RESOLUCIÓN No. 007298 DE 10 DE MAYO DE 2023

Por la cual se define el Marco de Referencia del Sistema de Gestión de Seguridad de la Información – SGSI, y se deroga la Resolución 4256 del 3 de marzo de 2015

RECTOR DE LA UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

En uso de sus atribuciones legales y estatutarias y,

CONSIDERANDO:

Que la Universidad Nacional Abierta y a Distancia (UNAD), creada por la Ley 52 de 1981 como UNISUR, transformada en su nombre por la Ley 396 de 1997 y, en su naturaleza jurídica, por el Decreto 2770 del 16 de agosto de 2006, es un ente universitario autónomo del orden nacional, con régimen especial en los términos de la Constitución y la ley.

Que, en consecuencia, cuenta con personería jurídica, autonomía académica, administrativa, presupuestal, contractual y financiera, y patrimonio independiente, por lo tanto, no pertenece a ninguna de las ramas del poder público; tiene capacidad para gobernarse y designar a sus directivas, y está vinculada al Ministerio de Educación Nacional, en los términos definidos en la normativa vigente.

Que la Universidad Nacional Abierta y a Distancia -UNAD cumple con seis responsabilidades sustantivas a saber: la formación, la investigación, la proyección social, la internacionalización, la inclusión y la innovación.

Que la normativa vigente reconoce a las universidades, en su condición de entes universitarios autónomos, entre otros derechos, el de darse y modificar sus estatutos, el de adoptar sus correspondientes regímenes y establecer, arbitrar y aplicar sus recursos para el cumplimiento de su misión social y de su función institucional.

Que la Universidad Nacional Abierta y a Distancia -UNAD tiene como misión contribuir a la educación para todos a través de la modalidad abierta, a distancia y en ambientes virtuales de aprendizaje, mediante la acción pedagógica, la proyección social, el desarrollo regional y la acción comunitaria, la inclusión, la solidaridad, la investigación, la internacionalización y la innovación en todas sus expresiones, con el uso intensivo de las tecnologías, en particular de la información y de las comunicaciones, para fomentar y acompañar el aprendizaje autónomo, significativo y colaborativo, generador de cultura y espíritu emprendedor que en el marco de la sociedad global y del conocimiento propicie el desarrollo económico, social y humano sostenible de las comunidades locales, regionales y globales con calidad, eficiencia y equidad social.

Que el artículo 15 de la Constitución Política de Colombia reconoce el derecho fundamental a la intimidad personal y familiar, al buen nombre y el deber del Estado de respetar y hacer respetar dichos derechos, estableciendo a la vez que la recolección, tratamiento y circulación de datos debe ser respetuoso con la libertad y demás garantías constitucionales.

RESOLUCIÓN No. 007298 DE 10 DE MAYO DE 2023

Por la cual se define el Marco de Referencia del Sistema de Gestión de Seguridad de la Información – SGSI, y se deroga la Resolución 4256 del 3 de marzo de 2015

Que el Documento CONPES 3995 de 2020 "Política Nacional de Confianza y Seguridad Digital" estableció un plan de acción orientado a fortalecer las capacidades en seguridad digital de la ciudadanía y los sectores público y privado, con el fin de aumentar la confianza digital en el país.

Que mediante Resolución número 00500 de 10 de marzo de 2021 del Ministerio de Tecnologías de la Información y las Comunicaciones se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.

Que mediante Resolución número 000746 del 11 de marzo de 2022 del Ministerio de Tecnologías de la Información y las Comunicaciones se "fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la resolución No. 500 de 2021"

Que mediante Resolución No. 004815 del 27 de Agosto de 2012, derogada por la Resolución No. 6018 del 5 de Diciembre de 2012, se establecieron las políticas para la clasificación y el manejo de la información confidencial en la UNAD.

Que mediante Resolución No. 004793 del 22 de Agosto de 2013, se establecieron los lineamientos sobre la seguridad de la información en la UNAD.

Que mediante Resolución No. 7966 del 16 de Octubre de 2014, modificatoria de la Resolución No. 006858 del 22 de Agosto de 2014 la UNAD, se conformó el Sistema Integrado de Gestión, y en el mismo se constituyeron el Componente de Gestión de la Seguridad de la Información y el Componente de Gestión de Servicios de Infraestructura Tecnológica.

Que mediante Resolución No. 004256 del 3 de Marzo de 2015, se estableció el Marco de Referencia del Sistema de Gestión de Seguridad de la Información (SGSI) en la UNAD.

Que la Ley Estatutaria 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales" establece una serie de principios relacionados con el tratamiento de datos personales, entre ellos, el principio de seguridad que impone el deber a responsables y encargados del tratamiento de datos, de adoptar las medidas técnicas, humanas y administrativas necesarias para garantizar la seguridad de los registros contenidos en bases de datos, evitando que estos sean adulterados, se pierdan o sean objeto de consulta, acceso o uso no autorizado o fraudulento.

Que la UNAD para satisfacer su creciente demanda educativa, ha aumentado su inventario tecnológico tanto en hardware, software e información, por lo que se hace necesario actualizar el Marco de Referencia del Sistema de Gestión de Seguridad de la Información (SGSI), tomando como base la Norma ISO 27001:2015 y demás normas concordantes, desde la cual se asegure la continuidad del Sistema de Gestión de la

Seguridad de la Información (SGSI) y la adecuada y eficiente articulación de los actores que intervienen.

Que conforme a lo anteriormente expuesto se hace necesario actualizar el marco de referencia del Sistema de Gestión de Seguridad de la Información en la Universidad Nacional Abierta y a Distancia -UNAD.

