UNACAR

Universidad Autónoma del Carmen

"Por la Grandeza de México"

Reglamento de uso y operación de la Firma Electrónica Avanzada de la Universidad Autónoma del Carmen

GACETA UNIVERSITARIA
Órgano Informativo de la Unacar

CONFRATERNIDAD UNIVERSITARIA PARA LA EXCELENCIA

Gaceta No. 299
Abril 2019

Reglamento de uso y operación de la Firma Electrónica Avanzada de la Universidad Autónoma del Carmen

UNACAR
Universidad Autónoma del Carmen
"Por la Grandeza de México"

Mtra. María Candelaria Figueroa Guzmán

Índice

Antecedentes

Las tecnologías de información y la comunicación (TIC) han generado transformaciones estructurales de tipo económico y social en todo el mundo. Están presentes en prácticamente todas las actividades humanas y hoy en día, representan un elemento táctico que proporciona soporte a los principales servicios universitarios, pero a corto plazo, están llamadas a convertirse en un elemento estratégico para las Instituciones de Educación Superior.

Conscientes de lo anterior, la Universidad Autónoma del Carmen (UNACAR) decidió apostar desde hace algunos años por la sistematización de procesos mediante la creación de un Sistema Integral de Información Administrativa (SIIA).

En el mismo sentido se planteó en el sexto eje del Plan de Desarrollo Institucional (PDI) 2013-2017 "Gobierno y gestión eficiente, eficaz y pertinente", el impulsar el fortalecimiento de los procesos de gestión a través de la automatización y el desarrollo de sistemas de información, por lo que el SIIA es de vital importancia para impulsar el plan.

Como parte del proceso de mejora continua y en el marco del uso de las tecnologías de la información en los procesos académicos y administrativos, se propuso iniciar la transición hacia un esquema donde todos los documentos de archivo se generen y conserven en medios electrónicos, en adición al resguardo del documento original en papel solo aplicará para aquellos documentos que establece la normatividad aplicable; por lo que tras el análisis de las tecnologías existentes, se decidió por la implementación de la Firma Electrónica Avanzada en módulos del SIIA que permitieran ser más eficientes en los tiempos de respuesta hacia los usuarios, mejorar los procesos de gestión, así como fomentar acciones para la conservación del medio ambiente.

Fundamento

Por acuerdo del Consejo Universitario Número OR 01 junio 15 09 se aprueba la implementación y validez de la Firma Electrónica Avanzada en la Universidad Autónoma del Carmen estableciendo la equivalencia funcional entre la información documentada en papel y la que existe entre un documento firmado electrónicamente con un certificado digital válido. Así mismo se autorizó la conformación del Comité Técnico quien es el organismo encargado de las decisiones en cuanto a la Firma Electrónica Avanzada (FIRMA-UNACAR) en la Universidad Autónoma del Carmen.

Derivado de lo anterior se da continuidad al proyecto de Firma Electrónica Avanzada en el Plan de Desarrollo Institucional 2017-2021; siendo el Eje 6 “Gobierno y gestión eficiente, eficaz y pertinente”, donde se plantea el objetivo de fortalecer el SIIA con módulos innovadores que apoyen la protección del medio ambiente a través de procesos automatizados de gestión administrativa y académica, mediante la estrategia de incorporación de FIRMA-UNACAR en procesos que impacten una gestión eficaz y eficiente.

Reglamento de uso y operación de la Firma Electrónica Avanzada de la Universidad Autónoma del Carmen

Capítulo I
Disposiciones Generales

Artículo 1. El presente reglamento es de observancia general para la comunidad universitaria, así como para las instancias públicas o privadas con las cuales se tenga convenio o contrato del servicio de autoridad certificadora de la Universidad Autónoma del Carmen.

Teniendo como objeto, lo siguiente:

I. Establecer las disposiciones que habrán de seguirse para implementar, operar y desarrollar la Firma Electrónica Avanzada en la UNACAR.

II. Regular el uso de la Firma Electrónica Avanzada en la UNACAR y de los certificados digitales emitidos en la UNACAR entre los miembros de la comunidad universitaria.

III. Definir las reglas de operación de los servicios de la Autoridad Certificadora UNACAR y la Firma Electrónica Avanzada.

Artículo 2. Están sujetos a las disposiciones del presente reglamento:

I. El Departamento de Desarrollo de Sistemas y responsable de la Firma Electrónica Avanzada de la UNACAR.

II. Los responsables de los sistemas estratégicos incorporados al Sistema de Firma Electrónica Avanzada.

III. Los agentes certificadores que en la realización de los actos a que se refiere este reglamento utilicen la Firma Electrónica Avanzada y emitan certificados UNACAR.

IV. Todos los miembros de la comunidad universitaria que utilicen la Firma Electrónica Avanzada.

V. Todos aquellos que hagan uso de los servicios de Firma Electrónica Avanzada de la UNACAR, independientemente de que pertenezcan o no a la comunidad universitaria.

