UNIVERSIDAD NACIONAL DE COLOMBIA

VICERRECTORÍA GENERAL
DIRECCIÓN NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES - DNTIC

MEMORANDO

Para:	**RECTOR** **VICERRECTOR GENERAL** **VICERRECTORES DE SEDE** **GERENCIA NACIONAL FINANCIERA Y ADMINISTRATIVA** **DIRECTORES SEDES PRESENCIA NACIONAL** **DIRECCIONES ADMINISTRATIVAS DE SEDE** **JEFES DE OFICINAS DE PLANEACIÓN** **JEFES DE OFICINAS DE TECNOLOGÍA** **UNIVERSIDAD NACIONAL DE COLOMBIA**
Consecutivo:	**DNTIC-0040-16**
Referencia:	**DIRECTRIZ TÉCNICA No. 16** **POLITICA DE SEGURIDAD INFORMATICA Y DE LA INFORMACION PARA BACKUPS Y RECUPERACIONES**
Fecha:	**27 DE ENERO DE 2016**

El Acuerdo 46 de 2009 *"por el cual se definen y aprueban las políticas de Informática y Comunicaciones que se aplicarán en la Universidad Nacional de Colombia"*, establece en el numeral 2 del artículo 4: "*Dando aplicación a las políticas de informática y comunicaciones y con el fin de garantizar la estandarización, la integración y la interoperabilidad de la plataforma tecnológica de la Universidad, la Dirección Nacional de Informática y Comunicaciones emitirá las directrices técnicas de acuerdo con la normatividad vigente".*

Las Políticas de seguridad informática y de la Información, en el literal c del Capítulo 2 "Marco Regulatorio de la Seguridad (MRS)", establece: "*De conformidad con los principios de no duplicidad funcional y de eficiencia, el área responsable de desarrollar los mecanismos para la aplicación de las Políticas de Seguridad informática y de la información y sus Directrices o Políticas Específicas es la Dirección Nacional de Tecnologías de Información y Comunicaciones (DNTIC), en desarrollo de las disposiciones propias de aplicación institucional y en concordancia con el Artículo 6 de la Resolución 464 de 2014, expedido por la Rectoría*".

Las Políticas de Seguridad Informática y de la información:

- Se aplicarán en todas aquellas actividades de carácter académico, laboral o contractual que tengan por objeto la creación intelectual en los campos del derecho de autor, derechos conexos, la propiedad industrial y las nuevas tecnologías, de conformidad con el Acuerdo 035 de 2003 expedido por el Consejo Académico de la Universidad y lo establecido en el literal e del Capítulo 2 "Marco Regulatorio de la Seguridad (MRS)". De igual forma, en cumplimiento a lo dispuesto en la Ley estatutaria 1581 de 2012 y a su Decreto Reglamentario 1377 de 2013, la Política de Seguridad Informática y de la Información y los mecanismos para tales fines, son aplicables a la Institución para el tratamiento y protección de datos personales.
- Se constituirán en un mecanismo fundamental para que las dependencias de la Universidad garanticen la recolección oportuna y técnica, la trascripción, el análisis, la divulgación y el

mantenimiento de los datos necesarios para la eficiente, eficaz y efectiva operación de los sistemas de información de la gestión académica y administrativa

Por lo anterior, se establece la siguiente Directriz Técnica también denominada "**Política de Seguridad informática y de la información para Backups y Recuperaciones**"

1. OBJETIVO

Proteger la información corporativa e institucional contra pérdida de datos y contar con capacidades para restaurar sin que las consecuencias comprometan a la Universidad.

2. DISPOSICIÓN

2.1. Control de copias de seguridad de la información, datos, software e imágenes del sistema deben efectuarse y debe garantizarse mediante pruebas de calidad efectuadas con regularidad que la Universidad está preparada para recuperar su información institucional.

2.2. DNTIC mantendrá una Guía de Aplicación de copias de seguridad para que los responsables y dueños, puedan definir los requisitos y dar aplicación a las actividades y procedimientos de Backups de la Institución considerando las copias de seguridad de información, software y sistemas de información misionales. La política de copias de seguridad o Backups, debe definir la retención, almacenamiento y requisitos de protección.

2.3. Se mantendrán copias de seguridad válidas, verificadas y servibles; disponibles en las instalaciones de las OTICs de cada sede, para asegurar que toda la información esencial y el software se pueden recuperar después de un incidente, desastre o falla de medios. Los jefes o coordinadores de OTIC de cada sede, de sistemas de información y de activos críticos son responsables de esta declaración.

