SISTEMA DE GESTIÓN	Número de Páginas: **56**	Revisión No: **1**
Nombre: **MANUAL INTEGRAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**		

Elaborado por:	Revisado por:	Aprobado por:
Eduardo Antonio Martinez Corena Profesional Especializado Oficina Asesora de Tecnologías de la Información y las Comunicaciones	Oscar Iván Varela Vélez Jefe Oficina Asesora de Tecnologías de la Información y las Comunicaciones	BG Hugo Rodríguez Duran Rector

CONTROL DE CAMBIOS

Razones del Cambio	Cambio a la Revisión #	Fecha de Emisión
Creación	0	08/08/2019

Tabla de contenido

INTRODUCCIÓN

La Universidad Militar Nueva Granada ha determinado la información como un activo de alta importancia, que permite el desarrollo continuo de su misión y el cumplimiento de los objetivos institucionales, lo que genera la necesidad de implementar reglas y medidas que permitan proteger la confidencialidad, integridad y disponibilidad en todo el ciclo de vida de la información.

Este manual establece las políticas que integra el Sistema de Gestión de Seguridad de la Información SGSI, las cuales deben ser adoptadas por los funcionarios (docentes y administrativos), estudiantes, contratistas, personal en comisión, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con la Universidad Militar Nueva Granada, estas políticas se encuentran enfocadas en el cumplimiento de la normatividad legal Colombiana vigente y a las buenas prácticas de seguridad de la información, basadas en la norma ISO 27001 vigente, Ley 527 de 1999 y al modelo de seguridad y privacidad de la información de la estrategia Gobierno en Línea (GEL) del Ministerio de Tecnologías de la Información y las Comunicaciones.

OBJETIVO

Establecer las políticas que regulan la seguridad de la información en la Universidad Militar Nueva Granada, de manera clara y coherente los elementos que conforman la Política de Seguridad que deben conocer, acatar y cumplir toda la Comunidad Universitaria, bajo la supervisión y liderazgo de la Oficina Asesora de Tecnologías de la Información y las Comunicaciones.

ALCANCE

Las Políticas de Seguridad de la Información son aplicables para todos los aspectos administrativos, educativos y de control que deben ser cumplidos por toda la Comunidad Universitaria, con el fin de tener un adecuado cumplimiento de sus funciones y un cumplir con un nivel alto de protección de seguridad y calidad de la información, aportando con su participación en la toma de medidas preventivas y correctivas, siendo un punto clave para el logro del objetivo y la finalidad de dicho manual.

Este Manual Integral de Políticas de Seguridad de la Información hace parte de Sistema de Gestión de Seguridad de la Información (SGSI), tiene alcance para todos los procesos de la Universidad Militar Nueva Granada, en todas sus sedes.

1. APLICABILIDAD DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Las políticas del SGSI aplican y son de obligatorio cumplimiento para toda la Comunidad Universitaria.

2. TÉRMINOS Y DEFINICIONES

Acción correctiva: Remediación de los requisitos o acciones que dieron origen al establecimiento de no una conformidad, de tal forma que no se vuelva a presentar.
Acción preventiva: Disposición de operaciones que buscan de forma preliminar, que no se presente en su ejecución, desarrollo e implementación una no conformidad.
Activo: [ISO/IEC 13335-12004]: Cualquier cosa que tiene valor para la organización. Se entiende por cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la Universidad Militar Nueva Granada. Se pueden clasificar de la siguiente manera:

- **Datos:** Son todos aquellos elementos básicos de la información, en cualquier formato que se generan, recogen, gestionan, transmiten y destruyen.
- **Aplicaciones:** Es todo el software que se utiliza para la gestión de la información
- **Personal:** Son todos los miembros de la Comunidad Universitaria que tienen acceso de una manera u otra a los activos de información.
- **Servicios:** Son el un conjunto de acciones, las cuales son realizadas para servir a alguien, algo o alguna causa.
- **Tecnología:** Son todos los medios utilizados para gestionar la información y las comunicaciones.
- **Instalaciones**: Son todos los lugares en los que se alojan los sistemas de información.
- **Equipamiento auxiliar:** Son todos aquellos activos que dan soporte a los sistemas de información y que no se hallan en ninguno de los tipos anteriormente definidos.

Administración de riesgos: Gestión de riesgos, es un enfoque estructurado para manejar la incertidumbre relativa a una amenaza, a través de una secuencia de actividades humanas que incluyen evaluación de riesgo, estrategias de desarrollo para manejarlo y mitigación del riesgo utilizando recursos gerenciales. Las estrategias incluyen transferir el riesgo a otra parte, evadir el riesgo, reducir los efectos negativos del riesgo y aceptar algunas o todas las consecuencias de un riesgo particular.
Administración de incidentes de seguridad: Procedimientos, estrategias y herramientas de control, enfocados a una correcta evaluación de las amenazas existentes, en este caso hacia toda la infraestructura de TI, se basa en un análisis continuo y mejorado del desempeño de todos los activos y recursos gerenciales que tiene la entidad.

Su objetivo principal es atender y orientar las acciones inmediatas para solucionar cualquier situación que cause una interrupción de los diferentes servicios que presta la entidad, de manera rápida y eficaz. No se limita a la solución de problemas específicos sino a buscar las causas que determinaron el incidente limitando el marco de acción de futuras ocurrencias, su enfoque se base en tres pilares fundamentales:

1. Detectar cualquier alteración en los servicios TI.
2. Registrar y clasificar estas alteraciones.
3. Asignar el personal encargado de restaurar el servicio.

APT: (Advance Persistent Threat) Amenaza Avanzada Persistente, especie de ciberataque que es responsable del lanzamiento de ataques de precisión y tienen como objetivo comprometer una máquina en donde haya algún tipo de información valiosa.

Alcance: Ámbito de la organización que queda sometido al Sistema de Gestión de Seguridad de la Información - SGSI. Debe incluir la identificación clara de las dependencias, interfaces y límites con el entorno, sobre todo si sólo incluye una parte de la organización.

Alerta: Una notificación formal de que se ha producido un incidente relacionado con la seguridad de la información que puede evolucionar hasta convertirse en desastre.

Almacenamiento externo: Cualquier formato de almacenamiento de datos que no está fijo de modo permanente dentro del equipo de cómputo.

Almacenamiento en la Nube: Del inglés cloud storage, es un modelo de almacenamiento de datos basado en redes de computadoras que consiste en guardar archivos en un lugar de Internet. Esos lugares de Internet son aplicaciones o servicios que almacenan o guardan archivos.