Artículo 3. Para los efectos del presente reglamento, se entenderá por:

I. **Acuerdo:** Documento que establece aprobar la implementación y validez de la Firma Electrónica Avanzada en la Universidad Autónoma del Carmen, asentada en acuerdo del Consejo Universitario Número OR 01 junio 15 09.

II. **Autoridad Certificadora (AC) de la UNACAR**: Entidad de confianza, responsable de emitir y revocar certificados digitales válidos en la institución, utilizados en la firma electrónica, para lo cual se emplea criptografía de clave pública.

III. **Autoridad Certificadora raíz**: Un certificado raíz forma parte de un esquema de infraestructura de clave pública.

IV. **Agente certificador (AgC):** Responsable designado por Departamento de Desarrollo de Sistemas, cuyas principales funciones son el realizar la identificación del titular solicitante del Certificado Digital, así como recabar documentación comprobatoria de su identidad y la generación de un requerimiento de certificación a la AC.

V. **Base 64:** es un sistema de numeración posicional que usa 64 como base. Es la mayor potencia de dos que puede ser representada usando únicamente los caracteres imprimibles de ASCII. Esto ha propiciado su uso para codificación de correos electrónicos, PGP y otras aplicaciones.

VI. **Certificado digital:** Mensaje de datos firmados electrónicamente que confirma el vínculo o la vinculación que existen entre el firmante y su clave pública.

VII. **Certificado válido:** Aquel certificado digital emitido por la instancia facultada para ello que a la fecha de la firma no hubiera sido revocado.

VIII. **Clave pública:** Datos que se usan para verificar la Firma Electrónica Avanzada y que pertenecen a un miembro de la Comunidad Universitaria, asociados a su Clave Privada y susceptibles de ser conocidos por cualquier persona.

IX. **Clave privada:** Datos únicos, conocidos sólo por el miembro de la Comunidad Universitaria, asociados a su clave pública, generados en un dispositivo bajo su control, para crear su Firma Electrónica Avanzada.

X. **Comité Técnico de Firma Electrónica Avanzada:** Miembros designados por el H. Consejo Universitario que cumplen lo establecido en el Acuerdo responsables de vigilar el cabal cumplimiento de la normatividad en materia de Firma Electrónica Avanzada en la UNACAR.

XI. **Comunidad Universitaria:** Autoridades, profesores, investigadores, técnicos académicos, alumnos y empleados de la UNACAR en términos de lo establecido por la legislación universitaria.

XII. **Destinatario:** Persona a la que el firmante dirige un mensaje de datos.

XIII. **Unidades y dependencias universitarias:** Escuelas, facultades o dependencia administrativa de la UNACAR que se incorpora al proceso de Firma Electrónica Avanzada.

XIV. **Entidades académica**s: todas aquellas que realizan actividades de docencia, investigación, difusión y extensión como son las facultades y escuelas, así como los centros de extensión universitaria.

XV. **Entidad certificadora:** Sede descentralizada de la Autoridad Certificadora, que pertenece a una entidad académica o dependencia administrativa, responsable del proceso de emisión de los certificados digitales de los miembros de su comunidad.

XVI. Firma Electrónica Avanzada: Datos asociados a un mensaje o conjunto de información digital, que son utilizados para acreditar la identidad del Firmante en relación con el mensaje y que indican que el Firmante asume como propia la información contenida en él, produciendo los mismos efectos jurídicos que la firma autógrafa.

XVII. FIRMA-UNACAR: Firma Electrónica Avanzada de la Universidad Autónoma del Carmen.

XVIII. Firmante: Propietario de un certificado digital de la UNACAR que conserva bajo su control su clave privada y la utiliza para firmar electrónicamente un mensaje de datos.

XIX. Hexadecimal: Sistema de numeración que tiene como base el número 16; se utiliza a menudo para una representación condensada del numero binario, mediante cadenas de 4 bits. "El sistema hexadecimal utiliza las cifras del 0 al 9 y las letras 'A', 'B', 'C', 'D', 'E' y 'F'.

XX. Reglamento: Consideraciones generales para la Implementación y Uso de la Firma Electrónica Avanzada en la Universidad Autónoma del Carmen establecidos en el Acuerdo.

XXI. Mensaje de datos: Es la información generada, enviada, recibida o archivada por medios electrónicos, ópticos o magnéticos.

XXII. Procesos de Certificación: Registro de datos, verificación de elementos de identificación, emisión, renovación y revocación de Certificados Digitales.

XXIII. Sistema de Firma Electrónica Avanzada: Constituido por la Autoridad Certificadora, el componente de Firma Electrónica Avanzada, los procesos inherentes, las reglas de operación, el personal e infraestructura destinada a proporcionar el servicio de Firma Electrónica Avanzada en la UNACAR.

