UNIVERSIDAD MILITAR
NUEVA GRANADA

RESOLUCIÓN NÚMERO 4352 DE

(11 NOV. 2016)

Por el cual se actualiza 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, artículo 28 y 57, Ley 805 de 2003, artículo 2, el Acuerdo 13 de 2010, numeral 6 y 11 de 2015 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 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 527 de 1999, por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

Que la Ley 603 del 2000, Por la cual se modifica el artículo 47 de la Ley 222 de 1995.

Que el Ley 679 de 2001, por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución.

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 Ley 1712 de 2014, Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

Que el Decreto 103 de 2015, "Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

Que el Decreto 2573 de 2014, Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.

Que la Circular Permanente No 22 de 2015, Por el cual se emiten nuevas instrucciones para dar cumplimiento a la Directiva Presidencial No 04 de 2012 y al Programa Uso Eficiente de Recursos no Renovables de la Universidad Militar Nueva Granada.

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

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

RESUELVE

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

ARTÍCULO SEGUNDO: Objetivos

- Proteger los activos de información de la Universidad Militar Nueva Granada, frente a amenazas internas y externas, deliberadas o accidentales.
- Proveer una directriz para el Sistema de Gestión de Seguridad de la Información en la Universidad Militar Nueva Granada, orientado a definir los aspectos necesarios para establecer, operar, mantener y dirigir de manera sistemática y organizada un sistema que permita el tratamiento seguro de la información.
- Promover, actualizar y mantener una cultura de seguridad de la información, así como lograr la concientización de todos los usuarios de los servicios informáticos de la Universidad Militar Nueva Granada, con el fin de minimizar la ocurrencia de incidentes de seguridad de la información.
- Coordinar los esfuerzos institucionales con el fin proteger los activos de información.
- Establecer los lineamientos del Plan de Continuidad de Negocio de la Universidad Militar Nueva Granada de manera integral con las políticas y requerimientos de seguridad de la información.
- Coordinar y centralizar los esfuerzos de seguridad integral de la Universidad a través del comité de Seguridad de la Información de la Universidad Militar Nueva Granada.

ARTÍCULO TERCERO: Definiciones

- **Acceso a Internet:** Se entiende por acceso a Internet, la conexión que permite acceder desde un dispositivo electrónico a la Internet, con el objeto utilizar los servicios que se encuentren disponibles en ella.
- **Activo de Información:** Se denomina activo a aquello que tiene algún valor para la organización y por tanto debe protegerse. De manera que un activo de información es aquel elemento que contiene o manipula información.

Activos de información son archivos, bases de datos, contratos y acuerdos, documentación del sistema, manuales de usuario, aplicaciones, sistema operativo, equipos informáticos, equipo de comunicaciones, respaldo de energía, soporte de aire acondicionado y las personas, que son las que en última instancia generan, transmiten y destruyen información. También pueden estar en esta clasificación, el hardware, software, personal, infraestructura y servicios, a través de los cuales se accede a los activos.

