Universidad Nacional Abierta y a Distancia

03 MAR 2015

RESOLUCIÓN No. 004256

Por la cual se definen las políticas del Marco de Referencia del SGSI

EL 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, transformada por la Ley 396 de 1997 y el Decreto 2770 del 16 de agosto de 2006, es un ente universitario autónomo del orden nacional, con régimen especial, personería jurídica, autonomía académica, administrativa y financiera, patrimonio independiente y capacidad para gobernarse, vinculado al Ministerio de Educación Nacional en los términos definidos en la Ley 30 de 1992.

Que el Artículo 28, de la Ley 30 de 1992, establece que: "La autonomía universitaria consagrada en la Constitución Política de Colombia y de conformidad con la presente Ley, reconoce a las universidades el derecho a darse y modificar sus estatutos, designar sus autoridades académicas y administrativas, crear, organizar y desarrollar sus programas académicos, definir y organizar sus labores formativas, académicas, docentes, científicas y culturales, otorgar los títulos correspondientes, seleccionar a sus profesores, admitir a sus alumnos y 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 UNAD tiene como misión contribuir a la educación para todos a través de la modalidad abierta y a distancia, mediante la investigación, la acción pedagógica, la proyección social y las innovaciones metodológicas didácticas, con la utilización de las tecnológicas de la información y de las comunicaciones para fomentar y acompañar el aprendizaje autónomo, 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 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 las políticas de 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 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 crear una la Política de Seguridad de la Información, basada en la norma ISO27001:2013, desde la cual se asegure el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del Sistema de Gestión de la Seguridad de la Información (SGSI).

En mérito de lo expuesto,

R E S U E L V E:

CAPÍTULO I
DISPOSICIONES GENERALES

Artículo 1. El presente conjunto de políticas tienen como finalidad brindar apoyo a la implementación del Sistema de Gestión de Seguridad de la Información a través de la estandarización de políticas particulares en los principales campos de acción que pueden afectar la integridad, confidencialidad y disponibilidad de la información institucional.

Artículo 2. Esta política aplica a todos los procesos y procedimientos que conforma el Sistema Integrado de Gestión de la Universidad, así como a todas las actuaciones administrativas que desarrollen sus distintas unidades, por intermedio de sus funcionarios administrativos, cuerpo docente o contratistas.

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

a. **Activos de Información:** Cualquier componente (humano, tecnológico, software, manuales, documentación, entre otros) que tiene valor para la organización y signifique riesgo si llega a manos de personas no autorizadas.

b. **Activos de Información críticos:** Activo de información cuya afectación o alteración puede generar un impacto negativo de carácter económico, legal o al buen nombre de la institución.

c. **Archivo:** Colección de datos e información del mismo tipo, almacenada en forma organizada como una unidad, que puede emplearse y tratarse como soporte material de la información contenida en éstos.

d. **Aplicación:** Programa informático diseñado para permitir a los usuarios la realización de tareas específicas en computadores, servidores y similares.

e. **Base de Datos:** Conjunto de datos almacenados y organizados con el fin de facilitar su acceso y recuperación.

f. **Backups o Copias de respaldo:** Copia que se realiza a la información institucional definida como 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

g. **Clasificación de seguridad del documento:** Clasificación estratégica adoptada por el Sistema de Gestión Documental de la Secretaría General, con el fin de llevar a cabo la gestión interna referente al mantenimiento de la seguridad de la información de acuerdo a su importancia para la organización, esta clasificación se define como:
   - **Público:** Información de dominio público, sean físicos o electrónicos, 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 cartelas de la entidad o en las páginas web de 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 auditoria interna o externa de la institución.
   - **Reservado:** Documentos estratégicos, o con información descriptiva de claves o datos técnicos de funcionamiento de las diversas unidades de la institución, que pueden ser físicos o electrónicos. Esta información solamente será 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

h. **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.

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

j. **Custodio:** Es el encargado de gestionar y administrar la adecuada operación del activo y la información relacionada con éste. En ocasiones el responsable y el custodio son la misma persona.

k. **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.).

