MAD. Gustavo Arturo Leal Maya, Secretario de Finanzas del Poder Ejecutivo del Estado de Querétaro, en ejercicio de las facultades previstas por los artículos 3, 19 fracción II y 22 primer párrafo, fracción XLIII de la Ley Orgánica del Poder Ejecutivo del Estado de Querétaro; 6 de la Ley de Firma Electrónica Avanzada para el Estado de Querétaro; 17 y Tercero Transitorio del Reglamento de la Ley de Firma Electrónica Avanzada para el Estado de Querétaro; y 1, 4, párrafo tercero y 5 del Reglamento Interior de la Secretaría de Finanzas del Poder Ejecutivo del Estado de Querétaro; y

CONSIDERANDO

I. Que, con fecha 07 de enero de 2022, se publicó en el Periódico Oficial del Gobierno del Estado de Querétaro, "La Sombra de Arteaga" la Ley de Firma Electrónica Avanzada para el Estado de Querétaro, la cual, tiene por objeto regular y promover en el Estado de Querétaro, el uso de medios digitales, documentos electrónicos y Firma Electrónica Avanzada por parte de los sujetos de la misma para facilitar, agilizar y hacer más accesible los actos en que intervengan, la cual fue reformada mediante Ley publicada el 29 de noviembre de 2022 en el citado medio de difusión oficial.

II. Que, el 27 de enero de 2023, se publicó en el Periódico Oficial del Gobierno del Estado de Querétaro, "La Sombra de Arteaga", el Reglamento de la Ley de Firma Electrónica Avanzada para el Estado de Querétaro, el cual, tiene por objeto establecer las normas reglamentarias para el uso de la Firma Electrónica, los medios digitales, y demás medios electrónicos a los que se refiere la Ley de Firma Electrónica Avanzada para el Estado.

III. Que el artículo 18 de la Ley de Firma Electrónica Avanzada para el Estado de Querétaro establece que la Firma Electrónica Avanzada vincula de manera indubitable al firmante con un documento electrónico, sea ésta de página escrita con caracteres alfanuméricos, o archivo de imagen, video, audio o cualquier otro formato tecnológicamente disponible, el cual se asocia por medio de un dispositivo de creación de firma, con los datos que se encuentran exclusivamente bajo control del firmante y que expresan en medio digital su identidad.

A su vez, el numeral 17, fracciones I, II, III y IV de la Ley en cita prevé que para que una firma electrónica se considere fiable o avanzada debe cumplir por lo menos, con lo siguiente:

- Los Datos de Creación de la Firma, en el contexto en que son utilizados, corresponden exclusivamente al Firmante;

- Los Datos de Creación de la Firma al momento de la firma, se encontraban bajo el control exclusivo del Firmante;

- Es posible detectar cualquier alteración de la Firma Electrónica hecha después del momento de la firma, y

- Respecto a la integridad de la información, la Firma Electrónica Avanzada permite que sea posible detectar cualquier alteración que se realice en el documento firmado.

IV. Que, para dichos efectos, el interesado debe presentar una solicitud de emisión de Certificado de Firma Electrónica ante la Autoridad Certificadora, por lo que es menester

contar con disposiciones jurídicas que regulen los procedimientos, requisitos, formatos asociados al enrolamiento, generación y obtención de un Certificado.

V. Que, adicionalmente, los documentos electrónicos suscritos por medio de Firma Electrónica deben permitir verificar la integridad y autenticidad de éstos de conformidad con disposiciones de carácter general.

VI. Que el 21 de febrero de 2022, se publicó en el Periódico Oficial del Gobierno del Estado de Querétaro "La Sombra de Arteaga", el Plan Estatal de Desarrollo 2021-2027, en el cual se estableció como visión el incrementar el nivel institucional y de servicios a partir de una administración pública eficiente, suficiente y transparente. Para ello se consideró como un proyecto prioritario integrar, consolidar y desplegar todas las estrategias de desarrollo digital en la administración pública del estado, así como aprovechar de manera eficiente el uso de las Tecnologías de Información, para brindar más y mejores servicios digitales a los ciudadanos a través de un Gobierno moderno, transparente y cercano.

VII. Que dentro del Eje rector 6 Gobierno Ciudadano, del citado Plan, en el que se contempla el enfoque de las acciones de gobierno a través de, entre otros rubros, la creación de nuevas políticas públicas y de herramientas para acercar los servicios a la población, con el fin de asegurar la gobernanza y la gobernabilidad del estado, se establece como Objetivo 1, ser un gobierno ciudadano y de alto desempeño de cara a la sociedad, a cuyo efecto se establecen las líneas estratégicas relativas al fomento de la gestión, la eficiencia gubernamental y la mentalidad de servicio y la consolidación de un gobierno digital, previéndose las acciones concernientes al fortalecimiento de la mejora regulatoria en el estado, a la potenciación de la capacidad operativa y técnica de las instancias gubernamentales, a la integración de un ecosistema de información que facilite la coordinación entre las distintas dependencias de gobierno, el desarrollo de competencias digitales en los ciudadanos, las empresas y los servidores públicos, así como el avance en la digitalización de trámites y servicios.

VIII. Que, en términos del artículo 6 de la propia Ley de la materia, así como del Artículo Tercero Transitorio de su Reglamento, corresponde a la Secretaría de Finanzas emitir los instrumentos jurídicos necesarios que aseguren la correcta aplicación de la misma, así como la adecuada incorporación de la Firma Electrónica Avanzada a los actos objeto de la misma.

Por lo anteriormente expuesto, he tenido a bien expedir las siguientes:

DISPOSICIONES GENERALES DE LA LEY DE FIRMA ELECTRÓNICA AVANZADA PARA EL ESTADO DE QUERÉTARO

Objeto.

PRIMERA. - Las presentes Disposiciones Generales son aplicables a los sujetos previstos en las fracciones I, II, III, IV y último párrafo del artículo 3 de la Ley de Firma Electrónica Avanzada para el Estado de Querétaro y tienen por objeto establecer:

I. Los requisitos, procedimientos, estándares y mecanismos tecnológicos que deberán cumplirse para la emisión y revocación de los certificados digitales previstos en la Ley de Firma Electrónica Avanzada para el Estado de Querétaro y su Reglamento, así como la prestación de servicios relacionados con la Firma Electrónica Avanzada;

II. La estructura que deberán cumplir los certificados digitales que emita la Unidad de Firma Electrónica Avanzada en su carácter de Autoridad Certificadora del Estado de Querétaro;

III. Los requerimientos técnicos mínimos que permitan que los sistemas informáticos, así como las herramientas tecnológicas o aplicaciones a cargo de los sujetos a que se refiere el artículo 3 de la Ley de Firma Electrónica Avanzada para el Estado de Querétaro, puedan llevar a cabo el firmado y/o sellado de documentos electrónicos y, en su caso, mensajes de datos en la realización de los actos y actuaciones;

IV. La manera en que se llevará a cabo la conservación de los mensajes de datos y de los documentos electrónicos con Firma Electrónica Avanzada o con sello electrónico;

V. La forma y términos en que la Unidad de Firma Electrónica Avanzada proporcionará el servicio de consulta sobre el estado de validez y vigencia, de los certificados digitales que emita, y

VI. Cualquier otra acción relacionada con la Firma Electrónica Avanzada del Estado de Querétaro, que establezcan las disposiciones aplicables.

Definiciones y acrónimos.

