpor caso fortuito o fuerza mayor se entenderá todo acontecimiento o circunstancia inevitable, más allá del controlrazonable 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 yreverso 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 aquídirección 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 "ElSolicitante".

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 elCertificado 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 situaciónque 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 direcciónelectrónica> 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 ElectrónicaAvanzada

Puesto / Rol Resp	**Tarea**	**Descripción de la tarea**	**Documentos invol**

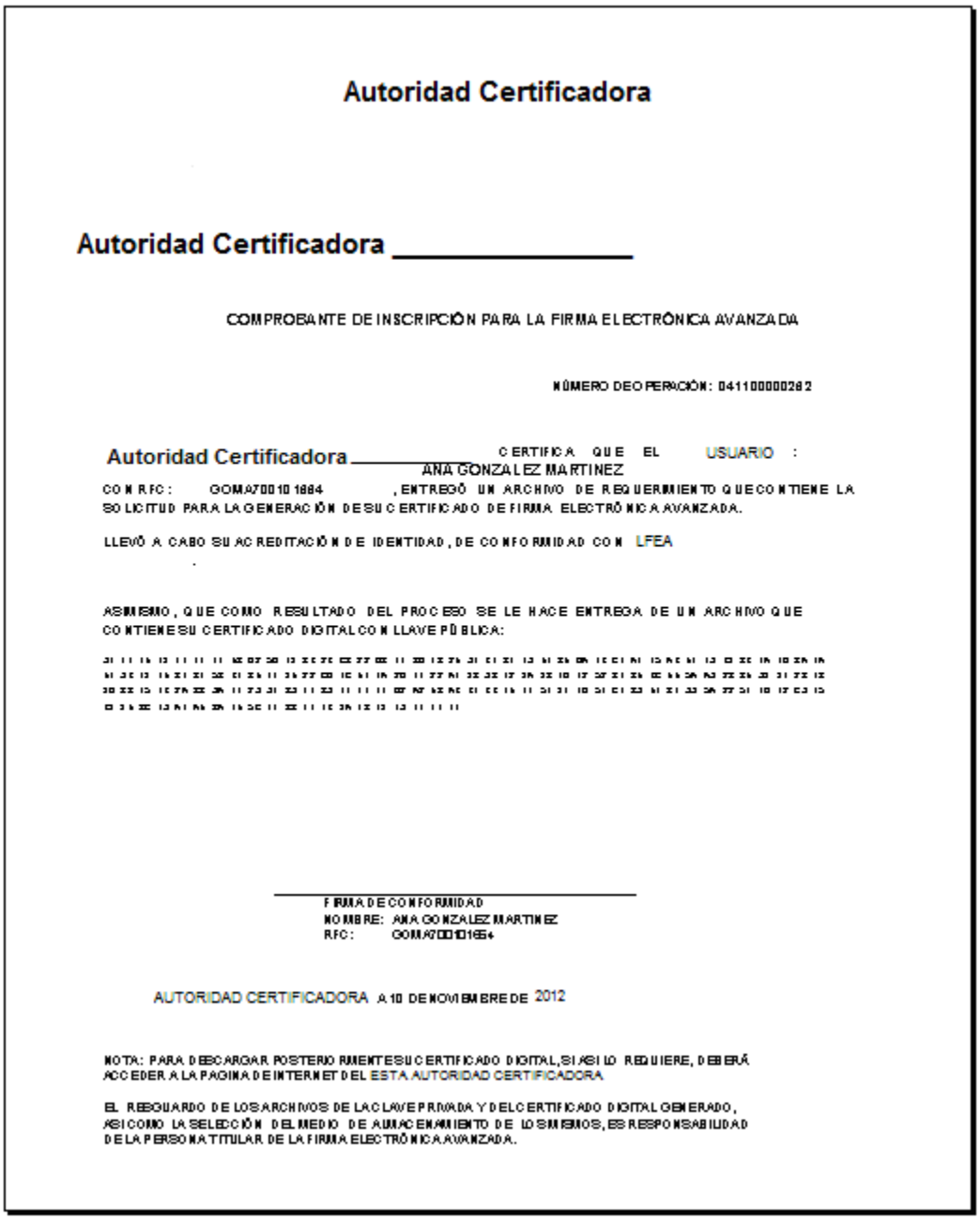
onsable			ucrados
Usuario		1. Accede a la página de la AC en Internet en lasección de Firma Electrónica Avanzada yprocede a bajar la aplicación para generar elrequerimiento [*.req] y la llave privada [*.key] ensu equipo de cómputo. 2. Instala en su PC la aplicación que genera el *.reqy *.key. 3. Ejecuta la aplicación de generación de archivosantes mencionados, y llena los datos requeridos,conforme es instruido en el aplicativo. 4. Respalda en una unidad de memoria extraíbleUSB o disco compacto [CD] el archivo *.req y lointegra a la documentación que presentará en laAC.	
		5. Acude a la AC presentando los documentosrequeridos al Agente Certificador para realizar eltrámite de emisión de Certificado Digital de FirmaElectrónica Avanzada. **Requisitos** Identificación oficial. Acta de nacimiento. Solicitud de Certificado de Firma ElectrónicaAvanzada, firmada de forma autógrafa. Archivo de requerimiento [USB o CD].	
Agente Certificador		6. Verifica que la documentación presentada estécompleta y determina. **Sí está la documentación completa** Continúa en la DT 8. **No está la documentación completa** Continúa en la DT 7.	

