ACUERDO POR EL QUE SE INSTALA EL COMITÉ DE USO DE FIRMA ELECTRÓNICA UNIVERSITARIA EN SUS MODALIDADES INTERNA Y AVANZADA Y SE EMITEN LOS LINEAMIENTOS DE FUNCIONAMIENTO.

DRA. CONSUELO NATALIA FIORENTINI CAÑEDO, RECTORA DE LA UNIVERSIDAD AUTÓNOMA DEL ESTADO DE QUINTANA ROO, CON FUNDAMENTO EN LOS ARTÍCULOS 3, 4 FRACCIÓN II, XI, XIV, 7 FRACCIÓN III, 23, 26 FRACCIONES II, IV, IX Y XVI DE LA LEY ORGÁNICA DE LA UNIVERSIDAD DE QUINTANA ROO; 4 FRACCIÓN IV, VI Y VIII, 26 FRACCIONES IV Y XVII DEL REGLAMENTO GENERAL DE LA UNIVERSIDAD AUTÓNOMA DEL ESTADO DE QUINTANA ROO, SE EMITEN EL SIGUIENTE ACUERDO POR EL QUE SE INSTALA EL COMITÉ DE USO DE FIRMA ELECTRÓNICA UNIVERSITARIA EN SUS MODALIDADES INTERNA Y AVANZADA Y SE EMITEN LOS LINEAMIENTOS DE SU FUNCIONAMIENTO AL TENOR DE LOS SIGUIENTES:

C O N S I D E R A N D O

I.- Que la Universidad Autónoma del Estado de Quintana Roo, es un organismo público descentralizado del Estado, que tiene entre sus fines impartir educación superior en los niveles técnicos, de licenciatura, estudios de posgrado, cursos de actualización y especialización mediante diferentes modalidades de enseñanza y especialización para formar profesionistas, profesores universitarios e investigadores que requiere el Estado, la región y el país en su armónico desarrollo socioeconómico y cultural.

II.- Que la Universidad en cumplimiento de sus funciones sustantivas no puede ser ajena al desarrollo y avances tecnológicos de los medios de comunicación electrónica, como tampoco a la digitalización de la información, al crecimiento del Internet como la automatización de los procesos, la creciente importancia del aspecto inmaterial los cuales devienen del resultado de los avances tecnológicos.

III.- Que ante el avance de las nuevas tecnologías se precisa adecuar el marco jurídico universitario que regule e implemente la Firma Electrónica Universitaria al interior de la Institución, basada en una tecnología que garantice la autenticación, la integridad y

confidencialidad de la información transmitida así como el no repudio de la misma; en los procesos, solicitudes y demás comunicaciones electrónicas; por ende y bajo tal premisa, la Universidad busca establecer una equivalencia funcional entre el consentimiento manifestado por medios electrónicos y la firma autógrafa de forma segura.

IV.- Que parte de las estrategias de modernización y transformación digital de la Universidad Autónoma del Estado de Quintana Roo y de los procesos de mejora continua, se identificó la necesidad de adoptar la Firma Electrónica en sus modalidades de Firma Electrónica Avanzada y Firma Electrónica Interna, con el objetivo de lograr la transición de archivos y documentos impresos a documentos electrónicos firmados y certificados. Esta tecnología de vanguardia permitirá que los procesos sean más eficientes, reduciendo costos y tiempos de respuesta, contribuyendo a su vez a la sostenibilidad, seguridad de la información y a la optimización de recursos materiales y humanos, toda vez que se han detectado en diversas áreas de la universidad oportunidades de mejora en la gestión de los procesos de servicio y operación administrativa, ya que la mayoría de los trámites y diligencias se basan en el uso de documentos en papel y signados físicos, así como la consecuente inversión de tiempo importante, es decir, se propone optimizar el proceso.

V.- Que el principio de equivalencia funcional y la neutralidad tecnológica encuentra su finalidad en la efectividad del uso de las tecnologías para acreditar la manifestación de la voluntad rompiendo las barreras que limitan la accesibilidad, eficacia y eficiencia de los procedimientos, amalgamado por el andamiaje legislativo a nivel estatal, nacional e internacional.