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

I. **AC:** Autoridad Certificadora;

II. **Claves criptográficas:** La clave pública y la clave privada;

III. **CRL:** Registro de certificados que han sido revocados (CRL, Certificate Revocation List por sus siglas en inglés);

IV. **Disposiciones Generales:** Las Disposiciones Generales de la Ley de Firma Electrónica Avanzada para el Estado de Querétaro.

V. **HTTP:** Protocolo utilizado para el intercambio de información en Internet (Hyper Text Transfer Protocol, HTTP por sus siglas en inglés);

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

VII. **Ley:** Ley de Firma Electrónica Avanzada para el Estado de Querétaro;

VIII. **OCSP:** Protocolo de consulta en línea del estatus de un certificado, el cual permite conocer el estatus de revocación del certificado en tiempo real (OCSP, Online Certificate Status Protocol, por sus siglas en inglés);

IX. **OID:** Es el número que se asigna para identificar un objeto sin ambigüedad, el cual se conforma de acuerdo al estándar del Instituto Nacional Estadounidense de Estándares (ANSI American National Standards Institute) (OID, Object Identifier, por sus siglas en inglés);

X. **Reglamento:** Reglamento de la Ley de Firma Electrónica Avanzada para el Estado de Querétaro;

XI. **Secretaría:** La Secretaría de Finanzas del Poder Ejecutivo del Estado de Querétaro; y

XII. **UFEA:** Unidad de Firma Electrónica Avanzada de la Secretaría de Finanzas del Poder Ejecutivo del Estado de Querétaro.

Emisión de certificados.

TERCERA. - Para obtener un certificado de Firma Electrónica Avanzada, el interesado deberá acceder a la dirección electrónica https://firma.queretaro.gob.mx, o la que al efecto se determine por conducto de la Secretaría, y llenar los datos requeridos a que se refiere el artículo 17 del Reglamento, adjuntando la documentación correspondiente, siendo indispensables los siguientes:

I. Acta de nacimiento;

II. Clave Única de Registro de Población (CURP);

III. Registro Federal de Contribuyentes (RFC);

IV. Comprobante de domicilio; e

V. Identificación oficial con fotografía, ya sea credencial de elector, pasaporte o cédula profesional.

CUARTA. - Para llevar a cabo el registro de datos y verificación de elementos de identificación, así como la emisión, renovación y revocación de certificados digitales, el interesado deberá utilizar los formatos descritos en los anexos 1, 2, 3 y 4 de las presentes Disposiciones Generales, mismos que podrá obtener en la dirección electrónica referida.

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

a. RFC 5958 "*Asymmetric Key Packages*", para la creación de la clave privada;

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

c. RFC 5652 "*Cryptographic Message Syntax (CMS)*", para la descripción del formato del mensaje de datos del certificado digital.

Asimismo, el procedimiento a seguirse para llevar a cabo la captura de biométricos deberá realizarse conforme al Anexo 4 de las presentes Disposiciones Generales.

En el supuesto que los sujetos previstos en las fracciones I, II, IV y último párrafo del artículo 3 de la Ley, consideren necesario generar Certificados Digitales para los sujetos previstos en las fracciones III y V del referido precepto, a efecto de que éstos participen en sus procesos, trámites o servicios, deberán comunicarlo por escrito a la UFEA, con al menos treinta días naturales de anticipación a la fecha en la que estime comenzar a utilizar la firma electrónica avanzada en los mismos, a efecto de que esta última se pronuncie en el sentido de manifestar si, atendiendo a su impacto y volumetría, resulta viable y factible la emisión de los referidos Certificados.

Lo anterior será aplicable a los acuerdos, convenios o bases de colaboración, que celebre la Secretaría con los diferentes sujetos a que se refieren las fracciones II a V, y último párrafo del artículo 3 de la Ley, relativos a la implementación y uso de los Certificados Digitales.

Autoridad Certificadora Raíz.

QUINTA.- La Autoridad Certificadora Raíz del Gobierno del Estado de Querétaro, a fin de garantizar la seguridad y el entorno de confianza de los procesos que de ella derivan, se mantendrá fuera de línea. Por ello, generará Autoridades Intermedias que serán denominadas "Autoridad Emisora Ciudadana" a través de las cuales se les emitirán certificados digitales de firma electrónica avanzada a ciudadanos y funcionarios.

El certificado de la Autoridad Certificadora Raíz del Estado de Querétaro contendrá al menos los siguientes datos:

I. Número de Serie: Incorporará un número entero positivo;

II. AC: Identificará a la AC con un nombre distintivo (DN Distinguished Name) de tipo "Name" del estándar X.509 con los atributos siguientes:

ATRIBUTOS	TIPO	LONGITUD	DESCRIPCIÓN
Nombre común (CN)	PrintableString o UTF8String	64	AUTORIDAD CERTIFICADORA RAÍZ
Organización (O)	PrintableString o UTF8String	64	GOBIERNO DEL ESTADO DE QUERÉTARO
Unidad organizativa (OU)	PrintableString o UTF8String	64	SECRETARÍA DE FINANZAS
Dirección	PrintableString o UTF8String	128	Calle 5 de mayo, Col. Centro
Código Postal	PrintableString o UTF8String	40	76000

País(C)	PrintableString	2	MX
Estado (S)	PrintableString o UTF8String	128	QUERETARO
Localidad (L)	PrintableString o UTF8String	128	SANTIAGO DE QUERETARO
Nombre sin estructura	PrintableString o UTF8String	128	Responsable: Unidad de Firma Electrónica Avanzada adscrita a la Secretaría de Finanzas del Poder Ejecutivo del Estado de Querétaro

III. **Algoritmo de firma**: Contendrá el identificador del algoritmo criptográfico que es utilizado por la AC para firmar el certificado digital;

El algoritmo utilizado para firmar el certificado digital deberá ser SHA384 con RSA, mismo que se deberá usar tanto para la firma de la AC como para la del ciudadano, a fin de proveer un nivel adecuado de seguridad; y

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

La AC utilizará el formato UTCTime (YYMMDDHHMMSSZ).

Estructura de certificados de las Autoridades Emisoras y de ciudadanos.

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

I. **Número de Serie:** Incorporará un número entero positivo;

II. **AC que lo emitió:** Identificará a la AC con un nombre distintivo (DN *Distinguished Name*) de tipo "*Name*" del estándar X.509 con los atributos siguientes:

Atributos	Tipo	Longitud	Descripción
Nombre común(CN)	PrintableString o UTF8String	64	AUTORIDAD EMISORA CIUDADANA
Organización (O)	PrintableString o UTF8String	64	SECRETARÍA DE FINANZAS
Unidad organizativa (OU)	PrintableString o UTF8String	64	UNIDAD DE FIRMA ELECTRÓNICA AVANZADA

Correo electrónico	PrintableString o UTF8String	64	ac@queretaro.gob.mx
País(C)	PrintableString	2	MX
Estado (S)	PrintableString o UTF8String	128	QUERETARO
Localidad (L)	PrintableString o UTF8String	128	SANTIAGO DE QUERETARO
Nombre sin estructura	PrintableString o UTF8String	128	Responsable: Unidad de Firma Electrónica Avanzada adscrita a la Secretaría de Finanzas del Poder Ejecutivo del Estado de Querétaro

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

IV. El algoritmo utilizado para firmar el certificado digital deberá ser SHA384 con RSA, mismo que se deberá usar tanto para la firma de la AC como para la del ciudadano, a fin de proveer un nivel adecuado de seguridad;

V. **Vigencia:** Contendrá la fecha de inicio y la de término del periodo de validez del certificado digital.

La AC utilizará el formato UTCTime (YYMMDDHHMMSSZ);

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

Atributos	Tipo	Longitud	Descripción
Nombre común (CN)	UTF8String	64	Nombre del titular del certificado digital
Nombre	UTF8String	64	Nombre del titular del certificado digital
Empresa	UTF8String	64	Nombre del titular del certificado digital
Número de serie (SN)	PrintableString	64	CURP del titular del certificado digital
País (C)	PrintableString	2	País (MX)
Estado (S)	PrintableString	64	Estado (QUERÉTARO)
Identificador único X500 (2.5.4.45)	BIT STRING		CURP del titular del certificado digital

Correo electrónico (E)	IA5String	128	Correo electrónico del titular del certificado digital

VII. **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 los ciudadanos, y por lo menos de 4096 bits para certificados digitales de la Autoridad Certificadora Raíz.