		7. Informa al Usuario de los faltantes. Devuelvedocumentación indicando que deberá hacer unanueva cita y traer los documentos que falten. **Concluye procedimiento**	
		8. Procede a validar la información de ladocumentación presentada que acredita laidentidad del solicitante. Si la información es consistente continúa en laDT10. En caso de identificar inconsistencias, continua enla DT9.	

		9.	Informa al solicitante que no es posible llevar acabo el trámite, por lo que será necesario quecorrija las inconsistencias reportadas. Concluye el procedimiento.
		10.	Digitaliza la documentación con la que acredita laidentidad del solicitante y la integra en unexpediente electrónico.
		11.	Canaliza al área de toma de biométricos.
		12.	Realiza la toma de biométricos, los valida y en sucaso los registra conforme al ProcedimientoTécnico de Captura de Información y elProcedimiento Técnico de Intercambio deInformación.
		13.	Registra los biométricos en el sistema y seprocede a generar el Certificado Digital de FirmaElectrónica Avanzada.
		14.	Se solicita al usuario registrar en el sistema suclave privada a fin de generar el CertificadoDigital de Firma Electrónica Avanzada y elarchivo llave.
		15.	Se emite el "Comprobante de Inscripción para laFirma Electrónica Avanzada" para que lo firmede forma autógrafa el solicitante.
Usuario		16.	Recibe y procede a firmar de recibido en los dostantos del "Comprobante de Inscripción para laFirma Electrónica Avanzada" y devuelve.
Agente Certificador		17.	La AC recibe y acusa de recibo con sello en losdos tantos del formato de "Solicitud deCertificado de Firma Electrónica Avanzada". LaAC entrega un tanto de este al Usuario junto conun tanto del "Comprobante de Inscripción para laFirma Electrónica Avanzada", los originales de sudocumentación y el dispositivo externo con suarchivo *.cer.
		18.	Anexa la documentación al o expediente delUsuario la nueva documentación recibida. **Fin del Procedimiento**

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 R.F.C: GOMA700101 1984 , 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:

FIRMA DE CONFORMIDAD
NOMBRE: ANA GONZALEZ MARTINEZ
R.F.C: GOMA700101954

AUTORIDAD CERTIFICADORA A 10 DE NOVIEMBRE DE 2012

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

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

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 ejerza n sus facultades, asícomo promover la estandarización de su operación a nivel nacional, con la finalidad d e brindar un servicio eficaz, eficiente y decalidad.

