UNIVERSIDAD MILITAR
NUEVA GRANADA
RECTORÍA

Bogotá, 29 de SET de 2011

CIRCULAR No. 07 /UMNG-RECTOR-OFIPROP

PARA: SEÑORES VICERRECTORES, DECANOS, JEFES DE OFICINA, JEFES DE DIVISIÓN Y DIRECTORES DE PROGRAMA

ASUNTO: SEGURIDAD DE LA INFORMACIÓN Y MANEJO DE MEDIOS INFORMÁTICOS

VIGENCIA: LA PRESENTE CIRCULAR TIENE VIGENCIA A PARTIR DEL MOMENTO DE SU PUBLICACIÓN Y HASTA QUE SE REGLAMENTE EN LOS ESTATUTOS DE LA UNIVERSIDAD.

La presente circular indica los criterios para el manejo de la información y de los medios informáticos puestos a disposición de la Comunidad Neogranadina, orientando la generación de políticas que le permita al Claustro Universitario, plasmar estas iniciativas en los reglamentos y estatutos vigentes. La propuesta será presentada en el próximo Consejo Superior para su respectiva aprobación.

La División de Informática desplegará todas las iniciativas posibles con el propósito de hacer efectivos los mecanismos tecnológicos a su alcance, a fin de preservar la información de la Universidad, y efectuar medidas activas que contrarresten vulnerabilidades en la red.

1. DEFINICIONES

Las definiciones que se transcriben a continuación, fueron tomadas de la Norma ISO 27001, en su sección 2 "Términos y Definiciones", que nos orientan a generar políticas en materia de seguridad y manejo de los medios informáticos de la Universidad Militar Nueva Granada.

- **Activo**: Cualquier cosa que tenga valor para la organización (ISO/IEC 13335-1:2004).
- **Amenaza**: Una causa potencial de un incidente no deseado, el cual puede resultar en daño a un sistema u organización (ISO/IEC 13335-1:2004).

- **Análisis del riesgo**: Uso sistemático de la información para identificar las fuentes y calcular el riesgo.
- **Confidencialidad**: Proteger la información de su revelación no autorizada; esto significa que la información debe estar protegida de ser copiada por cualquiera que no esté explícitamente autorizado por el propietario de dicha información.
- **Control**: Medios para manejar el riesgo; incluidas políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal.
- **Disponibilidad**: Los recursos de información deben ser accesibles cuando sea necesario.
- **Evaluación del riesgo**: Proceso de comparar el riesgo estimado con un criterio de riesgo dado para determinar la importancia del riesgo. (ISO/IEC 13335-1:2004).
- **Evento de seguridad de la información**: Cualquier evento de seguridad de la información es una ocurrencia identificada del estado de un sistema, servicio o red, indicando una posible falla en la política de seguridad de la información, falla en las salvaguardas o una situación previamente desconocida que puede ser relevante para la seguridad (ISO/IEC 13335-1:2004).
- **Gestión del riesgo**: Actividades coordinadas para dirigir y controlar una organización con relación al riesgo; ésta incluye tratamiento, aceptación y comunicación del riesgo. (ISO/IEC 13335-1:2004).
- **Incidente de seguridad de la información**: Un incidente de seguridad de la información se indica por un solo evento o una serie de eventos inesperados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información. (ISO/IEC 13335-1:2004).
- **Integridad**: Proteger la información de alteraciones no autorizadas por la organización.
- **Lineamiento**: Descripción que aclara qué se debiera hacer y cómo, para lograr objetivos establecidos en las políticas (ISO/IEC 13335-1:2004)
- **Medios de procesamiento de la información**: Cualquier sistema, servicio o infraestructura de procesamiento de la información o los locales físicos que los alojan.
- **Política**: Intención y dirección general expresada formalmente por la gerencia.
- **Responsabilidad**: En términos de seguridad, significa determinar que individuo en la institución, es responsable directo de mantener seguros los activos de cómputo e información.
- **Riesgo**: Combinación de la probabilidad de un evento y su ocurrencia (ISO/IEC 13335-1:2004).
- **Seguridad de la información**: Preservación de confidencialidad, integración y disponibilidad de la información; además, también puede involucrar otras propiedades como autenticidad, responsabilidad, no repudiación y confiabilidad.
- **Tercera persona**: Esa persona u organismo que es reconocido como independiente de las partes involucradas, con relación al ítem en cuestión. (ISO/IEC Guía 2: 1996)
- **Tratamiento del Riesgo**: Proceso de selección e implementación de medidas para modificar el riesgo'(ISO/IEC – Guía 73:2002).
- **Vulnerabilidad**: La debilidad de una activo o grupo de activos que puede ser explotada por una o más amenazas (ISO/IEC 13335-1:2004).