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

m. **Dispositivo móvil:** Aparato electrónico con capacidades de cómputo y conexión a redes inalámbricas cuyo tamaño y diseño permite ser fácilmente transportado para utilizarse en diversas ubicaciones con facilidad (portátiles, tablets, celulares inteligentes y demás dispositivos con características similares).

n. **Información sensible o vulnerable:** También llamado activo sensible, es el nombre que recibe la información personal o institucional (datos personales, información financiera, contraseñas de correo electrónico, datos personales, datos de investigaciones), la cual puede ser alterada, descompuesta, mal utilizada, divulgada y/o eliminada, causando graves daños a la organización propietaria. Se incluye aquella información que cada unidad identifique como reservada o controlada, según las definiciones del Sistema de Gestión Documental Institucional.

o. **Niveles de backup:** 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 backup de 1er. Nivel; si se tienen dos copias, de un backup de 2do. nivel. Cuanto mayor sea el número de niveles de backup, menor será el riesgo de perder los datos.

p. **Propietario:** En la estructura administrativa de la institución, se le otorga la propiedad del activo a cada una de las unidades estratégicas, divisiones organizacionales, gerencias, rectorías o vicerrectorías.

q. **Responsable:** El Jefe de Área o Gerente de cada una de dichas áreas, será el responsable ante el SGSI, de los activos de información registrados como de su propiedad.

r. **SAN (Storage Area Network) o Red de Área de Almacenamiento:** 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 al interior de la organización.

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

t. **Servidor:** Equipo de computación físico o virtual, en el cual funciona un software, cuyo propósito es proveer servicios a otros dispositivos dentro de la red.

u. **Servidor de Almacenamiento:** Equipo servidor dotado con varios discos duros destinados a respaldar y compartir datos.

v. **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.

CAPÍTULO II
POLÍTICA PARA DISPOSITIVOS MOVILES

Artículo 4. Se permite el uso de dispositivos móviles de conexión inalámbrica al interior de las instalaciones de la UNAD, únicamente para desarrollar y cumplir con los objetivos laborares y/o contractuales del personal, procurando que no se almacene en estos dispositivos información institucional.

Artículo 5. Los dispositivos móviles asignados a administrativos, contratistas y/o docentes, son de propiedad de la entidad, y los responsables de dichos equipos deberán velar por su adecuado uso, cuidado, mantenimiento y protección.

Artículo 6. Los medios de almacenamiento de estos dispositivos deben ser protegidos tecnológicamente con medios de cifrado de datos o mediante cualquier otro mecanismo definido por la Gerencia de Innovación y Desarrollo Tecnológico - GIDT, con el fin de evitar la interceptación y/o uso indebido de la información que en ellos se almacene. Por lo anterior, en el acta de entrega del dispositivo, se debe validar que dicha protección se haya implementado o se debe firmar la exclusión de dicha protección.

Parágrafo 1. El funcionario asumirá los riesgos y costos asociados a la perdida, fuga o uso indebido de la información que se encontraba en los dispositivos extraviados,

además del cumplimiento de las políticas y regulaciones vigentes por parte de la Gerencia Administrativa y Financiera -GAF, concernientes a los costos del activo físico.

Parágrafo 2. Respecto a los dispositivos entregados con antelación a la entrada en vigencia de esta resolución, la GIDT junto con la GAF, definirán los mecanismos a tener en cuenta para implementar las medidas de protección correspondientes.

Artículo 7. La solicitud de conexión de dichos dispositivos a la red inalámbrica de la institución se realizará por intermedio de la mesa de ayuda de tecnología o por los funcionarios debidamente autorizados por la GIDT.

Artículo 8. La autorización de retiro de las instalaciones de los dispositivos móviles se deberá regir por las regulaciones emitidas por la Oficina de Infraestructura Física de la GAF en lo concerniente a autorización de salida de elementos.