- **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
- **Base de Datos:** Bancos de información que contienen datos relativos a diversas temáticas y categorizados de distinta manera, pero que comparten entre sí algún tipo de vínculo o relación que busca ordenarlos y clasificarlos en conjunto.
- **Ciberataque:** Actos en los cuales se cometen agravios, daños o perjuicios en contra de las personas o grupos de ellas, entidades o instituciones, que por lo general son ejecutados por medio de computadoras y a través de la Internet.
- **Cibercrimen:** Acción criminal en el ciberespacio.
- **Ciberdefensa:** Conjunto de acciones y/u operaciones activas o pasivas desarrolladas en el ámbito de las redes, sistemas, equipos, enlaces y personal de los recursos informáticos y tele-informáticos de la defensa a fin de asegurar el cumplimiento de las misiones o servicios para los que fueran concebidos a la vez que se impide que fuerzas enemigas los utilicen para cumplir los suyos.
- **Ciberespacio:** Dimensión generada durante el tiempo de interconexión e interoperabilidad de redes, sistemas, equipos y personal relacionados con los sistemas informáticos cualesquiera sean estos y las telecomunicaciones que los vinculan.
- **Ciberguerra:** Conflicto en el ciberespacio.
- **Ciberseguridad:** Conjunto de acciones de carácter preventivo que tienen por objeto el asegurar el uso de las redes propia y negarlo a terceros.
- **Ciberterrorismo:** Acción terrorista en el ciberespacio.
- **Computación en la nube:** Es un modelo que permite acceso ubicuo (presente en muchos lugares al mismo tiempo) conveniente de una red con un conjunto compartido de recursos informáticos configurables. (UIT-T Y.3500)
- **Confidencialidad:** Información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados. (norma ISO 27001)
- **Continuidad del Negocio:** Planes y actividades, que se tienen para dar respuesta ante situaciones de riesgo, que pueden afectar de forma crítica las actividades de la Universidad.
- **Contraseña:** Forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso y es de responsabilidad exclusiva del usuario.
- **Correo electrónico Institucional:** Servicio de red que permite a los usuarios enviar y recibir mensajes mediante sistemas de comunicación electrónica, los correos institucionales de la Universidad Militar Nueva Granada son todos aquellos que su dominio es @unimitar.edu.co.
- **Datos Sensibles:** Es el que afecta la intimidad del titular o cuyo uso indebido puede generar su discriminación, como, por ejemplo: los que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales. de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos, entre otros, la captura de imagen fija o en movimiento,

huellas digitales, fotografías. iris. reconocimiento de voz. facial o de palma de mano. Resolución 3225 de 2013 de la Universidad Militar Nueva Granda.

- **Directorio Activo:** Servicio establecido en uno o varios servidores en donde se crean objetos tales como usuarios, equipos o grupos, con el objetivo de administrar los inicios de sesión en los equipos conectados a la red de datos de la Universidad Militar Nueva Granada, así como también la administración de políticas en toda la red de datos.
- **Disponibilidad:** Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran. (norma ISO 27001)
- **Equipo Institucional:** Todos aquellos equipos de cómputo de escritorio, portátiles, servidores o móviles, que son propiedad de la Universidad y se encuentran registrados en los inventarios, o están en alquiler por parte de la Institución.
- **Equipo No Institucional:** 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 no son portados por funcionarios o contratistas de la Universidad.
- **Hardware:** Toda parte físicas de un sistema informático.
- **Impresión:** Proceso y resultado de reproducir textos e imágenes con tinta sobre papel o cualquier otro elemento.
- **Incidente de seguridad de la información:** Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Información:** Conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen. (Ley 1712 de 2014, Artículo 6°. Definiciones)
- **Información pública:** Toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal. (Ley 1712 de 2014, Artículo 6°. Definiciones)
- **Información pública clasificada:** Información que estando en poder o custodia de la Universidad Militar Nueva en el cumplimiento de sus funciones, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014.
- **Información pública reservada:** Información que estando en poder o custodia de la Universidad Militar Nueva en el cumplimiento de sus funciones, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014.
- **Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos. (NTC 5411-1:2006)
- **Internet:** Red informática mundial de uso público. Proporciona acceso a varios servicios de comunicación, como la World Wide Web (la 'web'), y transmite archivos de correo electrónico, noticias, entretenimiento y datos. Definición de la ITU
- **Intranet:** Red interna de comunicaciones que utiliza protocolos de Internet y que permite la comunicación dentro de una organización (y con otras personas autorizadas). Normalmente, se encuentra protegida por un cortafuego para controlar el acceso. Definición de la ITU
- **Nube Comunitaria:** Es un modelo de nube privada que comparten varias organizaciones y que por lo general apoya un requisito específico (ejemplo, la misión, políticas, exigencias de seguridad). Puede ser manejado de

dominio propio, por varias organizaciones, un tercero o alguna de las combinaciones de ellos. (NIST SP 800-145)