En razón de lo anterior y con el objeto de brindar un apoyo eficaz he tenido a bien expedir el siguiente:

UNIVERSIDAD AUTÓNOMA DEL ESTADO DE QUINTANA ROO
DIRECCIÓN GENERAL DE ASUNTOS JURÍDICOS

ACUERDO POR EL QUE SE INSTALA EL COMITÉ DE USO DE FIRMA ELECTRÓNICA UNIVERSITARIA EN SUS MODALIDADES INTERNA Y AVANZADA Y SE EMITEN LOS LINEAMIENTOS DE FUNCIONAMIENTO.

A C U E R D O

PRIMERO. - Se instala el **Comité de firma electrónica universitaria** en la Universidad Autónoma del Estado de Quintana Roo, como también se emiten los lineamientos que regularán el funcionamiento de la misma en su modalidad interna y avanzada.

SEGUNDO. La implementación del uso de la Firma Electrónica Universitaria incluye el uso de la firma de manera interna y de manera externa (avanzada) contemplando los siguientes objetivos:

I. Permitir su utilización para la gestión de asuntos administrativos y académicos universitarios que para cada caso determine el Comité;
II. Equiparar a la firma autógrafa siempre que la Firma Electrónica Avanzada y la Firma Electrónica Interna se encuentren amparadas en un certificado digital válido y vigente a la fecha de la firma;
III. Crear e implementar una infraestructura de certificación efectiva en la Universidad;
IV. Utilizar un mecanismo que otorgue seguridad técnica y certeza jurídica en la suscripción de documentos vía electrónica;
V. Impulsar el uso en la administración universitaria de esquemas tecnológicos que permitan la realización de sus funciones de manera ágil y sencilla, economizando los tiempos de respuesta por vía electrónica;
VI. Establecer los procedimientos que permitan resguardar documentos electrónicos suscritos con la firma electrónica universitaria y,
VII. Posibilitar la prestación de servicios a distancia sin que se requiera la presencia física de los interesados.

TERCERO. - El Comité de la firma electrónica universitaria en sus dos modalidades, estará integrado de la siguiente forma:

a) Titular de la rectoría en su calidad de presidente(a) del Comité,
b) Titular de la Secretaría General en su calidad de suplente del (a) **presidente(a) del Comité.**
c) Titular de la Dirección General de Tecnologías de la Información, en su calidad de **coordinador(a) del comité y secretario(a)**.
d) Titular de la Coordinación de la Unidad Académica Zona Sur, en su calidad de **vocal académico**.
e) Titular de la Coordinación de la Unidad Académica Zona Norte, en su calidad de **vocal académico**.
f) Titular de la Dirección General de Administración y Finanzas, en su calidad de **vocal financiero**.
g) Jefe del Departamento de Desarrollo de Sistemas, en su calidad de **vocal de sistemas de información**.
h) Jefe del Departamento de Infraestructura Tecnológica, en su calidad de **vocal de infraestructura tecnológica y seguridad**.
i) Auditora Interna, en su calidad de **vocal de auditoría**.
j) Titular de la Dirección General de Asuntos Jurídicos, en su calidad de **asesor jurídico.**

La Dirección General de Tecnologías de la Información desarrollará y coordinará el sistema de la Firma Electrónica Universitaria, conforme a los acuerdos tomados por el Comité.

Sin menoscabo de las denominaciones anteriores, en caso de modificación a la estructura orgánica, las personas servidoras públicas con nivel de Director (a) o Jefe (a) en quienes recaigan las funciones antes señaladas o bien se equiparen a las mismas serán quienes integren el comité. La misma lógica se aplicará en caso de cambio de la persona servidora pública.

CUARTO. - Todos los integrantes del Comité, con excepción de la persona asesora, tendrán voz y voto en las sesiones y las decisiones se tomarán por mayoría.

QUINTO. - Cuando así se requiera, podrán comparecer invitados a las sesiones de trabajo del Comité, quienes sólo tendrán derecho a voz, a efecto de que proporcionen información relacionada con los temas que sean competencia o interés del Comité, así como para aclarar cualquiera de los puntos a tratar en la sesión de trabajo para la que fueron invitados.

Los colaboradores(as) internos(as) o externos(as) propuestos(as) por algún miembro del Comité como asesores o con fines específicos, cuando el caso lo amerite, participarán con voz y sin voto.

SEXTO. - El Comité, se reunirá periódicamente, de acuerdo con el calendario anual de sesiones ordinarias que el propio comité defina, y cuando la situación amerite, convocar a sesiones extraordinarias.