Parágrafo. Se excluyen del cumplimiento de este artículo, los teléfonos celulares de cualquier gama que permitan contener, capturar, almacenar información y en algunos casos acceder a las funcionalidades institucionales. Sin embargo, no se excluyen del cumplimiento de la política expuesta en el Artículo 5.

Artículo 9. Se prohíbe conectar a los perfiles de red institucionales dispositivos móviles de uso personal, salvo que exista autorización explícita emitida por la GIDT.

Artículo 10. Se prohíbe el ingreso de teléfono celulares y otros dispositivos móviles a los centros de datos y centros de cableado de la institución, salvo que exista una autorización explícita emitida por la GIDT.

Artículo 11. Para los visitantes y personal de apoyo que ingrese a la institución y que requiera para sus funciones o servicios a prestar, el uso de alguno de estos dispositivos móviles, deben aplicarse las mismas restricciones de uso; adicionalmente, deberá estar siempre acompañado del responsable por parte de la UNAD para esta visita, con el fin de evitar usos indebidos de las tecnologías.

CAPÍTULO III
POLÍTICA DE CONTROL DE ACCESO LÓGICO

Artículo 12. Es responsabilidad de la Gerencia de Talento Humano- GTHUM, informar a la GIDT sobre los nuevos administrativos, contratistas y/o docentes que ingresan a la institución, con el fin de poder asignar desde la GIDT, los respectivos permisos para el acceso a los recursos tecnológicos de la institución.

Artículo 13. La GIDT es la encargada de definir y suministrar los mecanismos de acceso lógico para la asignación de permisos y privilegios a los usuarios de acuerdo a sus funciones, términos contractuales y/o roles definidos al interior de la entidad,

así como la modificación los permisos y privilegios de los usuarios en los mecanismos y/o sistemas de autenticación definidos.

Artículo 14. La GTHUM es la encargada de notificar y dar los lineamientos para la creación, modificación y supresión de permisos y privilegios de usuarios.

Artículo 15. Se prohíbe el uso de las cuentas de usuario administrador local en la institución, salvo en aquellos casos que estén debidamente justificados y autorizados.

Artículo 16. Los propietarios, responsables y/o custodios de los activos de información de la institución deben revisar periódicamente los derechos de acceso de los usuarios.

Artículo 17. Los propietarios y/o responsables de los activos deben informar inmediatamente sobre las novedades de los derechos de acceso lógico de los usuarios.

Parágrafo. Para la creación y administración de las credenciales de acceso institucionales, estudiantes y egresados, se deben adoptar los lineamientos establecidos por la GIDT.

Artículo 18. 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.

CAPÍTULO IV
POLÍTICA SOBRE EL USO DE CONTROLES CRIPTOGRÁFICOS

Artículo 19. La UNAD a través de la GIDT establecerá la implementación de los sistemas y técnicas criptográficas para la protección de la información, con base en los análisis de riesgos efectuados y con el fin de mantener la confidencialidad, integridad y autenticidad de la información.

Parágrafo 1. Cada unidad de la Universidad debe velar por tener una óptima administración de la información y debe implementar sistemas y técnicas criptográficas a la información catalogada como reservada o controlada, acorde a los lineamientos institucionales, con el fin de prevenir riesgos relacionados con la fuga de información durante su transmisión o almacenamiento.

Parágrafo 2. Se deben definir custodios o responsables de la información de carácter reservado en cada dependencia de la UNAD.

Artículo 20. La GIDT debe brindar el apoyo necesario a administrativos, contratistas y docentes, en el uso de las herramientas tecnológicas para protección de la información sensible, que debe ser cifrada.

Artículo 21. La GIDT, debe definir las herramientas necesarias para el cifrado de datos, de tal forma que preserve la confidencialidad, la integridad y el no-repudio en la transmisión de información sensible entre la comunidad Unadista.

Artículo 22. La GIDT, debe definir un procedimiento de gestión de claves, donde incluirán los métodos para la generación, longitud, eliminación y recuperación de claves en caso de pérdida, divulgación o daño.

