ACUERDO No. 784 **FECHA: 16 DE SEPTIEMBRE DE 2015**

POR EL CUAL SE ESTABLECE LA POLÍTICA DE SEGURIDAD INFORMÁTICA PARA LA FUNDACIÓN UNIVERSITARIA AGRARIA DE COLOMBIA – UNIAGRARIA -

El Consejo Superior de la FUNDACION UNIVERSITARIA AGRARIA DE COLOMBIA, en uso de sus facultades legales conferidas por la Ley 30 de 1992, y demás normas concordantes y el Estatuto Orgánico de la Institución vigentes,

CONSIDERANDO:

1. Que la Ley 1581 de 2012 expidió el marco general de la protección de datos personales en Colombia.

2. Que el Decreto 1377 de 2013, reglamentó parcialmente la Ley 1581 de 2012 en los aspectos relacionados con la autorización del titular de información para el tratamiento de datos personales, las políticas de tratamiento de los Responsables y Encargados, el ejercicio de los derechos de los titulares de información, las transferencias de datos personales y la responsabilidad demostrada frente al tratamiento de dichos datos.

3. Que de conformidad con lo anterior, UNIAGRARIA, Institución de Educación Superior privada, de utilidad común, sin ánimo de lucro, cuyo carácter académico es el de Institución Universitaria, con Personería Jurídica reconocida mediante Resolución No. 2599 de 1986, según consta en el certificado expedido por el Ministerio de Educación Nacional, con domicilio en la Calle 170 No.54 A -10 de Bogotá D.C., debe dar cumplimiento a lo allí dispuesto

4. Que la Institución estableció la política de tratamiento de datos personales mediante Acuerdo No. 663 de septiembre 18 de 2013.

5. Que adicionalmente, es necesario definir las políticas de uso y control de los servicios y procedimientos tecnológicos que ofrece UNIAGRARIA a la comunidad académica que permitan elaborar reglamentos y procedimientos de los servicios informáticos.

6. Que corresponde al Consejo Superior estructurar las políticas de la Institución.

ACUERDA:

ARTÍCULO PRIMERO: Establecer la política de seguridad informática, así:

ACUERDO No. 784 **FECHA: 16 DE SEPTIEMBRE DE 2015**

FUNDACION UNIVERSITARIA AGRARIA DE COLOMBIA – UNIAGRARIA
POLÍTICA DE SEGURIDAD INFORMÁTICA

1. OBJETIVO

Determinar la voluntad y propósitos de la Fundación Universitaria Agraria de Colombia para la administración, almacenamiento, protección y confidencialidad de la información electrónica institucional, resguardándola en cualquiera de las fases del flujo de datos en un sistema de información de las amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de las características de integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información.

Teniendo en cuenta lo anterior, también se determinarán las responsabilidades de los funcionarios que lideran actividades de los procedimientos de cada área, además de los actores externos frente a los mecanismos de seguridad.

2. ALCANCE

Inicia desde el registro de la información por parte de los miembros de la comunidad Universitaria, hasta la generación de copias de seguridad que permitan su restauración ante cualquier situación de desastre o evento anormal que influya el flujo correcto de datos.

La institución se rige por el marco de la protección de datos establecida por el Gobierno Nacional en la Ley 1581 del 2012 y en el Decreto 1377 del 2013, en los cuales se reglamenta el ejercicio de los derechos de los titulares de la información, por lo cual los datos entregados por terceros solo serán utilizados en un ámbito académico o en aspectos informativos de sus servicios o eventos.

3. DEFINICIONES

- **Equipo de cómputo:** Son todos aquellos activos (Smartphone, Tablet portátil, servidor o pc de escritorio) para el procesamiento de información que la institución entrega a sus funcionarios.
- **Integridad:** Cuando la información es exacta y completa. Un ejemplo de control para garantizar la integridad son los algoritmos de cifras de control.
- **Disponibilidad:** Cuando la información es accesible a los usuarios autorizados en el momento de requerirla. Un ejemplo de control para garantizar la disponibilidad son los planes de contingencia.
- **Autenticación:** Cuando se puede garantizar la identidad de quien solicita acceso a la información. Ejemplo: El uso de Usuarios y Contraseñas para el ingreso a un sistema de información, Firmas digitales.
- **Autorización:** Cuando la información es accedida solo por los usuarios que tienen los privilegios necesarios y suficientes para hacerlo. Ejemplo: perfiles de usuario en las aplicaciones.
- **Confidencialidad de datos:** Conjunto de reglas que dan acceso total o restringido a la información contenida en una base de datos en la institución.