VIII. **Requisitos adicionales:**

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

b) Extensiones: Contendrá la siguiente información:

Atributos	Tipo	Descripción
authorityKeyIdentifier	No crítica	Permite identificar la clave pública correspondiente a la clave privada que la AC utilizó para firmar el certificado digital. Usar sólo el campo KeyIdentifier, el cual debe contener los 384 bits del SHA-2 del valor subjectPublicKey del certificado digital de la AC.
subjectKeyIdentifier	No crítica	Asigna un identificador de la clave pública del titular del certificado digital. Debe contener los 384 bits del SHA-2 del valor subjectPublicKey.
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	Permite identificar si el certificado digital corresponde a una Autoridad Certificadora.
extendedKeyUsage	No crítica	Indica uno o más propósitos de uso.
cRLDistributionPoint	No crítica	Establece la dirección de consulta de la Lista de Certificados Revocados.
authorityInfoAccess	No crítica	Indica cómo acceder a la información de la AC y sus servicios, aquí debe indicarse como

		mínimo la dirección electrónica de consulta de la AC.
certificatePolicies	Crítica	OID asignado por la UFEA, quien deberá llevar un registro de los mismos.

Requerimientos técnicos para el firmado de documentos.

SÉPTIMA. - La UFEA pondrá a disposición de las dependencias, entidades y demás entes públicos del Estado un servicio electrónico de firma de documentos. Para ello, la UFEA emitirá los lineamientos de firma electrónica de documentos, así como el o los Documentos Técnicos de Interoperabilidad necesarios para la integración de las Unidades Administrativas a dicho servicio.

Los lineamientos de firma electrónica de documentos determinarán al menos los siguientes elementos:

1. Atributos de firma electrónica que deben presentarse de conformidad con el artículo 12 del Reglamento.

2. Estándares de firma implementados y aceptados.

3. Uso del sello digital de marcado cronológico.

4. Algoritmos criptográficos a utilizar.

5. Mecanismos de verificación de firma.

Las dependencias, entidades y demás entes públicos del Estado, podrán implementar sus propios mecanismos de firmado, siempre y cuando éstos atiendan a los lineamientos publicados por la UFEA, debiendo consultar, con anterioridad a la emisión de la firma, el estatus del certificado.

Requerimientos técnicos para la consulta del estatus de un certificado.

OCTAVA.- Las dependencias, entidades, y demás entes públicos del Estado, deberán verificar el estatus del certificado a través del servicio OCSP que provee la UFEA. Adicionalmente, deberán de contar con la infraestructura tecnológica necesaria para la consulta de dicho servicio considerando:

I. Contar con la Infraestructura necesaria (equipos de cómputo y conexión a internet).

II. Implementar procesos de validación y consulta basados en el protocolo de comunicación OCSP que permita a los usuarios consultar el estado del Certificado Digital.

III. Configurar sus servicios de comunicación de acuerdo al estándar RFC 6960 â X.509 *Internet Public Key Infrastructure Online Certificate Status Protocol* â OCSP.

Para utilizar el protocolo de comunicación OCSP, las dependencias, entidades y demás entes públicos del Estado, deben:

1. Verificar que el certificado digital presentado se encuentra vigente.

2. Evitar completar el proceso de firma o transacción sin antes verificar el estatus del certificado.

3. Realizar la consulta del estatus del certificado a partir del protocolo del OCSP.

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

5. Interpretar las respuestas firmadas de las consultas al servicio OCSP utilizando el certificado de la UFEA para aceptar y, en su caso, rechazar la solicitud si el certificado ha sido revocado y, por lo tanto, no es válido a pesar de su vigencia.

Conservación de mensajes de datos.

NOVENA.- La conservación de los mensajes de datos y de los documentos electrónicos firmados con Firma Electrónica Avanzada se regirá por la naturaleza de la documentación de acuerdo con las disposiciones legales aplicables y se deberá asegurar que se ha mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y sea accesible para su ulterior consulta; para tales efectos, la UFEA generará una constancia y un sello de marcado cronológico, apegados al estándar establecido en la norma oficial mexicana NOM-151-SCFI-2016. Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos.

DÉCIMA. - La UFEA debe cumplir con la "*Matriz de control de seguridad para autoridades certificadoras*" agregada en el anexo 6 de las presentes Disposiciones Generales, a fin de evitar la falsificación, alteración o uso indebido de los certificados digitales.

Asimismo, debe cumplir con generar la Política de Certificados con base en las especificaciones del RFC 3647 o del ETSI TS 102 042.

Servicio de consulta de certificados.

DÉCIMA PRIMERA. - La UFEA proporcionará el servicio de consulta sobre el estado de los certificados digitales expedidos por su Autoridad Certificadora, el cual deberá:

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

II. Utilizar mensajes codificados que deberán ser transmitidos sobre el protocolo HTTPS;

III. Firmar la respuesta a la solicitud de verificación del estado de revocación utilizando el certificado digital emitido específicamente con esa finalidad, el cual deberá contar con el atributo de *ocspSigning*;

IV. Mantener operando el servicio con una disponibilidad del 99.95%; y

V. Contar con una dirección electrónica para llevar a cabo la consulta correspondiente, a través del protocolo OCSP.

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

La verificación de validez se realizará mediante consulta que formulen a la UFEA, a través del servicio de OCSP o de la CRL de acuerdo con las características definidas por ésta.

DÉCIMA TERCERA.- La UFEA llevará un registro de los certificados digitales que emita, identificando aquellos que hayan sido revocados, los cuales se integrarán en una Lista de Certificados Revocados, misma que será publicada en la dirección electrónica http://crl.queretaro.gob.mx/AC-QROCiudadana.crl, al menos cada 6 horas y que deberá cumplir con lo siguiente:

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

II. Contener fecha y hora de su emisión;

III. Contener la fecha y hora de la siguiente emisión; y

IV. Ser firmada por la UFEA.

DÉCIMA CUARTA. - En términos de lo dispuesto por los artículos 9 y 32 del Reglamento, las dependencias y entidades públicas que utilicen la firma electrónica avanzada o el sello electrónico en su gestión, deberán llevar un padrón actualizado de los servidores públicos que se encuentren facultados para su uso, debiendo informar a la Unidad o a los órganos garantes en materia de transparencia u otras autoridades competentes sobre dicha situación cuando les sea requerido.

