UNIVERSIDAD MILITAR
NUEVA GRANADA
RECTORÍA

UMNG-RECTOR-DIVINF

CIRCULAR PERMANENTE - 018 **BOGOTÁ,** 30 OCT. 2014

ASUNTO: NORMAS DE OBLIGATORIO CUMPLIMIENTO PARA EL USO DE EQUIPOS DE COMPUTO PERSONALES, RESPECTO AL MANEJO DE LA INFORMACIÓN.

PARA: PERSONAL ADMINISTRATIVO, DOCENTE Y CONTRATISTAS

VIGENCIA: A PARTIR DE LA FECHA DE SU PUBLICACIÓN

1. GENERALIDADES

Atendiendo la Resolución 2097 de 2013, que establece la Política de Seguridad de la Información de la Universidad Militar Nueva Granada, señala en su artículo 6, que: "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". Es así, que se hace necesario reglamentar el uso de los equipos de cómputo y equipos móviles que no son administrados por la Universidad Militar Nueva Granada.

2. OBJETIVO GENERAL

Prevenir, controlar y evitar la fuga y/o pérdida de información de valor institucional que tiene registrada la Universidad Militar Nueva Granada, por circunstancias atribuibles a uso no autorizado de equipos de cómputo o equipos móviles personales o no administrados por la Universidad Militar Nueva Granada.

2.1. FINALIDAD

Normatizar el uso de equipos de cómputo personales y equipos móviles, cuya seguridad, control, administración o/y operación no es responsabilidad directa de la Universidad Militar Nueva Granada, así como establecer las responsabilidades de su uso.

3. INFORMACIÓN GENERAL

Las normas del gobierno nacional sobre la necesidad de mantener niveles confiables de seguridad en la información de las instituciones, así como prevenir y contrarrestar eventos y/o sucesos que puedan vulnerarla, hace indispensable establecer protocolos, detallar normas y determinar parámetros de uso de equipos personales, portátiles, tabletas, móviles y demás equipos de cómputo de funcionarios de la academia, la administración, contratistas en todas sus modalidades y usuarios externos que en forma eventual, operan equipos para actividades propias de la gestión, las cuales se deben cumplir de manera coordinada, con protocolos y

normas internas, que condicionan el uso de equipos de cómputo que no sean administrados o de propiedad de la universidad, a fin de que cuenten con aval institucional, se definan los niveles de acceso a la información institucional y se establezcan documentos de confidencialidad y de responsabilidad en el manejo y uso de equipos moviles propios o suministrados por la UMNG.

3.1. PROPÓSITO

Definir protocolos, establecer normas y fijar restricciones en la utilización de equipos de cómputo y equipos móviles que no son administrados por la Universidad Militar Nueva Granada, en actividades ajenas al buen servicio, las cuales constituyen una vulnerabilidad y un riesgo a la seguridad de la información, pudiendo ser causal de tráfico, fuga o pérdida de información que por su valor estratégico, compromete los intereses y el Know How de la institución.

3.2. DEFINICIONES

- **Equipo Institucional:** Son todos aquellos equipos de cómputo de escritorio, portátiles, servidores o móviles, que son propiedad de la Universidad, se encuentran registrados en los inventarios, o están en alquiler por parte de la Institución.

- **Equipo No Institucional:** Son todos aquellos equipos de cómputo de escritorio, portátiles, servidores o móviles, que no son de propiedad o no están en alquiler por parte de la Universidad Militar Nueva Granada y que son portados por funcionarios o contratistas.

- **Información Sensible:** Es toda información que con su perdida podría afectar los intereses de la universidad y que está contenida en los formatos de inventario de información de la UMNG.

3.3. NORMAS DE USO PARA EQUIPOS DE CÓMPUTO

3.3.1. EQUIPO NO INSTITUCIONAL

a) La Administración, Control y Seguridad del Equipo No Institucional, es responsabilidad de su propietario. El empleo de estos equipos, debe sujetarse a las normas, políticas, e instrucciones que en asuntos de seguridad de la información de la Universidad se emitan.

b) En un Equipo no Institucional, no se debe almacenar ningún tipo de información sensible de la Universidad Militar Nueva Granada. Las dependencias definirán que tipo de información tiene clasificación y restricciones para su consulta en el formato de inventario de información de la UMNG.

c) La protección de la información que se almacena en un Equipo No Institucional, es de responsabilidad única y exclusiva de su propietario y de su mal uso responderá disciplinariamente el usuario.