Amenaza: [ISO/IEC 13335-1:2004): Causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

Análisis de riesgos: A partir del riesgo definido, se define las causas del uso sistemático de la información para identificar fuentes y estimar el riesgo.

Auditabilidad: Los activos de información deben tener controles que permitan su revisión. Permitir la reconstrucción, revisión y análisis de la secuencia de eventos.

Auditor: Persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.

Auditoría: Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización.

Autenticación: Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

Autenticidad: Los activos de información solo pueden estar disponibles verificando la identidad de un sujeto o recurso, es la propiedad que garantiza que la identidad de un

sujeto o recurso es la que declara y se aplica a entidades tales como usuarios, procesos, sistemas de información.

Base de datos de gestión de configuraciones (CMDB, Configuration Management Database)**:** Es una base de datos que contiene toda la información pertinente acerca de los componentes del sistema de información utilizado en una organización de servicios de TI y las relaciones entre esos componentes.

Características de la Información: las principales características desde enfoque de seguridad de información son: confidencialidad, disponibilidad e integridad.

Checklist: Lista de chequeo o de verificación, ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo.

CSIRT (Computer Security Incident Response Team): Equipo de Respuesta ante Incidencias de Seguridad Informática

Compromiso de la Dirección: Alineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI - Sistema de Gestión de la Seguridad de la Información.

Computación forense: También llamada informática forense, computación forense, análisis forense digital o examinación forense digital, es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

Comunidad Universitaria (Acuerdo 13/10 art.12): es el grupo humano integrado por estudiantes, egresados, docentes, administrativos y de servicios, vinculados a la Universidad y comprometidos con el desarrollo de sus funciones, el cumplimiento de los principios y el logro de los fines de la Universidad.

Confiabilidad: es la capacidad de un producto de realizar su función de la manera prevista. La probabilidad en que un producto realizará su función prevista sin incidentes por un período de tiempo especificado y bajo condiciones indicadas.

Confidencialidad: Acceso a la información por parte únicamente de quienes estén autorizados, [ISO/IEC 13335-1:2004]:" característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

Control: son todas aquellas políticas, procedimientos, prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

Control correctivo: Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas. Supone que la amenaza ya se ha materializado pero que se corrige.

Control disuasorio: Control que reduce la posibilidad de materialización de una amenaza.

Control preventivo: Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.

Correos especiales: son correos que están establecidos por las leyes vigentes en Colombia y las normatividades de la Universidad Militar para la comunicación de los usuarios hacia la Universidad.

Declaración de aplicabilidad: Se trata de un documento que enlista los controles de seguridad establecidos en el Anexo A del estándar ISO/IEC 27001.

Denegación de servicios: Acción iniciada por agentes externos (personas, grupos, organizaciones) con el objetivo de imposibilitar el acceso a los servicios y recursos de una organización durante un período indefinido de tiempo. La mayoría de ocasiones se busca dejar fuera de servicio los servidores informáticos de una compañía o en su defecto en situaciones más complejas ocasionar graves daños, para que no puedan utilizarse ni consultarse servicios importantes.

Desastre: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse afectada de manera significativa.

Directiva: [ISO/lEC 13335-1: 2004): una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.

Disponibilidad: [ISO/lEC 13335-1: 2004): característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

Evaluación de riesgos: [ISO/lEC Guía 73:2002]: proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.

Evento: [ISO/lEC TR 18044:2004]: Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardas, o una situación anterior desconocida que podría ser relevante para la seguridad.

Evidencia objetiva: Información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de seguridad de la información.

FTP: (File Transfer Protocol) es un protocolo de transferencia de archivos entre sistemas conectados a una red TCP basado en la arquitectura cliente-servidor, de manera que desde un equipo cliente nos podemos conectar a un servidor para descargar y/o subir archivos a él.

Gestión de claves: Controles referidos a la gestión de claves criptográficas.

Gestión de riesgos: Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos.

Gusano (Worm)**:** Es un programa malicioso de computador que tiene la capacidad de duplicarse a sí mismo. A diferencia del virus, no altera información, aunque casi siempre causan problemas de red debido al consumo de ancho de banda y su gran facilidad para mutar.

Impacto: Resultado de un incidente de seguridad de la información.

Incidente: Según [ISO/lEC TR 18044:2004]: 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: La información constituye un importante activo, esencial para las actividades de una organización y, en consecuencia, necesita una protección adecuada. La información puede existir de muchas maneras, es decir puede estar impresa o escrita en papel, puede estar almacenada electrónicamente, ser transmitida por correo o por medios electrónicos, se puede mostrar en videos, o exponer oralmente en conversaciones.

Ingeniería Social: Método utilizado por los atacantes para engañar a los usuarios informáticos, para que realicen una acción que normalmente producirá consecuencias negativas como la descarga de malware o la divulgación de información personal. [Guía para la Implementación de Seguridad de la Información MINTIC]

Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según [ISOIIEC 13335-1: 2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos.

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

IPS: Sistema de prevención de intrusos. Es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.

ISO: Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares.

ISO 17799: Código de buenas prácticas en gestión de la seguridad de la información adoptado por ISO transcribiendo la primera parte de BS7799. A su vez, da lugar a ISO 27002 por cambio de nomenclatura el 1 de Julio de 2007. No es certificable.

ISO 19011: "Guidelines for quality and/or environmental management systems auditing". Guía de utilidad para el desarrollo de las funciones de auditor interno para un SGSI.