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 huellasdactilares.

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

Tercera.- El Agente Certificador tendrá la responsabilidad de integrar al expediente electrónico corresp ondiente para lageneración de la Firma Electrónica Avanzada, la documentación que respalda el trámite d e revocación.

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

Extravío de la llave privada u olvido de la contraseña de acceso a la llave privada.

Cambio de nombre.

Cambio de Clave Única de Registro de Población.

Cambio de clave de Registro Federal de Contribuyentes.

Por suposición que su contraseña y/o llaves privadas fueron comprometidas.

Por haberse modificado la situación jurídica del solicitante

Quinta.- El Agente Certificador deberá requerir el escrito libre de solicitud de revocación, mismo que es pecificará la causapor la cual se solicita la revocación del Certificado Digital. El Agente Certificador proced erá conforme a lo siguiente:

Se cotejará la siguiente documentación:

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 desolicitud de revocación de certificados.	Escrito libre

Agente Certificador		2. Verifica que se presente la siguientedocumentación: Escrito libre con la solicitud de revocación. Original o copia certificada de laidentificación oficial del solicitante.	Escrito libre Identificación oficial del solicitante
Agente Certificador		3. ***Acredita la identidad del solicitante a travésde la validación de las huellas dactilares.***	
		4. Accede al sistema de revocación provisto por laAC, captura número de serie del certificado arevocar y RFC y procede a revocar.	
		5. Imprime comprobante y entrega al Solicitante losdos tantos y solicita firme acuse de recibo.	Comprobante de revocación de certificado
Usuario		6. Recibe, firma acuse de recibo y devuelve.	Comprobante de revocación de certificado
Agente Certificador		7. Entrega al solicitante copia del escrito libre, elcomprobante de revocación de certificado juntocon el original de la identificación oficial.	Escrito libre Identificación oficial Comprobante de revocación de certificado
		8. Digitaliza la información correspondiente a larevocación y la integra al expediente electrónicodel solicitante.	
		9. Integra al original del escrito libre el comprobantede 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:

_____
_____ycorreo elec trónico: _____

Por medio del presente y en apego al xxxxxxxxxxxxxx solicito a esta autoridad realice la revocación del C ertificado Digitalde 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 pr omover laestandarización de su operación a nivel nacional, con la finalidad de brindar un servicio eficaz, ef iciente y de calidad.

Alcance

El presente procedimiento es de aplicación para los Agentes Certificadores de las Autoridades Certifica doras (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 huellasdactilares.

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 corresp ondiente para lageneración de la Firma Electrónica Avanzada, la documentación que respalda el trámite d e renovación.

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

Cuando el certificado de Firma Electrónica Avanzada no está vigente.

