



RESOLUCIÓN NÚMERO 2097 DE
(26 JUL. 2013)

Por la cual se establece la Política de Seguridad de la Información de la Universidad Militar Nueva Granada

EL RECTOR DE LA UNIVERSIDAD MILITAR NUEVA GRANADA

En ejercicio de sus atribuciones legales y en especial de las que le confieren la Constitución Política artículo 69, las Leyes 30 de 1992 artículos 28 y 57, 805 de 2003 artículo 2, los Acuerdos 13 de 2010 numeral 6 y 23 de 2012 y

CONSIDERANDO:

Que el artículo 69 de la Constitución Política, preceptúa que se garantiza la autonomía universitaria, al determinar que las universidades podrán darse sus directivas y regirse por sus propios estatutos, de acuerdo con la ley. La Ley establecerá un régimen orgánico especial para las Universidades del Estado.

Que la Ley 30 de 1992 en el artículo 28, consagra la autonomía universitaria al reconocer a las universidades el derecho de darse y modificar sus estatutos, designar sus autoridades académicas y administrativas.

Que la Ley 527 de 1999, establece el acceso y uso de mensajes de datos, comercio electrónico, firmas digitales y entidades certificadoras.

Que la Ley 603 del 2000, establece los Derechos de Autor y antipiratería.

Que el Decreto 679 de 2001, establece el delito de Abuso sexual de menores, a través de medios electrónicos.

Que la Ley 805 de 2003, por la cual se transforma la naturaleza jurídica de la Universidad Militar Nueva Granada, en su artículo 1 estableció que "... es un ente universitario autónomo del orden nacional ..." y que según el artículo 2 de esta misma Ley "... es una persona jurídica con autonomía académica, administrativa y financiera, patrimonio independiente, con capacidad para gobernarse, designar sus propias autoridades ..."

Que la Ley 1273 de 2009, adiciona al Código Penal el Título VII BIS denominado "De la Protección de la información y de los datos".

Que la Ley 1581 de octubre de 2012, dicta las Disposiciones Generales para la Protección de Datos Personales

Que la Universidad Militar Nueva Granada debe adelantar las normas para el uso de los medios electrónicos de conformidad con la legislación vigente sobre la materia.

Que se hace necesario establecer las Políticas de Seguridad de la Información con el propósito de asegurar el correcto uso de los recursos informáticos de la universidad y dar cumplimiento a los requerimientos exigidos por el Ministerio de las Tecnologías de la Información y las Telecomunicaciones en relación a la Estrategia de Gobierno en Línea.

En mérito de lo expuesto, el Rector de la Universidad Militar Nueva Granada,

RESUELVE:

24

ARTÍCULO PRIMERO: Establecer la Política de Seguridad de la Información de la Universidad Militar Nueva Granada.

ARTÍCULO SEGUNDO: Los servicios informáticos que ofrece la Universidad Militar Nueva Granada son:

1. Correo electrónico Institucional
2. Acceso a Internet
3. Acceso a directorio activo
4. Base de datos
5. Acceso a aplicaciones y sistemas de información
6. Acceso a impresión
7. Servicio de red cableada e inalámbrica
8. Servicios de red como telefonía, video conferencia, navegación y nuevos servicios que requieran de la red cableada o Inalámbrica para su operación

ARTÍCULO TERCERO: Las contraseñas de los servicios informáticos que ofrece la Universidad Militar Nueva Granada deben tener las siguientes características:

1. La longitud mínima de la contraseña es de ocho caracteres alfanuméricos.
2. Las contraseñas deben estar conformadas por letras, números o caracteres especiales.
3. La clave del directorio activo tiene una vigencia máxima de 90 días.
4. La contraseña es personal, reservada e intransferible.

ARTÍCULO CUATRO: El usuario de los servicios informáticos es el único responsable por el cuidado y buen uso de los recursos asignados, los cuales deben ser utilizados única y exclusivamente para trabajos relacionados con las actividades laborales e institucionales.