3. APLICABILIDAD

Esta política es de aplicación a todas las dependencias que componen la comunidad académica e institucional, a sus recursos, a la totalidad de los procesos internos o externos vinculados a la universidad a través de contratos.

4. RESPONSABILIDAD

4.1. La Dirección Nacional de Tecnologías de la Información y las Comunicaciones (DNTIC) con el apoyo y la participación de las Oficinas de Tecnologías de Información y de las Comunicaciones (OTICs) y Coordinaciones de Informática, define los perfiles de acceso a sistemas informáticos y comunicaciones de la Universidad.

4.2. El diseño y ejecución de los Planes de Copias de seguridad es responsabilidad de los dueños de activos y sistemas de información, coordinadores o jefes de OTICs y responsables operativos de estas actividades; incluyendo cintotecas y manejos de medios.

5. REGLAS

5.1. En el diseño de un plan de copias de seguridad (Backups), los siguientes elementos son obligatorios:

5.1.1. Registros exactos y completos de las copias de seguridad y certificación de las pruebas de restauración mediante procedimientos documentados y registros de trazabilidad de lo ejecutado.

5.1.2. Desarrollo de actividades a la medida (por ejemplo: copia de seguridad completa – Full, Diferencial o Incremental) y la frecuencia de las copias de seguridad deben reflejar los requerimientos de protección institucional definidos a través de los ejercicios de Continuidad de negocio (RTO – recovery time objetive, tiempo objetivo de recuperación).

5.1.3. Las copias deben almacenarse en una ubicación remota, a una distancia suficiente para evitar cualquier daño de un desastre en el sitio principal. Esta definición estratégica y táctica debe ser documentada y manejada como información sensible, crítica o confidencial.

5.1.4. La realización de las copias de seguridad de la información es objeto de un adecuado nivel de protección física y ambiental, consistente con las normas que se aplican en el centro de cómputo;

exige en consecuencia, la apropiación y ejecución de disposiciones medio-ambientales como exigencia en los procesos de certificación de backups, retención y almacenamiento de información en centros de datos. Los jefes o coordinadores de OTIC certificarán este proceso y se dejará registro en las bitácoras de emisión de copias de seguridad de la información.

5.1.5. Medios de backups deben someterse regularmente a pruebas para asegurar que se puede confiar en su uso y en situaciones de emergencia cuando sea necesario; esto se combina con una prueba de ejecución de procedimientos de restauración y se comprueba con el tiempo de restauración. Los registros de estas actividades se mantendrán actualizados y serán clasificados como información sensible, crítica o confidencial, para lo cual se determinarán los controles y mecanismos de protección necesarios. De cualquier forma, estos registros son auditables y usados en procesos de responsabilidad y restauración. Se deben someter al manejo documental del Sistema de Gestión de Calidad Institucional.

5.1.6. Pruebas de la capacidad para restaurar los datos sobre las copias de seguridad, se deben realizar frecuentemente. Para tal efecto, no se podrá sobrescribir sobre el medio original. En caso que el proceso de restauración de copia de seguridad sea infructuoso o falle o se determinen daños irreparables o pérdidas de información, se tomarán las medidas inmediatas activando el plan de manejo de incidentes sin que ello interrumpa o altere la ejecución normal de la operación de la Universidad. Para los dos eventos indicados en este aparte, se requiere registros de trazabilidad e información documentada como parte del Sistema de Gestión de Calidad Institucional.

5.1.7. En situaciones donde la confidencialidad es importante, las copias de seguridad deben ser protegidas por medio de mecanismos de encriptación. Los procedimientos operativos a nivel tecnológico seguido por las OTICs, deben velar por la ejecución de las copias de seguridad y controlar los errores de las copias de seguridad programadas para asegurar la integridad de las copias de acuerdo con la política de copias de seguridad. Copia de seguridad de los sistemas y servicios deben someterse regularmente a pruebas para asegurar que cumplan con los requisitos de los planes de continuidad de negocio.

5.1.8. En el caso de sistemas de información misionales y servicios críticos, se debe abarcar todo el activo; es decir, Información de Plataforma como sistema operativo, base de datos, sistema información, aplicaciones y los datos necesarios para recuperar el sistema completo en caso de un desastre. El período de retención y almacenamiento de información esencial para la Universidad debe ser determinado, teniendo en cuenta cualquier requisito para copias archivadas; el cual se conservará permanentemente.