Artículo 23. El procedimiento de gestión de claves debe tener en cuenta la fecha de finalización de contratos o de retiro de cada responsable del activo de información; de esta manera podrán desactivar, bloquear o eliminar los accesos no autorizados durante el periodo no laboral para que la información no corra ningún riesgo que afecte la continuidad de los procesos de la universidad.

Parágrafo. Es responsabilidad de la GTHUM informar a la GIDT sobre las novedades de retiro, con el fin de poder realizar las acciones de desactivación, bloqueo o eliminación de los respectivos accesos.

CAPÍTULO V
POLÍTICA DE TRANSFERENCIA E INTERCAMBIO DE INFORMACIÓN

Artículo 24. La GIDT debe realizar acciones de mejoramiento respecto a la seguridad de la información, especialmente respecto al uso de protocolos para realizar transferencia de información digital y/o física entre unidades, usuarios y terceras partes de la institución.

Artículo 25. Los mensajes enviados a través de cualquier medio electrónico que contengan información pública, controlada o reservada, deben ir cifrados y se debe propender porque sólo sean conocidos por el emisor y por el receptor(es), del mensaje.

Artículo 26. Cada unidad y/o supervisor de los contratos firmados con terceros, está en la obligación de verificar la firma de los acuerdos de confidencialidad previo a la transferencia de información entre la Universidad y sus proveedores y/o contratistas.

Parágrafo. Las terceras partes involucradas se verán obligadas a firmar los formatos de confidencialidad aplicables. Estos formatos están disponibles en la página del Componente de Seguridad de la Información, según corresponda para Proveedores y/o Terceros, o administrativos, contratistas y docentes.

Artículo 27. Toda la información que se reciba o envié a través de impresoras, máquinas de fax u otros medios de reprografía y transmisión de datos, debe ser monitoreada por el funcionario que los esté utilizando y debe permanecer siempre sin ningún tipo de documentos o información clasificada como controlada o reservada.

Artículo 28. Toda la información verbal que sea intercambiada por conversaciones formales, atención de llamadas telefónicas y demás procesos que no dejen soportes físicos, debe cumplir con el protocolo de manejo y escalamiento de comunicaciones vigente para la institución.

Parágrafo. La GIDT debe realizar capacitaciones y/o difundir los lineamientos institucionales para evitar que se traten temas de la UNAD en sitios públicos o escenarios no autorizados formalmente para la divulgación de información.

Artículo 29. Salvo casos de estricta necesidad y bajo previa autorización y/o recomendación de la GIDT, no se suscribirán o diligenciarán formularios electrónicos para uso personal o para medios de investigación a través de internet, así mismo se debe evitar el diligenciamiento de los datos de ubicación física, teléfonos móviles, teléfonos fijos, estructura organizacional, divulgación de cargos o información sensible de la UNAD, cuando el personal se suscriba o diligencie formularios electrónicos para uso personal o para medios de investigación a través de internet.

Artículo 30. La GIDT es responsable de definir los roles para la administración, operación y gestión de la información. Cada uno de los líderes de unidades, o directores de CEADs, CCAVs y UDRs, son los encargados de asignar estos roles en cada una de las unidades y/o sedes a nivel nacional.

Artículo 31. Cada líder de unidad será el responsable de definir los permisos de acceso a la SAN, como repositorio de información institucional.

Parágrafo. La GIDT será la encargada de definir los mecanismos y lineamientos de uso de la unidad de almacenamiento SAN.

Artículo 32. La recepción de correspondencia rotulada como "Información Confidencial" únicamente podrá ser revisada y visualizada por el destinatario de los documentos.

Parágrafo 1. El envío de correspondencia rotulada como "Información Confidencial" solo podrá salir de la Universidad en medio impreso o digital con la expresa autorización del emisor.

Parágrafo 2. Cada unidad está encargada de solicitar a la Oficina de Infraestructura física, que la correspondencia rotulada como "No Confidencial" no sea abierta por parte del grupo de correspondencia.