PARÁGRAFO: Las cuentas de los servicios informáticos son de uso exclusivo e intransferible por cada usuario de la Universidad Militar Nueva Granada. El uso indebido constituye falta disciplinaria grave.

ARTÍCULO QUINTO: La información institucional consta de datos sobre los procesos misionales y de gestión de la Universidad Militar Nueva Granada, la cual es almacenada en los servidores institucionales. La custodia y confidencialidad de esta información es responsabilidad de los administradores de servicios electrónicos.

ARTÍCULO SEXTO: La custodia de la información almacenada en las estaciones de trabajo o equipos portátiles de la Universidad Militar Nueva Granada, es responsabilidad del usuario titular del equipo.

ARTÍCULO SÉPTIMO: En las estaciones de trabajo o equipos portátiles de la Universidad Militar Nueva Granada, sólo se permite instalar software licenciado o libre debidamente autorizado por la División de Informática, y para uso concerniente a actividades laborales.

ARTÍCULO OCTAVO: Los usuarios o funcionarios de la Universidad Militar Nueva Granada deberán reportar en forma inmediata a la División de Informática, cuando detecten algún riesgo real o potencial sobre equipos de cómputo, la información o equipos de comunicaciones, tales como caídas de agua, choques eléctricos, caídas o golpes o peligro de incendio, al correo informatica@unimilitar.edu.co.

ARTÍCULO NOVENO. Está prohibido a usuarios y funcionarios.

1. El acceso a páginas con restricciones por normas nacionales, internacionales o internas, juegos en línea, contenido terrorista, contenido sexual restringido o prohibido.
2. El uso de sitios de almacenamiento virtual que no estén autorizados por la Universidad Militar Nueva Granada.
3. Violaciones a derechos de cualquier persona o institución, derechos de autor, patentes o cualquier forma de propiedad intelectual.

4. Copia no autorizada de material protegido por derechos de autor que incluye: digitalización y distribución de imágenes o fotografías de cualquier origen, digitalización y distribución de música, audio o video, distribución o instalación de software sin licencia ni autorización de la Universidad.
5. Utilizar la infraestructura de tecnología de información y redes de la Universidad Militar Nueva Granada para conseguir o transmitir material con ánimo de lucro. De igual forma, está prohibido su utilización para hacer algún tipo de acoso, difamación, calumnia o cualquier forma de actividad hostil en contra de miembros de la comunidad universitaria y en general, de cualquier persona o institución.
6. Proporcionar información confidencial a personas o entidades, sin la debida autorización o violando las políticas sobre manejo de información confidencial.
7. Cualquier actuación que vaya en contra de las leyes vigentes en Colombia.

ARTÍCULO DÉCIMO: El uso adecuado de la tecnología para el procesamiento de la información en la Universidad Militar Nueva Granada aplica para estudiantes, contratistas, cuerpo académico, funcionarios de la Universidad y personal de apoyo no vinculado directamente con la Universidad pero que presten servicios a la misma y utilicen tecnología de información. La política aplica a los equipos propios de la Universidad o en arriendo y a los equipos de personas externas que sean conectados a las redes de la Universidad Militar Nueva Granada.

ARTÍCULO DÉCIMO PRIMERO: La Universidad Militar Nueva Granada no se hace responsable, directa ni subsidiariamente, por opiniones expresadas en los correos enviados por los miembros de la comunidad universitaria, por los usuarios o suscriptores que no tengan esta condición, ni por las expresiones manifestadas por ellos o por cualesquier persona en los espacios de debate público en cuentas de correo electrónico.

ARTÍCULO DÉCIMO SEGUNDO: Los datos que los usuarios crean o intervengan en los sistemas de la Universidad durante el desarrollo normal de sus actividades al servicio de la Institución, son de propiedad de la Universidad Militar Nueva Granada.