DÉCIMA QUINTA.- En caso de contingencia o no disponibilidad del servicio de consulta sobre el estado de validez de los certificados digitales a través del protocolo OCSP, las dependencias, entidades y demás entes públicos del Estado, podrán hacer uso de la última Lista de Certificados Revocados que la UFEA tenga disponible para su consulta en la dirección electrónica que haya destinado para esa finalidad, siempre y cuando dicha Lista de Certificados Revocados refleje el estado de validez de los certificados digitales hasta 6 horas antes del caso de contingencia o no disponibilidad del servicio.

En caso de que la contingencia incluya la dirección electrónica de publicación de la CRL, los sujetos interesados en el uso del certificado digital deberán suspender el proceso hasta en tanto no se encuentre disponible alguno de los mecanismos de verificación del estatus de revocación.

DÉCIMA SEXTA. - La interpretación para efectos administrativos de estas Disposiciones Generales, así como la resolución de los casos no previstos en las mismas, corresponderá a la Secretaría, a través de la UFEA.

Suspensión y Revocación de los certificados.

DÉCIMA SÉPTIMA. - El interesado podrá presentar su solicitud de suspensión o revocación del certificado emitido por la UFEA accediendo a la dirección electrónica https://firma.queretaro.gob.mx, debiendo en dicha solicitud hacer constar los hechos a que se refiere el artículo 22 del Reglamento y conforme al anexo 5 de las presentes Disposiciones Generales.

Para considerar válida su solicitud, la misma se deberá acompañarse de los siguientes datos:

1. Nombre completo.
2. CURP.
3. Número de serie del certificado.

La UFEA integrará el expediente correspondiente y valorará la información recibida. De considerarla procedente, revocará el certificado y emitirá en su caso el comprobante de revocación de certificado al interesado, pudiendo éste solicitar un nuevo certificado de conformidad con el procedimiento previsto en estas Disposiciones.

Con el fin de preservar la integridad del certificado y la seguridad respecto a su uso, la suspensión del certificado emitido por la UFEA conlleva la revocación del mismo, estando en posibilidad el interesado en todo momento de solicitar la emisión de un nuevo certificado, de conformidad con lo descrito en las Políticas de Certificación.

Uso de certificados expedidos por otras autoridades nacionales o extranjeras.

DÉCIMO OCTAVA. - En términos del artículo 27 de la Ley y 27 de su Reglamento, tratándose de certificados emitidos por otras autoridades nacionales o extranjeras, éstos producirán los mismos efectos jurídicos que un certificado expedido por la UFEA, siempre y cuando éstos presenten un grado de fiabilidad sustancialmente equivalente.

A efectos de determinar si un certificado presenta un grado de fiabilidad sustancialmente equivalente, la UFEA realizará un análisis técnico y tomará en consideración las normas internacionales reconocidas y cualquier otro factor pertinente, entre ellos, que cumpla con los principios a que se refiere el artículo 5 de la Ley.

Los certificados deberán observar el principio de neutralidad tecnológica, consistente en que la tecnología utilizada para la emisión de éstos no excluya, restrinja o favorezca alguna tecnología en particular.

De considerarlo procedente, la UFEA emitirá un dictamen técnico, a través del cual, se determine que el certificado cumple con un grado de fiabilidad sustancialmente equivalente y, por tanto, puede

ser utilizado por parte de las dependencias, entidades y demás entes públicos del Estado. En el citado dictamen se establecerán las condiciones bajo las cuales el certificado podrá ser utilizado.

DISPOSICIONES TRANSITORIAS

Primera.- Las presentes Disposiciones entrarán en vigor el día de su publicación en el Periódico Oficial del Gobierno del Estado de Querétaro, "La Sombra de Arteaga".

Segunda.- Las presentes Disposiciones serán aplicables a los sujetos previstos en el artículo 3, fracción V, de la Ley de Firma Electrónica Avanzada para el Estado de Querétaro, una vez que la Secretaría, a través de la UFEA, dictamine la viabilidad de la emisión de certificados digitales para dichos sujetos.

Dado en el Palacio de La Corregidora, sede del Poder Ejecutivo del Estado de Querétaro, en la Ciudad de Santiago de Querétaro, Qro., el día 29 (veintinueve) de agosto del 2023 (dos mil veintitrés).

MAD. Gustavo Arturo Leal Maya
Secretario de Finanzas
Poder Ejecutivo del Estado de Querétaro

ANEXO 1

SOLICITUD DE CERTIFICADO DIGITAL DE FIRMA ELECTRÓNICA AVANZADA

El suscrito, XXXXXXXXXX, con número de CURP XXXXXXXXXXXXXXX, manifiesto ante la Unidad de Firma Electrónica Avanzada dependiente de la Secretaría de Finanzas del Poder Ejecutivo del Estado Querétaro, en su carácter de Autoridad Certificadora, que es mi libre voluntad llevar a cabo el proceso de Solicitud de un Certificado Digital de Firma Electrónica Avanzada, para la obtención del archivo de certificado digital realizado ante esta Autoridad Certificadora, de conformidad con la Ley de Firma Electrónica Avanzada para el Estado de Querétaro, su Reglamento y demás disposiciones legales aplicables a la materia, por lo cual, he proporcionado los datos que me han sido requeridos a través del Sistema de Interacción, mismos que se presentan en este documento y respecto de los cuales manifiesto mi conformidad.

1. Clave Única de Registro de Población del solicitante:

_____

2. Primer apellido Segundo apellido Nombre(s):

_____

Primer apellido Segundo apellido Nombre(s)

3. Domicilio del solicitante:

Calle: _____ Número Exterior: _____

Número interior: _____ Colonia _____

Código Postal: _____ Ciudad: _____

Estado: _____

4. Documento de identidad vigente presentado:

Cartilla del Servicio Militar Nacional
Pasaporte expedido por la Secretaría de Relaciones Exteriores
Cédula profesional
Credencial de elector
Identificación expedida por el Gobierno Federal, Estatal o Municipal, que cuente con fotografía, firma y CURP del titular

5. Documento probatorio de identidad vigente que presenta:

Copia certificada del acta de nacimiento o documento migratorio
Carta de naturalización
Certificado de nacionalidad mexicana

Firma del solicitante:

_____

FECHA: XXXXXXXXX

ANEXO 2

COMPROBANTE DE EMISIÓN DE CERTIFICADO DIGITAL DE FIRMA ELECTRÓNICA AVANZADA.

La Unidad de Firma Electrónica Avanzada del Estado de Querétaro adscrita a la Secretaría de Finanzas, en su carácter de Autoridad Certificadora para la emisión de Certificados Digitales de Firma Electrónica Avanzada, certifica que el Solicitante:

XXXXXXXXXX, con número de CURP XXXXXXXXXXXXXX, generó un requerimiento de certificación que contiene la solicitud para la creación de su Certificado Digital de Firma Electrónica Avanzada.

Estando presente el Solicitante se llevó a cabo el procedimiento de emisión y registro de certificados digitales de conformidad con lo establecido en la Ley de Firma Electrónica Avanzada para el Estado de Querétaro, su Reglamento, y los Lineamientos aplicables a la implementación y uso de la Firma Electrónica Avanzada en el Estado de Querétaro.

Asimismo, que como resultado del proceso se generó su Certificado Digital con número de serie: XXXXXXXX y clave pública: XXXXXXXXXXXX.

