UNIVERSIDAD PEDAGOGICA NACIONAL

RESOLUCION N° 0694 DE 15 OCT. 2020

Por la cual se adopta el Manual de Políticas de Seguridad de la Información de la Universidad Pedagógica Nacional

EL RECTOR DE LA UNIVERSIDAD PEDAGOGICA NACIONAL

En ejercicio de sus facultades legales (Ley 30 de 1992), estatutarias (Acuerdo 35 de 2005 del Consejo Superior), y especialmente de las funciones delegadas mediante el artículo 1° del Acuerdo 002 de 2018 del Consejo Superior, y

CONSIDERANDO:

Que la Ley 1341 de 2009 establece los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC y se encuentra reglamentada por el Decreto Nacional 2693 de 2012, reglamentado parcialmente por el Decreto Nacional 2573 de 2014.

Que en virtud de lo dispuesto en el artículo 1° del Acuerdo 002 de 2018 del Consejo Superior, se facultó al Rector para adoptar políticas propias de los sistemas de Control Interno y de Gestión, en el sentido de adoptar, implementar y mantener mediante la expedición de los actos administrativos a que haya lugar, las políticas de Operación, las políticas de Administración del Riesgo y las políticas propias de los Sistemas de Gestión, así como las de Control Interno que le corresponda acoger a la Universidad y que hacen parte de su Sistema de Gestión Integral.

Que, para la Universidad Pedagógica Nacional, la información en es un activo primordial en la prestación de sus servicios a la comunidad y la toma de decisiones eficientes, razón por la cual existe un compromiso para su protección, la consolidación de una cultura de seguridad, y la administración de riesgos asociados a la seguridad de la información.

Que como directriz institucional se decidió expedir un Manual de Políticas de Seguridad de la información, para que la Universidad Pedagógica Nacional formalice su compromiso con el proceso de gestión responsable de información que tiene como fin garantizar la integridad, confidencialidad y disponibilidad de este importante activo, teniendo como eje el cumplimiento de los objetivos misionales.

Que, contando con un Manual de Políticas de Seguridad de la Información en la Universidad, será posible el desarrollo del Sistema de Gestión de Seguridad de la información (SGSI), el cual hará parte del Sistema de Gestión Integral de la Universidad Pedagógica Nacional y estará alineado con los demás subsistemas que lo conforman.

Que, en mérito de lo expuesto,

RESUELVE:

ARTÍCULO 1º. *Adopción.* Adoptar el Manual de Políticas de Seguridad de la Información en la Universidad Pedagógica Nacional, el cual hace parte integral del presente acto administrativo.

ARTÍCULO 2º. *Actualizaciones y modificaciones.* Autorizar a la Subdirección de Gestión de Sistemas de Información para que haga las modificaciones o actualizaciones al Manual de Políticas de Seguridad de la Información, previo visto bueno del Comité Directivo, las cuales serán presentadas al Comité de Gobierno Digital o quien haga sus veces; sin necesidad de realizar modificación o ajuste a la presente resolución.

ARTÍCULO 3º. *Ámbito de Aplicación.* El Manual de Políticas de Seguridad de la Información de la Universidad Pedagógica Nacional se aplicará en desarrollo de las actividades, funciones y obligaciones institucionales, así como en todas las instalaciones de la Universidad.

RESOLUCION N° 0694 DE 15 OCT. 2020

ARTÍCULO 4º. *Publicación.* Publicar el Manual de Políticas de Seguridad de la Información, en la página Web y en el Manual de Procesos y Procedimientos de la Universidad Pedagógica Nacional.

ARTÍCULO 5º. *Capacitación.* La Subdirección de Personal incluirá el tema de seguridad de la información en el Plan Institucional de capacitación y formación para el personal de la Universidad, además difundirá el Manual de Políticas de Seguridad de la Información Digital, en las inducciones y reinducciones que realice.

ARTÍCULO 6º. *Vigencia.* La presente resolución rige a partir de la fecha de su expedición.

PUBLÍQUESE, COMUNÍQUESE, Y CÚMPLASE

Dado en Bogotá a los 15 OCT 2020

LEONARDO FABIO MARTÍNEZ PÉREZ
Rector

V.B. CORREO ELECTRÓNICO:
Aprobó: Henry Augusto Córdoba Sánchez- Subdirector de Sistemas de Información.
Revisó: Fernando Méndez Diaz- Vicerrector Administrativo y Financiero
Revisó: Arelys Valencia Valencia - Jefe Oficina Control Interno
Revisó: Elsa Liliana Aguirre Leguizamo- Jefe Oficina Jurídica
Elaboró: Andrés Almonacid León- SSI

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD PEDAGÓGICA NACIONAL

TABLA DE CONTENIDO

INTRODUCCIÓN

En la actualidad la información, tanto pública como privada, en las universidades se reconoce como un activo valioso e importante; en la medida que los sistemas de información apoyan cada vez más los procesos de misión crítica se requieren estrategias de alto nivel que permitan el control y administración efectiva, oportuna y disponible de los datos. La Universidad, los sistemas y red de información enfrentan amenazas de seguridad que incluyen, entre muchas otras, el fraude por computadora, espionaje, sabotaje, vandalismo, fuego, robo e inundación, posibilidad de daño y pérdida de información por causa de código malicioso, mal uso o ataques de denegación de servicio se hacen cada vez más comunes.

El presente manual de políticas de seguridad de la información permitirá a la Universidad avanzar en los procesos diarios que interactúan con los sistemas informáticos desarrollados y adquiridos por la entidad, permitiendo un control y manejo de la información de forma oportuna y eficiente, facilitando interactuar a su vez con el Sistema de Gestión Integral de la Universidad, para aumentar la calidad y la eficiencia en sus procesos.

OBJETIVO

El objetivo de este documento es establecer el *Manual de políticas en seguridad de la información de la Universidad Pedagógica Nacional*, con el fin de conservar, salvaguardar y proteger la información producida por los procesos de la institución, evitando su posible pérdida mediante la exposición a amenazas latentes en el entorno como acceso, manipulación o deterioro de la información.

NORMATIVIDAD

La Universidad Pedagógica Nacional es una entidad estatal, que debe cumplir con los requerimientos establecidos en la siguiente normatividad:

- Constitución Política de Colombia. Artículo 15 y artículo 209.
- Decreto 1078 de 2015. Principios de la Política de Gobierno Digital.
- Decreto 1499 de 2017 Regulación de Políticas de Gestión y Desempeño Institucional.
- Conpes 3854 de 2016. Política Nacional de Seguridad Digital en la República de Colombia.
- MECI 1000:2014. Lineamientos Generales para la Implementación del Modelo Estándar de Control Interno para el Estado Colombiano.
- Ley 1273 de 2009. Delitos informáticos en Colombia.
- ISO 27001:2013. Sistemas de Gestión de Seguridad en la Información– Requerimientos.
- ISO 27002:2013. Controles para Seguridad de la Información.
- ISO 27004:2016 Métricas para la medición de la Gestión de Seguridad de la Información.
- NIST SP 800-30. Guía de Gestión de Riesgos para los Sistemas de Tecnología de la Información.
- NIST SP 800-55. Guía de Métricas de Rendimiento para Seguridad de la Información.
- Guía Para La Elaboración de la Política General de Seguridad y Privacidad de la Información. Min-Tic.

1. DEFINICIONES

Para efectos del presente manual se tendrán en cuenta las siguientes definiciones:

a) **Activo de información:** elemento de *hardware* o *software*, información que pertenece a la Universidad almacenada en diferentes medios (humano, tecnológico, *software*, documental o de infraestructura) y considerada como primordial para el cumplimiento de los objetivos misionales.

b) **Administración de riesgos:** proceso de identificación, control, reducción o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar la información. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.

c) **Acuerdo de confidencialidad:** documento en el cual los funcionarios de la entidad o los provistos por terceras partes, manifiestan su voluntad de mantener la confidencialidad de la información de la Universidad Pedagógica Nacional, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la misma.

d) **Amenaza:** peligro potencial de un incidente no deseado que puede provocar daños a un activo de información.

e) **Bases de datos:** conjunto de información organizada en forma de registros, de manera que pueda ser utilizada eficientemente.

f) **Confidencialidad:** es la garantía de que la información no está disponible o divulgada para personas, entidades o procesos no autorizados.

g) **Continuidad del negocio:** plan logístico para la práctica de como una organización debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o desastre.

h) **Comité Gobierno Digital:** el Comité de Gobierno Digital es un órgano colegiado responsable de orientar la implementación de la Política de Gobierno Digital, su creación, funciones y funcionamiento se encuentran establecidos en la Resolución Rectoral 0644 de 2019 o en la norma que la modifique o reemplace.

i) **Copia de Seguridad (*Backup*):** es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de pérdida.

j) **Cuentas de servicios informáticos o cuentas de usuario:** registro electrónico individual para un usuario de servicios informáticos institucionales. Está compuesto por los siguientes datos: nombre (ID usuario), contraseña (*password*) y otra información que identifica al titular y determina el tipo de vinculación con la organización.

k) **Custodio del activo de la información:** aplicación de normas y procedimientos que permiten asegurar y proteger los activos de información de la Universidad, evitando la pérdida de la confidencialidad, integridad y disponibilidad.

l) **Derechos de autor:** corresponde a las normas que protegen las creaciones o manifestaciones del espíritu humano, materializadas en determinada forma para que sean accesibles por los sentidos y sea posible ejercer control sobre su uso y explotación. (Acuerdo 011 de 2017 del Consejo Superior. art.14)

m) **Datacenter:** centro de datos de la Universidad Pedagógica Nacional, donde se almacena toda la infraestructura tecnológica de la Institución.

n) **Equipo de cómputo:** dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.

o) **Evaluación de riesgos:** proceso o procedimiento que permite realizar un análisis de las amenazas y vulnerabilidades de los activos de información, identificando la probabilidad e impacto de que un evento ocurra.

p) **Incidente de Seguridad Informática:** evento adverso en un sistema de computadoras, o red de computadoras, que compromete la confidencialidad, integridad, disponibilidad, legalidad o confiabilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad, intento o amenaza de romper los mecanismos de seguridad existentes.

q) **Información:** conjunto o serie de datos que tienen un significado.

r) **Política:** instrucciones mandatarias que indican la intención de la alta dirección respecto a la operación de la institución.

s) **Propietario de Activos de Información**: en el contexto de la norma NTC 27001, un propietario de activos de información es cualquier persona o Institución a la cual se le asigna la responsabilidad formal de custodiar y asegurar un activo de información o un conjunto de ellos.

t) **Prueba de Caja Blanca:** tipo de pruebas de *software* que se realiza sobre las funciones internas de un módulo.

u) **Pruebas de Caja Negra**: pruebas funcionales. Se parte de los requisitos funcionales a muy alto nivel, para diseñar pruebas que se aplican sobre el sistema sin necesidad de conocer como está construido por dentro.

v) **Recursos tecnológicos:** elementos de tecnología que pueden ser *hardware* y/o *software*, tales como equipos de cómputo, impresoras, teléfonos, fax, programas y aplicativos de *software*, dispositivos USB, entre otros.

w) **Responsable de Seguridad de la Información:** funcionario de la Subdirección de Gestión de Sistemas de Información (SSI), cuya función principal es la de velar y supervisar el cumplimiento del presente manual y los lineamientos de la Subdirección de Sistemas de Información.

x) **Sistema de Información:** conjunto ordenado de elementos cuyas propiedades se relacionan e interaccionan permitiendo la recopilación, procesamiento, mantenimiento, transmisión y difusión de información, utilizando diferentes medios y mecanismos tanto automatizados como manuales.

y) **Tecnología de la Información:** conjunto de *hardware* y *software* operados por el *alma mater*, o por un tercero en su nombre, que componen la plataforma necesaria para procesar y administrar la información que requiere la Universidad para llevar a cabo sus funciones.

z) **Vulnerabilidad:** debilidad de un activo o control que puede ser explotada por una o más amenazas.

2. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

2.1 Generalidades

Los datos y la información son recursos de gran valor para la Universidad Pedagógica Nacional, por ende, se debe garantizar la protección adecuada de los mismos.

La elaboración, desarrollo, redacción e implementación de la política de seguridad de la información permite asegurar la mitigación de los riesgos que se presentan frente a las amplias amenazas. Este *Manual de Políticas de Seguridad de la Información* pretende contribuir a minimizar los riesgos asociados a los activos de información como: las personas, la infraestructura, los procesos y servicios con los que cuenta la Universidad, garantizando el eficiente cumplimiento en los procesos y procedimientos realizados en la Universidad, habitualmente.