ARTÍCULO DÉCIMO TERCERO: Los funcionarios que tengan a cargo información en medios electrónicos y físicos propios de la Universidad, deben garantizar que se encuentran resguardados en lugares seguros, con llave y en las instalaciones de la Universidad.

ARTÍCULO DÉCIMO CUARTO: Todos los escritorios o mesas de trabajo deben permanecer limpios para proteger documentos en papel y dispositivos de almacenamiento como CD, Memorias USB y otros dispositivos de almacenamiento, con fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información. Los dispositivos de almacenamiento deben ser guardados bajo llave, especialmente aquellos en los cuales se hayan hecho copias de respaldo de archivos electrónicos.

ARTÍCULO DÉCIMO QUINTO: Escritorio Limpio después de la jornada laboral

1. Antes de abandonar la oficina, los funcionarios deben recoger y asegurar el material sensible (CD, DVD, Hojas impresas con información de la Universidad).
2. Antes de abandonar la oficina, los funcionarios deben asegurar, el equipo costoso y el almacenamiento de la información sensible (Portátiles, PDA, Memorias USB, entre otros).

ARTÍCULO DÉCIMO SEXTO: Bloqueo de las estaciones de Trabajo

1. El usuario debe mantener control sobre la estación de trabajo a cargo, para evitar riesgos de acceso a los sistemas de información, aun cuando el usuario no se encuentre frente a ella, por lo cual se requiere que esté bloqueada cuando el usuario se retire de su lugar, pues no hacerlo potencia el riesgo de utilizar los sistemas sin los privilegios adecuados, expone la información de la Institución de manera innecesaria y se considera un uso inadecuado de los recursos y de los sistemas de seguridad.
2. La Universidad, a través de la División de Informática, programará un bloqueo automático de sesión en los equipos de cómputo asignados a los funcionarios para control de acceso no autorizado. Pero el funcionario que se aleje de su puesto de trabajo, deberá bloquear su equipo, de manera manual.

ARTÍCULO DÉCIMO SÉPTIMO: No debe dejarse documentos que contengan información confidencial sobre el escritorio, el computador o en cualquier parte visible del puesto de trabajo, que pueda poner en riesgo el manejo de la información de la Universidad.

ARTÍCULO DÉCIMO OCTAVO: La confidencialidad de la información almacenada en un equipo asignado a un funcionario, es su responsabilidad.

ARTÍCULO DÉCIMO NOVENO: Los miembros de la comunidad universitaria deben utilizar los dispositivos tecnológicos de la Universidad, única y exclusivamente para desarrollar sus actividades laborales y académicas. Cualquier uso personal de los recursos de tecnología de información, están prohibidos y serán asumidos bajo su responsabilidad y riesgo.

ARTÍCULO VIGÉSIMO: Para adelantar mantenimiento de la red y seguridad, la División de Informática, podrá monitorear equipos, sistemas y tráfico de red en cualquier momento.

ARTÍCULO VIGÉSIMO PRIMERO: Cualquier miembro de la comunidad universitaria que sea encontrado, contraviniendo la política aquí definida, será investigado y podrá ser objeto de sanciones administrativas, sin perjuicio de las acciones disciplinarias, penales o fiscales que se deban adelantar los organismos competentes.

ARTÍCULO VIGÉSIMO SEGUNDO: La presente Resolución rige a partir de la fecha de su expedición.

COMUNÍQUESE Y CÚMPLASE

Dada en Bogotá, a los 26 JUL. 2013

Mayor General EDUARDO ANTONIO HERRERA BERBEL
Rector

Vo. Bo. Ing. Carlos Gilberto Delgado Beltrán, Jefe de la División de Informática
Vo. Bo. Dra. Elsa Liliana Aguirre L. Jefe de la Oficina Asesora Jurídica
Vo. Bo. Dra. Martha Bahamón Jara, Vicerrectora Académica
Vo. Bo. BG. Hugo Rodríguez, Vicerrector Administrativo
Vo. Bo. BG. Alberto Bravo Silva, Vicerrector General