ISO 27001: Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable. Primera publicación en 2005, segunda publicación en 2013.
ISO 27002: Código de buenas prácticas en gestión de la seguridad de la información (transcripción de ISO 17799). No es certificable. Cambio oficial de nomenclatura de ISO 17799:20005 a ISO 27002:20005 el 1 de Julio de 2007.
ISO 9000: Normas de gestión y garantía de calidad definidas por la ISO.
ISO/IEC TR 13335-3: "Information technology. Guidelines for the management of IT Security. Techniques for the management of IT Security." Guía de utilidad en la aplicación de metodologías de evaluación del riesgo.
ISO/IEC TR 18044: "Information technology. Security techniques. Information security incident management". Guía de utilidad para la gestión de incidentes de seguridad de la información.
ITIL: IT Infrastructure Library es un marco de gestión de los servicios de tecnologías de la información.
Keyloggers: Son software o aplicaciones que almacenan información digitada mediante el teclado de un computador por un usuario; es común relacionar este término con malware del tipo daemon (demonio), es decir, actúa como un proceso informático que no interactúa con el usuario, ya que se ejecuta en segundo plano. Usualmente puede ser un tipo de software o un dispositivo hardware que se encarga de registrar las pulsaciones que se hacen con el teclado, para posteriormente memorizarlas en un archivo o enviarlas a través de internet.
Legalidad: El principio de legalidad o primacía de la ley es un principio fundamental del derecho público conforme al cual todo ejercicio del poder público debería estar sometido a la voluntad de la ley de su jurisdicción y no a la voluntad de las personas. Por esta razón se dice que el principio de legalidad establece la seguridad jurídica, Seguridad de Información, Seguridad informática y garantía de la información.
Malware: es la abreviatura en ingles de software malicioso y este término enmarca todo tipo de programa o código informático cuya finalidad es dañar un sistema informático o causar un mal funcionamiento a los equipos de cómputo.
No conformidad: Situación aislada que, basada en evidencias objetivas, demuestra el incumplimiento de algún aspecto de un requerimiento de control que permita dudar de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo menor.
No conformidad grave: Ausencia o fallo de uno o varios requerimientos de la ISO 27001 que, basada en evidencias objetivas, permita dudar seriamente de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo inaceptable.
No repudio: Los activos de información deben tener la capacidad para probar que una acción o un evento han tenido lugar, de modo que tal evento o acción no pueda ser negado posteriormente.

PDCA Plan-Do-Check-Act: Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI).

PETI: Plan Estratégicos de Tecnologías de la Información.

Phishing: Tipo de delito encuadrado dentro del ámbito de las estafas, que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma, mediante una aparente comunicación oficial electrónica.

Plan de continuidad del negocio (Bussines Continuity Plan)**:** Plan orientado a permitir la continuación de las principales funciones de la Entidad en el caso de un evento imprevisto que las ponga en peligro.

Plan de tratamiento de riesgos (Risk treatment plan)**:** Documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Política de seguridad: Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información.

Política de escritorio limpio: Se define como la política que establece e indica a los funcionarios, contratista y demás colaboradores del Universidad Militar Nueva Granada a asegurar la información pública reservada o información pública clasificada (privada o semiprivada) en lugares que ofrezca la protección necesaria, así mismo los escritorios deben permanecer libres de documentos o informaciones susceptibles de ser afectados en su integridad, confidencialidad y/o disponibilidad.

Punto Único de Contacto (PUC)**:** Entiéndase como mesa de servicio de acuerdo a las mejores prácticas basadas en ITIL.

Protección a la duplicidad: La protección de copia, también conocida como prevención de copia, es una medida técnica diseñada para prevenir la duplicación de información. La protección de copia es a menudo tema de discusión y se piensa que en ocasiones puede violar los derechos de copia de los usuarios, por ejemplo, el derecho a hacer copias de seguridad de una videocinta que el usuario ha comprado de manera legal, el instalar un software de computadora en varias computadoras, o el subir la música a reproductores de audio digital para facilitar el acceso y escucharla.

Ransomware: Código malicioso para secuestrar datos, una forma de explotación en la cual el atacante encripta los datos de la víctima y exige un pago por la clave de descifrado.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Segregación de tareas: Separar tareas sensibles entre distintos funcionarios o contratistas para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.

Seguridad de la información: Según [ISO/IEC 27002:20005]: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad pueden ser también consideradas.
Selección de controles: Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.
SGSI Sistema de Gestión de la Seguridad de la Información: Según [ISO/IEC 27001: 2013]: Sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos.)
Servicios de tratamiento de información: Según [ISO/IEC 27002:2013]: cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizados para su alojamiento.
Spamming: Se llama spam, correo basura o sms basura a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming. La vía más usada es el correo electrónico.
Sniffers: Programa de captura de las tramas de red. Generalmente se usa para gestionar la red con una finalidad docente o de control, aunque también puede ser utilizado con fines maliciosos.
Spoofing: Falsificación de la identidad origen en una sesión: la identidad es por una dirección IP o Mac Address.
Tratamiento de riesgos: a partir del riesgo definido, se aplican los controles con los cuales se busca que el riesgo no se materialice.
Trazabilidad: Propiedad que garantiza que las acciones de una entidad se pueden rastrear únicamente hasta dicha entidad.
Troyano: Aplicación que aparenta tener un uso legítimo pero que tiene funciones ocultas diseñadas para sobrepasar los sistemas de seguridad.
UMNG: Universidad Militar Nueva Granada.
Usuario: en el presente documento se emplea para referirse a los miembros de la Comunidad Universitaria, debidamente autorizados para usar equipos, sistemas o aplicativos informáticos disponibles y a quienes se les otorga un nombre de usuario y una clave de acceso.
Valoración de riesgos: Según [ISO/IEC Guía 73:2002]: Proceso completo de análisis y evaluación de riesgos.
Virus: Programas informáticos de carácter malicioso, que buscan alterar el normal funcionamiento de una red de sistemas o computador personal, por lo general su

acción es transparente al usuario y este demora en descubrir su infección; buscan dañar, modificar o destruir archivos o datos almacenados.

VPN (Virtual Private Network): es una tecnología de red que permite una extensión segura de la red privada de área local (LAN) sobre una red pública o no controlada como Internet.

Vulnerabilidad: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. [ISO/lEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

3. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN.

La Universidad Militar Nueva Granada, ente autónomo del orden nacional, establece que la información es vital para el desarrollo de sus funciones misionales, en razón a que es una herramienta de gran importancia para la toma de decisiones, motivo por el cual, la Universidad se compromete a proteger sus activos de información, orientando sus esfuerzos a la preservación de la confidencialidad, integridad, disponibilidad, a la continuidad de sus operaciones, la administración y gestión de riesgos, la creación de una cultura y conciencia de seguridad en toda la Comunidad Universitaria, la efectividad de esta política depende finalmente del comportamiento de todos personas que conforman la Comunidad Universitaria y de los controles establecidos en las políticas de seguridad descritas en el presente documento, fundamentados en la norma técnica colombiana NTC-ISO-27001:2013 y el modelo de seguridad y privacidad de la información.

OBJETIVO

Definir las pautas, directrices y reglas para generar Seguridad y Protección de la Información de los procesos de la Universidad Militar Nueva Granada, estableciendo dentro del PETI su liderazgo y desarrollo.

CRITERIOS

- Definir implementar, revisar y actualizar las políticas de seguridad de la información.
- Establecer un programa que permita el fortalecimiento de la cultura y conciencia en seguridad de la información en la Comunidad Universitaria.
- Todos los usuarios de la infraestructura de tecnologías de la información y las comunicaciones de la Universidad, tienen la responsabilidad y obligación de cumplir con las políticas, normas, procedimientos y buenas prácticas de seguridad de la información establecidas en el presente manual de la política de seguridad de la información.