La Universidad debe garantizar y establecer mecanismos que permitan difundir, elaborar y actualizar el presente manual de políticas.

2.2 Política General de Seguridad de la información

La Universidad Pedagógica Nacional, mediante la adopción e implementación del modelo de seguridad y privacidad de la información del **Ministerio** de Tecnologías de la **Información y las Comunicaciones** (Min-Tic), protege, preserva y administra la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la información crítica, misional del alma mater, mediante una gestión integral de riesgos y la implementación de controles físicos, digitales, preventivos, correctivos, persuasivos y detectivos, previniendo las amenazas y vulnerabilidades que puedan presentarse en los activos críticos misionales de la Universidad, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información, logrando así el acceso, uso efectivo y apropiación masiva de las Tecnologías de la Información y las Comunicaciones a través de políticas y programas para mejorar la calidad de los procesos enmarcados en el Sistema de Gestión Integral de la Universidad Pedagógica Nacional.

2.3 Alcance

La política deberá aplicarse por parte de los responsables del manejo de la información (funcionarios, profesores, contratistas y estudiantes) en todas las dependencias e instalaciones de la Universidad Pedagógica Nacional, a sus activos y recursos informáticos en la totalidad de los procesos internos o externos y en las tareas o actividades que desempeñen dentro de la Universidad.

2.4 Objetivos específicos Seguridad de la información

a) Proteger, preservar y administrar objetivamente la información y los activos críticos misionales de la Universidad Pedagógica Nacional, con el propósito de garantizar la integridad, confidencialidad y disponibilidad de dicha información.

b) Asegurar y mantener una adecuada administración de los riesgos de información, teniendo en cuenta los riesgos, amenazas informáticas y vulnerabilidades que se van presentando a diario en los sistemas informáticos de la Universidad.

c) Monitorear y asegurar el cumplimiento de los requisitos o criterios establecidos de la Seguridad de la Información.

d) Capacitar a los funcionarios de la Universidad en los temas referentes a Seguridad de la Información.

2.5 Responsabilidad

a) El *Manual de Políticas de Seguridad de la Información* es de aplicación obligatoria para todas las personas vinculadas con la actividad institucional de la Universidad Pedagógica Nacional.

b) La Dirección aprueba el *Manual de Políticas de Seguridad de la Información* y será responsable de la autorización de sus modificaciones.

c) El Comité de Gobierno Digital de la Universidad Pedagógica Nacional, o quien haga sus veces, será el responsable de revisar y proponer al rector, para su aprobación, el *Manual de Políticas de Seguridad de la Información*, las funciones generales en materia de seguridad de la información y la estructuración, recomendación, seguimiento y mejora del Sistema de Gestión de Seguridad de la Información de la Institución. También definirá las estrategias de capacitación en materia de seguridad de la información al interior de la Universidad.

d) La Subdirección de Gestión de Sistemas de Información en cabeza del subdirector, o quien haga sus veces, debe designar un funcionario de la misma Subdirección, quien será el responsable de coordinar

las acciones con el Comité de Gobierno Digital e iniciar el desarrollo, elaboración, implementación y cumplimiento del presente manual.

e) La Subdirección de Gestión de Sistemas de Información**,** en cabeza del subdirector, o quien haga sus veces, es la responsable de cumplir funciones relativas a la seguridad de los sistemas de información de la Universidad, lo cual incluye la operación del Sistema de Gestión de Seguridad de la Información y supervisión del cumplimiento dentro de la dependencia de aspectos inherentes a los temas tratados en el presente manual. El nivel de supervisión que pueda realizar cada grupo responsable de seguridad está relacionado con el talento humano que lo conforma y en todo caso deberá ser aprobado por el Comité de Gobierno Digital.

f) Los propietarios de activos de información son responsables de la clasificación, mantenimiento y actualización de la misma; así como de documentar y mantener actualizada la clasificación efectuada, definiendo qué usuarios deben tener permisos de acceso a la información de acuerdo con sus funciones y competencias. En general, tienen la responsabilidad de mantener íntegro, confidencial y disponible el activo de información mientras que es desarrollado, producido, mantenido y utilizado.

g) La Subdirección de Personal (SPE) y el Grupo de Contratación (GCO) cumplirán la función de notificar a los servidores públicos vinculados y/o contratados por la Universidad, las obligaciones respecto al cumplimiento de la política de seguridad de la información y de todos los estándares, procesos, procedimientos, prácticas y guías que surjan del Sistema de Gestión de la Seguridad de la Información. De igual forma, será responsable de la notificación del presente manual como de los cambios que en este se produzcan a todo el personal, a través de la suscripción de los *Compromisos de Confidencialidad* y de tareas de capacitación continua en materia de seguridad según lineamientos dictados por el Comité de Gobierno Digital, bajo la coordinación de la SSI. Para el caso de los contratos de prestación de servicios será realizado el mismo procedimiento a través del GCO.

h) La Subdirección de Gestión de Sistemas de Información sigue las directrices de la presente política y cumplirá los requerimientos que en materia de seguridad informática se establezcan para la operación, administración, comunicación y mantenimiento de los sistemas de información y los recursos de tecnologías de la información de la Universidad. Adicionalmente, corresponde a dicha subdirección determinar el inventario de activos de recursos tecnológicos de los cuales son propietarios o custodios, el cual será revisado y avalado por la Subdirección de Servicios Generales.

i) La Oficina Jurídica asesora en materia legal a la Universidad en lo que se refiere a la seguridad de la información.

j) La Oficina de Control Interno verifica el cumplimiento de lo establecido en el Manual de Políticas de Seguridad de la Información de la Universidad Pedagógica Nacional, bajo las normas y procedimientos aplicables y en atención al plan de trabajo definido para cada vigencia.

3. CARACTERÍSTICAS DE LA SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información se entiende como la preservación, aseguramiento y cumplimiento de las siguientes características de la información:

a) **Confidencialidad:** los activos de información solo pueden ser accedidos y custodiados por usuarios con permiso para ello.

b) **Integridad:** el contenido de los activos de información debe permanecer inalterado y completo. Las modificaciones realizadas deben ser registradas asegurando su confiabilidad.
c) **Disponibilidad: l**os activos de información sólo pueden ser obtenidos a corto plazo por usuarios con permisos adecuados.

d) **Autenticidad**: un activo de información es creado, modificado, actualizado y custodiado por los servidores públicos de la Universidad para validar su contenido.
e) **Posibilidad de auditoría:** conservación de evidencias de las actividades y acciones que afectan a los activos de información.
f) **Protección a la duplicación**: los activos de información son objeto de clasificación y se llevan registros de las copias generadas de aquellos catalogados como confidenciales.
g) **No repudio:** los autores, propietarios y custodios de los activos de información pueden identificarse plenamente.
h) **Legalidad: l**os activos de información cumplen los parámetros legales, normativos y estatutarios de la entidad.

i) **Confiabilidad de la información:** contenido fiable de los activos de información, conservando la confidencialidad, integridad, disponibilidad, autenticidad y legalidad.

4. COMPROMISO DE LA DIRECCIÓN

El *Manual de Políticas de Seguridad de la Información* de la Universidad Pedagógica Nacional debe ser revisado y actualizado según se requiera anualmente por parte del Comité de Gobierno Digital, mediante propuesta presentada por la Subdirección de Gestión de Sistemas de Información, bajo los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). Una vez validada la actualización por el Comité de Gobierno Digital, se acogerán los cambios a través de los procedimientos propios del Sistema de Gestión Integral.

Debe Promover la cultura de la seguridad de la información en los servidores públicos, estudiantes y demás partes interesadas que tengan acceso a la información y deben velar por el cumplimiento de la Política General de Seguridad de la Información.

5. CLASIFICACIÓN Y VALORACIÓN DE LOS ACTIVOS DE INFORMACIÓN

5.1 Clasificación de la información

a) La Universidad Pedagógica Nacional define los niveles apropiados para la clasificación de la información conforme a su criticidad y sensibilidad, para ello la Subdirección de Gestión de Sistemas de Información, dispondrá de una guía concerniente a la clasificación de la información para que los propietarios de los activos y de la información la cataloguen y determinen los controles necesarios para su debida protección.

b) La presente guía define los controles administrativos y técnico-operativos que serán implementados en la Universidad Pedagógica Nacional con el propósito de asegurar la confidencialidad, disponibilidad e integridad de los activos de información en función del nivel de clasificación.

c) La información producida por la Universidad debe ser identificada, documentada y clasificada teniendo en cuenta la guía de clasificación de la información elaborada por la Subdirección de Gestión de Sistemas de Información.

d) Una vez clasificada la información, la Universidad proporciona los recursos necesarios para la aplicación de controles en busca de preservar la confidencialidad, integridad y disponibilidad de la misma, con el fin de promover el uso adecuado por parte de los funcionarios de la Universidad y los contratistas autorizados que requieran de la misma para la ejecución de sus actividades.

e) La Subdirección de Gestión de Sistemas de Información debe proveer los métodos de cifrado de la información, y administrar el *software* o herramienta utilizado para tal fin.

f) La Subdirección de Gestión de Sistemas de Información debe efectuar la eliminación segura de la información a través de los mecanismos necesarios en la plataforma tecnológica, ya sea para dar de baja o cambiar de usuario.

g) Los usuarios deben acatar los lineamientos de la guía de clasificación de la información para el acceso, divulgación, almacenamiento, copia, transmisión, etiquetado y eliminación de la información contenida en los recursos tecnológicos, así como de la información física de la Universidad Pedagógica Nacional.

h) La información física y digital de la Universidad Pedagógica Nacional debe tener un periodo de almacenamiento que puede ser dictaminado por requerimientos legales o misionales; este período debe ser indicado en las Tablas de Retención Documental (TRD).

i) Los funcionarios, profesores, estudiantes y contratistas deben tener en cuenta cuando impriman, escaneen, fotocopien y envíen faxes, verificar las áreas adyacentes a impresoras, escáneres, fotocopiadoras y máquinas de fax para asegurarse que no quedaron documentos relacionados o adicionales; asimismo, recoger de las impresoras, escáneres, fotocopiadoras y máquinas de fax, inmediatamente los documentos confidenciales para evitar su divulgación no autorizada.

j) Tanto los funcionarios como el personal provisto por terceras partes deben asegurarse de que en el momento de ausentarse de su puesto de trabajo sus escritorios se encuentren libres de documentos y medios de almacenamiento utilizados para el desempeño de sus labores; estos deben contar con las protecciones de seguridad necesarias de acuerdo con su nivel de clasificación.

k) La información que se encuentra en documentos físicos debe ser protegida, a través de controles de acceso físico y las condiciones adecuadas de almacenamiento y custodia.