SÉPTIMO. El **Comité de uso de Firma Electrónica Universitaria** tendrá las siguientes atribuciones:

I. Elegir el estándar a utilizar en la universidad para la implementación de la Firma Electrónica Universitaria en sus 2 modalidades;
II. Supervisar la infraestructura y establecer los perfiles necesarios para la implementación y operación de la Firma Electrónica Universitaria;
III. Verificar la tecnología que se utilizará para implementar la Firma Electrónica Universitaria;
IV. Evaluar periódicamente la tecnología utilizada, a fin de hacer los ajustes que se deriven de los avances e innovaciones técnicas y tecnológicas;

V. Revisar y en su caso proponer las modificaciones a los lineamientos que regulan el uso y alcances de la Firma Electrónica Universitaria.

VI. Las demás que se definan en los lineamientos que al efecto se emitan.

OCTAVO. Cualquier controversia que se suscite por el uso indebido de la información relativa a la firma electrónica universitaria, o en su caso, al no repudio de la firma y demás circunstancias que se encuentren vinculadas a tales actos, serán resueltas por el Comité. Tales resoluciones deberán ser notificadas dentro de los siguientes 30 días hábiles, contados a partir del acuerdo tomado por el Comité y a través de su secretario técnico a la autoridad o representación correspondiente.

NOVENO. – Para una mejor provisión de los servicios de la firma electrónica universitaria, se expiden los **lineamientos para el funcionamiento del comité de firma electrónica universitaria en sus dos modalidades para la Universidad Autónoma del Estado de Quintana Roo**, mismos que se adjuntan al presente acuerdo, los cuales serán de observancia obligatoria para la comunidad universitaria.

DÉCIMO. - Lo no previsto en este acuerdo, será resuelto por la persona Titular de la rectoría en su calidad de presidente(a) del Comité de firma electrónica universitaria.

TRANSITORIOS

PRIMERO. – El presente acuerdo entrará en vigor al día siguiente de su publicación.

SEGUNDO. - Notifíquese a las Coordinaciones, Direcciones Generales, Divisiones y Jefaturas de Departamento de la Universidad, a fin de que se establezca un vínculo de colaboración e implementación de los lineamientos que regulan el uso de la Firma Electrónica Universitaria en sus dos modalidades.

TERCERO. - La Dirección General de Tecnologías de la Información, como coordinadora del comité, cuenta con un plazo máximo de 30 días contados a partir de que entre en vigor el presente acuerdo para realizar las gestiones que sean necesarias para convocar la primera sesión ordinaria.

CUATRO. - La Dirección General de Tecnologías de la Información en coordinación con el Jefe del Departamento de Desarrollo de Sistemas, deberán realizar las gestiones necesarias para garantizar la operatividad de los proyectos relacionados con la firma electrónica universitaria.

QUINTA. - Se deja sin efectos cualquier disposición legal de igual o menor jerarquía.

Dado en la ciudad de Chetumal, capital del Estado de Quintana Roo, el día 02 de mayo del año 2025.

"Fructificar la razón: trascender nuestra cultura"

Dra. Consuelo Natalia Fiorentini Cañedo
Rectora

Lineamientos para el funcionamiento del comité de firma electrónica universitaria en sus dos modalidades.

Artículo 1: Objeto y competencia.

Los presentes lineamientos amparan el funcionamiento del comité de uso de firma electrónica universitaria en sus dos modalidades: interna y avanzada.

La aplicación de este instrumento normativo es obligatoria para la comunidad universitaria y su observancia es general para las personas externas que hagan uso de la firma electrónica.

Artículo 2: Glosario

Para los efectos del presente reglamento, se entenderá por:

I. **Acuerdo:** documento que establece aprobar la implementación y validez de la firma electrónica en la Universidad Autónoma del Estado de Quintana Roo.

II. **Agente certificador universitario:** responsable de realizar la identificación del titular solicitante del Certificado Digital, así como recabar documentación comprobatoria de su identidad y la generación de un certificado para la firma electrónica avanzada de la **Entidad Certificadora**.

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

IV. **Autoridad Certificadora:** entidad responsable de emitir y revocar certificados digitales válidos en la institución, utilizados en la firma electrónica avanzada, para lo cual se emplea criptografía de clave pública y privada.

V. **Autoridad Certificadora Avanzada**: entidad de confianza, responsable de emitir y revocar certificados digitales válidos en la institución, utilizados en la Firma Electrónica Avanzada, para lo cual se emplea criptografía de clave pública.