Artículo 33. Toda información clasificada como sensible o vulnerable que sea enviada por medios electrónicos, debe usar algoritmos de cifrado según los lineamientos de la GIDT.

Artículo 34. El custodio de la información de cada unidad, es el responsable de velar por el cumplimiento de la clasificación, foliación y rotulación de los documentos, de conformidad con los términos ordenados por el Sistema de Gestión Documental de la Universidad.

CAPÍTULO VI
POLÍTICAS DE DESARROLLO SEGURO

Artículo 35. Las solicitudes de desarrollos nuevos o modificación de las aplicaciones actualmente instaladas que se encuentran en producción, deben ser elevadas por el líder de cada unidad ante la GIDT durante los primeros quince días de cada trimestre (es decir los meses de enero, abril, julio y octubre). Las solicitudes realizadas en el tiempo estipulado, serán sometidas a un proceso de verificación y posterior aprobación o rechazo de la solicitud. La decisión tomada, será corroborada por el Gerente de Innovación y Desarrollo Tecnológico, quien comunicará al solicitante para que realice las acciones pertinentes.

Parágrafo. En caso que la solicitud sea extemporánea, será incluida en las solicitudes del siguiente periodo de recepción.

Artículo 36. La GIDT es la única unidad encargada de la realización de desarrollos dentro de la Universidad y dará cumplimiento a los lineamientos de construcción de aplicaciones seguras adoptados por la Universidad a través de esta gerencia.

Parágrafo. La UNAD apoyará la debida aplicación de los lineamientos de desarrollo mediante la facilitación de elementos y ambientes de trabajo adecuados para el equipo de desarrollo de la UNAD.

Artículo 37. Queda prohibido el acceso y/o uso de los recursos físicos y/o tecnológicos a personal no autorizado y en general, a los recursos asignados al grupo de desarrollo de la GIDT. El intento de uso total o parcial del código fuente de las aplicaciones administradas y/o adquiridas por la GIDT por parte de personal no autorizado queda expresamente prohibido.

Artículo 38. Con el fin de garantizar la seguridad, estabilidad y usabilidad de las soluciones, todos los desarrollos nuevos o modificaciones a desarrollos existentes, se deben realizar de conformidad con el "Instructivo de Pruebas de Software de la GIDT".

Parágrafo. Las áreas solicitantes de desarrollos nuevos o modificaciones a desarrollos ya existentes, deben asignar a funcionarios idóneos para colaborar en la realización y aprobación de los resultados de dichas pruebas.

Artículo 39. Las solicitudes de desarrollo o modificación de aplicaciones que no pueden ser atendidas por la GIDT, se regirán por el procedimiento de "Contratación de bienes y servicios" vigente en la UNAD.

CAPÍTULO VII
POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIOS

Artículo 40. El escritorio de trabajo de todos los administrativos, contratistas, docentes o proveedores de la institución, debe permanecer completamente despejado y libre de documentos controlados y/o reservados a la vista del público.

Parágrafo. Todos los documentos controlados y/o reservados y en general, toda la documentación clasificada como "Información confidencial" debe permanecer guardados en un lugar seguro (archivadores con llaves o cajas fuertes), ya sea en un espacio físico o virtual, siempre que mantenga las debidas condiciones de almacenamiento y claves de acceso.

Artículo 41. 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, sólo deben permanecer en la pantalla los íconos por defecto del sistema operativo instalado en el equipo.

Artículo 42. Todos los administrativos, contratistas, docentes y/o proveedor son responsables de velar por la adecuada protección de la información física y lógica al ausentarse de su puesto de trabajo.

CAPÍTULO VIII
POLITICA DE GESTION DE CAMBIOS

Artículo 43. Los recursos que se encuentran administrados por la GIDT que son cobijados por el procedimiento de Gestión de Cambios y Despliegue del Servicio y Despliegue del Servicio son: las Aplicaciones de Software que han sido desarrolladas internamente o desarrolladas externamente y entregadas formalmente para su administración, los equipos de cómputo misionales (Servidores), las redes de telecomunicaciones locales, extendidas y externas, los manejadores de bases de datos institucionales y la información documentada de los servicios gestionados por esta gerencia.