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

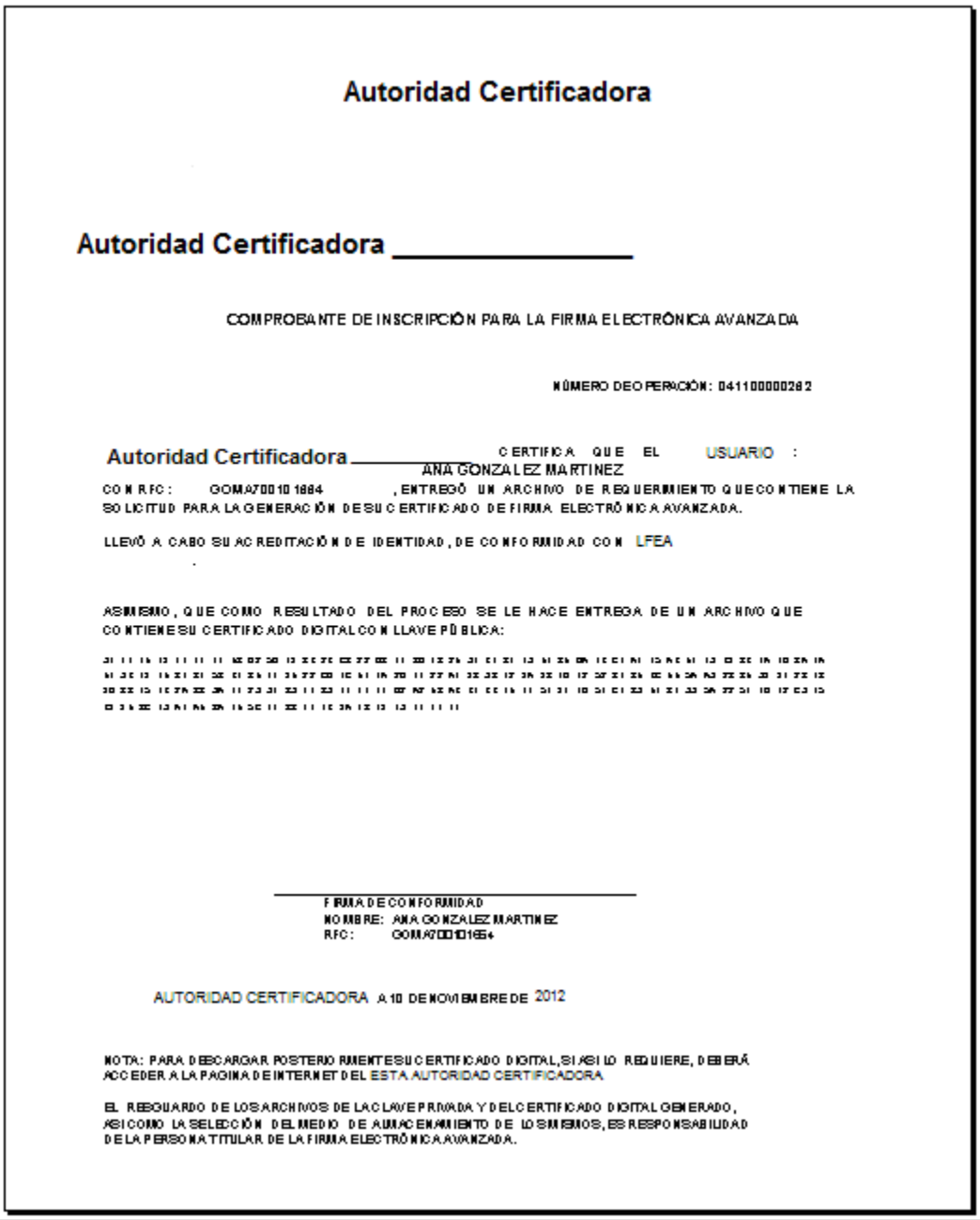
Usuario		1. Acude a la AC presentando los documentosrequeridos para realizar el trámite de renovacióndel Certificado Digital de Firma ElectrónicaAvanzada. **Requisitos de renovación:** Original o copia certificada de laidentificación oficial del solicitante. Archivo de requerimiento (dispositivo omecanismo de almacenamiento). Correo electrónico.	Identificación oficial Archivo *.req

Agente Certificador		2. Verifica que la documentación esté correcta. 3. Corrobora con el solicitante los datos de: RFC,CURP, nombre y domicilio desplegados enpantalla, también verifica que el apartado<**Biométricos**> señale la opción <**Sí**>. 4. Acredita la identidad del solicitante, a través de lavalidación de las huellas dactilares. 5. Genera e imprime en dos tantos la "solicitud derenovación" y recaba firma del solicitante. 6. Genera y almacena el Certificado Digital deFirma Electrónica Avanzada en el dispositivo omecanismo de almacenamiento. 7. Imprime en dos tantos el Comprobante deInscripción para la Firma Electrónica Avanzada yrecaba firma del solicitante. Extrae dispositivo omecanismo de almacenamiento.	Solicitud de renovación Comprobante de Inscripción para la Firma Electrónica Avanzada