d) El Equipo No Institucional debe contar con licencia legal de software, antivirus, firewall y antiespía (antispyware) actualizado y debe tener todas las actualizaciones críticas y de seguridad, con el fin de minimizar los riesgos de seguridad de la información y daños ocasionados por virus, la cual será verificada por el personal de la División de Informática, previa solicitud a través de la mesa de ayuda del Jefe de División u Oficina.

e) El Equipo No Institucional, no se puede utilizar en los servicios informáticos de:

- Usuario de Directorio Activo
- Bases de Datos Informática, Registro y Control Académico, Planeación, Financiera, Contratos, Control Interno, Control Interno Disciplinario.
- Acceso a Aplicaciones o Sistemas de Información
- Acceso a Impresión de todo tipo de documentos
- Servicio de red Cableada.
- Los demas servicios de red que se consideren institucionales.

f) Al Equipo No Institucional, no se le brinda soporte de mesa de ayuda, ni apoyo por parte del personal de la UMNG

g) En el Equipo No Institucional, no está permitido instalar software cuyo licenciamiento sea propiedad de la Universidad Militar Nueva Granada.

3.3.2. EQUIPO INSTITUCIONAL

a) El usuario de un Equipo Institucional es responsable de su seguridad, cuando el equipo abandone las instalaciones de la universidad.

b) El usuario de un Equipo Institucional es responsable de la seguridad de la información contenida en él, en todo momento y así mismo es responsable por el acceso a los servicios informáticos que se realicen desde este, tal como se establece en el artículo 4 de la Resolución 2097 de 2013.

4. SE CONSIDERAN AMENAZAS

a) Cualquier afectación que se realice desde un Equipo No Institucional a la infraestructura de informática de la Universidad, es considerada una amenaza o un ataque a la seguridad de la informacion y es responsabilidad de su propietario, y sus consecuencias estan explicitas en las políticas y reglamentos de seguridad de la información existentes en la UMNG.

b) El usuario de Equipo No Institucional que sea detectado haciendo análisis de protocolos, barridos de puertos de SNMP (Simple Network Magnanament Protocol), de ICMP (Internet Control Message Protocol), así como descubrimientos de red no autorizados en las redes de datos, es considerada una amenaza o un ataque a la seguridad de la información y se procederá a realizar una investigación a su propietario, bien sea disciplinaria o penal si fuere del caso, mediante informe a las autoridades competentes, con el fin de establecer las razones de dichas actividades y se aplicarán las sanciones que las investigaciones lo determinen.

5. REPORTE DE EQUIPOS NO INSTITUCIONALES

La Oficina de Protección al Patrimonio debe reportar a la División de Informática de manera diaria, los equipos no institucionales que ingresen y salen de las instalaciones de la Universidad y que sean registrados por personal administrativo y contratistas. En el reporte deben incluirse el nombre del propietario, el número del serial del equipo, la marca y la dirección MAC de éste.

6. CUMPLIMIENTO

a) Es responsabilidad de todo el al personal administrativo, docente y contratistas de la Universidad cumplir con la presente circular.

b) Es responsabilidad de los jefes de Vicerrectores, Jefes de Oficina, División y Secciones velar por el cumplimiento de la presente circular

7. DIVULGACIÓN

La divulgación de la presente circular, se realizará a través de la página Web de la Universidad, la Intranet, pantallas informativas, correo masivo al personal administrativo, docente y contratistas de la Universidad.

8. INTRUCCIONES GENERALES

a) El desconocimiento de esta circular, no exime al usuario de la responsabilidad administrativa, disciplinaria o penal si fuere del caso, por el mal uso de información y/o violación a las normas y restricciones de usabilidad dispuestas en la presente circular

b) Los jefes de dependencias académicas y administrativas, deben actuar como difusores de la presente circular y exigir de sus funcionarios cumplimiento de las normas aquí establecidas.

Cordialmente,

Mayor General **EDUARDO ANTONIO HERRERA BERBEL**
Rector

Los siguientes funcionarios con nuestro visto bueno, declaramos que hemos revisado detenidamente el contenido del presente documento, lo encontramos ajustado a los reglamentos internos de la Universidad, a las disposiciones legales y asumimos cualquier responsabilidad por su contenido.			
Elaboró **Jefe de la División de Informática**	**Vo.Bo.** **Vicerrector Administrativo**	**Vo.Bo.** **Vicerrector General**	**Vo.Bo.** **OFIJUR**
Ing. Carlos Gilberto Delgado Beltrán	BG.(r) Hugo Rodríguez Duran	BG.(R) Alberto Bravo Silva	Dra. Elsa Liliana Aguirre L.