En mérito de lo expuesto,

R E S U E L V E:

CAPÍTULO I
DISPOSICIONES GENERALES

Artículo 1. Finalidad La presente resolución tiene como finalidad definir el marco de referencia para la implementación del Sistema de Gestión de Seguridad de la Información – SGSI a través de la estandarización de componentes particulares en los principales campos de acción que pueden afectar la integridad, confidencialidad y disponibilidad de la información institucional.

Artículo 2. Aplicación. Estos componentes aplican a todos los procesos y procedimientos que conforman el Sistema Integrado de Gestión de la Universidad - SIG, así como a todas las actuaciones administrativas y académicas que desarrollen sus distintas unidades y dispositivos, por intermedio de los funcionarios administrativos, cuerpo docente, contratistas, consejeros, e-monitores y en general a todos aquellos que conforman la plataforma humana Unadista, independiente de su forma de vinculación.

Artículo 3. Definiciones. Para efectos de la aplicación de la siguiente resolución, se adoptan las siguientes definiciones:

a. **Activos de Información:** Cualquier componente (humano, tecnológico, software, manuales, documentos físicos y electrónicos, entre otros) que tiene importancia para la organización y signifique riesgo si llega a manos de personas no autorizadas al manejo de esta.

b. **Base de Datos:** Conjunto de datos almacenados y organizados en medios físicos o electrónicos con el fin de facilitar su tratamiento, acceso y recuperación.

c. **Ciberseguridad**: Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados.

d. Ciberdefensa: Conjunto de acciones de defensa activas, pasivas, proactivas, preventivas y reactivas para asegurar el uso propio del ciberespacio y negarlo al enemigo o a otras inteligencias en oposición[1].

e. CSIRT: *Computer Security Incident Response Team* (Equipo de respuesta a incidentes de seguridad cibernética).

f. CSIRT ACADEMICO: *Computer Security Incident Response Team* (Equipo de respuesta a incidentes de seguridad cibernética) que atienden comunidades académicas, universidades, facultades, escuelas o institutos.

g. Copias de respaldo o *Backups*: Copia que se realiza a la información institucional definida como importante, sensible o vulnerable; con el fin de utilizarla posteriormente para restablecer el original ante una eventual pérdida de datos, para continuar con las actividades rutinarias y evitar pérdida generalizada de datos.

h. Clasificación de seguridad del documento: Identificación estratégica adoptada por el Sistema de Gestión Documental adscrito a la Secretaría General para llevar a cabo la gestión interna referente al mantenimiento de la seguridad de la información, de acuerdo con su importancia para la organización. Esta clasificación se define como:

- **Público:** Información de dominio público física o electrónica que la universidad puede dar a conocer a terceras partes como estudiantes, proveedores, docentes y demás estamentos que tengan alguna relación directa o indirecta. Dicha información puede estar publicada en carteleras de la entidad, en las páginas web oficiales de la Universidad o en los medios de comunicación físicos o digitales usados de forma oficial por la Universidad.

- **Controlado:** Documentos de gestión físicos o electrónicos de las diversas unidades de la institución, que contienen los métodos de trabajo usados para su operación y/o para formación del personal. El acceso a esta información está restringido a los miembros de cada área o disponibles para los ejercicios de auditoría interna o externa de la institución.

- **Privilegiada:** Documentos confidenciales, en construcción, estratégicos o con información, descriptiva de claves, operacional, estratégica o datos técnicos de funcionamiento de las diversas unidades de la institución, que pueden ser físicos o electrónicos. Esta información solamente será

[1] http://www.cari.org.ar/pdf/ciberdefensa_riesgos_amenazas.pdf

accedida por personal autorizado para su uso y/o para atender solicitudes derivadas de los procesos de auditorías internas o externas y/o para atender requerimientos de orden legal o jurídico.

i. **Código fuente:** Conjunto de instrucciones escritas en algún lenguaje de programación de computadoras, hechas para ser leídas y transformadas por alguna herramienta de software (compilador, intérprete, ensamblador) en lenguaje de máquina o instrucciones ejecutables en el computador.

j. **Credenciales de acceso:** Privilegios de seguridad agrupados bajo un nombre y contraseña, que permiten acceso a aplicaciones y sistemas de información.

k. **Custodio:** Es el usuario final o persona que opera el activo y que se asegura que la información relacionada con este activo esté protegida. En ocasiones, el responsable y el custodio son la misma persona.

l. **Datacenter, Centro de Datos o CPD (Centro de Procesamiento de Datos):** Sala o construcción dispuesta para el alojamiento seguro de los equipos de cómputo necesarios para el procesamiento y almacenamiento de la información de una organización (Servidores, SAN, equipos de comunicación, etc.).

m. **Dispositivo de reconocimiento biométrico:** Elementos de seguridad utilizado en sistemas computarizados que sirve para identificar atributos físicos como rasgos faciales, patrones oculares, huellas digitales, la voz y la escritura.

n. **Dispositivo móvil:** Elementos tecnológicos de tamaño pequeño con capacidades de procesamiento, memoria y conexión a Internet (Incluye computadores portátiles).

o. **Dato sensible o vulnerable:** También llamado activo sensible, es el nombre que recibe la información personal o institucional de carácter confidencial y particularmente autorizada por su propietario del activo (datos personales, información financiera, contraseñas de correo electrónico, domicilio, datos de investigaciones).

p. **Dato Origen:** Elemento inicial para la construcción de información o conocimiento**,** susceptible de protección y control**.**

q. **Dato personal**: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. Se clasifican:

1. Dato personal público: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad decomerciante o de servidor público. Por su naturaleza, los datos públicos

pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

2. Dato personal privado: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. Tienen esta naturaleza los gustos o preferencias de las personas.