Previo a la emisión del presente certificado, el titular reconoce haber leído y aceptado los términos y condiciones de uso anexos al formato "Solicitud de Certificado Digital de Firma Electrónica Avanzada".

Asimismo, acepta la responsabilidad en caso de presentarse cualquier situación que pudiera implicar la reproducción o el uso indebido del Certificado Digital de Firma Electrónica Avanzada en tanto no sea revocado.

El resguardo de la clave privada relacionada con el certificado amparado por el presente Acuse, así como su medio de almacenamiento, es responsabilidad del titular del Certificado Digital de Firma Electrónica Avanzada.

Firma de conformidad
Nombre: XXXXXXXXXX
CURP: XXXXXXXXXX

Unidad de Firma Electrónica Avanzada de la Secretaría de Finanzas del Poder Ejecutivo del Estado de Querétaro a <poner fecha aquí>
NOTA: Para descargar posteriormente su certificado digital, deberá acceder a la dirección electrónica: https://firma.queretaro.gob.mx

ANEXO 3
ACUERDO DE TITULAR DE SELLO DIGITAL

• El suscrito, XXXXXXXXXXXXXXXX, con número de CURP, XXXXXXXXXXX, a quien en lo sucesivo se le denominará como "El Solicitante" para todos los efectos legales que deriven del presente documento, manifiesta ante la Unidad de Firma Electrónica Avanzada adscrita a la Secretaría de Finanzas del Poder Ejecutivo del Estado de Querétaro, en su carácter de Autoridad Certificadora, a quien en lo sucesivo se le denominará como "La Autoridad Certificadora" (AC), que es su libre voluntad contar con un Sello Digital en el que conste la clave pública que se encuentra asociada a la clave privada y frase de seguridad que manifiesta haber generado previamente y en absoluto secreto.

• Asimismo manifiesta su conformidad para que la "AC" genere un sello digital autofirmado con la firma electrónica avanzada que ha recibido con anterioridad.

• La "AC" manifiesta que los datos personales recabados de "El Solicitante" durante su comparecencia serán protegidos, incorporados y tratados en el Sistema de Interacción, de conformidad con la Ley de Firma Electrónica Avanzada para el Estado de Querétaro, su Reglamento y demás disposiciones legales aplicables, cuya finalidad es garantizar el vínculo que existe entre un Certificado Digital de Firma Electrónica Avanzada y Sello Digital.

• La Unidad Administrativa responsable de este sistema es la Unidad de Firma Electrónica Avanzada en su carácter de Autoridad Certificadora. "El Solicitante" podrá ejercer los Derechos de Acceso, Rectificación Cancelación y Oposición (ARCO) directamente a través de la Unidad de Transparencia del Poder Ejecutivo del Estado de Querétaro, en su portal http://bit.ly/2z7HBf6, al correo electrónico utpe@queretaro.gob.mx o en el buzón instalado en la entrada al edificio donde se ubica la Unidad de Transparencia.

• "El Solicitante" acepta el sello digital mencionado, valiendo este documento como el acuse de recibo más amplio que en derecho proceda.

• **"El Solicitante", acepta que el uso de la clave privada y frase de seguridad con base en las cuales dicho sello digital fue elaborado, quedarán bajo su estricta y absoluta responsabilidad**, la cual incluye en forma enunciativa, mas no limitativa, los daños y perjuicios, incluso aquellos de carácter financiero, que pudieran causarse por su uso indebido, no pudiendo alegar que tal uso se realizó por persona no autorizada.

• "El Solicitante" reconoce y acepta que la clave pública proporcionada por él y contenida en el Sello Digital, será de carácter público y podrá ser consultada libremente por cualquier interesado a través de los medios y formas que disponga la "AC".

• "El Solicitante" se obliga a mantener absoluta confidencialidad respecto de las clave privada y frase de seguridad, así como a realizar los trámites necesarios para la revocación de dicho certificado ante la "AC", mediante los mecanismos y procedimientos que el mismo establezca, en el evento de que por cualquier causa dicha información sea divulgada o se realice cualquier

supuesto por el que "El Solicitante" deba solicitar su revocación de conformidad con las disposiciones legales vigentes.

•"El Solicitante" manifiesta conocer el contenido y alcance de las disposiciones legales y reglamentarias relativas a la celebración de actos jurídicos mediante el uso de medios electrónicos, digitales o de cualquier otra tecnología, por lo que asume plena responsabilidad respecto de la información y contenido de todo documento electrónico o digital elaborado y enviado en el que se haga uso de la clave privada, toda vez que por ese solo hecho se considerará que el documento electrónico o digital le es atribuible.

CONDICIONES DE USO Y RESPONSABILIDAD DEL TITULAR:

• El Sello Electrónico previsto en el artículo 4, fracción XX de la Ley, y 32 de su Reglamento asignado a los funcionarios públicos del Estado de Querétaro es personal e intransferible y su uso es responsabilidad de la persona que lo solicita.

• El Sello Electrónico vincula la identidad legal de "El Solicitante", así como su relación directa con la Unidad Administrativa en la que presta sus servicios y se encuentra asociada a las facultades que le han sido otorgadas.

• El Sello Electrónico posee los mismos alcances y efectos que la firma autógrafa para la emisión de actos y resoluciones administrativas.

• El Sello Electrónico permite emitir resoluciones administrativas para los servicios y trámites electrónicos disponibles por el Gobierno del Estado de Querétaro.

• "El Solicitante" será responsable de las obligaciones derivadas del uso no autorizado de su sello electrónico.

• "El Solicitante" acepta que deberá notificar a "La AC", la invalidación, pérdida o cualquier otra situación que pudiera implicar la reproducción o uso indebido de su clave privada.

• "El Solicitante" acepta las condiciones de operación y límites de responsabilidad de la Unidad de Firma Electrónica Avanzada en su calidad de "La AC" que se encuentran disponibles en la dirección electrónica https://firma.queretaro.gob.mx para su consulta.

Firma de "El Solicitante"

Fecha: XXXXXXX

ANEXO 4

ACUERDO DE USUARIO DEL CERTIFICADO

El suscrito, XXXXXXXXXXXXXXXX, con número de CURP XXXXXXXXXXXXX, a quien en lo sucesivo se le denominará como "El Solicitante" para todos los efectos legales que deriven del presente documento, manifiesta ante la Unidad de Firma Electrónica Avanzada adscrita a la Secretaría de Finanzas, en su carácter de Autoridad Certificadora, a quien en lo sucesivo se le denominará como "La Autoridad Certificadora" (AC), que es su libre voluntad contar con un Certificado Digital de Firma Electrónica Avanzada en el que conste la clave pública que se encuentra asociada a la clave privada y frase de seguridad que manifiesta haber generado previamente y en absoluto secreto. Asimismo, manifiesta su conformidad en que "La AC" utilice el procedimiento de certificación de identidad de conformidad con la Ley de Firma Electrónica Avanzada para el Estado de Querétaro, su Reglamento y demás disposiciones legales aplicables

La "AC" manifiesta que los datos personales recabados de "El Solicitante" durante su comparecencia serán protegidos, incorporados y tratados en el Sistema de Interacción, con fundamento en el artículo 33 de la Ley de Firma Electrónica Avanzada para el Estado de Querétaro, 17 y 19 de su Reglamento, cuya finalidad es garantizar el vínculo que existe entre un Certificado Digital de Firma Electrónica Avanzada y su titular.