5.2 Lineamientos para la clasificación de la información

a) Todos los funcionarios, profesores y estudiantes deben cumplir con las directrices establecidas en la guía para la clasificación de la información, así como para la divulgación, almacenamiento, etiquetado, eliminación y transmisión de la información que se encuentra almacenada en los sistemas de información y recursos físicos de la Universidad.

b) La Subdirección de Servicios Generales - Archivo y Correspondencia, o quien haga sus veces, debe restablecer un periodo de almacenamiento para la información física y digital, con base en lo establecido en las Tablas de Retención Documental (TRD).

c) La Universidad Pedagógica Nacional, como propietaria de la información generada, procesada, almacenada y transmitida con su plataforma tecnológica, otorga la responsabilidad a las áreas sobre sus activos de información, asegurando el cumplimiento de las directrices que regulen el uso adecuado de la misma.

d) La información, archivos físicos, los sistemas, los servicios y los equipos (ej. estaciones de trabajo, equipos portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos y faxes, entre otros) propiedad de la Universidad, son activos de la institución y se proporcionan a los funcionarios y contratistas para cumplir con los objetivos de la UPN.

e) Toda la información sensible de la Universidad, así como los activos donde esta se almacena y se procesa, debe ser asignada a un responsable, debe inventariarse y posteriormente clasificarse, de acuerdo con los requerimientos y los criterios de la Subdirección de Gestión de Sistemas de Información. Los propietarios de los activos de información deben llevar a cabo el levantamiento y la actualización permanente del inventario de activos de información al interior de sus procesos o áreas.

f) Los recursos tecnológicos de la Universidad deben ser utilizados de forma ética y en cumplimiento de las leyes y reglamentos vigentes, con el fin de evitar daños o pérdidas sobre la operación o la imagen de la Universidad.

g) Los recursos tecnológicos de la Universidad provistos a funcionarios y contratistas son proporcionados con el único fin de llevar a cabo las labores de la Universidad; por consiguiente, no deben ser utilizados para fines personales o ajenos a este.

h) Los funcionarios, profesores y contratistas no deben utilizar sus equipos de cómputo y dispositivos móviles personales para desempeñar las actividades laborales, a menos que se requiera realizar actividades de forma remota, itinerante y virtual, previa autorización de las máximas autoridades de La Universidad.

i) Los funcionarios no deben utilizar *software* no autorizado o de su propiedad en la plataforma tecnológica de La Universidad.

j) Todas las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos son asignados a un responsable, por lo cual es su compromiso hacer uso adecuado y eficiente de dichos recursos.

k) En el momento de desvinculación o cambio de labores, los funcionarios deben realizar la entrega de su puesto de trabajo al vicerrector, director o jefe de oficina o quien este delegue; así mismo, deben encontrarse a paz y salvo con la entrega de los recursos tecnológicos y otros activos de información suministrados en el momento de su vinculación.

l) Cada dependencia debe elaborar su propio inventario de activos de información a su cargo. La clasificación del inventario debe tener la valoración, ubicación y acceso de la información, correspondiendo al responsable de seguridad de la información brindar herramientas que permitan la administración del inventario por cada dependencia, garantizando la disponibilidad, integridad y confidencialidad de los datos que lo componen.

m) La Subdirección de Servicios Generales (SSG) junto con la Subdirección de Gestión de Sistemas de Información comparten la responsabilidad de mantener el inventario completo y actualizado de los recursos de *hardware* y *software* de la institución.

n) La información, de acuerdo con su prioridad, tendrá la siguiente clasificación:
   - Pública: información que podrá ser compartida.
   - Uso Interno: información de interés general para la Universidad.
   - Información confidencial: información de interés para un área u oficina en particular o por reglamentación o normatividad de alguna ley de protección de datos o habeas data.

5.3 Etiquetado de la información

a) Para la información en medios magnéticos se debe realizar el inventario, haciendo la descripción y las características de dicha información, clasificando y etiquetando la información teniendo en cuenta niveles que se establecieron en la guía de clasificación.

b) Los jefes inmediatos de todas las dependencias son los responsables de la información que se encuentra almacenada en las unidades a su cargo, deben establecer las responsabilidades de los funcionarios y definir quién debe ser autorizado para realizar operaciones emergentes con la información.

5.4 Manejo de los soportes de almacenamiento

Los responsables de la información en la Universidad Pedagógica Nacional dan el adecuado manejo para que solo sea divulgada la información pública y de uso interno.

Así como el adecuado manejo de la información en sus soportes de almacenamiento en cuanto a su conservación, eliminación, modificación y destrucción.

5.4.1 Gestión de soporte extraíbles

La Subdirección de Gestión de Sistemas de Información debe otorgar los procedimientos y las herramientas tecnológicas para realizar la adecuada administración de los medios extraíbles teniendo en cuenta las necesidades de los funcionarios respecto a sus actividades y funciones desempeñadas.

Los equipos de cómputo, portátiles y tabletas tienen acceso a los puertos de entrada USB y unidades de dispositivos CD/DVD, por consiguiente, deben contar con los siguientes requisitos:

- Servicio de escaneo de antivirus institucional.

- Configuración en el *software* de antivirus del servicio y herramienta de bloqueo automático de ejecutables que contienen la información almacenada en DVD.

5.4.2 Eliminación de soportes

La Subdirección de Gestión de Sistemas de Información garantiza el adecuado procedimiento para que la información almacenada en los medios de almacenamiento sea eliminada de una forma segura, utilizando los mecanismos y herramientas para tal fin, asegurando que no queden rastros después de realizar el procedimiento.

5.4.3 Soportes físicos e información en tránsito

La Subdirección de Gestión de Sistemas de Información debe asegurar que los medios de almacenamiento que tienen la información de tipo confidencial de la Universidad tengan protección contra el mal uso, corrupción y acceso no autorizado durante el proceso de transporte.

La Subdirección de Gestión de Sistemas de Información garantiza que la información que se trasmite y envía a través de la infraestructura de red de la Universidad cuenta con los parámetros y protocolos establecidos en materia de seguridad, asegurando la confidencialidad, integridad y disponibilidad.

6. POLÍTICA DE SEGURIDAD EN EL RECURSO HUMANO

a) La Subdirección de Personal y el Grupo de Contratación, con apoyo de las unidades solicitantes y conforme a los procedimientos establecidos, deben realizar las verificaciones necesarias para confirmar la veracidad de la información suministrada por el personal candidato a ocupar un cargo en la Universidad Pedagógica Nacional o por los contratistas antes de su vinculación definitiva.

b) La Subdirección de Personal y el Grupo de Contratación disponen de los mecanismos o instrumentos para garantizar que los funcionarios de la Universidad Pedagógica Nacional manifiesten su acuerdo y/o cláusula de Confidencialidad y Aceptación de Políticas de Seguridad de la Información; las evidencias deben ser anexadas a los demás documentos relacionados con la ocupación del cargo.

c) Cada jefe de dependencia debe informar al funcionario de la existencia de acuerdos y/o cláusulas de confidencialidad y de la aceptación de políticas para contratistas, antes de otorgar acceso a la información de la Universidad.

d) Quienes estén vinculados a la actividad institucional y realicen labores en o para la Universidad, deben manifestar la aceptación del acuerdo y/o cláusula de confidencialidad y de las políticas de seguridad de la información contenidas en el presente manual, antes de que se les otorgue acceso a las

instalaciones y a la plataforma tecnológica de la Universidad. Deben tener un perfil asociado al directorio activo de la Universidad que garantice el adecuado uso de los recursos de información, el *hardware* y *software* asociado a este perfil.

e) La Subdirección de Gestión de Sistemas de Información debe mantener actualizado un directorio completo de los perfiles de usuario, de acuerdo a los procedimientos o guías establecidos para la misma.

f) El Comité de Gobierno Digital determina los atributos y características que deben definirse para los diferentes perfiles, de acuerdo a las propuestas de la Subdirección de Gestión de Sistemas de Información.

7. POLÍTICA DE ACTUALIZACIÓN DE ACCESO A LA PLATAFORMA TECNOLÓGICA POR CAMBIOS EN VINCULACIÓN DE FUNCIONARIOS Y CONTRATISTAS

a) Los jefes de las dependencias (vicerrectores, subdirectores, jefes de oficina, coordinadores, decanos, directores) y los supervisores de los contratos, según el caso, informan a la Subdirección de Gestión de Sistemas de Información para que se haga el correspondiente ajuste en cuanto al acceso a la plataforma tecnológica de la Universidad.

b) La Subdirección de Personal, con el apoyo de la Subdirección de Gestión de Sistemas de Información, se encarga de elaborar, actualizar, mantener y ejecutar el plan de capacitación en temas referentes a la Seguridad de la Información que incentive el continuo crecimiento en temas de concientización individual y colectiva referentes a la seguridad de la información, el cual será incluido en el Plan Institucional de Capacitación de la Universidad.

c) Los funcionarios, profesores y contratistas que por sus funciones u obligaciones hagan uso de la información de la Universidad, deben dar cumplimiento a las políticas, normas y procedimientos de seguridad de la información, así como asistir a las capacitaciones que sean referentes a seguridad de la información.

8. RESPONSABILIDADES DE LA COMUNIDAD UNIVERSITARIA Y USUARIOS EXTERNOS

8.1 Responsabilidades del personal de la Universidad

a) Todas las personas vinculadas a la actividad institucional, funcionarios, profesores, estudiantes y contratistas deben contar y firmar un acuerdo que contenga los términos y condiciones que regulan el uso de recursos de las tecnologías de la información y las directrices y usuarios con perfiles que permiten manipular y usar la información de la Universidad.

b) Todos los funcionarios de la Universidad deben ser cuidadosos de no divulgar información confidencial en lugares públicos, en conversaciones o situaciones que pongan en riesgo la seguridad y el buen nombre de la entidad.

c) Los procedimientos para obtener tales perfiles y las características de cada uno de estos deben ser mantenidos y actualizados por cada dependencia, de acuerdo con los lineamientos definidos por la Subdirección de Sistemas de Información, en cuanto a la información, dispositivos de *hardware* y los elementos de *software*.

d) La Subdirección de Personal con el apoyo de la Subdirección de Gestión de Sistemas de Información, se encarga de elaborar, actualizar, mantener y ejecutar el plan de capacitación en temas referentes a la seguridad de la información que incentive el continuo crecimiento en temas de concientización individual y colectiva referentes a seguridad de la información, el cual será incluido en el Plan Institucional de Capacitación de la Universidad.

e) Los funcionarios y contratistas que por sus funciones u obligaciones hagan uso de la información de la Universidad, deben dar cumplimiento a las políticas, normas y procedimientos de seguridad de la información, así como asistir a las capacitaciones que sean referentes a la seguridad de la información.

8.2 Responsabilidades de los estudiantes

Para utilizar los recursos tecnológicos de la Universidad, los estudiantes deben leer y aceptar los acuerdos y condiciones en temas referentes a seguridad de la información, cada vez que hagan el procedimiento para matricularse en la Universidad, indicando además que serán responsables de dar cumplimiento a los aspectos pertinentes contemplados en este manual, especialmente si les es otorgada una monitoria, participan en el grupo de protocolo o son beneficiarios del programa ASE, o hacen parte de otra actividad en la que sean responsables de información institucional. La Subdirección de Gestión de Sistemas de Información junto con la Subdirección de Admisiones y Registro deben garantizar los mecanismos para la divulgación y aceptación de dichas condiciones, utilizando los formatos designados para tal proceso.

8.3 Responsabilidades de usuarios externos

a) Todos los usuarios externos y personal de empresas externas deben estar autorizados por un funcionario de la Universidad, quien estará atento al control y vigilancia del uso adecuado de la información y los recursos de tecnologías de la información que pertenecen a la Universidad. El procedimiento definido para el registro de estos usuarios debe ser creado y mantenido por la Subdirección de Sistemas de Información de acuerdo con los manuales, procedimientos o guías establecidos, así como escalados por la Mesa de Ayuda Institucional.

b) Los proveedores, invitados y usuarios externos deben aceptar los términos y condiciones de uso de la información y recursos de tecnologías de la información institucionales. Las cuentas de usuarios externos deben ser de perfiles específicos y tener caducidad no superior a *treinta (30) días*, renovables de acuerdo con la naturaleza del usuario.

9. POLÍTICA DE CONTROL DE ACCESO

a) La Universidad Pedagógica Nacional cuenta con entornos que permiten tener control de acceso idóneos, garantizando el aseguramiento del perímetro en las oficinas, salones, salas de cómputo y laboratorios, evitando el acceso no autorizado a estos.

b) La Universidad Pedagógica Nacional, garantiza el control de las amenazas físicas internas y externas y provee las condiciones ambientales que se necesitan para el adecuado funcionamiento de la infraestructura tecnológica y para resguardar los activos de información digitales y físicos.

c) La Subdirección de Gestión de Sistemas de Información debe contar con controles de seguridad física efectivos.

d) La empresa de vigilancia que presta el servicio de vigilancia a la Universidad tiene la función de inspeccionar y asegurar que se cumplan las directrices en materia de seguridad en pro de:

- Las dependencias o áreas críticas con información deben permanecer cerradas y custodiadas.
- Las áreas donde se almacena información confidencial y sensible son de acceso limitado. La Universidad define y otorga los permisos por medio de la Subdirección de Gestión de Sistemas de Información.