3. Dato Semiprivado: Es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento interesa no sólo a su titular sino a cierto sector o grupo de personas. (Por ejemplo, cuando se trata de los datos financieros o crediticios.)

4. Dato sensible: Es aquel que afecta la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, organizaciones de derechos humanos o que promuevan intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos, entre otros.

r. **Niveles de Respaldo:** Se refiere a la cantidad de copias o respaldos que se tiene de datos determinados. Si se cuenta con una sola copia, se está hablando de un respaldo de 1er. Nivel; si se tienen dos copias, de una copias o respaldos de 2do. nivel. Cuanto mayor sea el número de niveles de copias o respaldos, menor será el riesgo de perder los datos.

s. **Oficial de Seguridad:** Profesional responsable de alinear las iniciativas de seguridad con los objetivos misionales, garantizando que los bienes y las tecnologías de la información estén adecuadamente protegidas.

t. **Propietario**: Individuo que se le otorga la propiedad del activo y del riesgo de este en cada una de las unidades y dispositivos que conforman la estructura organizacional de la UNAD.

u. **RBAC**: mecanismo de control de acceso que define los roles y los privilegios para determinar si a un usuario se le debe dar acceso a un recurso.

v. **Servidor:** Equipo de cómputo físico o virtual, cuyo propósito es proveer servicios a otros dispositivos dentro de la red.

w. **Servidor de Archivos:** Recurso compartido empleado como repositorio de información institucional tanto de funcionarios, docentes y/o contratistas como de grupos y unidades funcionales, donde se definen permisos de acceso de acuerdo a los roles asignados al interior de la organización.

x. **Seguridad de la Información:** Son todas aquellas medidas proactivas, preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información.

y. **Servidores de Almacenamiento:** Equipo servidor físico o virtual dotado con varios discos duros destinados a almacenar, respaldar y compartir datos.

z. **Sistema Operativo (SO) u Operating System (OS):** Programa o conjunto de programas que en un sistema informático gestiona los recursos de hardware y provee servicios a los programas de aplicación, ejecutándose en modo privilegiado respecto de los restantes.

aa. SOC: *Security Operations Center.* El Centro de Operaciones de Seguridad emplea personas, procesos y tecnología para monitorear y mejorar continuamente la postura de ciberseguridad y ciberdefensa de una organización mientras previene, detecta, identifica, protege, contiene, analiza, responde y se recupera a un incidente de ciberseguridad

bb.V-SOC: Virtual *Security Operations Center.*

cc. Usuarios: Entiéndase por aquel que hace uso de alguno de los sistemas que la universidad provee (Académico, Directivo, Administrativo, Operativo o de Gestión), mediante la asignación de un usuario y una contraseña.

CAPÍTULO II
DE LOS DISPOSITIVOS MÓVILES

Artículo 4. Objetivo del componente para Dispositivos Móviles. El objetivo de este componente es brindar las condiciones para el manejo de los dispositivos móviles asignados por la Universidad, para que los usuarios hagan un uso responsable de los mismos.

Artículo 5. Dispositivos móviles y portátiles. Los dispositivos móviles asignados a administrativos, contratistas, docentes, e-monitores, y en general a la plataforma humana Unadista, son de uso exclusivo de la entidad, y los responsables de dichos equipos deberán velar por su adecuado uso, cuidado, mantenimiento y protección, de acuerdo con lo dispuesto en la normatividad interna, el contrato, la resolución de vinculación respectiva o la convocatoria correspondiente para el caso de e-monitores.

Parágrafo 1. El usuario de los dispositivos móviles se hace responsable penal y disciplinariamente por los daños y perjuicios, que se derivan como consecuencia del mal uso o pérdida de estos y la información almacenada.

Parágrafo 2. El funcionario asumirá la responsabilidad administrativa, penal y disciplinaria y costos asociados a la pérdida del dispositivo, fuga o uso indebido de la información que se encontraba almacenada en el dispositivo perdido; además, deberá dar cumplimiento a las regulaciones vigentes emanadas desde la Gerencia Administrativa y Financiera (GAF) y la Gerencia de Plataformas e Infraestructura Tecnológica (GPIT), concernientes a los costos del activo físico.

Artículo 6. Uso Redes inalámbricas. Se permite que los usuarios hagan uso de las redes inalámbricas institucionales en los dispositivos asignados por la universidad, con fines laborales y para complementar los objetivos contractuales, respetando las políticas de red institucionales.

Parágrafo 1. Los usuarios deben evitar hacer uso de redes inalámbricas de uso público (poco seguras), para transferencia de información institucional.

Artículo 7. Proveedores y visitantes. Respecto del personal que preste sus servicios para los proveedores y aquellos visitantes que ingresen a la institución y que requieran para sus actividades o servicios a prestar el uso de equipos de cómputo portátiles de su propiedad o de la UNAD, se aplicarán las mismas restricciones de seguridad definidas en esta política y demás lineamientos definidos por la Gerencia de Plataformas e Infraestructura Tecnológica en adelante -GPIT.

CAPÍTULO III
DEL CONTROL DE ACCESO LÓGICO

Artículo 8. Objetivo del componente de control de acceso lógico. La UNAD establece los controles de acceso lógico para los usuarios que hacen uso de los recursos tecnológicos y los sistemas de información de la universidad, propendiendo por asegurar que los usuarios tengan acceso únicamente a los recursos necesarios para el desarrollo de sus labores.

