DIRECTRIZ TÉCNICA No. 22

Para: **DEPENDENCIAS DE TODAS LAS SEDES DE LA UNIVERSIDAD NACIONAL DE COLOMBIA**

Consecutivo: **DNTIC-0689-19**
Referencia: **DIRECTRIZ TÉCNICA No. 22**
CONTROL DE ACCESO PARA LA UNIVERSIDAD NACIONAL DE COLOMBIA
Fecha: **29 DE NOVIEMBRE DE 2019**

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 d del Capítulo 2 "Marco de 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*".

La Política y directrices 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 de 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 transcripción, 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 para "**Control de Acceso**".

1. OBJETIVO

Garantizar el acceso restringido a los activos de Información según las determinaciones brindadas por sus propietarios o dueños, de conformidad con los perfiles de acceso definidos, con el fin de evitar la adulteración, fuga, pérdida, consulta, uso o acceso no autorizado a la información y en

Carrera 45 # 26-85
Edificio Uriel Gutiérrez Piso 4
(+57 1) 3165087 - (+57 1) 3165000 EXT: 18197-18406
Bogotá, D. C., Colombia
dntic_nal@unal.edu.co

concordancia con los estándares y mejores prácticas de seguridad informática definidas para la Universidad.

2. DISPOSICIÓN

Con base en los numerales 1, 2 y 4 del Artículo 8 Acuerdo 046 de 2009 expedido por el Consejo Superior Universitario, se establece que

"1. La Dirección Nacional de Informática y Comunicaciones con el apoyo y la activa participación de las Oficinas de Informática o Centros de Cómputo de las diferentes sedes, ***implementará los mecanismos necesarios para garantizar la integridad, confiabilidad, oportunidad, disponibilidad y la seguridad, en los sistemas informáticos y de comunicaciones de la Universidad****.*

2. Teniendo en cuenta el alcance funcional de las dependencias usuarias, ***será responsabilidad de estas, velar por el manejo y mantenimiento adecuado de los datos, en cuanto a consulta, ingreso, modificación, eliminación y/o divulgación*** *de los datos del sistema de información.*

4. ***Con base en la estructura, roles y responsabilidades de la Universidad****, la Dirección Nacional de Informática y Comunicaciones en coordinación con las Oficinas de Informática o Centros de Cómputo de las diferentes sedes y las áreas funcionales,* ***definirá los perfiles de acceso a la información****."*

3. APLICABILIDAD

Esta directriz 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, convenios o acuerdos con terceros y a todo el personal de la Universidad Nacional de Colombia, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe dentro de alcance definido para el Sistema de Gestión de Seguridad informática y de la información y en general a todos los usuarios de la información o aquellos que sean beneficiados con el uso de la infraestructura, servicios, sistemas misionales de la Universidad Nacional de Colombia.

4. RESPONSABILIDAD

1. La Dirección Nacional de Informática y de las Comunicaciones (DNTIC) con el apoyo y la participación de las Oficinas de Tecnologías Informáticas y de las Comunicaciones o Centros de Cómputo (OTIC), define los perfiles de acceso a sistemas informáticos y comunicaciones de la Universidad.
2. Los propietarios de los Activos de Información son responsables de la clasificación, mantenimiento y actualización de la misma; así como de documentar y mantener actualizada esta clasificación, definiendo qué usuarios deben tener permisos de acceso de acuerdo con sus funciones y competencia y suministrarán a la DNTIC la información relevante para la definición de los perfiles de acceso a los sistemas de información. En general, los propietarios tienen la responsabilidad de mantener íntegro, confidencial y disponible el activo de información mientras que es desarrollado, producido, mantenido y utilizado.
3. Los usuarios de la información, infraestructura tecnológica, servicios utilizados para su procesamiento y sistemas misionales y de apoyo son responsables de conocer y cumplir la presente Directriz.

Carrera 45 # 26-85
Edificio Uriel Gutiérrez Piso 4
(+57 1) 3165087 - (+57 1) 3165000 EXT: 18197-18406
Bogotá, D. C., Colombia
dntic_nal@unal.edu.co

4. La Oficina de Control Interno es responsable de practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la gestión y directriz de control de acceso a activos de información y tecnologías de información referentes a Sistemas de Información. Es su responsabilidad informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por esta directriz y por las normas, procedimientos y prácticas que de ella surjan.
5. El supervisor (docente o administrativo de planta) es responsable de la solicitud de gestiones sobre identidades digitales (*U.PR.11.001.014 Gestión de Identidades digitales*) para los roles Contratista e Institucional.
6. El usuario de la identidad digital es el único responsable de las actividades y actuaciones que realicen con el uso y acceso de la identidad digital.