Usuario	8.	Recibe y firma de recibido en los dos tantos de la"Solicitud de renovación" y del Comprobante deInscripción para la Firma Electrónica Avanzada' ydevuelve.	Comprobante de Inscripción para la Firma Electrónica Avanzada
Agente Certificador	9.	Recibe y acusa de recibo con sello de la AC enlos dos tantos del formato de Solicitud derenovación, entrega un tanto de éste al solicitantejunto con un tanto del Comprobante deInscripción para la Firma Electrónica Avanzada' ylos originales de su documentación y sudispositivo o mecanismo de almacenamiento consu Certificado Digital de Firma ElectrónicaAvanzada.	Comprobante de Inscripción
	10.	Anexa la documentación digitalizada alexpediente electrónico e integra locorrespondiente al expediente físico delsolicitante la nueva documentación recibida.	
	.	Fin del Procedimiento	

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 R.F.C: GOMA700101884 , 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:

FIRMA DE CONFORMIDAD
NOMBRE: ANA GONZALEZ MARTINEZ
R.F.C: GOMA700101884

AUTORIDAD CERTIFICADORA A 10 DE NOVIEMBRE DE 2012

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

EL RESGUARDO DE LOS ARCHIVOS DE LA CLAVE PRIVADA Y DEL CERTIFICADO DIGITAL GENERADO, ASÍ 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 del proceso.	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.

	Liderazgo de la Alta Dirección	4	Liderazgo y compromiso	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. 2. Asegurar que los requerimientos de la seguridad de la información están integrados a los procesos organizacionales relacionados con los servicios del negocio. 3. Asegurar que se proporcionen los recursos requeridos para mantener la seguridad de la información del negocio. 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. 5. Asegurar que los requerimientos de seguridad de la información alcancen sus objetivos. 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.	Al inicio de solicitud, posteriormente actualizaciones cada que existan cambios en las directivas y políticas de seguridad. Deben cumplir con ISO27000, Risk IT o equivalente.	* Documento con la incorporación de la estrategia de seguridad en la del negocio. * Documento con los recursos asignados. * Documento con el programa de seguridad de la información. * Documento de reporte de asignación y supervisión de avance del programa de seguridad de la información.
		5	Política de seguridad de la información	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.	Al inicio de solicitud, posteriormente actualizaciones cada que existan cambios en las directivas y políticas de seguridad. Deben cumplir con ISO27000, Risk IT o equivalente.	Debe de implementar un Sistema de Gestión de Seguridad de la Información (SGSI), protocolizado de conformidad a ISO27000 por lo menos.

6	Políticas específicas de seguridad de la información	1. Política de seguridad de la información. - Contiene los lineamientos generales de las políticas de información. 2. Política de la organización de la seguridad de la información. Contiene los lineamientos bajo los cuales se rige la seguridad de la información. 3. Política para seguridad de los recursos humanos. - Políticas relacionadas a la administración del recurso humano. 4. Política de gestión de activos. - Políticas que definirán el proceso con lo cual se gestionarán los activos. 5. Política de control de accesos. - Política que detalla el acceso a las diferentes instalaciones.	Al inicio de solicitud, posteriormente actualizaciones cada que existan cambios en las directivas y políticas de seguridad. Deben cumplir con ISO27000, Risk IT o equivalente. *Las políticas deberán ser revisadas por lo menos una vez al año.	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. Debe de implementar un Sistema de Gestión de Seguridad de la Información (SGSI), protocolizado de conformidad a ISO27000 por lo menos.