VI. **Bóveda digital**: herramienta utilizada para almacenar y proteger los certificados digitales que se utilizan para firmar documentos almacenada bajo resguardo de la Dirección General de Tecnologías de la Información y el Comité.

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

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

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

X. **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.

XI. **Comité de Firma Electrónica:** es el comité de Firma Electrónica Universitaria responsables de vigilar el cabal cumplimiento de la normatividad en la materia de su competencia.

XII. **Convenio:** documento que establece la colaboración para la implementación y validez de la Firma Electrónica Avanzada con autoridad certificadora y la Universidad Autónoma del Estado de Quintana Roo.

XIII. **Comunidad Universitaria:** La comunidad universitaria señalada en la Ley Orgánica de la Universidad y demás normativa interna aplicable.

XIV. **Destinatario:** Persona a la que el firmante dirige un documento electrónico.

XV. **Entidad certificadora Avanzada:** sede descentralizada de la Autoridad Certificadora, responsable del proceso de emisión de los certificados digitales de los miembros de la comunidad universitaria de la Universidad, para uso de Firma Electrónica Avanzada.

XVI. **Entidad certificadora Interna:** la entidad responsable del proceso de emisión de los certificados digitales de los miembros su comunidad universitaria, para uso de Firma Electrónica Interna.

XVII. **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 con relación a documentos electrónicos, que serán emitidos al exterior de la Universidad.

XVIII. **Firma Electrónica Interna:** datos asociados a un mensaje o conjunto de información digital, que son utilizados para acreditar la identidad del Firmanteen 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 con relación a documentos electrónicos, que serán emitidos al interior de la Universidad.

XIX. **Firmante:** propietario de un certificado digital de la Universidad que conserva bajo su control su clave privada y la utiliza para firmar electrónicamente un mensaje de datos.

XX. **Lineamiento:** los presentes lineamientos para el funcionamiento del comité de firma electrónica avanzada, en sus dos modalidades para la Universidad Autónoma del Estado de Quintana Roo.

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

XXII. **Medios tecnológicos**: herramientas, procedimientos o mecanismos que se utilizan para facilitar, acelerar o controlar un proceso y alcanzar un objetivo.

XXIII. **Procesos de Certificación:** registro de datos, verificación de elementos de identificación, emisión, renovación y revocación de Certificados Digitales.

XXIV. **Sistema de Firma Electrónica:** constituido por la Autoridad Certificadora, el componente de Firma Electrónica, los procesos inherentes, las reglas de operación, el personal e infraestructura destinada a proporcionar el servicio de Firma Electrónica en la Universidad.

XXV. **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.

XXVI. **Universidad:** La Universidad Autónoma del Estado de Quintana Roo.

Artículo 3.- Integración del Comité.

El comité se integrará de conformidad con el acuerdo RECT-04-2025. A fin de garantizar, supervisar, atender y resolver situaciones anómalas de la actividad de los servicios que la Universidad ofrece, en cuanto a la seguridad, integridad y legalidad de los procesos de firma electrónica universitaria dentro del marco legal se observará lo dispuesto en las legislaciones de aplicación Estatal y Federal respecto al uso de las tecnologías de la información, la manifestación de la voluntad, capacidad y consentimiento, protección de datos personas y respeto a los derechos humanos.

Teniendo como objetivo, lo siguiente:

I. Establecer las disposiciones que habrán de seguirse para implementar, operar y desarrollar la Firma Electrónica en la Universidad, en sus modalidades Firma Electrónica Avanzada y Firma Electrónica Interna;

II. Regular el uso de la Firma Electrónica Avanzada y la Firma Electrónica Interna, así como los certificados digitales emitidos por la Autoridad Certificadora, y la universidad, respectivamente, entre los miembros de la comunidad universitaria;

III. Pronunciarse respecto a las controversias que surjan respecto al uso de la firma electrónica universitaria;

IV. Capacitar a los miembros de la comunidad universitaria sobre el uso de la firma electrónica universitaria;

V. Diseñar los avisos de privacidad que sean necesarios;

VI. Aprobar los documentos que serán objeto de la firma electrónica en su modalidad interna y en su modalidad avanzada, a fin de que la suscripción digital tenga la misma equivalencia funcional que la firma autógrafa; y

VII. Las demás funciones que tengan relación con la aplicación y alcance de la firma electrónica avanzada e interna.

Artículo 4: Las facultades del Comité

El comité de uso de firma electrónica tiene dentro de sus facultades las siguientes actividades:

I. La definición de políticas y procedimientos para la operación.

II. Proponer normas para crear y mantener un marco normativo que regule el uso de la firma electrónica en toda la universidad.