- Diseñar, programar y realizar los programas de auditoría del sistema de gestión de seguridad de la información - SGSI, los cuales estarán a cargo de la Oficina de Protección al Patrimonio.
- Los Jefes de dependencia deben asegurar que todos los procedimientos de seguridad de la información dentro de su área de responsabilidad, se realicen correctamente para lograr el cumplimiento de las políticas y estándares de seguridad de la información.

4. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

La Universidad Militar Nueva Granada, crea un esquema de seguridad de la información definiendo y estableciendo roles y responsabilidades que involucren las actividades de operación, gestión y administración de la seguridad de la información.

La Oficina Asesora de Tecnologías de la Información y las Comunicaciones debe establecer los roles, funciones y responsabilidades de operación y administración de los sistemas de información de la Universidad a los funcionarios, estos roles, funciones y responsabilidades, deberán estar debidamente documentadas y distribuidas.

4.1. POLÍTICA PARA USO DE DISPOSITIVOS MÓVILES

La Universidad establece las directrices de uso y manejo de dispositivos móviles (teléfonos móviles, teléfonos inteligentes “smart phones”, tabletas), entre otros, suministrados por esta y personales que hagan uso de los servicios de información de la UMNG.

- La configuración de acceso a correo electrónico institucional en dispositivos móviles personales, se autoriza para la Comunidad Universitaria y se rige las políticas de seguridad de la información que se establecen en el presente documento. La configuración de la cuenta en los dispositivos personales corre bajo responsabilidad del usuario dueño del dispositivo.
- No se autoriza la utilización de dispositivos móviles personales para procesar información de la universidad, excepto del envío de correos o el registro de calificaciones o notas por parte de los docentes.
- Los dispositivos móviles (teléfonos móviles, teléfonos inteligentes, tabletas, entre otros) suministrados por la universidad, son una herramienta de trabajo que se deben utilizar únicamente para facilitar las comunicaciones de los funcionarios de la Universidad.
- Los usuarios de dispositivos móviles institucionales deben tener instaladas únicamente las aplicaciones distribuidas, autorizadas por la Universidad.

- Los dispositivos móviles asignados por la Universidad, solo podrán configurarse las cuentas de correo electrónico asignadas al usuario por la Universidad.
- El sistema de mensajería instantánea autorizado para los dispositivos móviles institucionales es el Hangouts de Google con la cuenta de correo institucional.
- Los dispositivos móviles deben tener contraseña de ingreso y bloqueo del equipo de manera automática y manual, tener activado la función de borrado remoto, cifrar la memoria de almacenamiento.
- Los dispositivos móviles institucionales deben tener únicamente la tarjeta sim asignada por la Universidad, de igual forma la tarjeta sim únicamente debe instalarse en los equipos asignados.
- Ante la pérdida del equipo, ya sea por extravío o hurto, deberá informar de manera inmediata a la Oficina de Protección al Patrimonio, con el fin de realizar procedimiento administrativo por pérdida de elementos.
- Los teléfonos móviles institucionales, deben permanecer encendidos y cargados durante las horas laborales o de acuerdo a la responsabilidad y requerimientos propios del cargo.
- Es responsabilidad del usuario hacer buen uso del dispositivo suministrado por la Universidad con el fin de realizar actividades propias de su cargo o funciones asignadas.
- Los usuarios no están autorizados a cambiar la configuración, ni a la desinstalación de software de los equipos móviles institucionales posterior a su recibo; únicamente se deben aceptar y aplicar las actualizaciones.
- Los usuarios de dispositivos móviles institucionales no deben conectarlos en computadores y/o puertos USB de uso público, excepto a los equipos de la División de Comunicaciones y Publicaciones que están destinados a eventos públicos.
- Los únicos números de teléfonos móviles autorizados para impartir o recibir instrucciones u órdenes de trabajo, son los asignados por parte de la Universidad a sus funcionarios, de requerirse el uso de un número de teléfono móvil personal de un funcionario para actividades laborales, se requiere tener autorización expresa o consentida por parte del funcionario, esto con el fin de dar complimiento con la ley 1581 de 2012.

4.2. POLÍTICA DE SEGURIDAD PARA FUNCIONARIOS

La Universidad implementa acciones para asegurar que los Funcionarios de la Universidad y Contratistas, entiendan sus responsabilidades, como usuarios en los roles asignados, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información y de las instalaciones, para tal efecto llevará a cabo, las siguientes actividades:

- Los candidatos, aspirantes, contratistas y proveedores deben dar aprobación a la Universidad Militar Nueva Granada para el tratamiento de sus datos personales de acuerdo a la Ley 1581 de 2012, lo que se verá reflejado en las cláusulas de los contratos y en la recepción de las hojas de vida.
- Capacitar y sensibilizar a los funcionarios durante la inducción y reinducción sobre las Políticas de Seguridad de la Información.
- Asegurar que los funcionarios y contratistas, de la Universidad adopten sus responsabilidades en relación con las Políticas de Seguridad de la Información y actúen de manera consistente frente a las mismas, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información o los equipos empleados para el tratamiento de la información, el conocimiento de las políticas de seguridad de la información se notificarán mediante el diligenciamiento y firma del contrato de trabajo.
- En situaciones de incumplimiento o violaciones a las políticas de seguridad de la información se deberá tramitar el cumplimiento de la ley 734 de 2002 y demás normas que reglamentan los procesos disciplinarios para los empleados del estado.
- El funcionario o contratista debe entregar los activos de información a su cargo, una vez termine la relación con la Universidad o sea traslado de cargo o de funciones, al funcionario que el jefe de la dependencia designe.

4.3. POLÍTICA DE GESTIÓN DE ACTIVOS DE INFORMACIÓN

La Universidad Militar Nueva Granada es dueña de la propiedad intelectual de los avances tecnológicos e intelectuales desarrollados por sus funcionarios y los contratistas, derivadas del objeto del cumplimiento de funciones o tareas asignadas, como las necesarias para el cumplimiento del objeto del contrato.

La Universidad es propietaria de los activos de información y los administradores de estos activos son los funcionarios y contratistas (denominados “usuarios”) que estén autorizados y sean responsables por la información de los procesos a su cargo, de los sistemas de información, hardware o infraestructura de Tecnología y Sistemas de Información.