- **Nube Hibrida:** Es una composición entre dos o más distintas infraestructuras de nube, que permanecen entidades únicas, pero están unidas por la tecnología estandarizada o propietaria que permite que los datos y la portabilidad de aplicaciones. (NIST SP 800-145)
- **Nube Privada:** Esta infraestructura está preparada para el uso exclusivo de una sola organización que comprende varios consumidores. Puede ser de propiedad, administrado y operado por la organización, un tercero. (NIST SP 800-145)
- **Nube Pública:** Esta infraestructura de la nube está preparada para el uso abierto por el público en general, puede ser administrado y operado por una empresa o una organización gubernamental. (NIST SP 800-145)
- **Publicar o divulgar:** Significa poner a disposición en una forma de acceso general a los miembros del público e incluye la impresión, emisión y las formas electrónicas de difusión. (Ley 1712 de 2014, Artículo 6°. Definiciones)
- **Red de Datos:** Infraestructura cuyo diseño posibilita la transmisión de información a través del intercambio de datos. Los medios de trasmisión de la red pueden ser físicos (red Cableada) o puede ser el aire (red Inalámbrica)
- **Red social:** Estructura virtual que proporciona interactividad constante entre los usuarios, quienes comparten distintos intereses y relaciones en común. A través de este espacio se promueve la comunicación y participación de los cibernautas desde la publicación de imágenes, videos, links de referencias o contenidos de su interés. Tomado de Colombia Digital.
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
- **Software:** Conjunto de programas y rutinas que permiten a un equipo de cómputo realizar determinadas tareas.
- **Sistemas de Información:** Conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo.
- **Usuario:** Persona que solicita, usa o requiere habitualmente un servicio.
- **Videoconferencia:** Comunicación simultánea bidireccional de audio y vídeo, que permite mantener reuniones con grupos de personas situadas en lugares alejados entre sí.
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.

ARTÍCULO CUARTO: Los servicios informáticos son todos recursos de software, hardware, infraestructura, redes de datos IP, que la Universidad Militar Nueva Granada ofrece al servicio de la comunidad de estudiantes, docentes, personal administrativo y contratistas, con el fin de que pueden realizar el cumplimiento de sus funciones. Algunos servicios de red son:

- Bases de Datos
- Contratos de licenciamiento
- Conexión a Redes Nacionales e Internacionales que apoyan la educación e investigación
- Correo Electrónico Institucional
- Infraestructura de Servidores
- Infraestructuras de Red
- Salas de Internet
- Seguridad en la Red y Sistemas de Información

- Servicio de Internet
- Servicios de videoconferencias
- Sistemas de información y herramientas que soportan la administración y operación.
- Software y herramientas de desarrollo que apoyan las prácticas asociadas a las asignaturas de los programas académicos.

ARTÍCULO QUINTO: 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 funcionario o usuario de la Universidad Militar Nueva Granada. El uso indebido constituye falta disciplinaria.

ARTÍCULO SEXTO: Los usuarios o funcionarios de la Universidad Militar Nueva Granada deberán reportar en forma inmediata a la División de Informática, cuando detecten alguna vulnerabilidad, amenaza, o incidente de seguridad real o potencial a los activos y/o servicios informáticos de la Universidad, al correo informatica@unimilitar.edu.co

ARTÍCULO SÉPTIMO: El uso adecuado de la tecnología para el procesamiento de la información en la Universidad Militar Nueva Granada aplica para estudiantes, egresado, contratistas, cuerpo académico, funcionarios administrativos 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 institucionales y no institucionales que sean conectados a las redes de datos de la Universidad Militar Nueva Granada o estén en uso fuera de las instalaciones.

ARTÍCULO OCTAVO: Los miembros de la comunidad universitaria deben utilizar los dispositivos tecnológicos de la Universidad, única y exclusivamente para desarrollar sus actividades laborales, académicas y de investigación. Cualquier uso indebido de los recursos de tecnología de la información están prohibidos y el usuario asumirá la responsabilidad.