III. Definir roles y responsabilidades que implican asignar responsabilidades a los diferentes actores involucrados en los procesos de firma (usuarios, administradores, y los miembros de la comunidad universitaria de la Universidad).

IV. Supervisar los protocolos de seguridad para proteger la integridad y confidencialidad de los documentos firmados electrónicamente.

V. Gestionar Infraestructura tecnológica, para efecto del desarrollo del Sistema de Firma Electrónica, la Interoperabilidad entre los sistemas de Información, sistemas de almacenamiento, sistemas de energía y aquellos que ayuden a la operación, monitoreo, evaluación y mantenimiento, así como la auditoria y de procesos y el análisis de riesgos de la Firma Electrónica.

VI. Los mecanismos para capacitar y difundir toda aquella información que promueva, concientice y ayude a los usuarios al buen uso y las mejores prácticas de la operación de la Firma Electrónica.

Artículo 5. El alcance del uso de la firma electrónica.

La integración de la Universidad se encuentra definida en su Ley Orgánica y su reglamento, por lo que la aplicación de estos lineamientos se extenderá en todos aquellos lugares donde la Universidad tenga presencia incluyendo las plataformas digitales para la educación en línea, a distancia, dual o cualquier modalidad que se aprobada por el Consejo Universitario.

Artículo 6. Observancia en aplicación de documentos.

Las disposiciones de este reglamento son aplicables en los actos del uso exclusivo de la firma electrónica en sus dos modalidades, respecto a los documentos que sean aprobados por el comité para efectos de la equivalencia funcional y la neutralidad tecnológica.

Las instituciones públicas y privadas con las que la Universidad haya suscrito convenios de colaboración podrán hacer uso de la firma electrónica prevista en este reglamento siempre que exista la capacidad, consentimiento y la voluntad de las partes y su aplicación no se encuentre regulada

expresamente por una legislación específica a nivel estatal o federal.

Artículo 7. Efectos de validez.

Para que los documentos firmados a través de los medios digitales disponibles y su utilización surta los efectos jurídicos equivalentes a la firma autógrafa, 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 sidomodificada durante el proceso.

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

Artículo 8. Objetivos del uso de la firma electrónica

La Dirección General de Tecnologías de la Información, desarrollará y coordinará el Sistema de la Firma Electrónica de la Universidad.

El uso de la firma electrónica tiene los siguientes objetivos

I. Contribuir a la gestión de los distintos asuntos administrativos y académicos que determine del Comité de Firma Electrónica universitaria.

II. Establecer un servicio de certificación en la universidad.

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 Electrónica

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

Artículo 9. Uso distinto de la firma electrónica

Las unidades académicas y dependencias administrativas pueden utilizar recursos de identificación electrónicos distintos a la Firma Electrónica, en cualquiera de los casos siguientes:

I. Cuando para la atención de un trámite o solicitud no se requiera la Firma Electrónica 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 distintosa la Firma Electrónica, pero igualmente fiables.

Artículo 10. Uso de la firma electrónica universitaria

Los miembros de la comunidad universitaria, que requieran usar la Firma Electrónica Interna y Avanzada, quienes están debidamente identificados y definidos por la legislación universitaria deberán contar con:

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

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

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

Artículo 11. La autoridad certificadora raíz

El Departamento de Desarrollo de Sistemas, adscrita a la Dirección General de Sistemas de Información, funge como única Autoridad Certificadora Raíz Interna para la Firma electrónica Interna y como enlace con Autoridad Certificadora Raíz Avanzada para la Firma electrónica Avanzada.

Artículo 12. La vigencia de los certificados digitales

Los certificados digitales emitidos por la Universidad Autónoma del Estado de Quintana Roo en colaboración con la Autoridad Certificadora tendrán las vigencias que éstas establezcan.

Artículo 13. La responsabilidad de los agentes certificadores

Los agentes certificadores tienen las siguientes responsabilidades:

I. Emitir el certificado digital con apego a la normatividad en materia de certificados digitales y Firma Electrónica.

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

III. Los que la Entidad certificadora Avanzada y en el caso de Entidad certificadora Interna, por medio del Comité de firma Electrónica determinen.

IV. Generar el certificado digital en presencia del usuario.

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

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

VII. 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.

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

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

Artículo 14. La responsabilidad de los usuarios de sistemas estratégicos.