9.1 Política de acceso a redes y recursos de red

a) La Subdirección de Gestión de Sistemas de Información como responsable de las redes de datos y los recursos de red de la Universidad, debe propender porque dichas redes sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico.

b) La Subdirección de Gestión de Sistemas de Información debe establecer un procedimiento de autorización y controles para proteger el acceso a las redes de datos y los recursos de red de la Universidad.

c) La Subdirección de Gestión de Sistemas de Información debe asegurar que las redes inalámbricas de la Universidad cuenten con métodos de autenticación que eviten accesos no autorizados.

d) La Subdirección de Gestión de Sistemas de Información debe establecer controles para la identificación y autenticación de los usuarios en las redes o recursos de red de la Universidad, así

como velar por la aceptación de las responsabilidades de dichos usuarios; además, se debe formalizar la aceptación de las Políticas de Seguridad de la Información por parte de estos.

e) Los funcionarios y contratistas, antes de contar con acceso lógico por primera vez a la red de datos de la Universidad Pedagógica Nacional, deben diligenciar el formato de creación de cuentas de usuario debidamente autorizado y los términos y condiciones sobre el uso de las Tecnologías de la Información.

f) Los equipos de cómputo de usuario final que se conecten o deseen conectarse a las redes de datos de la Universidad deben cumplir con todos los requisitos o controles para autenticarse en estas y únicamente podrán realizar las tareas para las que fueron autorizados.

9.2 Categorías de acceso

Los accesos a los recursos de tecnologías de información institucionales deben estar restringidos según los perfiles de usuario definidos por la Subdirección de Gestión de Sistemas de Información, de acuerdo con las necesidades de las dependencias y las labores desarrolladas por cada uno de los funcionarios, según los lineamientos que se establezcan desde el Comité de Gobierno Digital, o quien haga sus veces. Así mismo, deberán ser avalados por el directivo o responsable de cada uno de los recursos tecnológicos.

9.2.1 Control de claves y nombres de usuario

a) El acceso a información restringida debe estar controlado. La Universidad propende el uso de sistemas automatizados de autenticación que manejen credenciales o firmas digitales.

b) Corresponde a la Subdirección de Gestión de Sistemas de Información elaborar, mantener y publicar los documentos de servicios de red que ofrece la institución a su personal, estudiantes, docentes y terceros.

c) La Subdirección de Gestión de Sistemas de Información debe elaborar una guía de administración de cuentas de usuario para el uso de servicios de red.

d) El acceso a los sistemas de información y la información almacenada es responsabilidad de los funcionarios a cargo de estos sistemas.

e) La Universidad debe actualizar, crear, eliminar y mantener la mínima cantidad de cuentas de usuario que el personal, los estudiantes, docentes y terceros deben poseer para acceder a los servicios de red.

f) La administración de las contraseñas de red y de los equipos de cómputo es responsabilidad de la Subdirección de Gestión de Sistemas de Información. Estas contraseñas deben tener mínimo el proceso de cifrado y almacenamiento seguro.

g) Las claves de administrador de los sistemas deben ser administradas y guardadas por la Subdirección de Gestión de Sistemas de Información y deben ser cambiadas cada 90 días o cuando el personal adscrito al cargo renuncie, fallezca o cambie de labores.

h) Las claves de administración de acceso a los servidores de aplicaciones físicos y virtuales de la Universidad y administración de bases de datos deben ser administradas por el personal adscrito o asignado por la Subdirección de Gestión de Sistemas de Información, teniendo en cuenta las directrices y lineamientos manuales, instructivos o guías establecidos para tal fin.

9.2.2 Computación móvil

a) La Universidad reconoce el alto grado de exposición que tiene la información y los datos almacenados en dispositivos tales como computadores, portátiles, notebooks, PDA, celulares, etc. La Subdirección de Personal junto con la Subdirección de Gestión de Sistemas de Información deben elaborar, mantener e implementar planes de capacitación que permitan concientizar en temas de seguridad de la información.

b) Las redes inalámbricas son potencialmente vulnerables a riesgos de seguridad, por ende, deben ser identificados, valorados y tratados de acuerdo con los lineamientos de la política de seguridad.

9.2.3 Acceso remoto

Para el proceso de acceso remoto a los servicios de la Universidad, se tendrán en cuenta los parámetros y directrices definidas por la Subdirección de Gestión de Sistemas de Información.

9.3 Gestión de acceso de usuarios

9.3.1 Política de administración de acceso de usuarios

a) La Universidad Pedagógica Nacional debe elaborar los privilegios concernientes al tema de control de acceso lógico de cada uno de los usuarios, los recursos tecnológicos y los sistemas de información de la Universidad. Garantiza que todas las personas vinculadas a la Universidad tengan los perfiles y permisos definidos para que tengan acceso únicamente a los recursos e información necesaria para el desarrollo de sus labores.

b) La Subdirección de Gestión de Sistemas de Información debe elaborar una guía para la administración de los usuarios que tienen acceso a la infraestructura de red, infraestructura tecnológica y los sistemas de información de la Universidad. Se debe garantizar que todos los perfiles y cuentas de usuario sean creados, modificados y eliminados de forma segura.

c) Los jefes de las dependencias (vicerrectores, subdirectores, jefes de oficina, coordinadores, decanos, directores) y los supervisores de los contratos, según el caso, solicitarán ante la Subdirección de Gestión de Sistemas de Información la creación, eliminación y bloqueo de los usuarios y perfiles que tienen acceso a los sistemas de información de la Universidad.

d) La Subdirección de Gestión de Sistemas de Información debe contar como mínimo con un *software* que administre y gestione las características que deben tener las contraseñas que tendrán acceso a la infraestructura tecnológica, los sistemas de información y los servicios de red.

e) La Subdirección de Gestión Sistemas de Información debe establecer los mecanismos y procedimientos que aseguren la eliminación y bloqueo de los privilegios de acceso sobre los recursos de infraestructura, los servicios de red y los sistemas de información de manera eficaz y oportuna.

f) La Subdirección de Gestión de Sistemas de Información garantiza que los usuarios que tienen asignados permisos por defecto a los diferentes sistemas de información de la universidad y a la infraestructura deben ser inhabilitados o eliminados de forma eficaz y segura.

g) La Subdirección de Gestión de Sistemas de Información junto con los dueños de los activos deben autorizar la creación o modificación de las cuentas de acceso a la infraestructura tecnológica y sistemas de información de la Universidad.

9.3.2 Política de responsabilidades de acceso de los usuarios

Los usuarios de los recursos tecnológicos y los sistemas de información realizarán un uso adecuado y responsable de dichos recursos y sistemas, salvaguardando la información a la cual se les ha permitido el acceso.

Normas de responsabilidad de acceso

a) Los estudiantes, profesores, funcionarios y contratistas que hacen uso de la plataforma tecnológica, los servicios de red y los sistemas de información de la Universidad Pedagógica Nacional, deben hacerse responsables de las acciones realizadas en los mismos, así como del usuario y contraseña asignados para el acceso a estos.

b) Ninguna persona debe compartir sus cuentas de usuario y contraseñas asignados para el ingreso a los servicios de red y los sistemas de información con otros miembros de la universidad o terceros.

c) Los estudiantes, funcionarios, profesores y terceros que posean acceso a la plataforma tecnológica, los servicios de red y los sistemas de información que la Universidad ofrece deben acogerse a las normas establecidas para la configuración de contraseñas designadas por la institución.

9.3.3 Registro y cancelación del registro de usuarios

a) La Subdirección de Gestión de Sistemas de Información debe contar con una base de datos que contenga la información de todos los usuarios y sus perfiles.

b) Para la creación de un nuevo usuario o reasignación de un rol que necesite acceder a un Sistema de Información de la Universidad se debe diligenciar en el formato de solicitud y tramitar según los medios, mecanismos y requisitos establecidos.

9.4 Control de acceso a sistemas y aplicaciones

9.4.1 Restricción de acceso a información

a) Todos los miembros de la Universidad Pedagógica Nacional y terceros son responsables por las credenciales (usuario y contraseña) que le sean asignadas y que reciben para el uso y acceso de los recursos.

b) Ningún usuario (profesor, funcionario, estudiante, graduado o contratista) recibe credenciales de acceso a la plataforma tecnológica, los servicios de red y los sistemas de información o aplicaciones, hasta que no acepte formalmente la Política de Seguridad de la Información vigente.

c) Todos los estudiantes, profesores, funcionarios, graduados, visitantes y contratistas deben autenticarse en los mecanismos de control de acceso provistos por la Subdirección de Gestión de Sistemas de Información antes de poder usar la infraestructura tecnológica de la Universidad Pedagógica Nacional.

d) Los funcionarios, profesores, estudiantes y contratistas no deben proporcionar información de los mecanismos de control de acceso en las instalaciones e infraestructura tecnológica de la Universidad a personal externo, a menos que se tenga el visto bueno del dueño de la información, de la Subdirección de Gestión de Sistemas de Información y de su jefe inmediato.

9.4.2 Procedimiento de inicio de sesión segura

La Subdirección de Gestión de Sistemas de Información:

a) Garantiza que todo acceso a los servicios de información solo se puede ingresar a ellos a través de un proceso de conexión seguro.

b) Instala todos los controles que sean necesarios para garantizar la protección de los servicios de información contra intentos de inicio de sesiones con procedimientos de ataques de fuerza bruta.

c) Diseña y genera alertas de advertencia global mostrando que solo pueden acceder a los quipos de cómputo los usuarios asignados para tal fin.

d) Consolida la información que es ingresada al finalizar o completar los datos de entrada ingresados. En caso de error, el sistema debe mantener la integridad de los datos ingresados y no debe señalar qué datos fueron correctos o incorrectos.

e) Habilita el registro de los intentos exitosos y fallidos de acuerdo con los perfiles de los usuarios en los sistemas de información necesarios.

f) Garantiza la transmisión segura de contraseñas sobre la red.

g) Garantiza el cierre total de sesiones inactivas después de un periodo de inactividad de cinco minutos.

9.4.3 Sistema de gestión de contraseñas

a) A los funcionarios, profesores, estudiantes y contratistas se les debe entregar junto con el nombre de usuario la contraseña de acceso a los servicios de red y Sistemas de Información de la Universidad. Esta contraseña debe ser cambiada en el primer intento de uso, para así garantizar la responsabilidad de uso y único conocimiento de la misma.

b) Los funcionarios, profesores, estudiantes y contratistas deben establecer una contraseña que contenga una longitud mínima de ocho caracteres alfanuméricos (mayúsculas, minúsculas, números y símbolos), diferentes a nombres propios o a cualquier otra palabra de fácil identificación.

c) La Subdirección de Gestión de Sistemas de Información debe cambiar las contraseñas o claves de Administrador de los diferentes Sistemas de Información de acuerdo a los parámetros definidos.

d) La Subdirección de Gestión de Sistemas de Información debe establecer los controles necesarios para que después de tres intentos no exitosos al digitar la contraseña del usuario esta se bloquee de manera inmediata y se debe solicitar el desbloqueo en la plataforma destinada para este fin.

e) Los profesores, administrativos, estudiantes y contratistas deben realizar su cambio de contraseña exclusivamente en la plataforma destinada para tal fin. No se podrán modificar por ningún otro medio.

f) La Subdirección de Gestión de Sistemas de Información debe asegurar que el número de sesiones concurrentes de un mismo usuario sea limitado.

g) La Subdirección de Gestión de Sistemas de Información debe establecer mecanismos para que las contraseñas o claves no sean iguales al nombre de usuario o cualquier variación (al revés, mayúsculas, etc.), alias o sobrenombre de la persona.

h) Los profesores, funcionarios, estudiantes y contratistas deben asegurarse de que la contraseña o clave no contiene palabras frecuentemente usadas y que se puedan asociar de manera rápida con su vida personal (nombre de hijos, fecha de nacimiento, número de cédula y número de celular, entre otros), no usan patrones como secuencias de números o caracteres y cadenas repetidas.

i) La Subdirección de Gestión de Sistemas de Información debe proporcionar los mecanismos necesarios para que los profesores, administrativos o estudiantes que olviden, bloqueen o extravíen su contraseña puedan restablecerla de forma segura.

j) Los profesores, funcionarios, estudiantes y contratistas deben asegurarse de que las contraseñas no se encuentren de forma legible en cualquier medio impreso y de no dejarlas en un lugar donde personas no autorizadas puedan descubrirlas.

k) Los estudiantes, funcionarios, profesores y contratistas deben cambiar inmediatamente la contraseña si tienen la sospecha de que esta es conocida por otra persona.

l) Los funcionarios, profesores, estudiantes y contratistas deben solicitar a la Subdirección de Gestión de Sistemas de Información el permiso para utilizar e instalar *software* para el almacenamiento de contraseñas que proporcione esta función.