ARTÍCULO NOVENO: La información institucional consta de datos sobre los procesos misionales, de gestión y de apoyo de la Universidad Militar Nueva Granada, la cual es almacenada en los Equipos Institucionales. La custodia y confidencialidad de la información es responsabilidad cada uno de los usuarios.

ARTÍCULO DECIMO: La información institucional no puede ser almacenada en Equipos No Institucionales. La contravención a este artículo constituye falta disciplinaria.

ARTÍCULO DÉCIMO PRIMERO: En lo Equipos Institucionales, sólo se permite instalar software licenciado, en caso de requerirse la instalación de software libre debe estar debidamente autorizado por la División de Informática, y para uso concerniente a actividades laborales.

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: Responsabilidad de los Usuarios. Es responsabilidad de los usuarios de los servicios informáticos:

1. Ingresar a los equipos de cómputo con clave y contraseña que se le asigno para el uso de los diferentes servicios.
2. No suministrar la clave y contraseña de los servicios informáticos asignados, a terceros. Cualquier uso indebido de estos servicios, es responsabilidad del funcionario al cual se le asignó este.
3. Cambiar las contraseñas de los servicios informáticos de forma periódica, de acuerdo con las normas de seguridad establecidas en la presente resolución.
4. Apagar los equipos de cómputo una vez termine su jornada laboral, esto con el fin de prevenir el acceso indebido a los equipos y como aporte a la responsabilidad con el ambiente.
5. Guardar la confidencialidad de los datos que se encuentren bajo su custodia.
6. Utilizar el correo institucional y el Sistema de Memorando como medio de comunicación oficial.
7. Custodiar la información almacenada en los Equipos Institucionales.
8. Los funcionarios que, por condiciones de su cargo, tengan información de propiedad de la Universidad en medios electrónicos y físicos, deben garantizar que se encuentran resguardados en lugares seguros.
9. Los funcionarios y usuarios de los servicios informáticos de la Universidad Militar Nueva Granada deben guardar la información que genere en el cumplimiento de sus labores en la herramienta que la universidad disponga para esto.
10. Atender a todas las disposiciones de seguridad de la información que la Universidad emita.

ARTÍCULO DÉCIMO CUARTO: Prohibiciones a los usuarios: Está prohibido a usuarios de los servicios informáticos:

1. El acceso a páginas y sitios web con restricciones por normas nacionales, internacionales o internas, los juegos en línea excepto los que están autorizados por la Universidad, el contenido terrorista y el contenido sexual restringido o prohibido.
2. El uso de sitios de almacenamiento virtual que no estén autorizados por la Universidad Militar Nueva Granada, excepto los que tengan dominio @unimilitar.edu.co
3. Violaciones a derechos de cualquier persona o institución, derechos de autor, atentes 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 pública reservada o Información pública clasificada a personas o entidades, sin la debida autorización o violando las políticas sobre manejo de información.
7. La utilización de memorias USB, unidades flash (SD, Micro SD, Mermory Stick, entre otros), disco duro externo, sistemas de almacenamiento virtual, almacenamientos en la nube publica, para la grabación o copia de información de los equipos de cómputo que se encuentran conectados en la red administrativa en todas las sedes de la Universidad.

8. El acceso a las redes sociales en los equipos de cómputo de las salas de internet y los que se encuentran conectados en la red administrativa en todas las sedes de la Universidad.
9. Cualquier actuación que vaya en contra de las leyes vigentes en Colombia.
10. Usar la infraestructura de la universidad para realizar ataques internos o externos.
11. Cualquier forma de interceptación de datos

ARTÍCULO DÉCIMO QUINTO: Equipos de Cómputo.