La Universidad mantiene actualizado el inventario de activos de información, quedando bajo la responsabilidad de cada área propietaria de información y quedo como evidencia de estos la incontenida en las tablas de retención documental.

La información de la configuración de los servidores, equipos activos de red, seguridad perimetral y demás equipos instalados en los Centros de Datos y Cuartos Técnicos de la Universidad Militar Nueva Granada, se debe mantener en una base de datos (CMDB - Base de datos de gestión de configuraciones / Configuration Management Database)

bajo la responsabilidad del Oficina Asesora de Tecnologías de la Información y las Comunicaciones.

4.4. POLÍTICA DE USO DE LOS ACTIVOS

La Universidad implementa las directrices para lograr y mantener la protección adecuada y uso de los activos de información mediante la asignación a los usuarios finales que deban administrarlos de acuerdo a sus roles y funciones:

- Los usuarios no pueden almacenar en los discos duros de los equipos de cómputo o en discos virtuales proporcionados por la Universidad, archivos de vídeo, música, y fotos y cualquier tipo de archivo que no sean de carácter institucional.
- Los activos de información contenidos en las bases de datos Institucionales son propiedad de la Universidad Militar Nueva Granada y su uso es exclusivo para el desarrollo de las funciones laborales.
- Para desempeñar las funciones asignadas los usuarios solo pueden utilizar los equipos de cómputo suministrados por la Universidad y el software contenido en este.
- La información creada, almacenada, recibida y procesada en los equipos de cómputo suministrados por la Universidad; es propiedad de la Universidad Militar Nueva Granada.
- Los funcionarios no podrán realizar copia de la información pública, clasificada o reservada contenida en los equipos de cómputo de la Universidad en unidades externas, para realizar esta acción se debe contar con autorización a su jefe inmediato. La copia, sustracción, daño intencional o utilización para fines distintos a las labores propias de la Universidad, esto es considerado una falta grave, esto de acuerdo con la Ley 734 de 2002, Artículo 50. Faltas graves y leves “Constituye falta disciplinaria grave o leve, el incumplimiento de los deberes, el abuso de los derechos, la extralimitación de las funciones, o la violación al régimen de prohibiciones, impedimentos, inhabilidades, incompatibilidades o conflicto de intereses consagrados en la Constitución o en la ley”.
- Periódicamente, la Oficina Asesora de Tecnologías de la Información y las Comunicaciones efectuará la revisión de los programas utilizados en cada dependencia. La descarga, instalación o uso de aplicativos o programas informáticos no autorizados será considera como una violación a las Políticas de Seguridad de la Información.
- Todos los requerimientos de aplicativos, sistemas y equipos informáticos deben ser solicitados por el Jefe de la dependencia a través de la mesa de servicio.
- Estarán bajo custodia de la Oficina Asesora de Tecnologías de la Información y las Comunicaciones los medios magnéticos o electrónicos que vengan originalmente con el software para uso de las funciones administrativas y sus respectivos manuales y licencias de uso, al igual que las claves para descargar el software de fabricantes de sus páginas web o sitios en internet y las claves de administración

de los equipos informáticos, sistemas de información o aplicativos. Los medios manuales y licencias de uso, las claves para descargar el software de fabricantes de sus páginas web o sitios en internet y las claves de aplicativos que no son para uso de las funciones administrativas, estarán a cargo de jefe de la dependencia que solicita el software o de la persona que este designe.

- En caso de ser necesario, el c o el Oficial de Seguridad de la Información de la Oficina de Protección al Patrimonio podrán acceder a revisar cualquier tipo de activo de información y material que los usuarios creen, almacenen, envíen o reciban, a través de Internet o de cualquier otra red o medio, en los equipos informáticos a su uso. previa autorización de la Oficina de Control Interno de Gestión u Oficina de Control Interno Disciplinario.
- Los recursos informáticos de la Universidad no podrán ser utilizados, sin previa autorización escrita, para divulgar, propagar o almacenar contenido personal o comercial de publicidad, promociones, ofertas, malware, propaganda política, material religioso o cualquier otro uso que no esté autorizado.
- Los usuarios no deben realizar intencionalmente actos que impliquen un mal uso de los recursos tecnológicos o que vayan en contravía de las políticas de seguridad de la información entre ellos envíos o reenvíos masivos de correos electrónicos o spam, práctica de juegos en línea, uso permanente de redes sociales personales, conexión de periféricos o equipos que causen molestia a compañeros de trabajo.
- Los usuarios no podrán efectuar ninguna de las siguientes labores sin previa autorización del Área de Tecnologías y Sistemas de la Información:
    - Instalar software en los equipos de cómputo propiedad de la Universidad Militar Nueva Granada.
    - Bajar o descargar software de Internet u otro servicio en línea en cualquier en los equipos de cómputo propiedad de la Universidad Militar Nueva Granada.
    - Modificar, revisar, transformar o adaptar cualquier software propiedad de la Universidad Militar Nueva Granada.
    - Descompilar o realizar ingeniería inversa en cualquier software de la Universidad Militar Nueva Granada.
    - Copiar o distribuir cualquier software de propiedad de la Universidad Militar Nueva Granada.
    - Cambiar la configuración de hardware de propiedad de la Universidad Militar Nueva Granada.
- Los usuarios deberán informar a través de la Mesa de Servicio o de los correos electrónicos tic.seguridad@unimilitar.edu.co, tic@unimilitar.edu.co, protección.patrimonio@unimilitar.edu.co o a través su Jefe Inmediato, sobre cualquier violación y/o debilidad de la Política de Seguridad de la Información de la Universidad que tenga conocimiento.

- El usuario será responsable de todas las transacciones o acciones efectuadas con su cuenta de usuario asignada por la Universidad.
- Ningún usuario deberá acceder a los servicios informáticos ofrecidos por la universidad, utilizando una cuenta de usuario o clave de otro usuario.
- Los usuarios no están autorizados a colocar cualquier equipo que propague la red administrativa o WIFI de la Universidad ya que esto compromete la seguridad de la Información.
- Todo archivo o software descargado o recibido a través de medio magnético, electrónico o descarga de Internet, deberá ser revisado para detección cualquier tipo de malware antes de ser instalados.
- Todos los archivos provenientes de equipos externos, deben ser revisados para detección de virus antes de ser utilizados.
- Todo cambio a la infraestructura informática deberá estar avalado por Oficina Asesora de Tecnologías de la Información y las Comunicaciones.
- La información de la Universidad debe ser respaldada de forma frecuente, almacenada en lugares apropiados en los cuales se pueda garantizar que la información esté segura y podrá ser recuperada en caso de un desastre o de incidentes con los equipos de procesamiento.
- Los funcionarios deberán realizar la devolución de todos los activos físicos, electrónicos y activos de información asignados por la Universidad en el proceso de desvinculación, de igual manera deberán documentar y entregar al funcionario destinado por la universidad los conocimientos importantes que posee de la labor que ejecutan.