ACUERDO No. 784 **FECHA: 16 DE SEPTIEMBRE DE 2015**

- **Sistema de Información:** Se entenderá como la aplicación o conjunto de aplicaciones utilizados para generar, enviar, recibir, archivar o procesar datos.
- **Copias de Seguridad (backup):** Imágenes de datos de tal forma que éstas puedan restaurar un sistema después de una pérdida de información.
- **Plataforma tecnológica:** Conjunto de elementos físicos, lógicos tangibles e intangibles utilizados en el procesamiento, almacenamiento o transferencia de datos en un sistema de información, los cuales están enmarcados por normas, procedimientos, métodos y técnicas que brindan esquemas de administración y seguridad ajustados a estándares de calidad.
- **Virus:** Programa o software que se auto ejecuta y se propaga insertando copias de sí mismo en otro programa o documento.
- **Base de datos:** Colección de información organizada de tal forma que un equipo de cómputo pueda guardarla, organizarla o consultarla con fidelidad.
- **Permisos de acceso:** Conjunto de privilegios dados a un usuario en un sistema de información para administrar y consultar los datos.
- **Restauración de información**: Proceso de recuperación de la información de una copia de seguridad en una base de datos en producción con el fin de enmendar errores o corregir pérdidas de información
- **Tiempos de resguardo:** Lapsos de tiempo definidos para resguardar una copia de seguridad son definidos de acuerdo a la periodicidad de la copia de seguridad y al nivel transaccional de la base de datos.
- **Proceso de encriptación:** Procedimiento por el cual se realizan labores de seguridad sobre las claves o accesos a procesos del sistema de información, en dicho procedimiento se valida que los datos no sea visible o extraíble por terceros.
- **Red social:** Es un servicio que utiliza medios tecnológicos para comunicarse con las personas y compartir intereses comunes y/o alguna relación, principalmente de amistad. Las redes sociales pueden ser privadas o públicas, algunos ejemplos de redes sociales son: Facebook, Twitter, herramientas de chat y servicios de mensajería que para efectos de la institución se pueden catalogar como redes sociales, whatsapp, lync, etc.

4. SEGURIDAD PARA EL ACCESO A LOS SISTEMAS DE INFORMACIÓN.

Teniendo en cuenta que la labor realizada por cada funcionario en la institución produce una gran cantidad de archivos y documentos los cuales son almacenados localmente en el equipo de cómputo asignado; es necesario brindar lineamientos de protección al acceso a los equipos así como a los datos allí albergados, es importante aclarar que este esquema debe cubrir los accesos no autorizados por parte de personal de la institución así como de personas ajenas a la misma.

4.1 Seguridad para los sistemas de información almacenados localmente o contratados como servicios externos.

- Se establecerán esquemas de seguridad que protejan y filtren los accesos o consultas de los sistemas de información en la red local así como los posibles ataques externos generados intencional o no intencionalmente (Virus, hackers, robo de identidad digital,

ACUERDO No. 784 **FECHA: 16 DE SEPTIEMBRE DE 2015**

software malicioso) garantizando no solo el buen estado de la información si no la confidencialidad de la misma.

- Los proveedores de servicios de administración o almacenamiento de procesos de tecnología deberán garantizar las buenas prácticas de los servicios ofrecidos, en lo posible que estén certificados en normas de calidad que cubran la gestión y seguridad de la información.
- El proveedor de servicios de gestión de tecnología externa deberá brindar accesos remotos seguros y controlados para la administración de la información almacenada así como el acceso a las copias de seguridad establecidas en el contrato de servicios, para así garantizar su funcionabilidad y el estado de este servicio.

4.2 Seguridad en el acceso a los centros de comunicación y cableado o al data center institucional

- Se establecerán controles de acceso a los centros de comunicaciones y data center a personal externo, interno o proveedores de la institución.
- Los accesos de personal externo a la institución o no autorizado al data center y a los centros de comunicación serán autorizados y monitoreados por la Gerencia Técnica de Sistemas de Información previa solicitud justificada.
- Se proyecta que la plataforma tecnológica utilizada para la seguridad de la información y redes de comunicación deberá ser renovada con una frecuencia no superior a 4 años teniendo en cuenta el crecimiento de usuarios, la obsolescencia de equipos de tecnología y los requerimientos tecnológicos que surgen cotidianamente con la apropiación y uso creciente de la tecnología por parte de la comunidad Universitaria.
- Es indispensable en la ejecución de cualquier labor o servicio tener en cuenta los planos de acometidas internas, ductos y centros de cableado actualizados de la institución.
- El proveedor de servicios se comprometerá a utilizar los planos institucionales y con ellos proyectar las obras a realizar, dichas labores deben contar con aprobación por parte de la institución, los diseños de obra deben ser cumplidos en su totalidad por el proveedor sin realizar alteraciones diferentes a las especificadas únicamente en las áreas y espacios definidos para dicho fin.
- Toda obra que genere cambios en los planos de acometidas internas, ductos y centros de cableado deberá ser documentada por el proveedor mediante la entrega del plano actualizado con los cambios realizados.