5.2. Las siguientes pautas para el manejo de los medios extraíbles son de estricto cumplimiento:

5.2.1. Se exige una autorización para medios retirados de la Institución y un registro de dichas mudanzas debe mantenerse con el fin de contar con registros de auditoría;

5.2.2. Todos los medios originales de Software deben ser almacenados en un ambiente seguro, de acuerdo con las especificaciones del fabricante;

5.2.3. Si la confidencialidad o integridad de los datos son requisitos importantes y su clasificación es Confidencial o Sensible, técnicas criptográficas deben ser utilizadas para proteger los datos en medios extraíbles; se controlará este proceso y se determinará el ciclo de vida de la información para efectos de garantizar la recuperación.

5.2.4. Para mitigar el riesgo de degradar los medios de comunicación (borrado de cintas, formateo de CD/DVD, discos duros), mientras que aún se necesitan datos almacenados, los datos deben ser transferidos a medios frescos antes de convertirse en ilegibles.

5.2.5. El registro de los medios extraíbles es obligatorio para limitar la posibilidad de pérdida de datos.

5.2.6. Las unidades de medios extraíbles sólo deben estar habilitadas si hay una razón de negocios para hacerlo; se debe dejar registro de las actuaciones realizadas.

5.2.7. Cuando exista la necesidad de utilizar medios extraíbles, la transferencia de información a tales medios debe ser monitoreada.

5.3. Procedimientos formales (trazables, e inscritos en el Sistema de Gestión de Calidad Institucional) para la habilitación de servicios de comunicaciones (VPN, FTP, almacenamiento en nube, entre otros) deben ser establecidos para minimizar el riesgo de fuga de información

confidencial a personas no autorizadas. Se requiere el análisis de riesgos, la determinación de criticidad de información, la definición de responsabilidades y el ciclo de vida de la información. Los procedimientos para la eliminación segura de los soportes que contengan información confidencial deben ser proporcionales a la sensibilidad de la información. Los siguientes elementos son exigibles:

5.3.1. Medios que contengan información confidencial deben almacenarse y eliminarse de forma segura, por ejemplo, por incineración o trituración, o el borrado de datos para su uso por otra aplicación dentro de la organización;

5.3.2. Los procedimientos deben estar en su lugar para identificar los elementos que podrían requerir la eliminación segura;

5.3.3. Puede ser más fácil organizar todos los elementos multimedia que deben recogerse y eliminarse de forma segura, en lugar de tratar de separar los productos sensibles;

5.3.4. Muchas organizaciones ofrecen servicios de recolección y eliminación de los medios; se debe tener cuidado en la selección de una parte externa y verificarse que cuente con controles y experiencias adecuadas; se requiere auditar los procesos realizados por el tercero escogido.

5.3.5. La eliminación de productos (hardware/software) e información sensible debe estar documentada con el fin de mantener registros de auditoría.

5.4. Las siguientes condiciones son obligatorias para proteger los medios de comunicación que contienen información almacenada:

5.4.1. Transporte fiable o Empresas especializadas de correo o mensajería deben ser utilizados;

5.4.2. El embalaje debe ser adecuado para proteger el contenido de cualquier daño físico probable que surja durante el tránsito y de acuerdo con las especificaciones de los fabricantes y de acuerdo a las disposiciones en materia de elementos materiales de prueba de cadenas de custodia (solo para cuando la información sea identificada como sensible, confidencial o critica), por ejemplo, la protección contra cualquier factor ambiental que puede reducir la eficacia de la restauración de los medios de comunicación, tales como la exposición al calor, la humedad o campos electromagnéticos;

5.4.3. Los registros deben mantenerse, identificando el contenido de los medios de comunicación, la protección aplicada, así como el registro de los tiempos de traslado a los custodios de tránsito y recepción en el destino.

5.4.4. La información puede ser vulnerable al acceso no autorizado, mal uso o la corrupción durante el transporte físico, por ejemplo, cuando el envío de medios se hace a través del servicio postal o por mensajería. En este control, los medios de comunicación incluyen documentos en papel. Cuando la información confidencial sobre los medios de comunicación no está cifrada, protección física adicional de los medios de comunicación debe ser considerada.

Cordialmente,

HENRY ROBERTO UMAÑA ACOSTA
Director

Fecha de impresión: 27/01/2016
Preparó: Ing. Adriana Jaramillo