Parágrafo único: La UNAD continuará implementando metodologías y tecnologías para garantizar el acceso, el control, la individualización e identificación y el no repudio de los accesos a los sistemas de información, plataformas y demás elementos tecnológicos de la Institución, así como también respecto de las acciones que se desarrollen dentro de los mismos.

Artículo 9. Responsabilidad de la GTHUM. El Gerente de Talento Humano será responsable de informar a la GPIT sobre las novedades del personal administrativo, contratista y/o docente de la institución, con el fin de poder asignar y gestionar desde la GPIT los respectivos permisos de acceso a los recursos tecnológicos institucionales.

Parágrafo único. Las novedades incluyen la creación, modificación, retiro y terminación de accesos y permisos de usuarios.

Artículo 10. Permisos y privilegios. La GPIT es la encargada de suministrar y modificar los permisos y privilegios a los usuarios, en los mecanismos y/o sistemas de autenticación definidos, así como también los accesos al sistema de información institucional y a las aplicaciones que sean complementarias al mismo.

Parágrafo 1. Permisos de acceso. Los líderes de unidad tienen la responsabilidad de definir y solicitar los permisos de acceso a los sistemas de información de la institución de acuerdo con los perfiles y necesidades de su personal, según sus funciones, términos contractuales o roles definidos al interior de la entidad.

Parágrafo 2. La GPIT es la unidad encargada de autorizar, gestionar y controlar los usuarios con permiso de "Administrador local" en equipos informáticos de la institución.

Artículo 11. Restricción. Se prohíbe el uso de las cuentas de usuario "Administrador local" en equipos informáticos de la institución, salvo en aquellos casos que estén debidamente justificados y autorizados por la GPIT.

Artículo 12. Credenciales de acceso: La creación y administración de las credenciales de acceso institucionales a los usuarios, se debe realizar a través de la GPIT o la unidad que dentro de la estructura organizacional haga sus veces, garantizando y documentando el control de acceso basado en roles (RBAC). Su asignación deberá hacerse a cada usuario de modo tal que se pueda controlar de manera específica su trazabilidad, uso y acciones que adelante a partir del permiso asignado.

Parágrafo 1. Los usuarios son los únicos responsables por la seguridad de sus credenciales de acceso (usuario y contraseña), las cuales son de uso exclusivo, único e intransferible.

Parágrafo 2. La GPIT establecerá los lineamientos de seguridad para la creación y actualización de las contraseñas para el acceso a los recursos lógicos de la institución.

Parágrafo 3. La UNAD recopilará y hará uso de la información producto de cada una de las interacciones únicamente entre los sistemas de información propios de la institución y los usuarios, con el fin de verificar la autenticidad de los usuarios.

Parágrafo 4. En caso de detectar un acceso que no cumpla con lo establecido la presente reglamentación, la GPIT determinará la posible suspensión de las credenciales de ingreso a los sistemas de la universidad, e informará inmediatamente a la Gerencia de Talento Humano (cuando se trate de la plataforma humana) y a la Oficina de Control Interno Disciplinario suministrando información concreta sobre la individualización e identificación de los posibles responsables del acceso irregular; a su vez, informará a la Fiscalía General de la Nación en aquellos casos en que dicho acceso pueda enmarcarse en uno de los tipos penales contemplados en el la

normatividad vigente. Dicha suspensión se mantendrá hasta que la Unidad afectada realice la verificación respectiva y emita un concepto definitivo.

Parágrafo 5. El incumplimiento a lo dispuesto en el parágrafo anterior se tendrá como incumplimiento de los deberes sustanciales de la GPIT y dará lugar a la actuación disciplinaria sin perjuicio de la eventual compulsa de copias a las autoridades penales competentes cuando las circunstancias así lo requieran.

CAPÍTULO IV
SOBRE EL USO DE CONTROLES CRIPTOGRÁFICOS

Artículo 13. Objetivo del componente sobre el uso de controles criptográficos. El objetivo del componente sobre el uso de controles criptográficos está asociado a la implementación de tecnologías y elementos que permitan encriptar datos para salvaguardar la integridad y confidencialidad la información.

Artículo 14. Controles criptográficos: La UNAD establecerá la implementación de procesos criptográficos en los casos en los que considere necesario, para la protección de la información sensible.

Parágrafo. La GPIT debe brindar el apoyo y soporte necesarios para los procesos y sistemas criptográficos, así como también los lineamientos, las actualizaciones de complejidad del algoritmo y recomendaciones necesarios para la implementación de controles criptográficos en las diferentes herramientas tecnológicas para protección de la información sensible, que debe ser cifrada.

CAPÍTULO V
DE LA TRANSFERENCIA E INTERCAMBIO DE INFORMACIÓN

Artículo 15. Objetivo del componente de transferencia e intercambio de información. Consiste en establecer los medios de transferencia e intercambio de la información con el fin de garantizar la disponibilidad, confidencialidad e integridad de la información

Artículo 16. Intercambio de información. Cada unidad con el apoyo de la GPIT debe realizar acciones técnicas básicas: integridad, confidencialidad y disponibilidad con respecto a la seguridad de la información y al uso de protocolos para realizar transferencia de información digital entre unidades, usuarios y terceras partes de la institución, respetando la normatividad relacionada con Protección de Datos de la UNAD.

Parágrafo 1. Está prohibido para los usuarios el envío de información que esté protegida por la política de privacidad de la información y que no sea para uso exclusivo de los procesos y/o procedimientos de la UNAD.