XXIV. Sistemas estratégicos: Sistemas que apoyan la gestión administrativa y académica con ventajas competitivas con un mayor impacto para la institución en la eficacia y eficiencia de sus procesos y servicios.

XXV. UNACAR: Universidad Autónoma del Carmen.

Artículo 4. Las disposiciones de este reglamento son aplicables en los actos del uso exclusivo de la FIRMA-UNACAR, siempre y cuando no contravengan los intereses de la comunidad universitaria o de las leyes vigentes.

Se exceptúa de lo determinado por este reglamento, en lo relativo al uso de la FIRMA-UNACAR, todos aquellos trámites en los que por ley o disposición judicial se requiera la firma autógrafa. Tampoco serán aplicables a las materias fiscal, aduanera y financiera de entidades externas a la UNACAR, salvo en los casos que por acuerdo de las partes se haga uso de la Firma Electrónica de la UNACAR, en cuyo caso se deberán acatar las disposiciones correspondientes.

Capítulo II

De la Naturaleza y Alcance

Artículo 5. En la UNACAR se establece la validez y la equivalencia funcional entre un documento firmado de manera autógrafa y un mensaje de datos firmado electrónicamente con un certificado digital válido.

Por ende, la FIRMA-UNACAR puede ser utilizada en documentos electrónicos, con la validez jurídica correspondiente.

Artículo 6. Para efectos de validez de la FIRMA-UNACAR, esta deberá cumplir con los requerimientos siguientes:

I. **Autenticación:** Garantía de que la información proviene del firmante.

II. **Confidencialidad:** Certeza de que solo pueden tener acceso al mensaje el destinatario y el firmante.

III. **Integridad:** Validación de que la información contenida en el mensaje no ha sido modificada durante el proceso.

IV. **No repudio:** El firmante no cuenta con elementos de convicción para negar la autoría del mensaje.

Artículo 7. El uso de la FIRMA-UNACAR tiene los siguientes objetivos:

I. Gestionar asuntos administrativos y académicos universitarios que determine el Comité.

II. Establecer un servicio de certificación en la UNACAR.

III. Proporcionar un mecanismo con seguridad técnica y certeza jurídica en la suscripción de documentos vía electrónica.

IV. Agilizar y simplificar la función universitaria reduciendo los tiempos de respuesta por vía electrónica.

V. Facilitar el resguardo de documentos electrónicos suscritos con la FIRMA-UNACAR

VI. Apoyar la prestación de servicios a distancia sin que se requiera la presencia física de los interesados.

Artículo 8. Las unidades académicas y dependencias administrativas pueden utilizar recursos de identificación electrónicos distintos a la FIRMA-UNACAR en cualquiera de los siguientes casos:

I. Cuando para la atención de un trámite o solicitud no se requiera la FIRMA-UNACAR del interesado.

II. Cuando la solicitud tenga por objeto requerir o consultar información que se encuentre a disposición del público en general, o corresponda a información que interesa al propio solicitante, y cuya consulta no alteraría su contenido.

III. Cuando previo acuerdo de voluntades entre las unidades académicas y dependencias administrativas se hayan establecido otros medios de identificación distintos a la FIRMA-UNACAR pero igualmente fiables.

Artículo 9. Los miembros de la comunidad universitaria que requieran usar la FIRMA-UNACAR, deberán contar con:

I. Un certificado digital vigente, emitido por la Autoridad Certificadora de la UNACAR

II. Una clave privada, generada bajo su exclusivo control.

III. Un acceso al sistema o aplicación donde se realizará el proceso de firmado.

Capítulo III

Del órgano regulador y su estructura

Artículo 10. La Secretaría Administrativa, con la asistencia de la Coordinación General de Tecnologías de la Información y la Comunicación, desarrolla y coordina el Sistema de la Firma Electrónica Avanzada.

Artículo 11. La estructura jerárquica de certificación en la UNACAR se compone de los siguientes elementos de responsabilidad:

I. Autoridad Certificadora Raíz: Entidad responsable de proporcionar servicios de certificación de clave pública a entidades académicas y dependencias de la UNACAR. El Departamento de Desarrollo de Sistemas es la autoridad certificadora raíz en la UNACAR.

II. Entidad Certificadora: Responsable del proceso de emisión de los certificados digitales de los miembros de la comunidad universitaria.

III. Agente certificador (AgC): Sujeto responsable avalado por el Departamento de Desarrollo de Sistemas de la UNACAR cuya función es entre otras, realizar la identificación del titular solicitante del certificado digital, recabar documentación comprobatoria de su identidad y la generación de un requerimiento de certificación a la Autoridad Certificadora.