9.4.4 Control de acceso a códigos fuente de aplicaciones

a) La Subdirección de Gestión de Sistemas de Información debe implementar los controles necesarios para asegurar que el acceso al código fuente de los aplicativos desarrollados sea limitado. Solamente el personal de desarrollo perteneciente a la Subdirección de Gestión de Sistemas de Información podrá contar con acceso a esta información y hará un uso moderado de la misma.

b) La Subdirección de Gestión de Sistemas de Información debe proporcionar las herramientas necesarias para realizar control de cambios sobre el código fuente de los aplicativos desarrollados por la misma, las cuales permitirán retroceder a una versión anterior del código.

c) La Subdirección de Gestión de Sistemas de Información debe ser responsable por la aprobación, supervisión y modificación de los códigos fuente de los aplicativos.

10. CIFRADO

10.1 Controles criptográficos

La Universidad Pedagógica Nacional debe asegurar el uso adecuado y eficaz de la criptografía que se va a implementar, garantizando la confidencialidad, autenticidad e integridad de la información de la Universidad en el proceso de transmisión y almacenamiento de la misma.

10.1.1 Política de usos de los controles criptográficos

La Subdirección de Gestión de Sistemas de Información:

a) Asegura los procedimientos o herramientas necesarias para garantizar la protección de claves de ingreso a la infraestructura de red y los Sistemas de Información de la Universidad.

b) Adecua los procedimientos necesarios de encriptación y cifrado para garantizar que los procesos en materia de transferencia y propagación de información confidencial se realicen en forma segura tanto para el proceso interno o externo.

c) Elabora una guía para el uso de la herramienta que permite encriptar la información privada y confidencial perteneciente a la Universidad por parte de los propietarios de la información (vicerrectores, subdirectores y jefes de oficina, decanos, coordinadores y demás directivos de la Universidad).

d) Cuenta con una política que permita cifrar la información para afianzar y asegurar la privacidad de la información que se respalda en medios de almacenamiento secundarios.

11. SEGURIDAD FÍSICA Y AMBIENTAL

11.1 Áreas seguras

a) La Universidad Pedagógica Nacional provee la implantación y vela por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones. Así mismo, controla las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas.

b) Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, serán de acceso restringido.

11.1.1 Controles físicos de entrada

a) Cualquier persona (estudiante, funcionario, docente o tercero) que tenga acceso a las instalaciones de la Universidad Pedagógica Nacional, debe registrar los equipos de cómputo que no sean de propiedad de la institución en los instrumentos establecidos por la Empresa de Vigilancia y Seguridad con contrato vigente con la Universidad, de acuerdo a los procedimientos definidos por la Subdirección de Sistemas de Información.

b) Los profesores, funcionarios, estudiantes o contratistas que requieran ingresar al *Data Center*, centros de cómputo y a los centros de cableado, deben realizar las solicitudes de acceso a la Subdirección de Gestión de Sistemas de Información mediante el mecanismo definido para tal fin. Adicionalmente, los responsables deben realizar un registro del ingreso de los visitantes en una bitácora ubicada en la entrada de estos lugares de forma visible.

c) Los profesores, funcionarios, estudiantes y contratistas deben cumplir completamente con los controles físicos implantados por la institución, ya que los ingresos y salidas a las instalaciones de la Universidad deben ser registrados de acuerdo a los lineamientos establecidos por la Oficina de Servicios Generales.

d) Todos los miembros de la comunidad y contratistas deben portar el carné que los identifica como tales en un lugar visible mientras se encuentren en las instalaciones de la institución; en caso de pérdida del carné deben reportarlo a la mayor brevedad posible.

e) Las dependencias que tienen bajo su custodia salas de cómputo, laboratorios y centros de cableado deben modificar de manera inmediata los privilegios de acceso físico a estos sitios en situaciones de desvinculación o cambio en las labores de una persona autorizada.

f) Las dependencias que tienen bajo su custodia salas de cómputo, laboratorios y centros de cableado deben velar por las condiciones físicas y medioambientales necesarias para certificar la protección y correcta operación de los recursos de la plataforma tecnológica ubicados en estos sitios. Para cumplir con esto deben existir:

- Sistemas de control ambiental de temperatura y humedad
- Sistemas de extinción de incendios
- Sistemas de vigilancia y monitoreo

g) Las dependencias que tienen bajo su custodia salas de cómputo, laboratorios y centros de cableado, en conjunto con la Subdirección de Servicios Generales, deben velar porque los recursos de la plataforma tecnológica ubicados en estos sitios se encuentren protegidos contra fallas o interrupciones eléctricas.

h) Las dependencias que tienen bajo su custodia salas de cómputo, laboratorios y centros de cableado, en conjunto con la Subdirección de Servicios Generales, deben certificar que estos sitios se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.

i) Las dependencias que tienen bajo su custodia salas de cómputo, laboratorios y centros de cableado, en conjunto con la Oficina de Servicios Generales, deben asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos sean realizadas por personal idóneo y previamente autorizado e identificado.

j) Las dependencias que tienen bajo su custodia salas de cómputo, laboratorios y centros de cableado, en conjunto con la Subdirección de Servicios Generales, deben llevar el control de la programación del mantenimiento preventivo a estos sitios, teniendo en cuenta los niveles de servicio acordados con los responsables de los servicios particulares y acorde con la operación de la Universidad.

k) Las dependencias que tienen bajo su custodia salas de cómputo, laboratorios y centros de cableado deben velar porque los niveles de temperatura y humedad relativa en estos sitios estén dentro de los límites requeridos por la infraestructura de cómputo allí instalada, para lo cual se deben usar sistemas de aire acondicionado según sea el caso.

l) Las dependencias que tienen bajo su custodia salas de cómputo, laboratorios y/o centros de cableado deben solicitar mantenimiento preventivo y pruebas de funcionalidad del sistema de UPS, plantas eléctricas, sistemas de detección de incendios y del sistema de aire acondicionado.

11.1.2 Protección sobre amenazas externas o ambientales

a) La Subdirección de Gestión de Sistemas de Información debe monitorear las variables de temperatura y humedad de las áreas de procesamiento de datos en el Data Center.

b) La Universidad debe designar y aplicar protección física para desastres como fuego, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humano.

c) Las oficinas y/o áreas que tienen en custodia salas de cómputo, laboratorios o centros de cableado deben velar por el ambiente adecuado para los activos informáticos como ventilación, iluminación, regulación de corriente, etc.

11.1.3 Trabajo en áreas seguras

La Universidad debe mantener áreas seguras para la gestión, almacenamiento y procesamiento de información en la Institución. Estas deben contar con:

- Protecciones físicas y ambientales, acordes con el valor y la necesidad de aseguramiento de los activos que se protegen.
- Definición de perímetros de seguridad.
- Controles de acceso físicos.
- Seguridad para protección de los equipos.
- Seguridad en el suministro eléctrico y cableado.
- Condiciones ambientales adecuadas de operación.
- Sistemas de contención, detección y extinción de incendios.

11.2 Equipos

11.2.1 Ubicación y protección de los equipos

a) Los estudiantes, funcionarios, profesores y contratistas no deben mover o reubicar los equipos de cómputo pertenecientes a la Universidad, instalar o desinstalar dispositivos, ni retirar marcas, logotipos ni hologramas de los mismos sin la autorización de la Subdirección de Gestión de Sistemas de Información.
b) Los funcionarios, profesores, estudiantes y contratistas deben conservar los equipos de cómputo en la ubicación autorizada por la Subdirección de Gestión de Sistemas de Información.

c) Los profesores, funcionarios, estudiantes y contratistas deben utilizar los equipos de cómputo asignados para uso exclusivo de las funciones del cargo que desempeñan en la entidad.

d) Los estudiantes deben utilizar los equipos de cómputo destinados como herramientas de apoyo (salas de cómputo y laboratorios) a las labores académicas o de investigación, sin vulnerar las políticas establecidas por la Institución y por las leyes vigentes del país.

e) Los profesores y funcionarios deben solicitar la capacitación necesaria para el correcto manejo de las herramientas informáticas que requieren para realizar sus labores, a fin de evitar riesgos por mal uso y para aprovechar al máximo los recursos proporcionados por la Institución.

f) Los profesores, funcionarios, estudiantes y contratistas no deben consumir alimentos o bebidas mientras utilizan los equipos de cómputo.

g) Los profesores, funcionarios y contratistas deben informar a la Subdirección de Gestión de Sistemas de Información cuando se requieran realizar cambios múltiples de los equipos de cómputo derivado de reubicación de lugares físicos de trabajo o cambios locativos, con cinco días de anticipación y un plan detallado.

h) Los profesores, funcionarios, estudiantes y contratistas no deben abrir o destapar los equipos de cómputo de la Universidad. Solo el personal de la Subdirección de Gestión de Sistemas de Información está autorizado para realizar esta labor.

11.2.2 Seguridad del cableado

La Subdirección de Gestión de Sistemas de Información:

a) Mantiene los cables de red de los centros de datos claramente marcados para identificar fácilmente los elementos conectados y evitar desconexiones erróneas.

b) Dispone, junto con la Subdirección de Servicios Generales, de los planos que describan las conexiones del cableado.

c) Mantiene el acceso a los centros de cableado solo para el personal autorizado.

11.2.3 Mantenimiento de equipos

a) La Subdirección de Gestión de Sistemas de Información es la dependencia responsable de llevar a cabo los servicios de mantenimiento y reparaciones al equipo informático, por medio de personal idóneo para la labor.

b) Los profesores, funcionarios, estudiantes y contratistas deben respaldar con copias de seguridad toda la información personal o confidencial que se encuentre en el equipo de cómputo asignado, previniendo así la pérdida involuntaria de la misma, derivada del proceso de reparación.

c) La Subdirección de Gestión de Sistemas de Información debe realizar procedimientos de borrado seguro en los equipos que se dan de baja y los equipos que son asignados a usuarios diferentes por temas de rotación.

11.2.4 Equipos de usuarios desatendidos

a) Los profesores, funcionarios y contratistas deben bloquear la sesión de sus equipos de cómputo cuando no se encuentren en su lugar de trabajo. Esto con el fin de que la sesión del usuario no quede activa con los privilegios a la mano (procedimiento de cierre por inactividad).

b) Los estudiantes deben cerrar sesión en los equipos de cómputo luego de terminar de usarlos para evitar el uso inadecuado de terceros.

11.2.5 Política de escritorio limpio y pantalla limpia

a) Los profesores, funcionarios y contratistas de la Universidad deben conservar el escritorio del equipo libre de información de uso interno o confidencial propia de la institución que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.

b) La Subdirección de Gestión de Sistemas de Información debe garantizar que los usuarios tengan la pantalla del equipo limpia o libre de archivos confidenciales por medio de mecanismos adecuados para este fin.

c) La Subdirección de Gestión de Sistemas de Información debe aplicar un fondo de pantalla institucional en todas las estaciones de trabajo y equipos portátiles de la Universidad, de forma que se active luego de diez minutos sin uso.

d) Los profesores, funcionarios y contratistas deben guardar en un lugar seguro cualquier documento, medio magnético u óptico removible que contenga información confidencial o de uso interno.

e) Los profesores, funcionarios y contratistas no deben dejar en el escritorio físico documentos de uso confidencial sin custodia.

f) La Subdirección de Gestión de Sistemas de Información debe establecer las medidas de control necesarias que permitan comprobar el correcto cumplimiento de los puntos anteriores.

12. SEGURIDAD DE LAS OPERACIONES

12.1 Procedimientos operacionales y responsabilidades

La Subdirección de Gestión de Sistemas de Información:

a) Realiza la documentación y actualización de los procedimientos relacionados con la operación y administración de los sistemas de información de la institución.

b) Proporciona a sus funcionarios manuales de configuración y operación de los servicios de red, bases de datos y sistemas de información que conforman las diferentes plataformas.

c) Provee los recursos necesarios para la implantación de controles que permitan la separación de ambientes de desarrollo, pruebas y producción, teniendo en cuenta consideraciones como:
   - Controles para el intercambio de información entre los ambientes de desarrollo y producción.
   - La inexistencia de compiladores, editores o fuentes en los ambientes de producción.
   - Acceso diferente para cada uno de los ambientes.