4.5. POLÍTICA DE USO DE INTERNET.

La Entidad permite el acceso a servicio de internet, estableciendo lineamientos que garanticen la navegación segura y el uso adecuado de la red por parte de los usuarios finales, evitando errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones.

- Los Vicerrectores o Jefes de Oficina pueden solicitar los cambios en los permisos de navegación a los usuarios de la Universidad, adicionalmente el Oficial de Seguridad de la Información podrá recomendar el cambio de permisos. Sin embargo, el Jefe de la Oficina Asesora de Tecnologías de la Información y las Comunicaciones es el único que puede autorizar la realización de los cambios.
- La Oficina Asesora de Tecnologías de la Información y las Comunicaciones implementa herramientas para evitar la descarga de software no autorizado o código malicioso en los equipos institucionales así mismo controla el acceso a la información contenida en portales de almacenamiento en internet para prevenir la fuga de información.

- Los usuarios que realicen funciones de docencia, investigación, y extensión tienen acceso a redes sociales, sistemas de mensajería instantánea, acceso a sistemas de almacenamiento en la nube públicas y cuentas de correo no institucional.
- Los usuarios que utilicen los activos de información de la Universidad tienen restringido el acceso a redes sociales, sistemas de mensajería instantánea, acceso a sistemas de almacenamiento en la nube públicas y cuentas de correo no institucional. En caso de ser requerido por las funciones del cargo, el jefe inmediato del funcionario debe remitir la solicitud a Jefe de la Oficina Asesora de Tecnologías de la Información y las Comunicaciones, para que sea autorizado y será objeto de auditorías de seguridad.
- La infraestructura, servicios y tecnologías usados para acceder a internet es propiedad de la Universidad Militar Nueva Granada, por lo tanto, se reserva el derecho de monitorear el tráfico de internet y el acceso la información, respetando en todo momento el derecho a la privacidad y a la seguridad de los datos personales consagrados en la Ley 1581 de 2012.
- No se permite la navegación a sitios con contenidos contrarios a la ley o que representen peligro para la entidad como: pornografía, terrorismo, hacktivismo, segregación racial u otras fuentes definidas por la Universidad. El acceso a este tipo de contenidos con propósitos de estudio de seguridad o de investigación, debe contar con la autorización expresa de la Vicerrectoría de Investigaciones, Oficina de Protección al Patrimonio y la Oficina de Control Interno de Gestión.
- La Oficina Asesora de Tecnologías de la Información y las Comunicaciones implementa herramientas para evitar la descarga de software no autorizado o código malicioso en los equipos institucionales así mismo controla el acceso a la información contenida en portales de almacenamiento en el internet para prevenir la fuga de información.
- La descarga de archivos de Internet debe ser con propósitos laborales y de forma razonable para no afectar el servicio.

4.5.2 PERFILES DE NAVEGACIÓN EN INTERNET

Los perfiles serán asignados a la Comunidad Universitaria, que por su cargo y funciones a desempeñar requiera tener acceso a servicios de navegación de internet, por lo cual la Universidad define los siguientes perfiles para los usuarios.

Los perfiles de navegación de internet relacionados a continuación incluyen características de los sitios y servicios web aprobados por la Universidad, no obstante, los sitios que las herramientas de seguridad perimetral identifiquen como no confiables, serán bloqueados.

La asignación de perfiles de navegación, acceso a aplicativos y la asignación de roles debe ser asignado de acuerdo con las funciones que el usuario desempeñe en la Universidad.

4.5.3 FUNCIÓN DIRECTIVOS

Este perfil tiene acceso a Internet, Intranet, almacenamiento en la nube bajo el dominio @unimilitar.edu.co, redes sociales, chats no Institucionales, almacenamiento público, correos personales. No tiene acceso a páginas cuyo contenido haya sido bloqueado por las autoridades colombianas.

4.5.4 FUNCIÓN ADMINISTRATIVAS

Este perfil tiene acceso a Internet, Intranet, almacenamiento en la nube bajo el dominio @unimilitar.edu.co. No tiene acceso a redes sociales, chats no Institucionales, almacenamiento público, correos personales y páginas cuyo contenido haya sido bloqueado por las autoridades colombianas.

4.5.5 FUNCIÓN DOCENCIA E INVESTIGACIÓN

Este perfil tiene acceso a Internet, Intranet, almacenamiento en la nube bajo el dominio @unimilitar.edu.co, redes sociales, chats no Institucionales, almacenamiento público, correos personales. No tiene acceso a páginas cuyo contenido haya sido bloqueado por las autoridades colombianas.

4.5.6 LABORATORIOS

Este perfil tiene acceso a Internet, almacenamiento en la nube bajo el dominio @unimilitar.edu.co, redes sociales, chats no Institucionales, almacenamiento público, correos personales. No tiene acceso a páginas cuyo contenido haya sido bloqueado por las autoridades colombianas.

4.5.7 ESTUDIANTES

Este perfil tiene acceso a Internet, almacenamiento en la nube bajo el dominio @unimilitar.edu.co, redes sociales, chats, almacenamiento público, correos personales. No tiene acceso a páginas cuyo contenido haya sido bloqueado por las autoridades colombianas. La conexión de estos usuarios se debe realizar a través de la red inalámbrica pública y en la red destinada a funciones académicas.

4.5.8 INVITADOS

Este perfil tiene acceso a Internet, redes sociales, chats, almacenamiento público, correos personales. No tiene acceso a páginas de contenido que vaya en contra de las normas colombianas e internacionales. La conexión de estos usuarios se debe realizar a través de la red inalámbrica pública.

4.6. POLÍTICA DE CLASIFICACIÓN DE LA INFORMACIÓN.

La Universidad Militar Nueva Granada consciente de la necesidad de asegurar que la información reciba el nivel de protección apropiado de acuerdo al tipo de clasificación establecido por la Ley 1712 de 2014, define reglas de cómo clasificar la información, liderado por el proceso de Gestión Documental.