Artículo 12. La FIRMA-UNACAR sustenta su operación en un Comité Técnico, el cual está integrado por un representante de las siguientes áreas:

I. Rector, (como Presidente del Comité), y su suplente, lo será el Secretario General.

II. Secretario Administrativo (como secretario).

III. Secretaria Académico.

IV. Coordinador General de Tecnologías de Información y la Comunicación (como Secretario Técnico).

V. Contralor General.

VI. Abogado General, asesor jurídico del comité,

VII. Director de la Facultad de Ciencias de la Información.

Todos los integrantes del Comité Técnico tienen voz y voto en sus sesiones y las decisiones se tomarán por mayoría de votos.

Cuando así se requiera, podrán comparecer invitados a las sesiones de trabajo del comité, quienes sólo tendrán derecho al uso de la voz, a efecto de que proporcionen información relacionada con la FIRMA-UNACAR, que se incluya en sus módulos, así como para aclarar cualquiera de los puntos a tratar en la sesión de trabajo del Comité para la que fueron invitados.

Artículo 13. El Comité Técnico de la FIRMA-UNACAR tiene las siguientes atribuciones:

I. Elegir el estándar en la UNACAR para la implementación de la FIRMA-UNACAR

II. Proponer la infraestructura y determinar los perfiles necesarios para la implementación y operación de la FIRMA-UNACAR.

III. Aprobar la tecnología que se utiliza para operar la Firma Electrónica Avanzada.

IV. Evaluar periódicamente la tecnología utilizada, a fin de hacer los ajustes que se deriven de los avances e innovaciones técnicas.

V. Proponer cambios en el reglamento de la FIRMA-UNACAR, los cuales deben regular:

- Los límites de responsabilidad de la UNACAR
- La responsabilidad del miembro de la comunidad universitaria en su función de firmante o destinatario de un mensaje de datos firmado electrónicamente.
- Los requisitos y reglas para la verificación de la identidad del firmante, así como para la emisión de certificados, incluyendo tiempos de respuesta, vigencia de los certificados y mecanismos para la conservación de mensajes de datos.
- Las políticas de seguridad, las cuales pueden ser auditables.

Artículo 14. El Departamento de Desarrollo de Sistemas adscrito a la Coordinación General de Tecnologías de Información y la Comunicación, es el responsable de implementar y ejecutar lo establecido por el Comité Técnico en materia de Firma Electrónica Avanzada en la UNACAR.

Sus atribuciones son:

I. Custodiar la autoridad certificadora de la UNACAR, y proteger mediante estrictas políticas de seguridad e infraestructura física, así como los certificados que de esta emanen.

II. Asesorar al comité técnico de la FIRMA_UNACAR, respecto de nuevas tecnologías en materia de seguridad y criptografía, con la finalidad de mantener a la vanguardia los procesos de la Autoridad Certificadora y el componente de Firma Electrónica Avanzada alineado a lo establecido por la normatividad y estándares tecnológicos nacionales e internacionales y con apego a los estándares nacionales e internacionales en la materia.

III. Revisar y evaluar de manera periódica los sistemas estratégicos de los usuarios de la FIRMA-UNACAR, con la finalidad de garantizar que los medios y mecanismos mediante los cuales se firman electrónicamente los documentos y transacciones se encuentran correctamente resguardados,

IV. Evaluar y analizar los sistemas susceptibles a incorporarse a la FIRMA-UNACAR y emitir las recomendaciones pertinentes para su aprobación en el Comité Técnico de FIRMA_UNACAR.

V. Fungir como órgano de apoyo técnico en la resolución de controversias, derivadas de actos relacionados con el uso del Sistema de Firma Electrónica Avanzada de la UNACAR, sin responsabilidad jurídica al respecto de ese apoyo.

VI. Proponer adecuaciones a la normatividad de Firma Electrónica Avanzada en apego a los cambios o modificaciones derivadas de cambios en la normatividad nacional o internacional, siguiendo los procedimientos institucionales correspondientes para tal efecto.

Sus responsabilidades son:

I. Mantener y salvaguardar la infraestructura tecnológica necesaria para la operación de la Autoridad Certificadora y el componente de FIRMA-UNACAR, garantizando altos niveles de seguridad y confiabilidad en los procesos.

II. Vigilar el cabal cumplimiento de la normatividad en materia de FIRMA-UNACAR

III. Adoptar las medidas necesarias para evitar la falsificación, alteración o uso indebido de certificados digitales y de los servicios relacionados con la FIRMA-UNACAR.

IV. Garantizar la autenticidad, integridad, conservación, confidencialidad y confiabilidad de la FIRMA-UNACAR, así como de los servicios relacionados con la misma.

V. Proporcionar los medios y mecanismos necesarios para que los sistemas estratégicos, otorguen servicios de certificación en la UNACAR.

VI. Mantener un registro de certificados, en el que quede constancia de los emitidos y figuren las circunstancias que incidan en la suspensión, pérdida o terminación de vigencia.