12.1.1 Gestión de cambios

a) La Subdirección de Gestión de Sistemas de Información establece los mecanismos para las solicitudes de cambios. De igual manera, coordina y controla los cambios realizados en los activos de información tecnológicos y los recursos informáticos.

b) La Subdirección de Gestión de Sistemas de Información debe garantizar que todo cambio realizado a un componente de la plataforma tecnológica, los cuales conlleven modificación de accesos, modificación o mantenimiento de *software*, actualización de versiones o modificación de parámetros, certifica y mantiene los niveles de seguridad existentes y no afecta la correcta operación de la misma ni de otros servicios.

c) Los responsables de los activos de información tecnológicos y recursos informáticos (directores de área, decanatura, dirección o dependencia) deben solicitar formalmente los requerimientos de nuevas funcionalidades, servicios o modificaciones sobre sus sistemas de información.

d) La Subdirección de Gestión de Sistemas de Información, como administradora de los activos de información tecnológicos y recursos informáticos, debe garantizar que las modificaciones o adiciones en las funcionalidades de los sistemas de información están soportadas por las solicitudes realizadas por los usuarios.

13. SEGURIDAD EN ENTORNOS DE DESARROLLO

La Subdirección de Gestión de Sistemas de Información debe establecer un procedimiento o protocolo para los procesos de desarrollo de *software* cuando este se realice de manera directa por la Universidad.

13.1 Externalización del desarrollo de *software*

De igual manera, cuando el proceso de desarrollo de *software* sea tercerizado, la Universidad Pedagógica Nacional, a través de la Subdirección de Gestión de Sistemas de Información, debe velar que la información sensible de la entidad se encuentre asegurada durante todo el proceso, así como la entrega de datos de prueba tenga la protección adecuada a través de los acuerdos de confidencialidad.

Pruebas de funcionalidad durante el desarrollo de los sistemas

Para garantizar que el producto de *software* que se está desarrollando, directamente por la Universidad o tercerizado, se encuentre acorde con los requerimientos funcionales y no funcionales del mismo, la Institución debe realizar a través de los desarrolladores de *software* de la Subdirección de Gestión de Sistemas de Información o a través de un interventor externo, pruebas de funcionalidad que garanticen que los procesos realizados en el nuevo sistema cumplan con los objetivos misionales de la Universidad y generen la información de acuerdo con los lineamientos establecidos.

Pruebas de aceptación

La Subdirección de Gestión de Sistemas de Información o a través de un interventor externo, debe establecer un plan de pruebas que garantice que el producto terminado esté listo para funcionar en el ambiente de producción, para lo cual debe realizar las siguientes pruebas:

- Prueba de Caja Negra
- Prueba de Caja Blanca
- Estrés
- Carga
- Conectividad
- Seguridad
- Integridad
- Disponibilidad
- Confidencialidad
- Consistencia

Una vez realizadas y aprobadas las pruebas se procede a realizar la implementación del *software* en el ambiente de producción. Sin este requisito la Subdirección de Sistemas de Información no dará por aceptado el producto y se establecen los mecanismos para subsanar las fallas encontradas o aplicar las cláusulas especificadas en el contrato de *software*.

En todo caso, la Universidad debe establecer y proteger adecuadamente los entornos para las labores de desarrollo e integración de sistemas que abarcan todo el ciclo de vida de desarrollo del *software*.

13.1.1 Separación de entorno de desarrollo, prueba y producción

La Subdirección de Gestión de Sistemas de Información:

a) Separa e instala los ambientes de desarrollo, pruebas y producción con el fin de reducir los riesgos de acceso no autorizado o cambios en el entorno operativo.
b) Asegura los recursos necesarios que permitan la separación de los ambientes de desarrollo, pruebas y producción.
c) Garantiza la independencia de los usuarios que usan los ambientes de desarrollo, pruebas y producción.
d) Todo desarrollo de *software* realizado directamente por la Universidad, tercerizado o Sistemas de Información instalados en la Institución, deben integrar el acceso de los usuarios con el Directorio Activo de la Universidad.
e) La creación de usuarios del Directorio Activo de la Universidad se estandarizará por medio de las cuentas de correo electrónico Institucional.

14. PROTECCIÓN CONTRA CÓDIGO MALICIOSO

14.1.1 Controles contra código malicioso

a) La Universidad Pedagógica Nacional proporciona los mecanismos necesarios que garanticen la protección de la información y los recursos de la plataforma tecnológica en donde se procesa y almacena, adoptando los controles necesarios para evitar la divulgación, modificación o daño permanente ocasionados por el contagio de *software* malicioso. Además, proporciona los mecanismos para generar cultura de seguridad entre sus funcionarios y personal provisto por terceras partes frente a los ataques de *software* malicioso.

b) Todos los sistemas informáticos deben ser protegidos teniendo en cuenta un enfoque multi-nivel que involucre controles humanos, físicos, técnicos y administrativos. La Subdirección de Gestión de Sistemas de Información, junto con el personal asignado para tal fin, elabora y mantiene un conjunto

de políticas, normas, estándares, procedimientos y guías que garanticen la mitigación de riesgos asociados a amenazas de *software* malicioso y técnicas de *hacking*.

c) Como control mínimo, los equipos de cómputo de La Universidad deben estar protegidos por el antivirus institucional. Este debe tener la capacidad de actualización automática en cuanto a firmas de virus. Los usuarios de la estación de trabajo (PC) no están autorizados para deshabilitar este control.

d) Los profesores, funcionarios, estudiantes y contratistas deben contar con el antivirus institucional actualizado en todos los equipos de cómputo que tienen para acceso y uso en sus actividades diarias.

e) Los profesores, funcionarios, estudiantes y contratistas deben verificar que la información y los medios de almacenamiento estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el *software* antivirus instalado por la Subdirección de Gestión de Sistemas de Información en los equipos de cómputo de la Universidad.

f) Los profesores, funcionarios, estudiantes y contratistas deben verificar, mediante el uso del *software* de antivirus que todo archivo, independiente de su procedencia, esté libre de virus antes de ser accedido.

g) Ningún profesor, funcionario, estudiante o contratista debe descargar *software* desde sistemas de correo electrónico, mensajería instantánea y redes de comunicaciones externas sin la debida autorización de la Subdirección de Gestión de Sistemas de Información.

h) Los profesores, funcionarios, estudiantes y contratistas que sospechen de alguna afectación por virus deben dejar de usar inmediatamente el equipo de cómputo y notificar a la Subdirección de Gestión de Sistemas de Información para la revisión y eliminación de los mismos.

i) Los funcionarios, profesores, estudiantes y contratistas por ningún motivo deben modificar o eliminar las configuraciones de seguridad básicas en el antivirus institucional, servicio de correo, *Office*, navegadores y programas de compresión de archivos que permiten detectar y prevenir virus.

j) La Universidad a través de la Subdirección de Gestión de Sistemas de Información puede hacer seguimiento al tráfico de la red cuando se tenga evidencias de actividad inusual o detrimentos en el desempeño.

k) La Subdirección de Gestión de Sistemas de Información debe mantener actualizada una base de datos con alertas de seguridad reportadas por organismos competentes y actuar de conformidad cuando una alerta pueda tener un impacto considerable en el desempeño de los sistemas informáticos.

14.2 Copias de respaldo

14.2.1 Copias de respaldo de la información

La Universidad Pedagógica Nacional asegura la generación de copias de respaldo y almacenamiento de su información crítica, proporcionando los recursos necesarios y estableciendo los procedimientos y mecanismos para la realización de estas actividades. Las áreas propietarias de la información, con el apoyo de la Subdirección de Gestión de Sistemas de Información, encargada de la generación de copias de respaldo, definen la estrategia a seguir y los periodos de retención para el respaldo y almacenamiento de la información.

Así mismo, la Universidad vela porque los medios magnéticos que contienen la información crítica sean almacenados en una ubicación diferente a las instalaciones donde se encuentra dispuesta.

a) La Subdirección de Gestión de Sistemas de Información debe realizar pruebas controladas para asegurar que las copias de seguridad pueden ser correctamente leídas y restauradas.

b) Los registros de copias de seguridad de los servidores institucionales deben ser guardados en un robot de cintas creado para tal fin.
c) Las copias de seguridad de la información guardadas en las cintas son custodiadas y almacenadas por un periodo de tres años, luego se realiza el proceso de borrado y reutilización de las mismas.

d) La copia de seguridad de información crítica debe ser mantenida de acuerdo con el lineamiento definido por la Subdirección de Gestión de Sistemas de Información.

14.2.2 Política para realizar copias de respaldo

La Subdirección de Gestión de Sistemas de Información:

a) Elabora un procedimiento de respaldo de toda la infraestructura tecnológica y de la información de los usuarios que permita realizar reinstalaciones en caso de sufrir un daño o percance.

b) Implementa las herramientas correctas para la realización de los *backups*. Se deben realizar los *backups* con las siguientes especificaciones: tipo de *backup*: incremental, semanal y mensual, y estos deben estar alojados en el robot de cintas en donde estarán almacenados durante el tiempo especificado por la Subdirección de Gestión de Sistemas de Información.

c) Se deben almacenar los *backups* en un lugar diferente de donde se encuentran principalmente con el objetivo de evitar la pérdida total de la información.

d) Garantiza la integridad de los *backups* almacenados, permitiendo así un óptimo proceso de restauración cuando se requiera.

e) La información que va a ser almacenada, respaldada y custodiada debe ser identificada y clasificada por cada uno de los dueños de los procesos, de acuerdo al nivel de clasificación definido.

f) Elabora y redacta un procedimiento que permita asegurar la integridad física de los *backups*, en caso de pérdida, robo y destrucción.

Roles y responsabilidades

La Subdirección de Gestión de Sistemas de Información debe elaborar el documento que contiene la información de los usuarios, roles y las responsabilidades asignadas dentro de la Universidad Pedagógica Nacional para el proceso, administración, elaboración y pruebas técnicas de los *backups* de los servidores de la Universidad, para esto define:

- Supervisor: funcionario encargado del monitoreo, administración, programación y puesta en marcha de los *backups* institucionales.
- Conductor: es el encargado de transportar las cintas que contienen los *backups* de la información de los servidores fuera de la Universidad.
- Probador: es el encargado de extraer las cintas del robot de cintas y realizar pruebas de funcionalidad y restauración de la información que contienen las cintas.

14.3 Control de software operacional

14.3.1 Instalación de *software* en sistemas operativos

La Universidad Pedagógica Nacional a través de la Subdirección de Gestión de Sistemas de Información:

- Asigna los responsables y establece los mecanismos que permitan controlar la instalación de los productos, herramientas y *software* en los equipos de cómputo pertenecientes a la Universidad.
- Se cerciora de que los proveedores cumplan con el soporte estipulado en los contratos de mantenimiento concerniente a la instalación y actualización de *software* a los sistemas de información que operan sobre la infraestructura de la Universidad.
- Designa las responsabilidades en los procedimientos que permitan controlar la instalación y actualización de software en los equipos de cómputo pertenecientes a la Universidad.

- Garantiza que todas las aplicaciones desarrolladas dentro de la Universidad y los desarrollos de proveedores o terceros ejecuten y garanticen pruebas de funcionalidad antes de salir a producción.
- Garantiza que los productos de *software* adquiridos e instalados en la infraestructura tecnológica de la Universidad cuentan con soporte necesario para garantizar su adecuado funcionamiento.
- Concede todos los accesos temporales que requieran los proveedores y terceros para realizar las respectivas actualizaciones de *software* que se requieran y monitorea estas actualizaciones.
- Analiza, valida y mitiga los riesgos que se pueden generar al momento de migrar las nuevas versiones del *software*.
- Redacta y documenta todas las restricciones para la implementación de nuevas versiones de *software* en los computadores de la Universidad.
- Redacta y documenta todas las limitaciones para la implementación de nuevas versiones de *software* en los computadores de la Universidad.

14.3.2 Adquisición, desarrollo y mantenimiento de sistemas *software*

a) La Universidad Pedagógica Nacional para apoyar y mantener los procesos estratégicos y operativos debe asegurar el uso de las tecnologías de la información. Los desarrollos de *software* tales como el sistema académico, financiero y administrativo pueden ser adquiridos y obtenidos por terceros o desarrollados por funcionarios o contratistas pertenecientes a la Subdirección de Gestión de Sistemas de Información.

b) Para el desarrollo de *software* interno de la Universidad se debe elaborar el documento de identificación y valoración de riesgos de proyectos de desarrollo de *software*. Los proyectos de desarrollo de *software* de la Universidad no pueden desarrollarse si tienen asociados riesgos altos y sin mitigar.

c) Los sistemas de información o desarrollos de sistemas adquiridos por terceros deben garantizar y certificar los estándares de calidad durante el proceso de desarrollo.