DE LA SEGURIDAD DE LA INFORMACIÓN

a) La Universidad Militar Nueva Granada define la información y los datos como un bien o un activo de la misma, que debe ser protegido y preservado.

b) El alcance de este capítulo es para los funcionarios, empleados o contratistas en cualquier modalidad o tipo de contrato y en general, para todas las personas naturales y jurídicas que tengan vínculo con la Universidad.

c) Los servicios de la red institucional son de exclusivo uso académico, de investigación, técnicos y para gestiones administrativas, que permitan cumplir con los objetivos institucionales y la misión de la Universidad.

d) Es necesario que la Universidad y todos sus funcionarios en cualquier modalidad de contratación, y empresas u organizaciones, generen actividades y controles para preservar la confidencialidad, integridad y disponibilidad de la información que cada uno maneja o tiene acceso.

e) Toda persona natural o jurídica con vínculo contractual con la Universidad, debe firmar un acuerdo de confidencialidad y no divulgación de datos institucionales o considerados confidenciales; éste debe reposar en su hoja de vida, carpeta del contrato o documento que lo vincule con la Universidad.

f) El Rector, Vicerrector, Jefe de Oficina, Jefe de División, Decano, Director de Programa, Jefe de Centro o Instituto de cada unidad académica o administrativa dentro de la red institucional y en general, todos los funcionarios, son los únicos responsables de las actividades procedentes de sus acciones y la información que se genere de la red.

g) Todo usuario de la red institucional de la Universidad, tiene absoluta privacidad sobre su información o la información que provenga de sus acciones, salvo en casos, en que se vea involucrado en actos ilícitos o contraproducentes para la seguridad de la red institucional, sus servicios o cualquier otra red ajena a la Institución.

h) Los usuarios tendrán acceso a Internet, siempre y cuando se cumplan los requisitos mínimos de seguridad para acceder a este servicio y se acaten las disposiciones de conectividad de la División de Informática.

i) Las actividades académicas (clases, exámenes, prácticas, tareas, etc.), en los centros de cómputo, tienen la primera prioridad, por lo cual a cualquier usuario, utilizando otro servicio (Internet o chat), sin estos fines, se le podrá solicitar que deje libre la estación de trabajo, si fuere necesario para satisfacer la demanda de estaciones en horas pico o el uso de estaciones con software especializado.

j) La información procesada, manipulada o almacenada por el funcionario en cumplimiento de sus obligaciones contractuales o manuales de funciones específicas, es propiedad exclusiva de la Universidad.

k) Todo usuario tiene la obligación de mantener secreto profesional sobre los datos que conozca en el desarrollo de sus funciones, aún después de finalizar la relación laboral que le une a la Institución.

l) La información que maneja o manipula el empleado, no puede ser divulgada a terceros o fuera del ámbito laboral, sin las autorizaciones que correspondan, acordes al tipo de información que se trate.

m) El acceso a los sistemas y servicios de información, es permitido únicamente a los usuarios que dispongan de los permisos necesarios para su ejecución.

n) Un funcionario puede enviar por medios electrónicos o impresos, compartir o almacenar documentos en medios de Internet y medios removibles siempre y cuando tenga plena validación y autorización de su jefe inmediato y del autor del mismo.

RESPONSABILIDAD POR LOS ACTIVOS

a) Cada área académica o administrativa, tendrá un responsable por el/los activo/s crítico/s de mayor importancia para la Facultad, Departamento y/o Universidad.

b) La persona o entidad responsable de los activos de cada unidad organizativa o área de trabajo, velará por la salvaguarda de los activos físicos (hardware y medios magnéticos, aires acondicionados, mobiliario), activos de información (bases de datos, archivos, documentación de sistemas, procedimientos operativos, configuraciones), activos de software (aplicaciones, software de sistemas, herramientas y programas de desarrollo.

c) Los administradores de los sistemas son responsables de la seguridad de la información almacenada en estos recursos.

MAYOR GENERAL EDUARDO HERRERA BERBEL
Rector
Una Universidad de todos y para todos

Elaborado y Proyectado: Angeline Zevooluni Rodríguez – Oficina de Protección del Patrimonio y Seguridad Integral
VoB: Cr. Rafael Mejía Roa - Jefe Oficina de Protección del Patrimonio y Seguridad Integral
Revisó: Dra. Elsa Liliana Aguirre – Jefe Oficina Jurídica
Revisó: Ing. Carlos Delgado – Jefe División de Informática
Revisó: BG. Alberto Bravo Silva – Vicerrector General