VII. Garantizar la disponibilidad del componente de firma y las transacciones que se deriven del proceso.

VIII. Poner a disposición de las unidades académicas, dependencias administrativas y miembros de la comunidad una herramienta de verificación de las transacciones y documentos firmados, con la finalidad de verificar la integridad de la firma electrónica y su validez en el tiempo.

IX. Mantener la información pública de los certificados digitales emitidos. El contenido privado estará a disposición del destinatario y de las personas que lo soliciten cuando así lo autorice el firmante, así como en los casos a que se refieran las reglas generales que al efecto establezca la UNACAR considerando las políticas y normas para la protección de datos personales.

X. Disponer de procedimientos claros y definidos de los servicios de certificación, así como las sanciones que apliquen en cada caso.

XI. Informar oportunamente al Comité Técnico de Firma Electrónica Avanzada, a los sistemas estratégicos y a las unidades académicas y dependencias administrativas de cambios en la tecnología, operación y modificación de políticas de uso de los certificados digitales, la Autoridad Certificadora y la Firma Electrónica Avanzada.

XII. Mantener la confidencialidad de la información y establecer los mecanismos necesarios para garantizar la protección de datos personales y sensibles derivados de las transacciones realizadas a través del sistema de Firma Electrónica Avanzada, en apego a la Ley de Transparencia y Acceso a la Información Pública del Estado de Campeche y la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche.

Capítulo IV

De los Agentes Certificadores

Artículo 15. El Departamento de Desarrollo de Sistemas adscrito a la Coordinación General de Tecnologías de la Información y la Comunicación, funge como única Autoridad Certificadora Raíz en la UNACAR.

Artículo 16. Los agentes certificadores tienen las siguientes responsabilidades:

I. Emitir el certificado digital con apego a la normatividad en materia de certificados digitales y FIRMA-UNACAR.

II. Acreditar la identidad del solicitante de un certificado digital mediante:

- Cotejo entre identificación oficial y solicitante.
- Documentación probatoria en copia con verificación de original.

III. Generar el certificado digital en presencia del usuario.

IV. Recabar la documentación probatoria de identidad del solicitante, así como la firma autógrafa en original de la carta compromiso del firmante.

V. Eliminar los archivos generados durante el proceso de emisión del certificado digital (.pfx) en presencia del usuario.

VI. Abstenerse de ingresar, teclear o conocer la clave privada y frase de seguridad del solicitante de un certificado digital.

VII. Explicar al solicitante las responsabilidades en el uso del certificado digital, la vigencia y los motivos de revocación así como el procedimiento a seguir.

VIII. Apoyar y orientar al solicitante en los procesos de emisión y revocación del certificado.

IX. Proporcionar información veraz, clara y concisa a los solicitantes y evitar cualquier acto que implique violación a la normatividad en materia de Firma Electrónica Avanzada.

X. Mantener, clasificada y relacionada la documentación recabada de los solicitantes de certificados digitales.

XI. Reportar al jefe del Departamento de Desarrollo de Sistemas cualquier situación que contravenga las disposiciones y lineamientos en materia de Firma Electrónica Avanzada.

XII. Proporcionar apoyo al usuario del certificado digital para los procesos relativos a la Firma Electrónica Avanzada.

Capítulo V

De la Integración de nuevos sistemas a la FIRMA-UNACAR

Artículo 17. El Comité Técnico de la FIRMA-UNACAR aprobará la integración de nuevos sistemas y aplicaciones la FIRMA-UNACAR, a partir de criterios de pertinencia, usabilidad y factibilidad.

Artículo 18. Los sistemas que soliciten la integración a la FIRMA_UNACAR, deberán cumplir con los siguientes requisitos:

I. Ser una aplicación que esté integrada al Sistema Integral de Información Administrativa (SIIA).

II. Cumplir con criterios de pertinencia y relevancia, así como justificar la inclusión de sus procesos.

III. Realizar solicitud oficial al Comité Técnico de Firma Electrónica Avanzada.

IV. Proporcionar información pertinente sobre el proceso a incorporar (manuales, esquemas, diagramas).

V. Entregar listado de usuarios considerados en el sistema o proceso.

VI. Obtener la autorización correspondiente por parte del Comité Técnico de la FIRMA-UNACAR.

VII. Conocer y apegarse a la normatividad vigente en materia de FIRMA-UNACAR.

Artículo 19. Entre las responsabilidades de los sistemas estratégicos que se incorporen a la FIRMA-UNACAR están:

I. Hacer uso de la FIRMA-UNACAR exclusivamente en aquellos servicios y aplicaciones para los que haya sido autorizado por el Comité Técnico.

II. Utilizar exclusivamente los medios y herramientas proporcionados por el Departamento de Desarrollo de Sistemas para emitir y revocar certificados digitales de la UNACAR.