4.3 Seguridad en el uso de la plataforma de comunicación y tecnología

- La Gerencia Técnica de los Sistemas de Información velará no solo por el buen uso de los sistemas de información sino también por el fortalecimiento y buen desempeño de la plataforma de comunicaciones brindando los servicios necesarios para la permanente disponibilidad, mejora de tecnología y crecimiento de la misma.
- A los equipos en la red local se restringirá el acceso a páginas web que no se consideren de carácter académico, investigativo o que no aporten al desarrollo integral de las personas de la comunidad Universitaria, es así que se definirán las estrategias para evitar el acceso a pornografía y páginas que inciten a la violencia.

ACUERDO No. 784 **FECHA: 16 DE SEPTIEMBRE DE 2015**

- Se restringirá el uso de carpetas compartidas en la red interna, salvo la debida justificación y autorización de la Gerencia Técnica de Sistemas de Información.
- Los usuarios se autenticarán con usuario y contraseña para acceder al equipo de cómputo, redes sociales, sistemas de información así como a la red interna. Para la asignación de contraseñas se utilizarán procesos de encriptación mediante las funcionalidades de los sistemas y servicios de tecnología.
- Se controlará y monitoreará la instalación de programas que creen puentes o accesos remotos hacia los equipos de la institución (Teamviewer, tunelier,...etc.), en caso de ser estrictamente necesario se hará la debida solicitud a la Gerencia Técnica de Sistemas de Información. También se controlará la descarga de música, videos o programas en general con el objetivo de garantizar el funcionamiento adecuado de la plataforma de comunicaciones.
- El almacenamiento de información institucional en la nube, aplicaciones de chat, canales de video o streaming solo estará permitido en las herramientas dispuestas por la Gerencia Técnica de Sistemas de Información o bajo justificación por parte del jefe de área sustentada.
- Corresponde a la Gerencia Técnica de Sistemas de Información mantener una base de datos actualizada que contenga un inventario del software autorizado para su uso e instalación en los sistemas informáticos institucionales.
- Los equipos asignados a los funcionarios no deberán almacenar información diferente a la de carácter institucional, de ser así la Gerencia Técnica de Sistemas de Información no se hará responsable por backup alguno de dicha información.
- La consulta, actualización o borrado de información en un equipo local deberá ser solicitada y autorizada por el jefe de área.
- El funcionario que tenga a su cargo un equipo de cómputo se hace responsable de la información almacenada en el mismo, debiendo coordinar con la División de Sistemas las copias de seguridad que requiera planificando la tasa de retención que requiera.
- Se prohíbe a funcionarios realizar copias y/o distribuir la información o bases de datos de la institución.
- Los proveedores de servicios de hosting deben mantener confidencialidad de la información institucional almacenada en su data center dentro de un contrato de servicios adquirido por la Universidad.
- La propiedad intelectual de los datos producidos por los funcionarios en los equipos de cómputo asignados o producto de su gestión en los sistemas de información institucionales se considera de propiedad de UNIAGRARIA.

4.4 Permisos, privilegios para el acceso a los sistemas de información

- Todo estudiante, personal administrativo o docente tendrá definido un perfil de acceso a los sistemas de información institucional los cuales serán asignados teniendo en cuenta los parámetros de uso dispuestos para cada caso en cada aplicativo.
- Cada usuario es responsable del uso de las credenciales asignadas (usuario, contraseña) en cada sistema de información, la restitución y/o verificación de contraseñas para el ingreso a cualquier aplicativo solo se efectuará de manera personal dentro de las instalaciones de la institución, salvo casos de fuerza mayor debidamente documentados y avalados por los entes correspondientes. Se tiene

proyectado implementar aplicaciones que permita el restablecimiento de contraseñas de manera remota verificando la identidad del usuario y así cumplir los parámetros de seguridad y privacidad de la información.