Entre las responsabilidades de los usuarios de sistemas estratégicos que se incorporen a la Firma Electrónica Universitaria están:

I. Hacer uso de la Firma Electrónica exclusivamente en aquellos servicios y aplicaciones para los que haya sido autorizado por el Comité de Firma Electrónica.

II. Informar de cualquier cambio relevante, nueva aplicación o uso, de la Firma Electrónica en sus sistemas.

III. Utilizar los certificados digitales y el componente de la Firma Electrónica Universitaria, exclusivamente en trámites y servicios de la Universidad.

IV. Acatar la normatividad vigente en materia de Firma Electrónica de la Universidad.

V. Abstenerse de utilizar la Firma Electrónica 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 15. Obligaciones y deberes del Departamento de Desarrollo de Sistemas.

El Departamento de Desarrollo de Sistemas, proporcionará a los sistemas estratégicos que se incorporen en la utilización de la Firma Electrónica, lo siguiente:

I. Información clara y suficiente de los procesos, reglas de operación y políticas deuso de Firma Electrónica.

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

III. Disponibilidad de los servicios de Firma Electrónica, 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 Electrónica.

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

Artículo 16. Medidas de seguridad para el uso de la firma

Es responsabilidad de la Dirección General de Tecnologías de Información,

implementar las medidas de seguridad física y perimetral necesarias para garantizar la transmisión segura y confiable de los datos y los sistemas estratégicos que hagan uso de la Firma Electrónica.

En esa misma lógica deberá proponer al Comité 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 17. Documentos en los que se faculta el uso de la firma electrónica interna y avanzada

Los documentos que el comité determine conforme a sus criterios.

Artículo 18. El contenido de la transmisión de datos

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.

La Autoridad Certificadora Avanzada de la Universidad y la Autoridad Certificadora Interna de la Universidad, 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 19. La estructura del certificado digital

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 certificadodigital;

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 20. La validez del certificado raíz de la Autoridad Certificadora

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

Artículo 21. Requisitos del certificado digital para su emisión y validez

Para la emisión de un certificado digital emitido por la Autoridad Certificadora Avanzada e Interna, el solicitante debe cumplir los siguientes requisitos:

I. Ser miembro activo de la comunidad universitaria.

II. Estar integrado a una aplicación y/o sistema que utilice la Firma Electrónica Universitaria en sus procesos.

III. Estar habilitado por su entidad académica o dependencia universitaria para realizar la 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 la Firma Electrónica Universitaria.

Artículo 22. Obligaciones al solicitar un certificado digital

El solicitante de un certificado digital está obligado a:

a) Firma electrónica avanzada

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.

b) Firma electrónica interna

Disponer de su e.firma actualizada emitida por el Sistema de Administración Tributaria (SAT).

Artículo 23. Obligaciones, derechos y responsabilidades del titular del certificado digital y el uso adecuado del mismo

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 contraseña.

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.

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 digital, 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 seantatados 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.

El titular de un certificado digital es el responsable del uso indebido de su firma electrónica sea esta interna o externa, de los daños y perjuicios ocasionados en cualquiera de los Sistemas de Información de la Universidad, contra actos que lesionen o menoscaben el orden el interés y/o el patrimonio de la universidad, siendo también responsable ante terceros, dando lugar a los procedimientos o sanciones que correspondan de acuerdo a lo establecido por la normatividad de la Universidad por el Comité de firma Electrónica.

Artículo 24. Causales de revocación del certificado

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

I. Olvido de la contraseña 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 de los lineamientos al emitir un certificado sin el consentimiento explícito 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. Separación definitiva o temporal del cargo.

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 contraseña, así como de informarlo inmediatamente al Comité de Firma Electrónica.

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.

Artículo 25. La renovación de los certificados digitales

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 devigencia.

Los certificados digitales de los usuarios deberán ser renovados en coordinación con las áreas académicas y administrativas universitarias durante los periodos que no afecten el ejercicio de los procesos determinados.

Los certificados digitales serán renovados al término de la vigencia de estos 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 administrativa.

Artículo 26. Exclusión de responsabilidad de la universidad respecto al mal uso de la firma electrónica universitaria

La universidad, 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 electrónica de los certificados digitales y su infraestructura.