1. La administración, control y seguridad del Equipo No institucional, es responsabilidad de su propietario. El empleo de estos equipos, debe acogerse a las normas, políticas, e instrucciones que en asuntos de seguridad de la información emita la Universidad.
2. En un Equipo no Institucional, no se debe almacenar ningún tipo de dato sensible de la Universidad Militar Nueva Granada.
3. La protección de la información que se almacena en un Equipo No Institucional, es de responsabilidad única y exclusiva de su propietario
4. Por el mal uso de un Equipo no Institucional es responsabilidad única y exclusiva de su propietario y responderá disciplinariamente por este uso.
5. El Equipo No Institucional que se conecte a la red de datos cableada de la Universidad, debe tener 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.
6. A un Equipo No Institucional no se le puede asignar clave de Directorio Activo.
7. A un Equipo No Institucional no se le puede asignar clave de Impresión.
8. El Equipo No Institucional, no puede acceder a los sistemas de información institucionales o a las Bases de Datos.
9. Un Equipo No Institucional no se puede utilizar en las Divisiones o Jefaturas de Registro y Control Académico, Planeación, Financiera, Contratos, Control Interno, Control Interno Disciplinario.
10. Al Equipo No Institucional, no se le brinda soporte de mesa de ayuda, ni apoyo por parte del personal de la Universidad Militar Nueva Granada.
11. En el Equipo No Institucional, no está permitido instalar software cuyo licenciamiento sea propiedad de la Universidad Militar Nueva Granada.
12. El usuario de un Equipo Institucional es responsable de su seguridad, cuando el equipo abandone las instalaciones de la universidad.
13. 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.
14. Se debe hacer la baja de los equipos de cómputo asignados a los funcionarios que sean retirados o dejan de prestar servicios para la Universidad Militar Nueva Granada.
15. Cuando se realice la baja de un servidor, una estación de trabajo o un PC que cumpla esta función, se deben realizar borrado seguro y proceder a destruir los discos duros en un plazo que no supere los 30 días calendario.

ARTÍCULO DÉCIMO SEXTO: Contraseñas. Las contraseñas de los servicios informáticos que ofrece la Universidad Militar Nueva Granada deben tener las siguientes características y estas deben ser cumplidas por la comunidad de estudiantes, docentes, personal administrativo y contratistas:

1. La longitud mínima de la contraseña es de ocho caracteres alfanuméricos.

2. Las contraseñas deben estar conformadas por letras mayúsculas, minúsculas, números y caracteres especiales.
3. La clave del directorio activo tiene una vigencia máxima de tres meses.
4. Las contraseñas se deben cambiar cada tres meses, si el sistema no pide cambio.
5. La contraseña es personal, reservada e intransferible.

ARTÍCULO DÉCIMO SÉPTIMO: Correo electrónico

1. Los correos electrónicos institucionales de la Universidad Militar Nueva Granada se clasifican de acuerdo al tipo de usuario al cual se le asigne:

Tipo de Usuario	Nombre de la Cuenta	Dominio	Tipo de correo
Rector	Rector	@unimilitar.edu.co	Oficina o dependencia
Vicerrector	Siglas de la Vicerrectoria	@unimilitar.edu.co	Oficina o dependencia
Jefe de Oficina	Siglas del Nombre de la Oficina	@unimilitar.edu.co	Oficina o dependencia
Jefe de División	Siglas del Nombre de la División	@unimilitar.edu.co	Oficina o dependencia
Correos especiales	Nombre del correo. Ejemplo: protecciondedatos	@unimilitar.edu.co	Oficina o dependencia
Funcionario de Planta	nombre.apellido + condicional	@unimilitar.edu.co	Personal
Funcionario de Prestación de Servicios	tmp.nombre.apellido + condicional	@unimilitar.edu.co	Personal
Estudiante de Pregrado o Posgrado	nombre.apellido + condicional	@unimilitar.edu.co	Personal

Los correos especiales, son correos que están establecidos por las leyes vigentes en Colombia y las normatividades de la Universidad Militar para la comunicación de la comunidad en general hacia la Universidad

El condicional se coloca si algún usuario presenta homónimo al momento de crear el usuario de correo y un diferenciador, para este caso el condicional ser un número consecutivo, para todos los usuarios creados ante del año 2017, ser permitirá la utilización de un alias por procesos de transición.