Artículo 44. Cualquier modificación a las condiciones actuales de funcionamiento de los recursos administrados por la GIDT y que son cobijados por el procedimiento de Gestión de Cambios y Despliegue del Servicio y Despliegue del Servicio, serán considerados como Cambios Tecnológicos y por tanto, deben cumplir con los procedimientos y protocolos emitidos por la GIDT.

Artículo 45. Las solicitudes de cambio deben ser debidamente registradas en las condiciones determinadas en el procedimiento de Gestión de Cambios y Despliegue

del Servicio y Despliegue del Servicio Vigente. Dicha solicitud, será evaluada y aprobada o rechazada según los criterios definidos por la GIDT.

Artículo 46. La GIDT determinará las fechas y responsables de efectuar la validación de condiciones y la correspondiente ejecución controlada del cambio.

Parágrafo. En casos de emergencia manifiesta, que estén afectando directamente la normal prestación de los servicios de la UNAD en cualquiera de sus unidades, se podrán realizar cambios en la configuración de recursos y servicios de infraestructura tecnológica; sin que estos cambios sean susceptibles de revisión posterior por parte de la GIDT.

Artículo 47. La UNAD propenderá porque los servicios tecnológicos que se encuentran tercerizados, cuenten con procedimientos y/o protocolos definidos para la Gestión de Cambios y Despliegue del Servicio sobre los servicios contratados.

CAPÍTULO IX
POLÍTICA DE VERSIONES

Artículo 48. La GIDT es la responsable de gestionar la implementación, prueba y despliegue de versiones y de versiones de emergencia, así como de realizar la entrega de nuevas funcionalidades, cambios o servicios nuevos sin afectar la integridad de los servicios ya existentes.

Parágrafo. La gestión debe contemplar que todas las versiones aprobadas e implementadas pueden ser probadas, verificadas, desplegadas en producción (instaladas) y retiradas (o desinstaladas) cuando sea necesario.

Artículo 49. La GIDT será la responsable de definir los planes de pruebas e implementación de los servicios nuevos o mejorados con cada uno de sus interesados.

Parágrafo 1. El Gerente de Innovación y Desarrollo Tecnológico o su delegado será el responsable de aprobar cada uno de estos planes con apoyo del líder de equipo interno de trabajo encargado de realizar el despliegue.

Parágrafo 2. La solicitud de la nueva versión deberá documentarse utilizando los lineamientos definidos en el Procedimiento de Gestión de Cambios y Despliegue del Servicio y Despliegue del Servicio y su verificación y aceptación formal estará a cargo del Gerente de Innovación y Desarrollo Tecnológico o su delegado, el líder de equipo interno de trabajo encargado de realizar el despliegue y el usuario solicitante del cambio.

Artículo 50. La GIDT se encargará de implementar los repositorios, medios y herramientas seguras, para realizar la gestión y el control de las versiones de manera eficiente y respetando los medios de identificación definidos para su manejo y trazabilidad.

Artículo 51. La frecuencia de cada tipo de control o actualización de versiones, estará sujeta al análisis de riesgos y el nivel de impacto particular que se realice desde la solicitud.

Artículo 52. La nomenclatura y descripción de cada uno de los controles o actualización de versiones implementados se hará de acuerdo a los lineamientos brindados por la Gerencia de Innovación y Desarrollo Tecnológico.

Parágrafo. La nomenclatura y descripción de cada uno de los controles o actualización de versiones aplicables a la documentación se hará de acuerdo a los lineamientos brindados por el Sistema Integrado de Gestión y el grupo de Gestión Documental de la institución.

Artículo 53. El líder del equipo de trabajo encargado junto con su equipo de trabajo serán los responsables de aplicar las condiciones de los controles o actualización de versiones, de acuerdo a la agrupación de cambios solicitados o planificados.