Parágrafo 2. Cada supervisor de contratos suscritos por la UNAD deberá hacer seguimiento al estricto cumplimiento de las disposiciones contenidas en el presente marco de referencia del sistema de gestión de la seguridad de la información, previo a la transferencia de información tanto física como en digital[2].

Parágrafo 3. En el caso, que la UNAD requiera compartir información sensible con algún proveedor, este deberá suscribir y autorizar el Acuerdo de Confidencialidad, en el marco de la ejecución contractual. De ser datos personales esta transferencia deberá estar contemplada en la autorización que otorga el titular para el tratamiento de los mismos.

Artículo 17. Difusión. La GPIT y el CSIRT Académico UNAD generará campañas de buenas prácticas para la gestión de la seguridad de la información digital.

Artículo 18. Espacio de almacenamiento institucional. La GPIT será la unidad encargada de definir los mecanismos y lineamientos para el uso del espacio de almacenamiento institucional.

Parágrafo 1. Los usuarios de cada unidad son responsables de la adecuada administración, gestión y seguridad de los espacios físicos o digitales de almacenamiento de información asignados por la institución,

Parágrafo 2. El propietario del activo de información debe informar al oficial de Seguridad y la Secretaria General el tipo de dato almacenado según ley 1712 de 2014, y si debe estar reportado ante el Registro Nacional de Bases de Datos y si los datos que contiene son públicos, semiprivados, privados o sensibles según ley 1581 de 2012.

CAPÍTULO VI
DEL DESARROLLO SEGURO

Artículo 19. Objetivo del componente de desarrollo de software. Establecer los lineamientos de desarrollo seguro de software para la UNAD.

Artículo 20. Desarrollo de software. La GPIT, la Vicerrectoría de Innovación y Emprendimiento, en adelante VIEM, serán las unidades encargadas de realizar la revisión de la estructura e integración de los desarrollos de software realizados por y para la institución, validando la capacidad de ofrecer un entorno de operación seguro.

Relacionado con el INSTRUCTIVO DE PROGRAMA DE GESTIÓN DOCUMENTAL FÍSICA Y ELECTRÓNICA – Código:I-2-2-1, ítem 11.7.2 Generalidades de las Transferencias Documentales.

Parágrafo 1. La UNAD establece los lineamientos de desarrollo y facilitará los elementos y ambientes de trabajo tecnológico adecuados, para el equipo de desarrollo de software de la institución.

Parágrafo 2. Las áreas solicitantes de desarrollos nuevos o modificaciones a desarrollos ya existentes deben asignar recursos financieros, funcionarios o contratistas, idóneos en el tema solicitado, para la realización y aprobación de los diferentes desarrollos de software y es el CSIRT Académico UNAD[3] quien realice la validación de seguridad del aplicativo previo a su puesta en operación.

Parágrafo 3. La UNAD se reserva el derecho de acceso y control al código fuente de las aplicaciones informáticas y del desarrollo de software de autoría de la UNAD, realizados para la operación de la institución

Parágrafo 4. La GPIT se reserva el derecho a no implementar desarrollos de software que no hayan cumplido con los lineamientos establecidos para tal fin por esta unidad. Sin embargo, las aplicaciones de terceros o externos que sean de uso obligatorio de la UNAD tendrán soporte de la GPIT en el marco de sus funciones y de sus competencias.

Parágrafo 5. Las solicitudes de desarrollo o modificación de aplicaciones que no pueden ser atendidas por la VIEM y/o GPIT se tercerizarán, para lo cual se deberá cumplir con el procedimiento de "Contratación de bienes y servicios" vigente y lineamientos de desarrollo de la UNAD.

Artículo 21. Registro. El Registro de soporte lógico de los desarrollos de software de la Universidad o contratados por la misma, se liderará por el equipo de transferencia tecnológica y transformación del conocimiento de la VIEM. La Secretaria General adelantará las acciones necesarias ante la instancia de registro que corresponda, previa solicitud de la VIEM, atendiendo a los lineamientos definidos por la UNAD.

Parágrafo único. Corresponde a cada unidad adelantar la actualización periódica del registro interno de activos intangibles en la aplicación que disponga la Universidad para tal fin.

CAPÍTULO VII
DEL ESCRITORIO Y PANTALLA LIMPIOS

Artículo 22. Objetivo del componente de escritorio y pantalla limpios. Pretende concientizar a los usuarios acerca de la necesidad que los escritorios de trabajo y pantallas de los equipos tecnológicos limpios con el fin de optimizar su correcto uso.

[3] Centro de innovación y Productividad: Centro de Respuesta a Incidentes Informáticos

Artículo 23. Medidas de seguridad para escritorios y pantallas. El escritorio de trabajo de todos los administrativos, contratistas y docentes debe permanecer completamente despejado y libre de documentos controlados, de documentos en construcción y/o reservados a la vista del público.

Parágrafo 1. Este componente aplica también para los proveedores cuando les sea asignado equipo de cómputo por parte de la UNAD.

Parágrafo 2. Todos los documentos controlados y/o reservados ya sea físico o virtuales, y en general toda la documentación clasificada como "Información confidencial o reservada", debe permanecer almacenada y custodiada en un lugar seguro, siempre que mantenga las debidas condiciones de almacenamiento y claves de acceso.

Parágrafo 3. El escritorio o la pantalla de inicio del computador, *tablet*, escritorio virtual o cualquier dispositivo que permita el acceso a información institucional, debe permanecer libre de documentos, carpetas e íconos de acceso directo a archivos y/o carpetas que contengan documentos. En lo posible, solo deben permanecer en la pantalla los íconos por defecto que establezca la GPIT.