				6. Política de criptografía. - Política de uso de criptografía en aplicaciones y servicios. 7. Política de seguridad física y ambiental. - Políticas que rigen la seguridad física y ambiental de las distintas instalaciones. 8. Política de seguridad en las operaciones. - Políticas con las consideraciones de seguridad para las operaciones diarias. 9. Política de seguridad en las comunicaciones. - Políticas que rigen las comunicaciones para los activos que participan en el proceso. 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. 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. 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. 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). 14. Política para el cumplimiento. - Reglas que se van a tomar en cuenta para el seguimiento y cumplimiento de las normativas de la AC. '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		
				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 protección de las mismas.		

				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. 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. 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.		
	Estructura organizacional	7	Roles, responsabilidades y autoridad con respecto a la seguridad de la información.	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. 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.	Deben cumplir con ISO27000, Risk IT o equivalente.	* Documentos con las cartas responsivas de los participantes. * Organigrama * Roles dentro del organigrama.

8	Marco de trabajo seleccionado para la gestión de riesgos de seguridad de la información.	Gestión de administración del riesgo: 1.-Diseño o elección del marco de trabajo para administrar el riesgo. 2.-Implementar la administración de riesgos. 3.-Monitorear y revisar el marco de trabajo. 4.- Mejora continua del marco de trabajo. Lo anterior es enunciativo mas no limitativo.	Deben cumplir con ISO27000, Risk IT o equivalente.	Documento con el marco de trabajo.

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

		12	Competencias	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) 2. Plan de capacitación o entrenamiento para alcanzar o retener las competencias requeridas para desempeñar las funciones.	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.	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: 1. ¿Qué es lo que se debe de comunicar? 2. ¿Cuándo se debe de comunicar? 3. ¿A quién se le debe de comunicar? 4. ¿Quién lo debe de comunicar? 5. Los procesos que pueden ser afectados por la comunicación.	Deben cumplir con ISO27000, Risk IT o equivalente.	Documento que detalle la gestión de comunicación.
		14	Concientización	El personal que este participando debe de tener conocimiento de: 1. La política de seguridad de la información. 2. Su participación para la efectividad de la seguridad de la información y sus beneficios. 3. Las implicaciones de no cumplir con los requerimientos de la seguridad de la información. 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. Los puntos son enunciativos mas no limitativos.	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 acción para mitigar cualquier efecto adverso.	Deben cumplir con ISO27000, 31000, Risk IT o equivalente.	Plan operativo de seguridad de la información, controles de cambio, controles de seguridad de la 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.	La AC deberá evaluar si el desempeño y efectividad de su servicio y la seguridad se encuentran acorde a sus políticas y procesos: 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. * Se debe de considerar el servicio ofrecido al solicitante y su operación interna.	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	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. 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. Se deberá revisar el cumplimiento de la matriz presente. Se deberá planear, establecer e implementar un plan de auditoría, que incluya frecuencia, seguimiento del resultado de las auditorías y responsable de las actividades.	1 vez al año como mínimo.	Reporte de auditoría.

	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, subscripciones 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 recepcionistas) 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 asegurar que sólo se permita acceso al personal autorizado.	Deben cumplir con ISO27000, ISO31000, Risk IT o equivalente.	Política y bitácoras de acceso a las instalaciones.

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: - 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.	* 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.	* 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: - 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.	* 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: 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 mane jo de certificados que cubra como mínimo los siguiente puntos: 1.- Proceso de identificació n y autenticación de la entida d 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	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: 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	La AC debe de contar con un proceso formal de manejo de certificados que cubra lo siguiente: 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	La AC deberá de implementar el servicio de OCSP público para validación del estado de los Certificados Digitales de Firma Electrónica Avanzada.	Debe cumplir RFC 6960.	Disponibilidad del servicio 99.999%

Lista de certificados revocados (CRL, por sus siglas en inglés, Certificate Revocation List)	45	Servicio de CRL	La AC deberá de implementar el servicio de CRL público para validación de certificados revocados de firma electrónica avanzada	Debe cumplir RFC 5280.	Disponibilidad del servicio 99.999%, actualizado cada 12 horas al menos.