III. Informar de cualquier cambio relevante, nueva aplicación o uso, de la FIRMA-UNACAR en sus sistemas.

IV. Utilizar los certificados digitales y el componente de la FIRMA-UNACAR exclusivamente en trámites y servicios de la UNACAR.

V. Acatar la normatividad vigente en materia de Firma Electrónica Avanzada de la UNACAR.

VI. Abstenerse de utilizar la FIRMA-UNACAR en trámites y servicios que contravengan los intereses y derechos de los miembros de la comunidad universitaria o en aquellos que por ley o disposición judicial se requiera firma autógrafa.

Artículo 20. El Departamento de Desarrollo de Sistemas proporcionará a los sistemas estratégicos que se incorporen en la utilización de la FIRMA-UNACAR, lo siguiente:

I. Información clara y suficiente de los procesos, reglas de operación y políticas de uso de FIRMA-UNACAR.

II. Soporte técnico para la incorporación de sus procesos a los sistemas de Firma Electrónica Avanzada.

III. Disponibilidad de los servicios de FIRMA-UNACAR, tanto de la autoridad certificadora como del componente, salvo en aquellos casos fortuitos.

IV. Notificación en forma oportuna de posibles suspensiones programadas del servicio (ventanas de mantenimiento).

V. Información de los cambios y mejoras en el sistema de FIRMA-UNACAR.

VI. Mecanismos que les permita conocer información inherente a los procesos de generación de certificados digitales y Firma Electrónica Avanzada en su ámbito, siempre y cuando no contravengan las políticas de Seguridad implementadas

Capítulo VI

De las transacciones electrónicas y mensajes de datos

Artículo 21. El Departamento de Desarrollo de Sistemas, en su calidad de Autoridad Certificadora, custodiará la información que sea enviada a firmar electrónicamente, asegurando en todo momento la transmisión segura de la misma y su confidencialidad.

Los mensajes de datos y los documentos electrónicos que contengan datos personales, estarán sujetos a las disposiciones aplicables al manejo, seguridad y protección de los mismos, en términos a la Ley de Transparencia y Acceso a la Información Pública del Estado de Campeche y la Ley de Protección de Datos personales en Posesión de Sujetos Obligados del Estado de Campeche.

Artículo 22. El Departamento de Desarrollo de Sistemas es el responsable de la información enviada a firmar y su contenido a través de los sistemas estratégicos, garantizando el almacenamiento de la información firmada.

Artículo 23. Los sistemas estratégicos, deben conservar en medios electrónicos los mensajes de datos y los documentos con Firma Electrónica Avanzada, derivados de los actos a que se refiere este reglamento, durante los plazos de conservación previstos en la normatividad aplicable según la naturaleza de la información.

Artículo 24. Los Sistemas estratégicos que se incorporen a la FIRMA-UNACAR, deberán cumplir con las normas técnicas especificadas por el Departamento de Desarrollo de Sistemas.

Artículo 25. El Departamento de Desarrollo de Sistemas, facilitará los medios elec-

trónicos necesarios, en caso de que exista duda sobre la integridad del documento electrónico firmado. Los elementos involucrados serán:

I. La interfaz de validación de la firma;

II. La cadena original firmada del documento o transacción almacenada por el sistema estratégico;

III. El certificado digital (vigente o no); y

IV. Los involucrados (firmante, sistema estratégico, representante del Comité Técnico y tercero confiable).

Artículo 26. La resolución de controversias será resuelta por el Comité Técnico de FIRMA-UNACAR, con mayoría calificada de votos. La notificación de la resolución no podrá exceder 30 días hábiles a partir de la emisión del dictamen técnico por parte del Departamento de Desarrollo de Sistemas.

Capítulo VII

De la transmisión y envíos de datos

Artículo 27. Es responsabilidad de los sistemas estratégicos implementar las medidas de seguridad física y perimetral necesarias para garantizar la transmisión segura y confiable de los datos.

Artículo 28. Los sistemas estratégicos deben establecer los mecanismos para el almacenamiento de la información firmada, garantizando en todo momento la integridad de las bases de datos y estableciendo los medios de acceso pertinente.

Artículo 29. La transmisión de datos debe ser codificada, con la finalidad de no enviar información interpretable de forma directa, permitiendo que los datos permanezcan íntegros durante su transmisión entre múltiples plataformas; para ello se podrán implementar diversas representaciones de datos.

Capítulo VIII

Del Certificado Digital y la Autoridad Certificadora

(Estructura y características)

Artículo 30. La Autoridad Certificadora de la UNACAR, cuenta con una longitud de llave raíz (base) de 4096 bits y los certificados digitales que emanan de la misma tienen una longitud (base) de 2048 bits.