• La Unidad Administrativa responsable de este sistema es la Unidad de Firma Electrónica Avanzada en su carácter de Autoridad Certificadora. "El Solicitante" podrá ejercer los Derechos de Acceso, Rectificación Cancelación y Oposición (ARCO) directamente a través de la Unidad de Transparencia del Poder Ejecutivo del Estado de Querétaro, en su portal http://bit.ly/2z7HBf6, al correo electrónico utpe@queretaro.gob.mx o en el buzón instalado en la entrada al edificio donde se ubica la Unidad de Transparencia.

• "El Solicitante" reconoce que para la emisión del referido Certificado Digital de Firma Electrónica Avanzada, la "AC" revisó la documentación requerida de conformidad con el artículo 19 del Reglamento de la Ley de Firma Electrónica Avanzada para el Estado de Querétaro y Tercera de las Disposiciones Generales de la Ley de Firma Electrónica del Estados de Querétaro, con la cual se identificó, verificando a simple vista que los documentos corresponden a los rasgos fisonómicos y caligráficos de "El Solicitante", por lo que este último asume la responsabilidad exclusiva respecto de la autenticidad de los datos y documentación por él proporcionada a la "AC". De la misma forma "El Solicitante" asume la responsabilidad exclusiva del debido uso del Certificado Digital de Firma Electrónica Avanzada.

"El Solicitante" en este acto acepta el certificado digital mencionado, sirviendo este documento como el acuse de recibo más amplio que en derecho proceda.

"El Solicitante", acepta que el uso de la clave privada y frase de seguridad, en las cuales dicho certificado fue elaborado, quedarán bajo su estricta y absoluta responsabilidad, la cual incluye en

forma enunciativa, mas no limitativa los daños y perjuicios, incluso aquellos de carácter financiero, que pudieran causarse por su uso indebido, no pudiendo alegar que tal uso se realizó por persona no autorizada.

"El Solicitante" reconoce y acepta que la clave pública proporcionada por él y contenida en el Certificado Digital de Firma Electrónica Avanzada, así como en cualquier otro certificado digital que con posterioridad se obtenga, será de carácter público y podrá ser consultada libremente por cualquier interesado a través de los medios y formas que disponga la "AC".

"El Solicitante" se obliga a mantener absoluta confidencialidad respecto de las clave privada y frase de seguridad, así como a realizar los trámites necesarios para la revocación de dicho certificado ante la "AC", mediante los mecanismos y procedimientos que se establezcan, en el evento de que por cualquier causa dicha información sea divulgada o se realice cualquier supuesto por el que "El Solicitante" deba solicitar su revocación en los términos de las disposiciones legales vigentes.

"El Solicitante" declara conocer el contenido y alcance de las disposiciones legales y reglamentarias relativas a la celebración de actos jurídicos mediante el uso de medios electrónicos, digitales o de cualquier otra tecnología, por lo que asume plena responsabilidad respecto de la información y contenido de todo documento electrónico o digital elaborado y enviado en el que se haga uso de la citada clave privada, toda vez que por ese solo hecho se considerará que el documento electrónico o digital le es atribuible.

"El Solicitante" reconoce y acepta que la "AC" únicamente es responsable de los errores que, en su caso, llegare a cometer con motivo de culpa grave en el proceso de generación, registro, entrega y revocación del certificado digital, según corresponda, así como que no será responsable por los daños y perjuicios que se pudieran causar a "El Solicitante" o a terceros, cuando por caso fortuito o fuerza mayor no puedan realizarse registros, verificaciones, revocaciones o tramitar documentos electrónicos cifrados con las claves públicas y privadas relacionadas con dicho certificado. Por caso fortuito o fuerza mayor se entenderá todo acontecimiento o circunstancia inevitable, más allá del control razonable de la "AC", que le impida el cumplimiento de sus funciones con el carácter que le corresponde y reconoce a través de su firma autógrafa asentada en la Solicitud como prueba fehaciente de la aceptación de todo lo especificado.

CONDICIONES DE USO Y RESPONSABILIDAD DEL TITULAR:

- La Firma Electrónica Avanzada asignada es personal e intransferible y el uso de la misma es responsabilidad de la persona que la solicite.
- La Firma Electrónica Avanzada vincula la identidad legal de "El Solicitante".
- La Firma Electrónica Avanzada tiene los mismos alcances y efectos que la firma autógrafa.
- Mediante la Firma Electrónica Avanzada, será posible hacer uso de servicios y trámites electrónicos disponibles en principio a cargo del Poder Ejecutivo del Estado de Querétaro y conforme se adhieran al esquema del resto de los Poderes del Estado, de sus Órganos Autónomos y Municipios.
- "El Solicitante" será responsable de las obligaciones derivadas del uso no autorizado de su firma.
- "El Solicitante" acepta que deberá notificar a la "AC", la invalidación, pérdida o cualquier otra situación que pudiera implicar la reproducción o uso indebido de su clave privada.

• "El Solicitante" acepta las condiciones de operación y límites de responsabilidad de la Unidad de Firma Electrónica Avanzada en su calidad de "AC" que se encuentran disponibles en la dirección electrónica https://firma.queretaro.gob.mx para su consulta.

Firma de "El Solicitante"

Fecha: XXXXXXX

ANEXO 5

SOLICITUD DE REVOCACIÓN DE CERTIFICADO DIGITAL DE FIRMA ELECTRÓNICA AVANZADA

El suscrito, XXXXXXXXXX, con número de CURP XXXXXXXXXXXXXXX, manifiesto ante la Unidad de Firma Electrónica Avanzada dependiente de la Secretaría de Finanzas del Poder Ejecutivo del Estado Querétaro en su carácter de Autoridad Certificadora, que es mi libre voluntad llevar a cabo el proceso de Revocación de mi Certificado Digital de Firma Electrónica Avanzada con número de serie XXXXXX, generado por esta Autoridad Certificadora, de conformidad con la Ley de Firma Electrónica Avanzada para el Estado de Querétaro, su Reglamento y demás disposiciones legales aplicables, para lo cual proporciono los siguientes datos:

1. Clave Única de Registro de Población del solicitante:

---

2. Primer apellido Segundo apellido Nombre(s):

Primer apellido Segundo apellido Nombre(s)

Firma del solicitante:

FECHA: XXXXXXXXX

ANEXO 6 DISPOSICIONES GENERALES

Matriz de gestión de seguridad de la Información	
Nombre del documento:	Declaración de aplicabilidad - Controles de Seguridad de la AC del Estado
Versión	1.0.0

INFORMACIÓN DE LA ENTIDAD			
Nombre de la entidad	Unidad de Firma Electrónica Avanzada del Estado de Querétaro		
Nombre de quien elabora			
Cargo		Dependencia	Secretaría de Finanzas
Fecha de elaboración			

Declaración de Aplicabilidad

RL: requerimientos legales, OA: obligaciones adminsitrativas, RN/MP: requerimientos del negocio/mejores prácticas adoptadas , AR: resultado de la valoración de riesgos