14.4 Gestión de vulnerabilidades

La Universidad, por intermedio de la Subdirección de Gestión de Sistemas de Información, elabora o actualiza los mecanismos que permitan realizar el análisis de vulnerabilidades técnicas que atentan contra la infraestructura tecnológica y de red de la Universidad. Estas pruebas de vulnerabilidad se ejecutan cada seis (6) meses con el propósito de modificar y mejorar los hallazgos detectados en el análisis, así mismo debe:

a) Desarrollar, elaborar, implementar, monitorear y ejecutar los planes de acción requeridos para garantizar la mitigación de las vulnerabilidades detectadas en la infraestructura tecnológica, cada seis (6) meses.

b) Identificar, evaluar y revisar en periodos no superiores a tres (3) meses las nuevas vulnerabilidades técnicas y deben reportarse al responsable de infraestructura tecnológica de la Universidad con el propósito de definir mecanismos de seguridad para la exposición de estos riesgos.

14.4.1 Restricciones sobre la instalación de *software*

El subdirector de Gestión de Sistemas de Información junto con el responsable de infraestructura tecnológica debe:

a. Delegar la instalación y actualización de *software* en los equipos de cómputo suministrados por la Universidad.

b. Autorizar la instalación en los equipos de cómputo pertenecientes a la Universidad y de herramientas de *software* libre, previa autorización de la Subdirección de Gestión de Sistemas de Información.

c. Elaborar y mantener documentada una lista con el *software* autorizado e instalado en los equipos de cómputo de la Universidad.

14.5 Consideraciones sobre auditorias de sistemas de información

14.5.1 Controles sobre auditorias de sistemas de información

a) A través de los procesos de auditorías internas la dependencia competente de la Universidad debe incluir la validación de los requisitos y normatividad vigente, así como las normas técnicas que se consideren adecuadas (como el compendio de Normas ISO 27000), que cumplan con los mecanismos para evaluar y medir el alcance del presente Manual.

b) Se acogerán los procedimientos y demás documentación interna para la realización de auditorías al Sistema de Gestión de Seguridad de la Información, de acuerdo al plan de auditorías y cronograma que se defina durante el año.

15. SEGURIDAD DE LAS COMUNICACIONES

15.1 Políticas de gestión de la seguridad en redes

La Universidad, por medio de la Subdirección de Gestión de Sistemas de Información, establece los procedimientos, mecanismos y guías necesarios para asegurar la disponibilidad de las redes de datos y los servicios de tecnología que soportan las mismas. Debe garantizar el desarrollo de mecanismos de seguridad que permitan proteger la integridad, confidencialidad y disponibilidad de la información que se comunica a través de estas redes de datos.

La Subdirección de Gestión de Sistemas de Información proporciona el aseguramiento, control del tráfico y la protección interna y confidencial de la información de la Universidad que se transmite por estas redes. Por ello la SSI:

a) Desarrolla medidas para garantizar la disponibilidad en todo momento de los servicios y recursos de red que presta la Universidad.

b) Elabora controles y medidas de protección que permitan minimizar las amenazas que pueden atentar contra la infraestructura de red de la Universidad.

c) Mantiene las redes de datos segmentadas por VLANS para su adecuado uso y administración.

d) Elabora y redacta los mecanismos necesarios de seguridad y niveles de servicio que garanticen el adecuado funcionamiento y soporte a las redes de datos.

e) Instaura los estándares y mecanismos técnicos de configuración de los dispositivos de red pertenecientes a la Universidad, teniendo en cuenta los estándares y protocolos de configuración segura.

f) Los dispositivos de seguridad como los IPS, *firewall* y balanceadores deben contar con los mecanismos, estándares y protocolos de configuración segura.

g) Redacta y elabora una guía de todos los servicios de red, protocolos y puertos accesibles en la infraestructura de red de datos de la Universidad. Configura en el *firewall* perimetral e inhabilita todos los servicios de red que estén habilitados por defecto y no se requieran para el buen funcionamiento y seguridad de las redes de datos.

h) Instala protección de autenticación de usuarios en las redes *wi-fi* de la Universidad.

i) Garantiza el adecuado funcionamiento del enrutamiento y encaminamiento de las redes de datos.

j) Configura los *switches*, *firewall* y demás dispositivos de seguridad que estén instalados en la red de la Universidad, así como documentarlos y respaldarlos a través de copias de seguridad.

k) Revisa, registra, configura y aprueba todo equipo de infraestructura de TI antes de que se ponga en funcionamiento en la red de la Universidad. Se deben desconectar de la red todos los dispositivos que no pertenezcan a la infraestructura tecnológica de la Universidad y deben reportarse como un incidente de seguridad para su respectiva verificación e investigación.

15.2 Política de uso correo electrónico

La Universidad Pedagógica Nacional para garantizar el uso adecuado de intercambio de información entre los funcionarios, contratistas y terceros mantiene habilitado el servicio de correo institucional en la nube, garantizando un servicio ágil, seguro y fácil de interactuar en las actividades diarias que realizan dentro de la Universidad, garantizando y permitiendo la confidencialidad, integridad, autenticidad y disponibilidad al momento de redactar comunicaciones por este medio o servicio.

La Subdirección de Gestión de Sistemas de Información:

a) Elabora y comunica el procedimiento para la administración de cuentas de correo electrónico y toda la normativa concerniente para el adecuado uso del servicio de correo electrónico.

b) La plataforma de correo electrónico debe contar con los controles y herramientas necesarios que logren proteger y detectar la integridad de las comunicaciones redactadas y que se envían a través de la plataforma de correo.

c) El servicio de correo debe garantizar y mantener que todos los mensajes de correo estén protegidos contra *spam*, *malware* y virus adjuntos y que estos sean trasmitidos por este medio.

d) Realiza campañas de concientización a todos los funcionarios, profesores, estudiantes y contratistas sobre el buen uso del servicio de correo electrónico.

e) La Subdirección de Gestión de Sistemas de Información asigna a un funcionario la tarea de administración de la consola del servicio de correo electrónico.

f) Los funcionarios, profesores, estudiantes y contratistas pueden utilizar el servicio de correo institucional para el envío y recepción de comunicaciones que tengan que ver solo con las labores y actividades que realizan dentro de la Universidad.

g) Los funcionarios y profesores deben reportar a la Subdirección de Gestión de Sistemas de Información las anomalías que se presenten en el servicio de correo electrónico tales como *spam*, cuentas de correo que no conozcan el remitente, adjuntos de remitentes desconocidos, mensajes de bancos con dudosa reputación. Por ningún motivo deben abrir correos con adjuntos que no sean conocidos que permitan la propagación de *malware*, *spam* y que atenten contra la infraestructura y la red que tienen la Universidad.

h) Los profesores, funcionarios y estudiantes no deben adjuntar ni enviar archivos, programas ejecutables de dudosa reputación y de contenido malicioso que afecten o atenten contra el servicio de correo e infraestructura de red de la Universidad.

i) El servicio de correo electrónico cuenta con un formato estándar para la firma del remitente y la imagen del logo corporativo de la Universidad. Por ningún motivo los profesores y funcionarios deben modificar este formato e imagen corporativa.

15.3 Política de uso adecuado de Internet

La Universidad Pedagógica Nacional para el desempeño de sus actividades y labores académicas y administrativas debe contar siempre con el servicio de internet para el desarrollo de estas actividades y labores. Debe proporcionar siempre los recursos y herramientas para garantizar y asegurar el funcionamiento y disponibilidad de este servicio dentro de la Universidad, para ello:

a) Garantiza y adecua los recursos necesarios para la administración, implementación y mantenimiento requeridos para la adecuación, prestación segura y oportuna del servicio de internet, de acuerdo a los perfiles de acceso establecidos.
b) Elabora, implementa y desarrolla los procedimientos que permitan mantener y establecer la continuidad o el restablecimiento del servicio de internet en caso de daño o contingencia.
c) Administra y monitorea siempre el canal o canales del servicio de internet, referente a tráfico, balanceo o carga.
d) Elabora procedimientos y desarrolla controles y permisos para evitar la descarga de *software* malicioso, dañino o no autorizado proveniente de internet y garantizando que los funcionarios, estudiantes y contratistas no tengan acceso a sitios restringidos como pornografía y páginas con *malware*, *spam* y *ransomware*.
e) Elabora bitácoras en cuanto a la navegación y los accesos de los usuarios a internet, generando reportes de navegación por usuarios.
f) Realiza campañas para concientizar a los profesores, funcionarios, estudiantes y contratistas en cuanto al uso adecuado y las precauciones necesarias que se deben tener cuando se haga uso de los servicios de internet**.**
g) Los funcionarios, profesores, estudiantes y contratistas por ningún motivo deben utilizar, instalar y manipular *software* y herramientas que pueden tener código malicioso que vayan en contra y afecten la disponibilidad del servicio de red que tiene la Universidad.
h) La información descargada de internet (videos, imágenes) y utilizada por parte de los funcionarios y administrativos no debe atentar contra la propiedad intelectual de sus dueños.
i) Los funcionarios, profesores, estudiantes y contratistas por ningún motivo deben utilizar el servicio de internet para realizar indebidamente intercambio de información confidencial perteneciente a la Universidad.

15.4 Transferencia de información

La Universidad Pedagógica Nacional asegurará el proceso de protección de la información que garantice la transferencia e intercambio de la misma con otras entidades a nivel local o por convenios en el extranjero. Para ello establece todos los procedimientos y mecanismos de control que sean necesarios para el intercambio de dicha información y se constituirán acuerdos de confidencialidad y de intercambio de la información con los terceros a los cuales se realizarán los intercambios. La entidad garantizará las tecnologías de información y telecomunicaciones necesarias para poder realizar el intercambio de información. Se debe establecer un mecanismo o procedimientos para los casos en cuales se realice intercambio o transferencia de información en medios de almacenamiento de forma física.

15.4.1 Políticas y procedimientos de transferencia de información

a) La Universidad debe elaborar lineamientos para el desarrollo de acuerdos concernientes a la confidencialidad, transferencia e intercambio de información entre la Universidad y funcionarios, profesores, contratistas y terceros incorporando las directrices y compromisos que se van a adquirir y las penalidades a que haya lugar por el incumplimiento de estos acuerdos.

b) Los contratos suscritos por la Universidad deben contar con una cláusula de confidencialidad de la información. El Grupo de Contratación con el apoyo de la Oficina de Jurídica establece la redacción de la cláusula.

c) Los funcionarios, profesores, contratistas y terceros deben emplear los procedimientos y herramientas definidas por parte de la Universidad para la recepción y envío de la información confidencial de la Institución.