- Se considera información toda forma de comunicación o representación de conocimiento o datos digitales, escritos en cualquier medio, ya sea magnético, papel, visual u otro que genere la Universidad Militar Nueva Granada como:
  - Formularios.
  - Información en los sistemas, equipos informáticos, medios magnéticos, electrónicos o medios físicos como papel.
  - Otros soportes magnéticos, electrónicos removibles, móviles o fijos.
  - Información o conocimiento transmitido de manera verbal o por cualquier otro medio de comunicación.
- Los usuarios responsables de la información, deben minimizar los riesgos a los que está expuesta la información de sus áreas, teniendo en cuenta que la información pueda ser copiada, divulgada, modificada o destruida física o digitalmente por personal interno o externo.
- Un activo de información es un elemento definible e identificable que almacena registros, datos o información en cualquier tipo de medio y que es reconocida como valiosa para la Universidad, independiente del tipo de activo, se deben considerar las siguientes características.
  - El activo de información es reconocido como valioso para la Universidad, debido a que genera valor a las funciones misionales de la Universidad.
  - No es fácilmente reemplazable sin incurrir en costos, habilidades especiales, tiempo, recursos o la combinación de los anteriores.
  - Forma parte de la identidad de la organización y sin el cual la Universidad puede estar en algún nivel de riesgo.
  - Los niveles de clasificación de la información valiosa que se ha establecido son:
    - Información Pública Reservada
    - Información Pública Clasificada (Privada y Semiprivada)
    - Información Pública.

- Las reglas Gestión Documental y Clasificación de la Información serán dadas por la Sección de Gestión Documental.

4.7. POLÍTICA DE MANEJO DISPOSICIÓN DE INFORMACIÓN, MEDIOS Y EQUIPOS

La Universidad establece actividades para evitar la divulgación, la modificación, el retiro o la destrucción no autorizada de información almacenada en los medios proporcionados, velando por la disponibilidad y confidencialidad de la información.

Los medios y equipos donde se almacena, procesa o comunica la información, se deben mantener con las medidas de protección físicas y lógicas, que permitan su monitoreo y correcto estado de funcionamiento, para ello se debe realizar los mantenimientos preventivos y correctivos que se requieran.

Se debe realizar el procedimiento de borrado seguro en los equipos de cómputo y demás dispositivos que lo requieran, una vez el funcionario haya sido retirado de la entidad.

Está restringida la copia de archivos en medios removibles de almacenamiento, por lo cual se deshabilita la opción de escritura en dispositivos USB, unidades ópticas de grabación en todos los equipos de cómputo institucionales que brinden apoyo a las funciones administrativas; la autorización de uso de los medios removibles debe ser tramitada a través de la Oficina Asesora de Tecnologías de la Información y las Comunicaciones previo visto bueno de la Oficina de Protección al Patrimonio y será objeto de auditorías de seguridad mediante el módulo de prevención de pérdidas de datos de la entidad

Los usuarios que realicen funciones de docencia, investigación y extensión tienen acceso a medios removibles de almacenamiento.

4.8. POLÍTICA DE CONTROL DE ACCESO.

La Universidad define las reglas para asegurar un acceso controlado, físico o lógico, a la información y a la plataforma informática de la Universidad, considerándose como importantes para el SGSI.

La conexión remota a la red de área local de la Universidad debe realizarse a través de una conexión VPN, segura suministrada por la Universidad, la cual debe ser aprobada, registrada y auditada, por la Sección de Análisis y Seguridad de la Información Oficina Asesora de Tecnologías de la Información y las Comunicaciones. La conexión por VPN se entrega a solicitante por un tiempo determinado y esta conexión caducará después de este tiempo. El uso de la VPN se debe realizar desde un equipo de cómputo en una locación segura, no se permite el acceso desde sitios de acceso público. No se permite conexiones a través de aplicaciones de escritorio remoto como AnyDesk o Teamviewer debido a que no se encuentran licenciados por la universidad.

La creación de cuenta de usuario para sistemas de Información se realiza través de la mesa de servicio, la solicitud debe ser realizada por el jefe de la dependencia a la cual pertenece el funcionario, indicando claramente los perfiles a los que se debe tener acceso.

La División de Gestión de Talento Humano, debe notificar del traslado o la desvinculación de un funcionario de la Universidad, con el fin que sean removidos los permisos que se tienen sobre los sistemas de información.

También se autorizará el acceso a la plataforma de tecnología y sistemas de información a proveedores de servicios, que por la naturaleza de sus actividades requieran acceder a estos servicios en forma periódica previa firma del formato de confidencialidad previa autorización del supervisor del contrato y visto bueno del Líder de la Sección de Análisis y Seguridad de la Información de la Oficina Asesora de Tecnologías o el Jefe de la Oficina Asesora de Tecnologías de la Información y las Comunicaciones.

4.9. POLÍTICA DE ESTABLECIMIENTO, USO Y PROTECCIÓN DE CLAVES DE ACCESO.

Ningún usuario deberá acceder a los servicios informáticos o sistemas de información de la Universidad, utilizando una cuenta de usuario o clave de otro usuario.

La Universidad suministrará a los usuarios las claves de acceso a los servicios informáticos y sistemas de información a los que hayan sido autorizados, las claves son de uso personal e intransferible.

El cambio de contraseña sólo podrá ser solicitado por el titular de la cuenta, a través de la mesa de servicio, en donde se llevará a cabo la validación de los datos personales. En ningún caso puede ser solicitado el cambio de contraseña de un usuario diferente al asignado. Las excepciones son las expresadas en la Ley Colombiana.

4.10. POLÍTICA DE USO DE DISCOS VIRTUALES.

La información institucional que se trabaje en los equipos de cómputo de la universidad debe ser resguardada en el almacenamiento virtual que posee disponible, esto con el fin de asegurar la información por daño del hardware.

Está prohibido almacenar archivos que incumplan leyes de derechos de autor, información no relacionada con las funciones asignadas al usuario, información personal calificada como sensible de acuerdo con la ley 1581 de 2012, o aquellas que la

modifiquen, información de naturaleza íntima del usuario. Archivos que puedan ocasionar o constituir riesgos informáticos, como Software o código malicioso.

Se prohíbe extraer, divulgar o publicar información de cualquiera de los discos virtuales, sin expresa autorización del jefe inmediato.

4.11. POLÍTICA DE USO DE PUNTOS DE RED DE DATOS.

Se controlará el acceso a los servicios de la red tanto internos como externos. La sección de Análisis y Seguridad de la Información de la Oficina Asesora de Tecnologías de la Información y las Comunicaciones tendrá a cargo el otorgamiento del acceso a los servicios y recursos de red.