CAPÍTULO X
BACKUPS O COPIAS DE SEGURIDAD

Artículo 54. La responsabilidad de la gestión de las copias de respaldo y la administración de los equipos de respaldo masivo de datos estará a cargo de la persona designada por el Gerente de Innovación y Desarrollo Tecnológico.

Parágrafo. El encargado de la administración de equipos de respaldo masivo de datos, velará por los backups y por el resguardo de los datos contenidos en ellos; así como por su integridad, disponibilidad y confidencialidad.

Artículo 55. Los medios de respaldo empleados para efectuar las copias de seguridad en la UNAD serán los definidos por la Gerencia de Innovación y Desarrollo Tecnológico en el procedimiento de Copias de Respaldo o aquel que lo supla.

Parágrafo. El responsable de la administración de equipos de respaldo masivo de datos, velará por los respectivos medios de respaldo (y los datos contenidos en éstos) y serán quienes tengan acceso a ellos.

Artículo 56. Se hará Respaldo a los archivos, aplicaciones, bases de datos y configuración de los sistemas operativos de los servidores calificados como críticos para la UNAD, contemplados en el Inventario de Servidores Críticos asociado al Procedimiento Copias de Respaldo.

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

Artículo 57. La GIDT será la responsable de definir los mecanismos adecuados para la ejecución de los respaldos de información, así como la periodicidad, etiquetado, lugar de archivo y el tiempo de retención de las copias.

Artículo 58. Para todos los casos de criticidad definidos en el Inventario de Servidores Críticos, será obligatorio contar con mínimo dos niveles de respaldo.

Artículo 59. La ejecución de las copias de seguridad debe llevarse a cabo en horas de poca o ninguna actividad laboral; por lo tanto la GIDT será la responsable de definir el horario de ejecución de éstas.

Parágrafo. En los casos en que el backup no finalice exitosamente dentro de los tiempos establecidos, éste se relanzará después de evidenciado el fallo, en los tiempos establecidos en el procedimiento de Copias de Respaldo.

Artículo 60. Cuando sea necesario un respaldo por demanda de los servidores críticos, se debe solicitar formalmente a través de la mesa de ayuda o mediante correo electrónico por parte del personal autorizado, para informar mínimo con 24 horas de antelación sobre posibles interrupciones en el servicio a las personas afectadas.

Artículo 61. Todos los respaldos se revisarán con la periodicidad definida en el Procedimiento de Copias de respaldo y se evidenciarán en la bitácora de backups.

Artículo 62. La Comprobación periódica del estado de las copias se llevará a cabo con el fin de garantizar la disponibilidad e integridad de los datos almacenados. Los responsables de la administración de equipos de respaldo masivo de datos evidenciarán la comprobación periódica del estado de las copias de seguridad en el formato para pruebas periódicas de restauración de backups.

Artículo 63. Los equipos para el respaldo de información de la UNAD deben estar ubicados en centros de datos (Datacenters) con las medidas de seguridad pertinentes, y tener contratos de soporte y mantenimiento regular vigentes.

Artículo 64. Los medios de almacenamiento de datos deben tener un manejo adecuado para mitigar la ocurrencia de daños físicos y por consiguiente la pérdida de la información

CAPÍTULO XI
POLÍTICA DE GESTIÓN, ADMINISTRACION Y CONSERVACION DOCUMENTAL

Artículo 65. La UNAD está obligada a la creación, organización, preservación y control de los archivos, teniendo en cuenta los principios de procedencia, orden original, el ciclo vital de los documentos y la normatividad archivística.

Artículo 66. 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 tenerse en cuenta las especificaciones técnicas existentes sobre áreas de archivos, como lo establece el Archivo General de la Nación.

Artículo 67. La documentación institucional es producto y propiedad de la UNAD, y ésta ejercerá el pleno control de sus recursos informativos. Los archivos públicos, por ser un bien de uso público, no son susceptibles de enajenación.

Parágrafo. La Universidad podrá contratar con personas naturales o jurídicas, los servicios de custodia, organización, reprografía y conservación de documentos de archivo, esto teniendo en cuenta lo establecido por el Archivo General de la Nación.