Parágrafo 4. La plataforma humana de la UNAD, terceros y/o proveedores son responsables de velar por la adecuada protección de la información física y lógica dentro de su entorno de trabajo.

CAPÍTULO VIII
DE LA GESTIÓN DEL CAMBIO

Artículo 24. Componente de gestión del cambio. Se encarga de velar por la correcta articulación y gestión del cambio de la infraestructura tecnológica de la universidad.

Artículo 25. Recursos. Los recursos tecnológicos de la universidad corresponden a los activos de información que soportan la gestión de la información relacionados con: datos, claves criptográficas, servicios, software de desarrollo propio o software subcontratado, software estándar y entregadas formalmente para su administración, hardware, equipos de comunicación, equipos auxiliares, dispositivos de almacenamiento, personas e instalaciones locativas; los manejadores de bases de datos institucionales y la información documentada de los servicios gestionados por la GPIT.

Artículo 26. Modificaciones en los recursos tecnológicos. Cualquier modificación a las condiciones actuales de funcionamiento de los recursos tecnológicos administrados por la GPIT serán considerados como cambios tecnológicos siendo documentados para la trazabilidad del mismo establecido por el SIG.

Parágrafo único. En caso de presentarse una situación que genere afectación y que requiera tomar medidas preventivas o correctivas inmediatas, que estén afectando directamente la normal prestación de los servicios de la UNAD, se podrán realizar cambios de emergencia por parte de la GPIT.

CAPÍTULO IX
DEL RESPALDO Y CONTINUIDAD DE LA OPERACIÓN

Artículo 27. Objetivo del componente de respaldo y continuidad de la operación. El objetivo del componente de respaldo y continuidad de la operación es generar las condiciones apropiadas para el respaldo de la información institucional, que permitan la continuidad de la operación de los sistemas de información de la universidad, cuando esto sea requerido.

Artículo 28. Copias de respaldo y administración de equipos. El Gerente de GPIT designará el personal responsable de la gestión de las copias de respaldo y la administración de los equipos de respaldo masivo de datos.

Parágrafo 1. El encargado de la administración de equipos de respaldo masivo de datos velará por las copias de respaldo y por el resguardo de los datos contenidos en ellos; de igual forma por su integridad, disponibilidad y confidencialidad.

Parágrafo 2. Los medios de respaldo empleados para efectuar las copias de seguridad en la UNAD serán definidos por la GPIT.

Parágrafo 3. Se hará respaldo a los archivos, aplicaciones, bases de datos y sistemas operativos de los servidores físicos y virtuales acordes a su nivel de criticidad para la UNAD, contemplados en el Inventario de Servidores de la UNAD.

Parágrafo 4. Se incluye como información a respaldar las configuraciones completas de los servidores, relacionados en el Inventario de Servidores de la UNAD.

Parágrafo 5. La GPIT será la responsable de definir los mecanismos adecuados para la ejecución de los respaldos de información, así como la periodicidad, horario de realización lugar de almacenamiento y el tiempo de retención de las copias.

Parágrafo 6. Cuando sea necesario un respaldo por demanda, se debe solicitar formalmente a través de la Mesa de Ayuda por parte del usuario y/o administrador del activo de información.

Artículo 29. Responsables. Los responsables de la administración de equipos de respaldo masivo de datos realizarán la comprobación periódica del estado de las

copias y restauración, con el fin de garantizar la disponibilidad e integridad de los datos almacenados.

Parágrafo 1. Los responsables de la ejecución de copias de respaldo deben aplicar los lineamientos establecidos en el documento "Instructivo para Respaldo de Información"[4].

Parágrafo 2. Cada usuario es responsable de la ubicación de la información del equipo local, dentro de los espacios de almacenamiento que la UNAD tiene destinados para tal fin.

Artículo 30. Medidas de emergencia. En caso de alto riesgo de seguridad de la información, ataque informático y/o capacidad de continuidad de la operación, el Vicerrector de Innovación y Emprendimiento de la UNAD podrá determinar y disponer la desconexión de servicios, aplicaciones y/o sistemas de información que se encuentren comprometidos para salvaguardar la integridad de la información institucional, teniendo presente el manual de crisis para la desconexión de servicios y el plan de comunicaciones.

CAPITULO X

DE LA GESTIÓN, ADMINISTRATIVA Y CONSERVACIÓN DOCUMENTAL

Artículo 31. **Alcance.** La UNAD está obligada a la creación, organización, preservación y control e los archivos, teniendo en cuenta los principios de procedencia, orden original, el ciclo vital de los documentos y la normatividad archivística, en el marco de los lineamientos, la normatividad y los instructivos internos que para el efecto genere el Sistema de Gestión Documental y Función Notarial de la UNAD.

Artículo 32. **Conservación de los Archivos**. La UNAD deberá garantizar los espacios y las instalaciones necesarias para la conservación de sus archivos. En los casos de construcción de edificios públicos, adecuación de espacios, adquisición o arrendamiento, deberán tener en cuenta las especificaciones técnicas existentes sobre áreas de archivo, como lo establece el Archivo General de la Nación.

Artículo 33. Propiedad de la Documentación La documentación institucional es producto y propiedad de la UNAD, y esta ejercerá el pleno control de sus activos de información. Los archivos públicos, por ser un bien de uso público, no son susceptibles de enajenación.

[4] https://www.csirt.unad.edu.co

Artículo 34. Apoyo de Terceros La UNAD podrá contratar con personas naturales o jurídicas, los servicios de custodia, organización, reprografía y conservación de documentos de archivo, con sujeción a los lineamientos establecidos por el Archivo General de la Nación y a la normatividad interna vigente.