1. Los comunicados internos de la Universidad Militar deben ser dirigidos a los correos de tipo personal
2. Los correos que se definen como oficina o dependencia, son correos que se utilizan como medios de comunicación de la comunidad en general hacia la Universidad.
3. El correo electrónico institucional debe ser usado únicamente para propósitos concernientes a las funciones de su cargo.
4. Los usuarios del correo electrónico institucional no deben enviar mensajes personales, ofensivos, cadenas de mensajes, que se relacionen con actividades ilegales, no éticos, o que atenten contra el buen nombre de la Institución de alguna persona en particular.
5. La Universidad Militar Nueva Granada no se hace responsable, directa ni subsidiariamente, por opiniones expresadas en los correos enviados por usuarios desde el correo institucional, ni por las expresiones manifestadas por ellos o por cualquiera persona en los espacios de debate público o en cuentas de correo electrónico.
6. Los mensajes de correo electrónico son considerados documentos formales y activos de información. y por lo tanto debe seguir los lineamientos de acuerdo a la ley 527 del 1999
7. No se debe utilizar una cuenta de correo electrónico que pertenezca a otro funcionario. En caso de ausencias o vacaciones, se debe recurrir a mecanismos alternos como redirección de mensajes.
8. Los usuarios de correo electrónico institucional que identifiquen en su correo contenido sospecho o con posibles virus, deben notificarlo a la

División de Informática, y/o al correo electrónico soporte.informatica@unimilitar.edu.co

9. Todo correo institucional tiene la misma valides de un documento físico, por tal motivo no requerir la impresión para validar su legitimada. De acuerdo con la Ley 527 de 1999.

ARTÍCULO DÉCIMO OCTAVO: Sistemas de Información

1. Los usuarios y las claves de los funcionarios administrativos, docentes y contratistas serán asignados por el procedimiento de asignación de usuarios de la universidad.
2. Los funcionarios administrativos, docentes y contratistas que sean trasladados para realizar nuevas funciones o se retiren de la Universidad, la Division de Gestion del Talento Humano debe realizar las notificaciones a la División de Informática para modificar los permisos o dar de baja la clave, según sea el caso.
3. Los sistemas de información de la Universidad Militar Nueva Granada, incluye los programas, aplicaciones, bases de datos y archivos electrónicos; y sólo pueden utilizarse para fines relacionados con el desempeño de sus funciones.
4. Los sistemas de información y las herramientas asociadas a estos sólo podrán ser utilizados por personal debidamente autorizado y será responsabilidad de cada área definir las tareas que conllevan el acceso a estos.
5. Cada usuario será individualmente responsable por el manejo adecuado de las claves de acceso o contraseñas asignadas.
6. La correspondiente asignación de claves de acceso no impedirá que el uso de los Sistemas de Información sea auditado por el personal autorizado por la Oficina de Control Interno de Gestion o la Oficina de Protección al Patrimonio, con el propósito de garantizar el uso apropiado de los recursos y la privacidad de la información. De acuerdo con la ley 1581 de 2012 y de la resolución 3225 del 2013.
7. El uso de los recursos de sistemas de información o equipo que tenga como objetivo cualquier tipo de ganancia económica personal está prohibido.
8. El acceso no autorizado a los sistemas de información de la Universidad está prohibido
9. Ningún funcionario debe usar la clave o contraseña de otro funcionario, y de la misma manera ninguno debe dar a conocer su calve y contraseña, excepto en casos que faciliten la reparación o el mantenimiento de algún servicio o equipo y en este caso debe dar a conocer estos datos única y exclusivamente al funcionario de la División de Informatica autorizado a realizar esta labor y este debe generar el procedimiento de cambio de contraseña una vez termine la labor.
10. La información que reposa en las bases de datos de los sistemas de información de la Universidad Militar Nueva Granada es y será utilizada en el desarrollo de las funciones propias, en su condición de Institución de Educación Superior, de forma directa o a través de terceros.
11. La información almacenada en las bases de datos de los sistemas de información de la Universidad o en cualquier medio de almacenamiento debe regirse por el Manual de Políticas de Privacidad de los Datos Personales, actual y vigente de la Universidad Militar Nueva Granada, y el usuario es responsable de los datos al interior de la Infraestructura.