La universidad no podrá ser objeto de responsabilidad respecto a los daños operjuicios que se ocasionen por la imposibilidad de firmar transacciones electrónicas con Firma Electrónica 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 o sitios no autorizados o reconocidos como oficiales para procesos de Firma Electrónica Avanzada en la universidad.

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 27. La responsabilidad de la universidad

La universidad será responsable de:

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

II. Proporcionar la infraestructura de Firma Electrónica y garantizar el correcto funcionamiento de esta en procesos de emisión de certificados digitales y Firma Electrónica Avanzada en sistemas y aplicaciones autorizadas de la universidad.

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

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

Artículo 28. Aprobaciones de nuevos sistemas y aplicaciones de firma electrónica

El Comité de Firma Electrónica, aprobará la integración de nuevos sistemas y aplicaciones la Firma Electrónica, a partir de criterios de pertinencia, usabilidad y factibilidad.

Artículo 29. Requisitos para integrar nuevos sistemas y aplicaciones de firma electrónica.

Los sistemas que soliciten la integración a la Firma Electrónica deberán cumplir con los siguientes requisitos:

I. Ser una aplicación que esté integrada al Sistema (mencionar nombre del primer sistema a usar)

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

III. Realizar solicitud oficial al Comité de Firma Electrónica Universitaria.

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 de Firma Electrónica

VII. Conocer y apegarse a la normatividad vigente en materia de Firma Electrónica.

Artículo 30. Estructura de la certificación digital de la firma electrónica

La estructura jerárquica de certificación en la Universidad 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 Universidad. Dirección Generalde Tecnologías de la Información es la autoridad certificadora raíz en la Universidad (Interna) y la Autoridad Certificadora para la firma externa (Externa).

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

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

Artículo 31. Obligaciones del responsable de la implementación y ejecución de las directrices instruidas por el Comité.

El Departamento de Desarrollo de Sistemas adscrito a la Dirección General de Tecnologías de la Información, es el responsable de implementar y ejecutar lo establecido por el Comité de Firma Electrónica en materia de Firma Electrónica Universitaria.

Su obligación y responsabilidad de extiende a:

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

II. Asesorar al Comité de Firma Electrónica y a la comunidad universitaria de la firma de la universidad, respecto de nuevas tecnologías en materia de seguridad y criptografía, con la finalidad de mantenera 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 electrónica, 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 electrónica y emitir las recomendaciones pertinentes para su aprobación en el Comité de Firma Electrónica Universitaria;

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 Universidad, sin responsabilidad jurídica al respecto de ese apoyo;

VI. Proponer la difusión en la página institucional de la universidad el material audio visual que facilite la comprensión y el uso del sistema y de la firma electrónica en sus dos modalidades.

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

VIII. Deberán poner a disposición de los interesados en obtener Certificados Digitales, la información relativa a los derechos y obligaciones que adquieren como titulares de un Certificado Digital.

Sus responsabilidades son:

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

II. Vigilar el cabal cumplimiento de la normatividad en materia de Firma Electrónica Universitaria.

III. Adoptar las medidas necesarias para evitar la falsificación, alteración o uso indebido de certificados digitales y de los servicios relacionados con la Firma Electrónica Universitaria.

IV. Garantizar la autenticidad, integridad, conservación, confidencialidad y confiabilidad de la Firma Electrónica Universitaria, así como de los

servicios relacionados con la misma.

V. Establecer los medios y mecanismos necesarios para que los sistemas estratégicos otorguen servicios de certificación en la universidad.

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

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

XI. 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 legislación que salvaguarda los datos personales, el acceso a la información, respeto a los derechos humanos y uso de las tecnologías de la información y comunicación.

Artículo 32. Aclaración en caso de duda del contenido de la integridad de documentos firmas electrónicamente a través de los sistemas institucionales de la Universidad.

El Departamento de Desarrollo de Sistemas, facilitará los medios electrónicos necesarios, en caso de que exista duda sobre la integridad del documento electrónico firmado, a petición del comité. 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 de Firma Electrónica y tercero confiable).

Artículo 33. Opinión para la resolución de controversias.

El comité se encuentra obligado a coadyuvar con las autoridades o representaciones de la Universidad para la investigación y dictaminación en su caso respecto a las controversias que puedan suscitarse con relación al uso de las plataformas digitales y la firma electrónica.

Artículo 34: Vigencia y modificación del lineamiento

El presente lineamiento, podrá ser modificado, previa aprobación comité para la presentación a la autoridad de la Universidad facultada para la emisión de normas institucionales.