- La institución se reserva el derecho de la asignación de credenciales temporales que requieran una renovación de contraseñas en determinado tiempo, así como también la implementación de un plan de renovaciones periódicas de las credenciales que podría incluir la renovación del formato establecido.
- Las credenciales en los sistemas de información institucionales del personal administrativo o docente serán bloqueadas previa notificación del área de Gestión Humana acerca del cese de actividades del funcionario, a diferencia de los estudiantes, a los cuales se les mantendrá su acceso al sistema de información académico a los servicios académicos y al correo electrónico, tan solo se hará en casos excepcionales en los que se infrinja los reglamentos establecidos por la institución.
- Las credenciales asignadas para el ingreso a los sistemas de información institucionales administrativos y académicos son de uso personal e intransferible por lo tanto es responsabilidad del titular, velar por el correcto uso de las mismas, en cuanto a la administración de contraseñas e información gestionada con ellas.

4.5 Copias de seguridad

- La información es un recurso valioso para la institución, por consiguiente debe ser protegida garantizando su confidencialidad, confiabilidad, integridad y disponibilidad.
- El personal autorizado para realizar copia remota será determinado por la Gerencia Técnica de los Sistemas de Información mediante autenticación al sistema de información o al equipo de cómputo que la alberga.
- Se mantendrá una solución tecnológica para almacenar las copias de seguridad acorde con las necesidades y requerimientos de la institución.
- El responsable del almacenamiento de las copias de seguridad en la institución es el Director de Tecnología.
- El primer responsable por la seguridad, almacenamiento y manejo de la información de los equipos personales es la persona a la que se le asigna cada equipo.

4.6 Resguardo de copias de seguridad

- La retención en copias de seguridad para los equipos de cómputo se acordará con los usuarios, sin embargo estará limitada por la disponibilidad del espacio de almacenamiento institucional, por lo tanto se mantendrá de manera general una retención por un periodo de un mes.
- Para los sistemas de información de misión crítica, la retención de las copias es diaria por un periodo de tiempo mensual de acuerdo con el procedimiento definido para tal fin.

ACUERDO No. 784 **FECHA: 16 DE SEPTIEMBRE DE 2015**

4.7 Restauración de información

- Para restaurar copias de información el jefe de área deberá solicitar a la dirección de tecnología la entrega y cargue de datos copiados, indicando la fecha de la copia a restaurar así como el equipo de cómputo en el que se realizará el proceso.
- Al restaurar una copia de seguridad se creará en el equipo de cómputo una carpeta con el nombre del backup y la fecha de realización y en ésta se copiará toda la información recuperada.
- La restauración de datos en los sistemas de misión crítica solo se realizará en el marco de un proceso de malfuncionamiento o de recuperación de desastre, esta deberá estar autorizada por el Gerente Técnico de Sistemas de Información y el responsable del sistema en el área afectada (Académica, Financiera, RRHH, etc.)

5. CORREO ELECTRÓNICO INSTITUCIONAL Y REDES SOCIALES

El medio de comunicación autorizado por UNIAGRARIA para el manejo de información es el correo institucional, por tal fin solo será utilizado por la comunidad universitaria para enviar y recibir contenidos relacionados con asuntos laborales y/o académicos.

5.1 Utilización de correo electrónico institucional

- El servicio de correo electrónico institucional y redes sociales estará suscrito con proveedores externos, por lo tanto la institución se acoge a las políticas de seguridad y protección de información establecidas por el proveedor del servicio.
- Los Sistemas de Información y las herramientas académicas y administrativas utilizadas por la institución para su operación y servicios académicos, dispondrán de procedimientos de modificación y recuperación de contraseñas basados en el uso de la tecnología, sin embargo la institución también pondrá a disposición de sus usuarios procedimientos personales y presenciales que permitan a los usuarios de los sistemas solicitar servicios de recuperación y de modificación de contraseñas.
- La herramienta de administración de cuentas de correo debe contar con las funcionalidades necesarias para controlar y restringir el acceso indebido a la información de las cuentas de correo, así como también debe aplicar procesos de encriptación sobre las contraseñas con el objetivo de que no sean identificadas por usuarios ni por los administradores del sistema. Será responsabilidad de la Gerencia Técnica de Sistemas de Información la administración de la plataforma tecnológica del servicio de correo electrónico institucional.
- El usuario se compromete a abrir los correos electrónicos sólo cuando se conozca al remitente. Asimismo, ser particularmente cuidadoso con los correos electrónicos que traen archivos adjuntos.
- Está terminantemente prohibido enviar o reenviar correos o mensajes tanto masivos como a un solo destinatario que contengan temas políticos, pornográficos, racistas, discriminatorios, ofensivos, religiosos o protegidos por derechos de autor que no cuenten con las autorizaciones o licencias correspondientes.
- El correo electrónico institucional, redes sociales de la institución así como la información contenida y gestionada dentro de los mismos es de propiedad de UNIAGRARIA, y por lo tanto podrá disponer de ella en cualquier momento.