Artículo 31. El certificado digital contiene en su estructura:

I. Número de serie;

II. Autoridad certificadora que lo emitió;

III. Algoritmo de firma;

IV. Vigencia;

V. Dirección de correo electrónico del titular del certificado digital;

VI. Clave Única del Registro de Población (CURP) del titular del certificado digital;

VII. Clave pública; y

VIII. Los demás requisitos que, en su caso, se establezcan en las disposiciones generales que se emitan en términos de este lineamiento.

Artículo 32. El periodo de validez del certificado raíz de la Autoridad Certificadora UNACAR es de diez años a partir de su fecha de emisión y de cuatro años para los certificados digitales emitidos.

Capítulo IX

De los Derechos, obligaciones y responsabilidades del titular del Certificado Digital

Artículo 33. Para la emisión de un certificado digital emitido por la Autoridad Certificadora UNACAR, el solicitante debe cumplir los siguientes requisitos:

I. Ser miembro activo de la comunidad universitaria de la UNACAR.

II. Estar integrado a una aplicación y/o sistema que utilice la FIRMA-UNACAR en sus procesos.

III. Estar habilitado por su entidad académica o dependencia universitaria para realizar firma en la aplicación o sistema.

IV. Presentar la documentación oficial que acredite su identidad.

V. Tramitar un único certificado digital para todos los sistemas en los que se incorpore para utilizar FIRMA-UNACAR.

Artículo 34. El solicitante de un certificado digital está obligado a:

I. Acudir personalmente a la emisión de su certificado digital.

II. Presentar una identificación oficial vigente con fotografía, CURP y entregar una copia simple de la primera por ambos lados, a la entidad certificadora.

III. Responder por la veracidad de los datos personales que proporcione a la entidad certificadora.

IV. Generar la Clave Privada y frase de seguridad en absoluta confidencialidad.

V. Verificar los datos contenidos en el certificado digital, así como el período de vigencia y número de serie del certificado digital que consta al final de la Carta compromiso del firmante.

VI. Signar la Carta compromiso.

Artículo 35. El titular de un certificado digital está obligado a:

I. Utilizar el certificado digital exclusivamente para los fines que le fueron designados.

II. Mantener absoluta confidencialidad respecto a la clave privada y frase de seguridad.

III. Evitar la utilización no autorizada de la clave privada y actuar con el debido cuidado para impedir el mal uso del certificado.

IV. Solicitar de manera inmediata a la entidad certificadora la revocación del certificado digital cuando se considere que la clave privada, o el dispositivo que la contiene, está comprometida o en riesgo, por la pérdida o cualquier otra situación que pudiera implicar la reproducción o uso indebido de los datos de creación de firma electrónica y del certificado digital.

V. Responder por el uso no autorizado de la clave privada, cuando no se hubiere actuado con el debido cuidado para impedir su utilización, así como cuando no se haya solicitado oportunamente la revocación del certificado digital.

VI. Resguardar en lugar seguro el certificado digital.

VII. No compartir, transferir o prestar el certificado digital a un tercero.

Artículo 36. El titular de un certificado digital tendrá derecho a ser informado por la entidad certificadora que lo emita, de lo siguiente:

I. Las características y condiciones precisas para la utilización del certificado digi-

tal, así como los límites de uso;

II. Las características generales de los procedimientos para la generación y emisión del certificado digital y la creación de la clave privada, y la revocación del certificado digital;

III. Que los datos e información que proporcione a la autoridad certificadora sean tratados de manera confidencial, en términos de las disposiciones jurídicas aplicables; y

IV. Solicitar la modificación de datos personales del certificado digital, cuando así convenga a sus intereses.

Artículo 37. El titular de un certificado digital es el responsable del uso indebido de su FIRMA-UNACAR, de los daños y perjuicios ocasionados en cualquiera de los módulos del Sistema Institucional de Información Administrativa de la UNACAR en los cuales se solicite la FIRMA-UNACAR, dando lugar a los procedimientos o sanciones que correspondan de acuerdo a lo establecido por la normatividad de la UNACAR.

Capítulo X

De la Revocación de un Certificado Digital

Artículo 38. El certificado digital será revocado por la entidad certificadora que lo emitió, por alguno de los motivos siguientes:

I. Olvido de frase de seguridad del certificado digital.

II. Pérdida del certificado por parte del miembro de la comunidad universitaria.

III. Cumplimiento del periodo de vigencia.

IV. Actualización de datos del usuario impactando en cambio de CURP.

V. Defunción.

VI. Incumplimiento del reglamento en cuanto se refiere a emisión de carta compromiso.

VII. Jubilación.

VIII. Incumplimiento del reglamento al emitir un certificado sin la presencia del miembro de la comunidad universitaria.

IX. Error de procedimiento por parte del agente certificador durante la emisión del certificado digital.

X. A solicitud expresa del usuario.

XI. Terminación laboral.

El Departamento de Desarrollo de Sistemas, en su carácter de Autoridad Certificadora, se reserva el derecho de revocar el certificado digital del usuario cuando este incurra en actividades que contravengan el reglamento de emisión y uso del certificado digital o bajo sospecha de riesgo o compromiso de la secrecía de la frase de seguridad.