Artículo 68. Los funcionarios, contratistas y docentes de la Universidad, al desvincularse de las funciones titulares, 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 69. La Secretaría General, tendrá la obligación de velar por la integridad, autenticidad, veracidad y fidelidad de la información de los documentos de archivo, liderando mediante su Sistema de Gestión Documental la planeación, control, dirección, organización, capacitación, inspección o vigilancia, promoción y otras actividades involucradas en la gestión del ciclo de vida de la información, incluyendo la creación, mantenimiento (uso, almacenamiento, recuperación), y disposición, independientemente de los medios o soportes., así como la prestación de los servicios archivísticos en el Archivo Central e Histórico.

Artículo 70. Los funcionarios de archivo trabajarán sujetos a los más rigurosos principios de la ética profesional, a lo dispuesto en la Constitución Política de Colombia, a las leyes y disposiciones que regulen su labor.

Artículo 71. La Universidad podrá incorporar tecnologías de avanzada en la administración, gestión, seguimiento, control y conservación de sus archivos, empleando cualquier medio técnico, electrónico, informático, óptico o telemático, 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, la 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 72. La Gestión Documental dentro del concepto de archivo total, comprende procesos tales como la producción o recepción, distribución, consulta, organización, recuperación y disposición final de los documentos.

Artículo 73. Será obligatorio para la Universidad elaborar y adoptar las respectivas tablas de retención documental y valoración documental.

Artículo 74. Es obligación de la Universidad elaborar inventarios de los documentos que produzcan en ejercicio de sus funciones, de manera que se asegure el control de los documentos en sus diferentes fases.

Artículo 75. Todas las personas tienen derecho a consultar los documentos de archivos públicos y a que se les expida copia de los mismos, siempre que dichos documentos no tengan carácter reservado conforme a la Constitución o a la ley.

Parágrafo. La Universidad garantizará 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 76. Sólo por motivos legales, la Universidad podrá autorizar la salida temporal de los documentos de archivo, previa autorización del Sistema de Gestión Documental de la Secretaría General.

Artículo 77. El Archivo de carácter histórico, podrá autorizar de manera excepcional, la salida temporal de los documentos que se conservan con fines investigativos, culturales, científicos, legales e históricos y en tal evento la Secretaría General, mediante su Sistema de Gestión Documental, deberá tomar todas las medidas que garanticen la integridad, la seguridad, la conservación o el reintegro de los mismos.

Artículo 78. La Universidad contará con instrumentos de planeación, y control para la ejecución de las actividades del Sistema de Gestión Documental 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 o de control.

Artículo 79. La Universidad a través de un Sistema Integrado de Conservación liderado y estructurado por el Grupo de Gestión Documental, 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 XII
APLICABILIDAD

Artículo 80. El contenido de este documento aplica a todos los procesos y procedimientos que conforman el Sistema Integrado de Gestión de la Universidad, así como a todas las actuaciones administrativas que desarrollen las distintas unidades, por intermedio de sus administrativos, contratistas y/o docentes.

Artículo 81. Se sancionará disciplinaria, administrativa, civil y/o penalmente a toda persona que viole las disposiciones del presente documento de conformidad con lo establecido en las leyes colombianas vigentes.

La presente resolución rige a partir de su fecha de expedición y deroga la Resolución 5452 de 2012, la Resolución 5602 de 2012, la Resolución 6018 de 2012 y Resolución 4793 de 2013.

COMUNÍQUESE Y CÚMPLASE

Dada en la ciudad de Bogotá D. C., 03 MAR 2015

JAIME ALBERTO LEAL AFANADOR
Rector

Vo. Bo. ANDRES ERNESTO SALINAS DUARTE
Gerente Innovación y Desarrollo Tecnológico

Vo. Bo. LEONARDO EVEMELETH SANCHEZ TORRES
Secretario General

Vo. Bo. JOSE HUMBERTO GARZON GARZON
Jefe Oficina de Adquisiciones e Inventarios