ACUERDO No. 784 **FECHA: 16 DE SEPTIEMBRE DE 2015**

- UNIAGRARIA desactivará, suspenderá o bloqueará cualquier cuenta de correo electrónico o usuario de su propiedad desde la que se infrinja cualquier norma que atente contra la seguridad de la institución así como también, se vulnere la honra y el buen nombre las personas o de la institución, así mismo podrá disponer y entregar los datos allí contenidos a las autoridades correspondientes.
- Las credenciales del correo institucional y red social son de uso personal e intransferible, por lo tanto es responsabilidad del titular de la cuenta, velar por el correcto uso de la misma, en cuanto a la administración de contraseñas e información allí gestionada, almacenada, así como también será responsable por la información enviada o recibida.

5.2 Utilización y publicación en redes sociales

- Los perfiles en las redes sociales de UNIAGRARIA tienen como fin emitir contenidos de valor para toda la comunidad, adicionalmente divulgar las actividades de la institución.
- Los usuarios podrán emitir comentarios sobre los mensajes publicados manteniendo un vocabulario cordial y un lenguaje amable así la comunicación será más efectiva y respetuosa.
- Los usuarios son responsables de sus aportes y comentarios así como de las consecuencias que puedan tener sobre su reputación e imagen.
- Las redes sociales institucionales son un espacio de intercambio de opiniones o para el debate constructivo, no es el ámbito apropiado para crear polémica, descalificar a otros usuarios o a terceros.
- Las opiniones expresadas por los usuarios o por los funcionarios o docentes no reflejan la posición institucional de UNIAGRARIA ni representan sus principios.
- No se permitirá publicar publicidad no relacionada con la función de la institución por parte de los seguidores de nuestras redes sociales.
- UNIAGRARIA podrá seguir en sus perfiles corporativos la información de entidades, instituciones o personas sin que esto implique aval alguno de la misma.
- Los logos de UNIAGRARIA hacen parte de la Propiedad Intelectual de la institución, los usuarios de las redes sociales deben respetarlos y no utilizarlos sin la debida autorización.
- La institución debe preservar el buen uso de sus perfiles e imagen, por ello dispondrá de un administrador de contenidos que se reserva el derecho a eliminar, sin derecho a réplica, cualquier aportación que:
    a. Considere ilegal, irrespetuosa, amenazante, infundada, calumniosa, inapropiada, ética o socialmente discriminatoria o laboralmente reprochable o que, de alguna forma, pueda ocasionar daños y perjuicios materiales o morales contra la institución, sus empleados, colaboradores o terceros.
    b. Incorpore datos de terceros sin su autorización.
    c. Incorpore publicidad no relacionada con la institución.
- UNIAGRARIA no se hace responsable de los sitios web no propios a los que se puede acceder mediante vínculos (links) desde los contenidos puestos a su disposición por terceros, que incluyan fotos, documentos, vídeos y otros contenidos, sin embargo podrá retirar los enlaces a estos sitios en caso que lo considere pertinente.

ACUERDO No. 784 **FECHA: 16 DE SEPTIEMBRE DE 2015**

- UNIAGRARIA se reserva el derecho a modificar, suspender, cancelar o restringir el contenido de los perfiles en las redes institucionales así como los vínculos o la información obtenida a través de ella, sin necesidad de previo aviso.

PARAGRAFO 1: La presente política interna para la seguridad informática está sujeta en un todo a las disposiciones vigentes, las normas que las modifiquen, aclaren, complementen o sustituyan.

ARTICULO SEGUNDO: UNIAGRARIA, podrá modificar la presente política como consecuencia de circunstancias que así lo justifiquen, de lo cual se dará el correspondiente aviso a la comunidad académica.

ARTICULO TERCERO: La política que aquí se adopta y rige a partir de la fecha y por el tiempo que sea necesario para la ejecución de las actividades asignadas a cada finalidad.

COMUNÍQUESE Y CUMPLASE

ALVARO ZÚÑIGA GARCÍA
Presidente

JOHN JAIRO GUARIN RIVERA
Secretario General

UNIAGRARIA
Fundación Universitaria Agraria de Colombia
Secretario General