Artículo 39. Cuando sea revocado el certificado digital, este perderá su vigencia. Y se emitirá un nuevo certificado digital con la misma temporalidad establecida en este reglamento.

Capítulo XI

De la Renovación de un Certificado Digital

Artículo 40. Se entenderá por renovación de los certificados digitales, al proceso mediante el cual el certificado digital de un usuario, es necesario volver a generar por perdida de vigencia.

Artículo 41. Los certificados digitales de los usuarios deberán ser renovados por parte de las unidades académicas y dependencias administrativas universitarias durante los periodos que no afecten el ejercicio de los procesos determinados.

Artículo 42. Los certificados digitales serán renovados al término de la vigencia de los mismos o cuando al menos hayan cumplido más de las dos terceras partes de su vigencia, en función de criterios de pertinencia para procesos internos de cada unidad académica y dependencia administrativa universitaria.

Capítulo XII

Del límite de responsabilidad de la UNACAR

Artículo 43. La UNACAR, no será responsable de los daños y perjuicios ocasionados por el usuario o cualquier otro tercero causado directa o indirectamente por perjuicio derivado de un uso distinto al autorizado en la normatividad de FIRMA-UNACAR, de los certificados digitales y la infraestructura de Firma-UNACAR.

Artículo 44. La UNACAR se deslinda de cualquier responsabilidad derivada de daños o perjuicios que se ocasionen por la imposibilidad de firmar transacciones electrónicas con FIRMA-UNACAR en los siguientes casos:

I. Funcionamiento incorrecto de equipos personales.

II. Causas imputables al desconocimiento del proceso por parte del usuario.

III. Uso del certificado digital en aplicaciones ~~y/o~~ sitios no autorizados o reconocidos como oficiales para procesos de Firma Electrónica Avanzada en la UNACAR.

IV. Por daños, alteraciones o corrupción del certificado digital, cuando el usuario no atienda a las recomendaciones de uso y almacenamiento.

V. Por situaciones de fuerza mayor o elemento fortuito derivado de situaciones como catástrofes, fenómenos sociales y naturales, entre otros, que impidan el funcionamiento de telecomunicaciones e infraestructura de la Firma Electrónica Avanzada.

Artículo 45. La UNACAR no se responsabiliza de:

I. Daños o perjuicios en hardware o software derivados de procesos no autorizados o ajenos a los procesos de emisión de certificados y Firma Electrónica Avanzada.

II. De instalación de software de sitios no autorizados por la Coordinación General de Tecnologías de la Información y la Comunicación.

III. Contenidos de la información firmada, así como daños, perjuicios ocasionados, así como las acciones legales derivadas de los contenidos, mutilaciones o alteraciones de esta.

IV. Deterioro físico del dispositivo de almacenamiento del certificado digital por acciones derivadas de malas prácticas, así como por el cumplimiento del ciclo natural de vida del dispositivo.

Artículo 46. La UNACAR será responsable de:

I. Otorgar garantía de integridad, confidencialidad y no repudio de la información firmada.

II. Proporcionar la infraestructura de FIRMA-UNACAR y garantizar el correcto funcionamiento de la misma en procesos de emisión de certificados digitales y Firma Electrónica Avanzada en sistemas y aplicaciones autorizadas UNACAR.

III. Garantizar la disponibilidad de los medios a través de los cuales se firme electrónicamente en términos de seguridad y robustez.

IV. Mantener plataformas actualizadas y estar pendiente de avances tecnológicos que permitan mantener los procesos en un ámbito de modernidad y robustez tecnológica.

V. Plataforma tecnológica de Autoridad Certificadora y componente de Firma Electrónica Avanzada con total apego a normatividad y estándares nacionales e internacionales en materia de infraestructura de llave pública (PKI) y Firma Electrónica Avanzada.

VI. Proporcionar los medios que permitan validar modificaciones o alteraciones a la información firmada, así como apoyar procesos de validación ante terceros en caso de controversia o proceso legal.

Transitorios

Primero. El presente reglamento entrará en vigor partir del día siguiente hábil de su publicación en la Gaceta Universitaria, en forma digital o impresa, previa aprobación del H. Consejo Universitario.

Segundo. Se derogan todas aquellas disposiciones legales y administrativas que se opongan a lo previsto en este reglamento.

Tercero. Lo no previsto en este reglamento, será dirimido y resuelto por el Comité de Firma Electrónica Avanzada.

Dado mediante acuerdo del H. Consejo Universitario, del acta número 06/2019, en la Sesión Ordinaria, celebrada en la Sala del Consejo Universitario, con fecha once de abril del año dos mil diecinueve. Ciudad del Carmen, Campeche.