	Gestión de cuentas	46	Altas, Bajas y Cambios de Accesos de Usuarios	La AC debe documentar procedimientos formales para las Altas, Bajas y Cambios de accesos de usuarios, que incluyan como mínimo: - Bloqueo de las cuentas por intentos fallidos de autenticación. - Bloqueo de cuentas por periodo de inactividad. Los accesos remotos sólo se deberán proporcionar bajo circunstancias de excepción y con un estricto proceso de autorizaciones y monitoreo.	Deben cumplir con ISO27000 e ITIL o equivalente.	Procedimiento de gestión de cuentas.
		47	Gestión de Privilegios	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.	Deben cumplir con ISO27000 e ITIL o equivalente.	Procedimiento de gestión de cuentas con privilegios.
		48	Gestión de Contraseñas de Usuarios	La AC debe contar con procedimientos formales de asignación de contraseñas, mismos que deben contar por lo menos con las siguientes reglas: - 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	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.	6 meses.	Procedimiento de altas o cambios de accesos de usuarios.
Seguridad Física	50	Ubicación del Centro de Datos	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 cableado de electricidad y gas, etc. y deberá estar dispuesta como una instalación no evidente.	100 m	Plano de ubicación del centro de datos y sus colindancias.	

		51	Control de Accesos Físicos	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. El personal que acceda al centro de datos no deberá introducir medios de almacenamiento extraíbles sin autorización. Las bitácoras de acceso deberán resguardarse en un lugar seguro.	Deben cumplir con ISO27000 e ITIL o equivalente.	Autenticación para el acceso.

		52	Vigilancia y Monitoreo	El centro de datos debe contar con personal de vigilancia las 24 horas y un sistema de monitoreo de las instalaciones (CCTV, etc.). 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. El personal debe estar debidamente capacitado y contar con las herramientas necesarias para responder en caso de emergencias.	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	Las instalaciones deben contar con señalización que indique claramente: - 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 TIERIV 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 partición exclusiva. - Inhabilitación de puertos, protocolos usuarios y servicios innecesarios. - Recomendaciones de seguridad del fabricante del equipo y sistema operativo.	Deben cumplir con ISO27000 e ITIL o equivalente.	Documento con configuración y línea base de seguridad del aplicativo, listado de activos, versión del sistema.

		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.
	Respaldos	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 alterno, 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: - Solicitud y Autorización explícitas de la destrucción o borrado. - Actas de destrucción o borrado firmadas por el personal que lo realiza.	Deben cumplir con ISO27000, ISO31000, Risk IT o equivalente.	Acta de destrucción, ordenes de servicio de destrucción.

	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 especifiqué el método y la criptografía usada en caso de tener servicios expuestos.
70	Protección de Llaves y Certificados	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: - 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 qu e 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 segurida d 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 Secretaria, en su caso a la SE o al SAT, e n 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 d e cambios de los mismos.
Protección Contr a 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. Las bitácoras están enfocadas al personal administrativo de la aplicación o servicio.	12 meses en sistema y 5 años en histórico.	Bitácoras, pantallas.
	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.
	Encripción de Datos	82	Encripción 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 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.	Deben cumplir con ISO27000, ISO31000, Risk IT o equivalente.	Documento de proceso de gestión de la integridad.

		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 comunicación. Configuración del sistema. Seguridad en la base de datos. Administración de archivos. Mejores prácticas de codificación.	Deben cumplir con ISO27000 e ITIL o equivalente.	Documento con las políticas y procedimientos para llevar a cabo la validación de los datos ingresados.

	SLAs	86	Deberán mantenerse y registrarse los niveles de servicio	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. 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.	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.
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	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. El aspirante deberá indicar que conoce su responsabilidad de verificar el cumplimiento del marco jurídico aplicable a la materia. El aspirante deberá indicar que exime a la Secretaría de cualquier responsabilidad derivada del incumplimiento de las leyes aplicables.		Documento firmado por el representante legal.
	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.