ARTÍCULO DÉCIMO NOVENO: Normas de Escritorio Limpio

1. 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.

2. Antes de abandonar la oficina, los funcionarios deben recoger y asegurar el material sensible (CD, DVD, Hojas impresas con información de la Universidad).
3. Antes de abandonar la oficina, los funcionarios deben asegurar, los equipos y almacenar de la información sensible (Portátiles, PDA, Memorias USB, entre otros).
4. 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.
5. 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 VIGÉSIMO: Acceso a la Red de Datos

1. Se controlará el acceso a los servicios de red tanto internos como externos. La División de Informática tendrá a cargo el otorgamiento del acceso a los servicios y recursos de red.
2. El acceso a Internet será utilizado con propósitos autorizados o con el destino por el cual fue provisto. División de Informática definirá el procedimiento para solicitar y aprobar accesos a Internet.
3. El uso de las Rede de Datos de la Universidad debe limitarse a tareas educativas y administrativas, dependiendo en qué red se encuentre el usuario, siendo responsabilidad del usuario el no realizar un uso ilícito de la red.
4. La División de Informatica se reserva el derecho a monitorear la actividad que se realice a través de las redes. Además, el acceso a Internet podrá ser filtrado y controlado no estando permitido el uso de técnicas, sistemas o aplicaciones que permitan evitar dicho control.
5. El uso indebido de las Redes de Datos, es causal de falta disciplinaria, según corresponda al caso de acuerdo en esta resolución o por las leyes nacionales vigentes.

ARTÍCULO VIGÉSIMO PRIMERO: Plan de Continuidad del Negocio

1. El Comité de Gobierno en Línea y Seguridad de la Información deberá revisar por lo menos una vez al año los planes de continuidad del negocio, con el fin de realizar los ajustes necesarios a estos.
2. El Comité de Gobierno en Línea y Seguridad de la Información establecerá un cronograma de pruebas periódicas de cada uno de los planes de contingencia.
3. La Oficina de Protección el con apoyo de la División de Informática elaborarán los planes de contingencia o continuidad del negocio necesario para garantizar la continuidad de las actividades de la Universidad. Estos procesos deberán ser propuestos por el Comité de Gobierno en Línea y Seguridad de la Información.
4. Se debe realizar pruebas de los Back Ups de los sistemas de información en un ambiente pruebas una vez cada 6 meses.

ARTÍCULO VIGÉSIMO SEGUNDO: La ocurrencia de cualquier delito informático en los servicios informáticos de la universidad y que este contemplado por las leyes nacionales o internacionales vigentes, son causales de falta disciplinaria, según corresponda al caso.

ARTÍCULO VIGÉSIMO TERCERO: 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 CUARTO: 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 QUINTO: La presente Resolución rige a partir de la fecha de su expedición y deroga la Resolución 2097 de 2013, la Circular No 07 de 2011, la Circular No 04 de 2013, la Circular No 010 de 2013, la Circular No 018 de 2014.

COMUNÍQUESE Y CÚMPLASE

Dada en Bogotá, D.C. a los

BRIGADIER GENERAL HUGO RODRÍGUEZ DURAN
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	*Vo. Bo.* **Jefe División de Informatica**	*Vo. Bo.* **Vicerrector Administrativo**	*Vo. Bo.* **Vicerrector Académico**	*Vo. Bo.* **Jefe Oficina Jurídica**	*Vo. Bo.* **Vicerrector General**
Ing. Eduardo Antonio Martínez Corena Profesional Especializado División de Informatica	Ing. Oscar Iván Varela Vélez Jefe División de Informática	SN (R) Rafael Antonio Tovar Mondragón	Dra. Rosa Yanneth Méndez Martín	Dra. Elsa Liliana Aguirre Jefe de la Oficina Asesora Jurídica	MG (R). Jairo Alfonso Aponte Prieto