ISO 27001:2013 Controles de Seguridad			Controles Actuales	Aplicabilidad del control	Aspectos del control o justificación de la exclusión	Razones de selección del control				Tipo soporte	Formato del soporte	Ubicación del soporte
Cláusula	Sección	Objetivo de Control / Control				RL	OA	RN/MP	AR			
A.5 Políticas de seguridad de la información	5.1	Dirección de la Alta Gerencia para la Seguridad de la Información										
	5.1.1	Políticas de Seguridad de la Información		..*		NO	SI	SI	NO	..*	..*	
	5.1.2	Revisión de las Políticas de Seguridad de la Información		..*		..*	..*	..*	..*	..*	..*	
A.6 Organización de la seguridad de la información	6.1	Organización Interna										
	6.1.1	Roles y Responsabilidad para la Seguridad de la Información		..*		..*	..*	..*	..*	..*	..*	
	6.1.2	Separación de deberes		..*		..*	..*	..*	..*	..*	..*	
	6.1.3	Contacto con las autoridades		..*		..*	..*	..*	..*	..*	..*	
	6.1.4	Contacto con grupos de interés especial		..*		..*	..*	..*	..*	..*	..*	
	6.1.5	Seguridad de la información en la gestión de proyectos		..*		..*	..*	..*	..*	..*	..*	
	6.2	Dispositivos móviles y teletrabajo										
	6.2.1	Política de dispositivos móviles		..*		..*	..*	..*	..*	..*	..*	
	6.2.2	Teletrabajo		..*		..*	..*	..*	..*	..*	..*	
A.7 Seguridad de los recursos humanos	7.1	Previo al Empleo										
	7.1.1	Verificación de antecedentes		..*		..*	..*	..*	..*	..*	..*	
	7.1.2	Términos y condiciones del empleo		..*		..*	..*	..*	..*	..*	..*	
	7.2	Durante el Empleo										
	7.2.1	Responsabilidades de la Alta Gerencia		..*		..*	..*	..*	..*	..*	..*	
	7.2.2	Conciencia, educación y entrenamiento de Seguridad de la Información		..*		..*	..*	..*	..*	..*	..*	
	7.2.3	Proceso disciplinario		..*		..*	..*	..*	..*	..*	..*	
	7.3	Terminación y Cambio de Empleo										
	7.3.1	Termino de responsabilidades o cambio de empleo		..*		..*	..*	..*	..*	..*	..*	
A.8 Gestión de activos	8.1	Responsabilidad de los Activos										
	8.1.1	Inventario de activos		..*		..*	..*	..*	..*	..*	..*	
	8.1.2	Propiedad de activos		..*		..*	..*	..*	..*	..*	..*	
	8.1.3	Uso aceptable de los activos		..*		..*	..*	..*	..*	..*	..*	
	8.1.4	Devolución de activos		..*		..*	..*	..*	..*	..*	..*	
	8.2	Clasificación de la Información										
	8.2.1	Clasificación de la información		..*		..*	..*	..*	..*	..*	..*	
	8.2.2	Etiquetado de la información		..*		..*	..*	..*	..*	..*	..*	
	8.2.3	Manejo de activos		..*		..*	..*	..*	..*	..*	..*	
	8.3	Manejo de Medios										
	8.3.1	Gestión de medios removibles		..*		..*	..*	..*	..*	..*	..*	
	8.3.2	Eliminación de medios		..*		..*	..*	..*	..*	..*	..*	
	8.3.3	Transferencia de medios físicos		..*		..*	..*	..*	..*	..*	..*	
A.9 Control de acceso	9.1	Requerimientos de Negocio para el Control de Acceso										
	9.1.1	Política de control de acceso		..*		..*	..*	..*	..*	..*	..*	
	9.1.2	Uso de servicios de red		..*		..*	..*	..*	..*	..*	..*	
	9.2	Gestión de Accesos de Usuario										
	9.2.1	Registro y baja del usuario		..*		..*	..*	..*	..*	..*	..*	
	9.2.2	Suministro de acceso de usuarios		..*		..*	..*	..*	..*	..*	..*	
	9.2.3	Gestión de privilegios		..*		..*	..*	..*	..*	..*	..*	
	9.2.4	Gestión de información de autenticación secreta de usuarios		..*		..*	..*	..*	..*	..*	..*	
	9.2.5	Revisión de derechos de acceso de usuarios		..*		..*	..*	..*	..*	..*	..*	
	9.2.6	Eliminación o ajuste de derechos de acceso		..*		..*	..*	..*	..*	..*	..*	
	9.3	Responsabilidades del Usuario										
	9.3.1	Uso de información de autenticación secreta		..*		..*	..*	..*	..*	..*	..*	
	9.4	Control de Acceso de Sistemas y Aplicaciones										
	9.4.1	Restricción de acceso a la información		..*		..*	..*	..*	..*	..*	..*	
	9.4.2	Conexión segura		..*		..*	..*	..*	..*	..*	..*	
	9.4.3	Sistema de gestión de contraseñas		..*		..*	..*	..*	..*	..*	..*	
	9.4.4	Uso de programas y utilidades privilegiadas		..*		..*	..*	..*	..*	..*	..*	
	9.4.5	Control de acceso al código fuente del programa		..*		..*	..*	..*	..*	..*	..*	
A.10 Criptografía	10.1	Controles Criptográficos										
	10.1.1	Política en el uso de controles criptográficos		..*		..*	..*	..*	..*	..*	..*	
	10.1.2	Gestión de llaves		..*		..*	..*	..*	..*	..*	..*	
A.11 Seguridad física y del entorno	11.1	Áreas Seguras										
	11.1.1	Perímetro de seguridad físico		..*		..*	..*	..*	..*	..*	..*	
	11.1.2	Controles físicos de entrada		..*		..*	..*	..*	..*	..*	..*	
	11.1.3	Seguridad de oficinas, habitaciones y facilidades		..*		..*	..*	..*	..*	..*	..*	
	11.1.4	Protección contra amenazas externas y del ambiente		..*		..*	..*	..*	..*	..*	..*	
	11.1.5	Trabajo en áreas seguras		..*		..*	..*	..*	..*	..*	..*	
	11.1.6	Áreas de entrega y carga		..*		..*	..*	..*	..*	..*	..*	
	11.2	Equipo										
	11.2.1	Instalación y protección de equipo		..*		..*	..*	..*	..*	..*	..*	
	11.2.2	Servicios de suministro		..*		..*	..*	..*	..*	..*	..*	
	11.2.3	Seguridad en el cableado		..*		..*	..*	..*	..*	..*	..*	
	11.2.4	Mantenimiento de equipos		..*		..*	..*	..*	..*	..*	..*	
	11.2.5	Retiro de activos		..*		..*	..*	..*	..*	..*	..*	
	11.2.6	Seguridad del equipo y activos fuera de las instalaciones		..*		..*	..*	..*	..*	..*	..*	
	11.2.7	Disposición segura o reutilización de equipos		..*		..*	..*	..*	..*	..*	..*	
	11.2.8	Equipo de usuario desatendido		..*		..*	..*	..*	..*	..*	..*	
	11.2.9	Política de escritorio limpio y pantalla limpia		..*		..*	..*	..*	..*	..*	..*	
	12.1	Procedimientos Operacionales y Responsabilidades										
	12.1.1	Documentación de procedimientos operacionales		..*		..*	..*	..*	..*	..*	..*	
	12.1.2	Gestión de cambios		..*		..*	..*	..*	..*	..*	..*	