Artículo 35. Entrega de activos de información. Los funcionarios, contratistas y docentes de la Universidad, al desvincularse de las funciones titulares o de sus actividades, entregarán los documentos y archivos a su cargo debidamente organizados e inventariados, conforme a las normas y procedimientos que establezca la Universidad, sin que ello implique exoneración de la responsabilidad a que haya lugar en caso de irregularidades.

Artículo 36. Conservación Documental. La Secretaria General, a través del Sistema de Gestión Documental y Función Notarial, velará por la disponibilidad, integridad, confidencialidad y autenticidad de los documentos de archivo, la planeación, control, dirección, organización, capacitación, inspección o vigilancia, promoción y otras actividades involucradas con la gestión del ciclo de vida de la información, incluyendo la creación mantenimiento (uso, almacenamiento, recuperación), y disposición, independiente de los medios o soportes, así como la prestación de los servicios archivísticos en el Archivo Central Histórico, de acuerdo al marco de referencia del Sistema de Gestión Documental y Función Notarial y los lineamientos que se impartan para tal fin

Artículo 37. Control. Los funcionarios del archivo trabajarán sujetos a los más rigurosos principios de ética profesional, a lo dispuesto en la Constitución Política de Colombia, a las leyes, a los lineamientos del Archivo General de la Nación -AGN y disposiciones que regulen su labor.

Artículo 38. Tecnologías. La Universidad podrá incorporar tecnologías de avanzada en la administración, gestión, seguimiento, control y conservación de sus archivos, empleando cualquier medio técnico, electrónico, siempre y cuando cumpla con los siguientes requisitos mínimos:

a) Organización archivística de los documentos;
b) Realización de estudios técnicos para la adecuada toma de decisiones, teniendo en cuenta aspectos como la conservación física, las condiciones ambientales y operacionales, seguridad, perdurabilidad y reproducción de la información contenida en estos soportes, así como el funcionamiento razonable del sistema a impactar en toda la UNAD.

Artículo 39. Proceso Documental. La gestión documental frente al concepto de archivo total comprende procesos tales como la producción o recepción, distribución, consulta, organización, recuperación y disposición final de los documentos.

Artículo 40. Retención y valoración. La Universidad elaborará, adoptará, implementará y mantendrá actualizadas las respectivas tablas de retención y valoración documental.

Artículo 41. Inventario. Cada unidad es responsable, de acuerdo con los lineamientos impartidos por el Sistema de Gestión Documental y Función Notarial, de elaborar un inventario de los documentos que produzcan en ejercicio de sus funciones, procesos, procedimientos y actividades a su cargo, de manera que se asegure el control de los documentos en sus diferentes fases.

Artículo 42. **De la consulta**. Todas las personas tienen derecho a consultar los documentos de archivo público y a que se les expida copia de estos, siempre que dichos documentos no tengan el carácter de privilegiado, reservado o de documento en construcción conforme a la Constitución o a la Ley. La consulta de documentación que repose en el archivo central de la Universidad se adelantará conforme a los procedimientos definidos para tal fin.

Artículo 43. Derecho Personal. La Universidad garantizara el derecho a la intimidad personal y familiar, honra y buen nombre de las personas y demás derechos consagrados en la Constitución y las Leyes.

Artículo 44. Salida Documental Solamente por motivos legales la Universidad podrá autorizar la salida temporal de los documentos de archivo, previa autorización del Sistema de Gestión Documental y Función Notarial adscrito a la Secretara General. Respecto del archivo de carácter histórico se podrá autorizar de manera excepcional, la salida temporal de los documentos que se conservan con fines investigativos, culturales, científicos, legales e históricos, y en tales eventos, la Secretaría General, mediante el Sistema de Gestión Documental y Función Notarial, deberá tomar todas las medidas que garanticen la integridad, la seguridad, la conservación o el reintegro de estos.

Artículo 45. De la Gestión. La Universidad contará con instrumentos de planeación, control para la ejecución de las actividades del Sistema de Gestión Documental y Función Notarial a nivel nacional, mediante el Plan Institucional de Archivos, Programa de Gestión Documental físico y/o electrónico, Sistema Integrado de Conservación y demás instrumentos informacionales archivísticos y de control.

Artículo 46. De la Preservación. La Universidad a través de un Sistema Integrado de Conservación liderado y estructurado por el Sistema de Gestión Documental y Función Notarial establecerá los diferentes mecanismos, instrucciones o pasos a seguir en temas relacionados con la preservación y conservación a largo plazo de los archivos tanto físicos como electrónicos en cualquier soporte material, el cual tenga características de documento de archivo.

CAPÍTULO XI

DE LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Artículo 47. Objetivo de la gestión de incidentes de seguridad de la información. El objetivo de este componente es prevenir, detectar, contener, dar respuesta y evaluar los incidentes de seguridad de la información que puedan afectar la disponibilidad y la continuidad de los servicios, los procesos y procedimientos que se encuentran soportados por la Infraestructura lógica, física y tecnológica con la que cuenta la UNAD.

Artículo 48. Reporte de eventos o incidentes de la Seguridad de la Información. Cualquier usuario que tenga acceso a los servicios académicos, administrativos, operativos funcionales o misionales prestados por la Universidad, deberá reportar de manera inmediata a la GPIT los eventos, acciones o incidentes técnicos o tecnológicos que atenten contra la disponibilidad, confidencialidad, integridad, trazabilidad y autenticidad de los activos de información de la UNAD.