5. REGLAS

1. Como resultado de un análisis y evaluación del riesgo, implementar mecanismos y controles que aseguren un efectivo registro, identificación y autenticación de los usuarios que acceden a Activos de información de la Universidad (ver Guía de Gestión Riesgos Institucional).
2. Reportar periódicamente las novedades de información de acceso de usuarios a sistemas misionales y servicios informáticos de la Universidad.
3. Otorgar acceso a servicios que requieren mayor nivel de seguridad o que involucran medios de pago sólo a usuarios autorizados. Se requiere limitar el acceso solo para usuarios identificados y autenticados apropiadamente.
4. Implementar una administración efectiva de los derechos de acceso de usuarios y asignar dicha responsabilidad al personal apropiado (administradores de accesos).
5. Implementar la vigencia de los derechos de acceso y su revocación, una vez finalice el período asignado, o haya pérdida de las credenciales, o se detecte uso indebido de los recursos por parte de los usuarios. Las credenciales de acceso y los dispositivos de autenticación robusta deben quedar inválidos ante eventos de revocación.
6. Solo usuarios autorizados por el Grupo de Infraestructura o las Oficinas de Tecnologías de cada sede, estarán autorizados para instalar software o hardware en los equipos, servidores e infraestructura de telecomunicaciones de la Universidad.
7. El acceso a los centros de cómputo es responsabilidad exclusiva del personal con cargos de responsabilidad de cada OTIC.
8. Las claves de administrador de los sistemas de información (*a cualquier nivel, ej. plataforma, base de datos, sistema operativo y aplicativo, entre otros*), deben ser conservadas por la dirección o coordinación de cada OTIC o centro de cómputo de sede y deben ser cambiadas en intervalos regulares de tiempo y en todo caso cuando el personal adscrito al cargo cambie.
9. El usuario final, sea funcionario o contratista es el responsable de la información contenida en sus equipos y solicitará el establecimiento de mecanismos de seguridad para la protección de la información dependiendo del grado de clasificación que se haya otorgado.
10. El responsable de Gestión de Identidad Digital se encargará de gestionar a nivel nacional los aspectos operativos para la creación, modificación, inactivación o eliminación de identidades digitales, previa solicitud por parte de las dependencias o supervisores, para lo cual estos deberán realizar las verificaciones del caso, a fin de evitar errores o inconvenientes que puedan afectar los intereses de la Universidad.
11. De llegar a presentarse alguna inconsistencia o reclamación sobre la gestión realizada a la identidad digital, será la dependencia o el supervisor los directos responsables y deberán tomar las medidas correctivas del caso. Los mismos comunicarán oportunamente al

Carrera 45 # 26-85
Edificio Uriel Gutiérrez Piso 4
(+57 1) 3165087 - (+57 1) 3165000 EXT: 18197-18406
Bogotá, D. C., Colombia
dntic_nal@unal.edu.co

responsable de Identidad Digital, los cambios operativos que deban realizarse sobre las identidades.

12. La gestión de identidades digitales se regirá por la Directriz técnica emitida desde la Dirección Nacional de Tecnologías de Información y comunicaciones DNTIC.
13. Únicamente las identidades tipo egresados y pensionados tienen carácter de perpetuidad. Para los demás roles las dependencias responsables y los supervisores deberán gestionar, mediante la correspondiente solicitud al responsable de esta gestión, la eliminación, suspensión de permisos de acceso o inactivación, de acuerdo con el procedimiento de Gestión de Identidades Digitales emitido por DNTIC, garantizando la desvinculación completa de los sistemas de información y servicios de la Universidad cuando esta vinculación termine. Se precisa informar al usuario sobre la inactivación de la identidad.
14. La inactivación de la identidad se realizará al término de la vinculación del personal administrativo, docente, contratista o con la pérdida de la calidad de estudiante.
15. El control de acceso a todos los Sistemas de Información de la Universidad y en general a cualquiera de los servicios de Tecnologías de Información, debe realizarse por medio de la identidad digital, la cual es de uso exclusivo e intransferible.
16. Los roles asociados a la identidad digital harán parte de lo estipulado por el Procedimiento de Gestión de Identidades Digitales.

Cordialmente,

GUSTAVO ADOLFO PÉREZ ZAPATA
Director

Carrera 45 # 26-85
Edificio Uriel Gutiérrez Piso 4
(+57 1) 3165087 - (+57 1) 3165000 EXT: 18197-18406
Bogotá, D. C., Colombia
dntic_nal@unal.edu.co