15.5 Política de uso del Data Center

a) El acceso al *Data Center* debe ser autorizado con anterioridad. Los usuarios, proveedores o terceros deberán siempre tener acompañamiento por un funcionario de la Subdirección de Gestión de Sistemas de Información que tenga acceso al *Data Center* a través del sistema biométrico y tarjeta.
b) Los funcionarios, contratistas proveedores y terceros solo tienen acceso al *Data Center* en las áreas específicas donde tienen instalado sus equipos, servicios o infraestructura a la cual prestan soporte y será controlado por medio de tarjetas de control de acceso. Para el caso de proveedores y terceros contarán siempre con el acompañamiento de un funcionario de la Subdirección de Gestión de Sistemas de información.
c) Las tarjetas de control de acceso son asignadas por la Subdirección de Gestión de Sistemas de Información a los funcionarios y contratistas encargados del *Data Center*. Por ningún motivo se deben prestar estos dispositivos de control entre funcionarios. En caso de pérdida o robo se debe reportar a

la Subdirección de Servicios Generales y a la Subdirección de Gestión de Sistemas de Información para que realice el procedimiento de investigación que sea necesario para la recuperación de la tarjeta o reposición de la misma bajo los protocolos o mecanismos de seguridad que sean necesarios.

d) Los materiales catalogados como peligrosos e inflamables, como cajas, cartón, papel o cualquier otro material similar, no deben estar almacenados dentro de ningún espacio que se encuentre disponible en el *Data Center*.
e) Los funcionarios o contratistas asignados por la Subdirección de Gestión de Sistemas de Información deben mantener limpio y ordenado en todo momento el *Data Center*.
f) No se autoriza ni permite ingerir alimentos, consumir bebidas, tabaco, etc., dentro del *Data Center*.
g) No se autoriza ni permite el acceso de cámaras fotográficas, cámaras de video y el uso de las mismas dentro del *Data Center*.
h) El sistema de monitoreo del *Data Center*, cuarto de comunicaciones, cuarto eléctrico, sistemas de humedad, ventilación y de refrigeración será responsabilidad del funcionario responsable de la infraestructura tecnológica asignado por la Subdirección de Gestión de Sistemas de Información.
i) Los funcionarios, contratistas y proveedores no pueden ingresar ni manipular ninguno de los siguientes elementos en el *Data Center*:

- Cigarrillos o derivados del tabaco
- Elementos inflamables o explosivos
- Pistolas de protección personal
- Elementos químicos
- Sustancias ilegales
- Aparatos electromagnéticos
- Elementos radioactivos

15.6 Política de seguridad para la relación con los proveedores

a) El Grupo de Contratación debe establecer las directrices y lineamientos para el cumplimiento de las obligaciones contractuales que garanticen los procesos de seguridad de la información en la relación terceros o proveedores.
b) El Grupo de Contratación o quien haga sus veces debe establecer los requisitos y mecanismos regulatorios concernientes a la protección de los datos personales, derechos de autor y de propiedad intelectual en los contratos que se suscriban y ejecuten en la Universidad.
c) El Grupo de Contratación o quien haga sus veces debe establecer los riesgos concernientes a seguridad de la información y los compromisos establecidos referentes a la confidencialidad e integridad de la información y establecer un mecanismo para el cumplimiento de las políticas de seguridad establecidas en el presente Manual al momento de suscribir contratos.

d) La Subdirección de Gestión de Sistemas de Información debe garantizar y establecer los permisos y controles que sean necesarios cuando un contratista o proveedor requiera tener acceso a la infraestructura tecnológica de la Universidad y Sistemas de Información.
e) La Subdirección de Gestión de Sistemas de Información elabora una guía que permita el aseguramiento de gestión de cambios a nivel de la infraestructura tecnológica de la Universidad, Sistemas de Información, servicios tecnológicos y aplicativos que cuentan con el soporte de proveedores y contratistas para poder garantizar la seguridad, calidad y eficiencia y permita determinar los responsables y actividades a seguir para cumplir a cabalidad con la gestión de los cambios.
f) Cada área, oficina o dependencia de la Universidad que tenga o establezca relación con los proveedores debe solicitar acompañamiento a la Subdirección de Gestión de Sistemas de Información para dar a conocer las políticas de seguridad con las que cuenta la Universidad.

15.7 Política de seguridad para el trabajo virtual, itinerante y remoto

a) Para todo lo concerniente a la modalidad de trabajo virtual, itinerante y remoto la Subdirección de Gestión de Sistemas de Información debe definir los mecanismos de seguridad correspondientes.

b) La Subdirección de Gestión de Sistemas de Información define el mecanismo de acceso para ingresar a la red de la Universidad para trabajo virtual, itinerante y remoto.

c) La Subdirección de Gestión de Sistemas de Información define y habilita los usuarios con acceso a la red interna teniendo en cuenta los usuarios definidos en el directorio activo, manteniendo las mismas características de seguridad definidas en este rol.

d) La Subdirección de Gestión de Sistemas de Información debe proporcionar a los equipos de cómputo de la Universidad las herramientas ofimáticas, antivirus y dispositivos de seguridad para el trabajo virtual, itinerante y remoto.

e) La Subdirección de Gestión de Sistemas de Información define las estrategias de seguridad de la información para los equipos de cómputo no pertenecientes a la Universidad que sean utilizados para el desarrollo de las funciones asignadas al trabajo virtual, itinerante y remoto autorizadas por la Universidad.

f) Para todo lo concerniente al trabajo virtual, itinerante y remoto la Subdirección de Gestión de Sistemas de Información debe establecer mecanismos de monitoreo y soporte técnico sobre las conexiones y los servicios tecnológicos a los que el funcionario, profesor y contratista tiene acceso.

g) El acceso a la red interna se debe realizar por medio de un usuario y contraseña definido por el directorio activo, previa configuración en el dispositivo por parte de la Subdirección de Gestión de Sistemas de Información.

h) La Subdirección de Gestión de Sistemas de Información garantiza que los funcionarios y profesores tengan un acompañamiento en el proceso de *backups* a los equipos que fueron designados para la modalidad de trabajo virtual, itinerante y remoto. La Subdirección de Gestión de Sistemas de Información no se hace responsable de la información personal que se encuentre en los equipos y por ende no realizará el acompañamiento para la obtención de *backups* de este tipo de información.

i) Todos los funcionarios, profesores y contratistas deben cumplir con las directrices impartidas en temas de seguridad de la información del presente Manual al momento de realizar el trabajo virtual, itinerante y remoto. La Subdirección de Gestión de Sistemas de Información acompañará en el proceso de concientización en los temas de seguridad de la información.

j) Los funcionarios, profesores y contratistas no están autorizados para instalar *software* sin licenciamiento o demás componentes en los equipos pertenecientes a la Universidad destinados para el trabajo virtual, itinerante y remoto. Para el tema de herramientas *open source* o *software* libre deben solicitar la autorización de la instalación a la Subdirección de Gestión de Sistemas de Información, para que esta escale y cree el caso a la mesa de ayuda para luego realizar el procedimiento de instalación.

16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

16.1 Gestión de incidentes y mejoras en la seguridad de la información

La Subdirección de Gestión de Sistemas de Información debe desarrollar y elaborar un reporte concerniente a incidentes de seguridad de la información y presentarlo al Comité de Gobierno Digital de la Universidad o al Comité Directivo cuando las circunstancias lo ameriten.

El responsable de seguridad de la información será el encargado de administrar, investigar, solucionar y dar respuesta a los incidentes reportados concernientes al tema de seguridad de la información, teniendo en cuenta actividades necesarias que se deben realizar para evitar la reincidencia y poder escalar los incidentes en caso de ser necesario, de acuerdo a su criticidad.

La Subdirección de Gestión de Sistemas de Información realizará el proceso de reporte de incidentes de seguridad ante los entes judiciales y de control e informará al Comité de Gobierno Digital sobre estas actuaciones.

16.1.1 Responsabilidades y procedimientos

a) Los subdirectores, jefes de oficina o coordinadores y demás directivos, dueños de los activos de información deben realizar los reportes concernientes a seguridad de la información a la Subdirección de Gestión de Sistemas de Información en caso de materialización o daño en los activos.

b) La Subdirección de Gestión de Sistemas de Información establece los mecanismos y procedimientos para garantizar una respuesta inmediata, efectiva y ordenada ante los incidentes de seguridad presentados en la Universidad.

c) La Subdirección de Gestión de Sistemas de Información evalúa y determina los incidentes de seguridad de la información de acuerdo a las circunstancias en que se presenten.

d) La Subdirección de Gestión de Sistemas de Información le asigna al responsable de seguridad de la información las tareas concernientes a investigación de incidentes de seguridad reportados dentro de Universidad, identificando las causas y elaborando las soluciones, previniendo su ocurrencia mediante un mecanismo de seguridad efectivo.

e) La Subdirección de Gestión de Sistemas de Información tendrá como mecanismo de seguridad bases de datos concernientes a los incidentes de seguridad presentados con las respectivas soluciones en pro de garantizar el mejoramiento en los tiempos de respuestas a incidentes futuros.

f) Los funcionarios, profesores, estudiantes y contratistas deben informar a la Subdirección de Gestión de Sistemas de Información cualquier evento o incidente concerniente a la seguridad de la información en un tiempo breve.

g) Los profesores, funcionarios, estudiantes y contratistas deben reportar a la Subdirección de Gestión de Sistemas de Información la divulgación y pérdida de información no autorizada que está clasificada como interna o confidencial para realizar el trámite correspondiente a la misma.

17. CUMPLIMIENTO

17.1 Cumplimiento de requisitos legales y contractuales

La Universidad Pedagógica Nacional vigila todo lo concerniente a la documentación y cumplimiento de las normas legales aplicables relacionadas con la seguridad de la información, entre todas lo concerniente a propiedad intelectual y derechos de autor. Por ende, debe estar atenta a que todo el *software* que se instale en la Universidad cumpla con todas las normas, leyes y licenciamientos aplicables.

17.1.1 Identificación de la legislación aplicable y de los requisitos contractuales

a) La Subdirección de Gestión de Sistemas de Información debe actualizar y documentar toda la reglamentación y normatividad contractual concerniente y relacionada a la Seguridad de la Información.

b) La Subdirección de Gestión de Sistemas de Información debe asegurar que el software que se instale, desarrolle y ejecute en la Universidad cumpla con la ley de derechos de autor y se necesite licencia de uso.

c) Los funcionarios, profesores, estudiantes y contratistas no deben realizar procedimientos de eliminación e instalación de *software* en los equipos de cómputo que se entregaron exclusivamente para el desempeño de sus labores académicas o administrativas sin el consentimiento y la previa autorización de la Subdirección de Gestión de Sistemas de Información.

d) Los profesores, funcionarios, estudiantes y contratistas garantizarán el cumplimiento de las leyes concernientes a derechos de autor y los consensos para los licenciamientos de *software*. Duplicar e instalar *software* no licenciando y reproducción no autorizada en la Universidad es ilegal y acarreará las sanciones pertinentes ante estas faltas.

17.1.1.1 Privacidad y protección de datos personales

a) Dando cumplimento a Ley 1581 de 2012, en la cual se especifican las disposiciones para el proceso de tratamiento de los datos personales, y la resolución 0767 de 2018, por la cual se adopta el Manual de política interna y de procedimientos de datos personales de la Universidad Pedagógica Nacional, la Universidad garantiza los procesos concernientes a la protección de los datos personales de los estudiantes, profesores, egresados y terceros donde realice proceso de administración de dichos datos concernientes a esta ley.

b) Se establecen las definiciones, naturalezas y finalidades en las cuales la Universidad Pedagógica Nacional, como responsable de los datos personales recolectados de sus distintas fuentes de información y atención, maneja la información de todos los funcionarios, personas o terceros que tenga relación con las actividades, procesos o procedimientos en donde proporcionaron datos personales. En caso de contratar un tercero para el tratamiento de los datos personales, la Universidad requerirá al tercero implantar los procedimientos y directrices necesarios para la protección de los datos personales que se contempla en el *Manual de tratamiento de datos de la Universidad Pedagógica Nacional*.

c) La Universidad propende proteger la información sensible de todos los funcionarios validando los controles necesarios para resguardar la información que la Universidad preserva en sus bases de datos, garantizado que la información almacenada de ellos se utiliza únicamente para funciones inherentes de la Universidad y no sea manipulada, publicada o entregada a funcionarios o terceros sin la debida autorización.

d) Los jefes o directivos de las dependencias responsables de realizar el proceso de tratamiento de datos personales deben dar la autorización a los funcionarios, profesores, estudiantes y contratistas para obtener, resguardar, usar, eliminar, transferir y compartir los datos personales en las actividades desarrolladas en la Universidad.

e) Las dependencias que realizan el proceso de tratamiento de datos personales a los funcionarios, profesores, estudiantes o contratistas deben garantizar que únicamente los funcionarios o personas que tengan algún vínculo con la Universidad son las únicas autorizadas para tener acceso a esta información.

f) Las dependencias que realizan el proceso de tratamiento de datos personales a los funcionarios, profesores, estudiantes o contratistas deben aceptar las directrices o políticas establecidas para el envío de mensajes por correo electrónico a estos usuarios.

g) La Subdirección de Gestión de Sistemas de Información establece, implanta e instaura los controles concernientes al proceso de tratamiento de los datos personales que tienen que ver con los estudiantes, profesores, terceros y funcionarios durante el proceso de obtención y administración de la información almacenada en las bases de datos o repositorios institucionales con el fin de evitar su publicación, divulgación, actualización y eliminación sin la respectiva autorización.

h) Los funcionarios y profesores no deben divulgar la información que se encuentra almacenada en los repositorios y bases de datos de la Universidad, garantizando la absoluta reserva con respecto a esta información cuando tengan conocimiento en el ejercicio de sus funciones.

CONTROL DE CAMBIOS

FECHA	VERSIÓN	DESCRIPCIÓN DEL CAMBIO
15-10-2020	01	Creación del Documento

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Equipo de Trabajo Subdirección de Sistemas Informaticos	**Henry Augusto Córdoba Sánchez Subdirector Sistemas Informaticos**	**Leonardo Fabio Martínez Pérez Rector**