Artículo 49. Control. El CSIRT validará el impacto del evento y remitirá a la GPIT quien a través de quien ostente el rol de oficial de seguridad desarrollará las estrategias y hará uso de las capacidades y las herramientas técnicas y tecnológicas para atender, analizar, clasificar, responder, mitigar e investigar los incidentes de seguridad informática, a fin de ejercer controles sobre los activos tecnológicos y de información de la institución, respetando la cadena de custodia y demás elementos legales que permitan preservar la integridad y autenticidad de la evidencia en caso de un proceso jurídico y/o judicial.

Parágrafo 1. Las anteriores acciones se harán sin perjuicio del deber que tiene la GPIT y el oficial de seguridad, de informar inmediatamente a la Gerencia de Talento Humano y a la Oficina de Control Interno Disciplinario, suministrando información concreta sobre la individualización e identificación de los posibles responsables del incidente de seguridad informática; a su vez, informará a la Fiscalía General de la Nación en

aquellos casos en que dicho acceso pueda enmarcarse en uno de los tipos penales contemplados en la normatividad vigente.

Parágrafo 2. La GPIT adelantará el control, seguimiento, monitoreo y aseguramiento de la información que se produzca a través de elementos tecnológicos, así como también de las bases de datos que produzca la Universidad.

Parágrafo 3. Los roles de oficial de seguridad de la información y oficial de bases de datos, estarán asignados en virtud de sus funciones a liderazgos adscritos a la GPIT.

Artículo 50. Responsable del activo de información. Son actores del metasistema Unadista y propietarios de los activos de información delegados por la unidad interesada, los encargados de gestionar y tratar los datos para garantizar su integridad, confidencialidad y disponibilidad que se encuentran en los sistemas de información y bases de datos físicas y digitales de la UNAD, siendo sujetos de control y seguimiento por parte de la GPIT todas las descargas o almacenamientos locales o remotos de información propietaria de la institución, así como su destinación.

CÁPITULO XII
OTROS DEBERES

Artículo 51. Cualificación específica. La GPIT y el CSIRT adoptarán una estrategia orientada a que cada uno de los integrantes de estas unidades del metasistema adquieran y/o actualicen sus conocimientos sobre seguridad de la información y ciberseguridad, de acuerdo a la normatividad nacional vigente y a la que para el efecto produzca la UNAD en ejercicio de su autonomía.

Artículo 52. Deberes de la GPIT y el CSIRT en el marco de actuaciones disciplinarias. La GPIT y el CSIRT deberán suministrar información completa, verídica, exacta, detallada y en lenguaje comprensible a las oficinas y unidades que lo requieran, cuando estás adelanten indagaciones previas o investigaciones disciplinarias o se encuentren en etapa de juzgamiento relacionados con accesos irregulares a los sistemas informáticos de la Universidad o con cualquier otro incidente que atente contra la seguridad informática de la institución. En el mismo sentido, tanto la GPIT y el CSIRT brindarán la asesoría y asistencia que requieran estas dependencias para esclarecer los hechos con alcance disciplinario y determinar responsables en eventos relacionados con el uso irregular, ilícito o abusivo a los sistemas informáticos de la Universidad.

Parágrafo único. Para dicho efecto la GPIT y el CSIRT designarán el o los funcionarios que cumplirán el rol de perito en investigaciones disciplinarias y/o penales, labor que será realizada por una persona idónea con los suficientes conocimientos técnicos en seguridad informática, informática forense y demás que se requieran en la

labor de peritaje. En caso de no contar con la tipología experta se debe entregar el perfil del perito para adelantar lo procedente dentro de la investigación.

Artículo 53. Deberes de articulación con las autoridades judiciales. La GPIT y el CSIRT designarán el o los responsables de la articulación que se deberá desarrollar con la Fiscalía General de la Nación, Policía Nacional, Dirección de Investigación Criminal de la Policía Nacional y demás autoridades competentes cuando el incidente o evento requieran la intervención ante un evento informático o de ciberseguridad.

Parágrafo único: En el marco de este deber, los funcionarios designados deberán suministrar información inmediata a dichas autoridades sobre los accesos abusivos, incidentes que atenten contra la seguridad informática de la Universidad y demás hechos que puedan constituir delito.

CAPÍTULO XIII
DE LA APLICABILIDAD

Artículo 54. Acciones. Será objeto de sanción disciplinaria, administrativa, civil y/o penal según sea al caso y luego de adelantar la actuación o procedimiento correspondiente, a toda persona y/o usuario que viole las disposiciones de la presente resolución de conformidad con lo establecido en las leyes colombianas vigentes. En caso de que se documente la ocurrencia de incidentes informáticos, se levantará por parte de la GPIT el correspondiente informe técnico que servirá como fundamento para la interposición de las acciones legales pertinentes y el CSIRT construirá la respectiva documentación y medición del impacto presente y /o futuro.

Artículo 55. Vigencia. La presente resolución rige a partir de su fecha de expedición, derogando la Resolución 4256 del 3 de marzo de 2015 y aquellas disposiciones que le sean contrarias.

COMUNÍQUESE Y CÚMPLASE

Dada en la ciudad de Bogotá D. C., a los diez (10) días del mes de mayo de 2023.

JAIME ALBERTO LEAL AFANADOR
Rector

Revisó: Esther Constanza Venegas Castro
Secretaria General

Revisó: Andrés Ernesto Salinas Duarte
Vicerrector de Innovación y Emprendimiento

Revisó: Rafael Ramírez
Gerente de Plataformas e Infraestructura Tecnológica