ANEXO 6 DISPOSICIONES GENERALES

	12.1.3	Gestión de la capacidad		...*		...*	...*	...*	...*	...*	...*	
	12.1.4	Separación de los ambientes de desarrollo, pruebas y operación		...*		...*	...*	...*	...*	...*	...*	
	12.2	Protección de Software Malicioso										
	12.2.1	Controles contra software malicioso		...*		...*	...*	...*	...*	...*	...*	
	12.3	Respaldo										
	12.3.1	Respaldo de información		...*		...*	...*	...*	...*	...*	...*	
	12.4	Registro y Monitoreo										
A.12 Seguridad de las Operaciones	12.4.1	Registro de eventos		...*		...*	...*	...*	...*	...*	...*	
	12.4.2	Protección de registros de información		...*		...*	...*	...*	...*	...*	...*	
	12.4.3	Registros de Administrador y Operador		...*		...*	...*	...*	...*	...*	...*	
	12.4.4	Sincronización de relojes		...*		...*	...*	...*	...*	...*	...*	
	12.5	Control de Software Operacional										
	12.5.1	Instalación de software en sistemas operacionales		...*		...*	...*	...*	...*	...*	...*	
	12.6	Gestión de Vulnerabilidades Técnicas										
	12.6.1	Gestión de vulnerabilidades técnicas		...*		...*	...*	...*	...*	...*	...*	
	12.6.2	Restricciones en la instalación de software		...*		...*	...*	...*	...*	...*	...*	
	12.7	Consideraciones de Auditoria de Sistemas de información										
	12.7.1	Controles de Auditoría de Sistemas de Información		...*		...*	...*	...*	...*	...*	...*	
	13.1	Gestión de Seguridad en Red										
	13.1.1	Controles de red		...*		...*	...*	...*	...*	...*	...*	
	13.1.2	Seguridad de los servicios en red		...*		...*	...*	...*	...*	...*	...*	
	13.1.3	Segregación en redes		...*		...*	...*	...*	...*	...*	...*	
A.13 Seguridad de las comunicaciones	13.2	Transferencia de Información										
	13.2.1	Políticas y procedimientos para la transferencia de información		...*		...*	...*	...*	...*	...*	...*	
	13.2.2	Acuerdos en la transferencia de información		...*		...*	...*	...*	...*	...*	...*	
	13.2.3	Mensajería electrónica		...*		...*	...*	...*	...*	...*	...*	
	13.2.4	Acuerdos de confidencialidad o no-revelación		...*		...*	...*	...*	...*	...*	...*	
	14.1	Requerimientos de Seguridad de Sistemas de Información										
	14.1.1	Análisis y especificación de requerimientos de seguridad		...*		...*	...*	...*	...*	...*	...*	
	14.1.2	Aseguramiento de servicios de aplicación en redes públicas		...*		...*	...*	...*	...*	...*	...*	
	14.1.3	Protección de transacciones de servicios de aplicación		...*		...*	...*	...*	...*	...*	...*	
	14.2	Seguridad en el Proceso de Desarrollo y Soporte										
	14.2.1	Política de desarrollo seguro		...*		...*	...*	...*	...*	...*	...*	
	14.2.2	Procedimientos de control de cambios		...*		...*	...*	...*	...*	...*	...*	
A.14 Adquisición, desarrollo y mantenimiento de sistemas	14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa		...*		...*	...*	...*	...*	...*	...*	
	14.2.4	Restricción de cambios a paquetes de software		...*		...*	...*	...*	...*	...*	...*	
	14.2.5	Procedimientos de construcción de sistemas seguros		...*		...*	...*	...*	...*	...*	...*	
	14.2.6	Entorno de desarrollo seguro		...*		...*	...*	...*	...*	...*	...*	
	14.2.7	Desarrollo tercerizado		...*		...*	...*	...*	...*	...*	...*	
	14.2.8	Pruebas de seguridad del sistema		...*		...*	...*	...*	...*	...*	...*	
	14.2.9	Pruebas de aceptación del sistema		...*		...*	...*	...*	...*	...*	...*	
	14.3	Datos de Prueba										
	14.3.1	Protección de datos de prueba		...*		...*	...*	...*	...*	...*		
	15.1	Seguridad en Relaciones con el Proveedor										
	15.1.1	Política de Seguridad de la Información para relaciones con proveedores		...*		...*	...*	...*	...*	...*	...*	
A.15 Relaciones con los proveedores	15.1.2	Atención de tópicos de seguridad dentro de los acuerdos con proveedores		...*		...*	...*	...*	...*	...*	...*	
	15.1.3	Cadena de suministros de TIC		...*		...*	...*	...*	...*	...*	...*	
	15.2	Gestión de Entrega de Servicios de Proveedor										
	15.2.1	Monitoreo y revisión de servicios de proveedor		...*		...*	...*	...*	...*	...*	...*	
	15.2.2	Gestión de cambios a servicios de proveedor		...*		...*	...*	...*	...*	...*	...*	
	16.1	Gestión de Incidentes de Seguridad de la Información y Mejoras										
	16.1.1	Responsabilidades y Procedimientos		...*		...*	...*	...*	...*	...*	...*	
	16.1.2	Reporte de eventos de Seguridad de la Información		...*		...*	...*	...*	...*	...*	...*	
A.16 Gestión de incidentes de seguridad de la información	16.1.3	Reporte de debilidades de Seguridad de la Información		...*		...*	...*	...*	...*	...*	...*	
	16.1.4	Valoración y decisión de eventos de Seguridad de la Información		...*		...*	...*	...*	...*	...*	...*	
	16.1.5	Respuesta a incidentes de Seguridad de la Información		...*		...*	...*	...*	...*	...*	...*	
	16.1.6	Aprendizaje de incidentes de Seguridad de la Información		...*		...*	...*	...*	...*	...*	...*	
	16.1.7	Recolección de evidencia		...*		...*	...*	...*	...*	...*	...*	
	17.1	Seguridad de la Información en la Continuidad										
	17.1.1	Planeación de Seguridad de la Información en la continuidad		...*		...*	...*	...*	...*	...*	...*	
A.17 Aspectos de seguridad de la información de la gestión de continuidad de negocio	17.1.2	Implementación de Seguridad de la Información en la continuidad		...*		...*	...*	...*	...*	...*	...*	
	17.1.3	Verificación, revisión y evaluación de Seguridad de la Información en la continuidad		...*		...*	...*	...*	...*	...*	...*	
	17.2	Redundancias										
	17.2.1	Disponibilidad de facilidades de procesamiento de información		...*		...*	...*	...*	...*	...*	...*	
	18.1	Cumplimiento con Requerimientos Legales y Contractuales										
	18.1.1	Identificación de legislación aplicable y requerimientos contractuales		...*		...*	...*	...*	...*	...*	...*	

ANEXO 6 DISPOSICIONES GENERALES

A.18 Cumplimiento	18.1.2	Derechos de propiedad intelectual (IPR)		..*		..*	..*	..*	..*	..*	..*	
	18.1.3	Protección de información documentada		..*		..*	..*	..*	..*	..*	..*	
	18.1.4	Privacidad y protección de información personal identificable		..*		..*	..*	..*	..*	..*	..*	
	18.1.5	Regulación de controles criptográficos		..*		..*	..*	..*	..*	..*	..*	
	18.2	Revisiones de Seguridad de la Información										
	18.2.1	Revisión independiente de Seguridad de la Información		..*		..*	..*	..*	..*	..*	..*	
	18.2.2	Cumplimiento con políticas y estándares de seguridad		..*		..*	..*	..*	..*	..*	..*	
	18.2.3	Inspección de cumplimiento técnico		..*		..*	..*	..*	..*	..*	..*	

Revisó:		Aprobó:	