El acceso a Internet será utilizado con propósitos educativos y/o que se relacionen con las labores institucionales. La Oficina Asesora de Tecnologías de la Información y las Comunicaciones definirá el procedimiento para solicitar y aprobar accesos a Internet.

El uso de las Red de Datos de la Universidad debe limitarse a tareas educativas y administrativas, dependiendo de la red se encuentre el usuario, siendo responsabilidad del usuario el no realizar un uso ilícito de la red.

La Universidad a través de la Oficina Asesora de Tecnologías de la Información y las Comunicaciones de la Información 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.

El uso indebido de las Redes de Datos, es causal de falta disciplinaria, según corresponda al caso de acuerdo con este manual o por las leyes nacionales vigentes.

No se pueden colocar dispositivos sobre la red de datos de la universidad sin previa autorización de la Oficina Asesora de Tecnologías de la Información y las Comunicaciones de la Información.

4.12. POLÍTICA DE USO DE IMPRESORAS Y DEL SERVICIO DE IMPRESIÓN.

Los documentos que se impriman en los equipos multifuncionales que pertenecen a la Universidad Militar Nueva Granada o que están contratadas en la modalidad de Outsoursing deben ser de carácter institucional.

Es responsabilidad del usuario conocer el adecuado manejo de los equipos multifuncionales o de impresión para que no se afecte su correcto funcionamiento.

Ningún usuario debe realizar labores de reparación o mantenimiento de los equipos multifuncionales. En caso de presentarse alguna falla, ésta se debe reportar a la mesa de servicio.

Los funcionarios en el momento de realizar impresiones de documentos con clasificación pública reservada o información pública clasificada (privada o semiprivada), debe mantener control de la impresora, por lo cual no la deberán dejar desatendida, preservando la confidencialidad de la información.

La responsabilidad de los documentos impresos o escaneados en los equipos multifuncionales o de impresión de la Universidad, será asumida por el usuario de sistema desde el cual se envía a imprimir o a escanear los documentos.

4.13. POLÍTICA DE ACCESOS A LOS CENTROS DE DATOS Y A LOS CUARTOS TÉCNICOS

Los funcionarios de la Oficina Asesora de Tecnologías de la Información y las Comunicaciones, pertenecientes a la Sección de Servicios Tecnológicos y la Sección de Análisis y Seguridad de la Información son los únicos autorizados para el Ingreso a los Centros de Datos y a los Cuartos Técnicos de la Universidad.

El Ingreso de contratistas o terceros a los centros de datos, con el fin de realizar labores de mantenimiento de la Infraestructura, debe ser autorizado por el Líder de la Sección de Servicios Tecnológicos de la Oficina Asesora de Tecnologías de la Información y las Comunicaciones.

El enrolamiento de los funcionarios autorizados a ingresar a los Centros de Datos se realiza por el Líder de la Sección de Análisis y Seguridad de la Información de la Oficina Asesora de Tecnologías de la Información y las Comunicaciones. En caso de emergencia la oficina de Protección al Patrimonio puede liberar las puertas de los centros de datos por el sistema de control de acceso.

4.13.1. POLÍTICAS DE SEGURIDAD CENTROS DE DATOS Y CUARTOS TÉCNICOS.

En las instalaciones de los centros de datos o de los cuartos técnicos, no está permitido:

- Fumar.
- Introducir alimentos o bebidas
- El porte de armas de fuego, corto punzantes o similares.
- Mover, desconectar y/o conectar equipo de cómputo sin autorización.

- Modificar la configuración del equipo o intentarlo sin autorización.
- Alterar software instalado en los equipos sin autorización.
- Alterar o dañar las etiquetas de identificación.
- Extraer información de los equipos en dispositivos externos.
- Abuso o mal uso de los sistemas de información.
- Toda persona debe hacer uso únicamente de los equipos y accesorios que les sean asignados y para los fines que se les autorice.

Cada rack contiene llave de ingreso o tarjeta de proximidad, así como cada cuarto técnico, las cuales deben permanecer bajo custodia de la Oficina Protección al Patrimonio.

El Jefe de la Oficina Asesora de Tecnologías de la Información y las Comunicaciones, el Líder de la Sección de Servicios Tecnológicos o el Líder de Sección de Análisis y Seguridad de la Información pueden autorizar el ingreso de cualquier elemento o herramienta a los Centros de Datos o Cuartos Técnicos.

La grabación de vídeo o toma de fotografías en el centro de datos o en los cuartos técnicos debe estar expresamente autorizada por el Jefe de la Oficina Asesora de Tecnologías de la Información y las Comunicaciones, el Líder de la Sección de Servicios Tecnológicos o el Líder de la Sección de Análisis y Seguridad de la Información

La Oficina Asesora de Tecnologías de la Información y las Comunicaciones debe garantizar que el control de acceso a los Centros de Datos o Cuartos Técnicos.

4.13.2. POLÍTICAS DE SEGURIDAD DE LOS EQUIPOS CÓMPUTO

El Universidad establece reglas que permitan orientar usuarios en la correcta utilización de estaciones de trabajo.

Las Directrices de uso de equipos de cómputo que se encuentran definidas son:

- La instalación de software en los computadores suministrados por la Universidad, es una función exclusiva del funcionario de la Oficina Asesora de Tecnologías de la Información y las Comunicaciones destinado para este fin, para los equipos destinados a funciones Administrativas y Docentes, para los equipos cómputo de laboratorios, esta función es asumida por el laboratorista.
- Los usuarios no deben almacenar en los discos duros de los equipos de cómputo o discos virtuales asignados por la universidad, archivos de vídeo, música, fotos y cualquier tipo de archivo que no sean de carácter institucional.

- Los equipos de cómputo deben ser instalados en las áreas de trabajo seguras que cumplan con la normatividad de Seguridad y Salud en el Trabajo, deben contar con protecciones en el suministro de energía, las cuales deben ser certificadas por la División de Servicios Generales en la Sede Bogotá o por la Dirección Administrativa del Campus Nueva Granada.
- La red de energía regulada de los puestos de trabajo solo se pueden conectar equipos cómputo, escáneres e impresoras que sean propiedad de la Universidad Militar Nueva Granada o presten servicio en cualquier modalidad de contratación. Cualquier otro elemento debe conectarse a la red no regulada.

4.14. POLÍTICA DE ESCRITORIO LIMPIO.

Todos los funcionarios y contratistas de la Universidad deben conservar su escritorio libre de información, propia de la entidad, que pueda ser alcanzada, copiada o utilizada por personal que no tenga autorización para su uso o conocimiento.

Los usuarios de los sistemas de información y comunicaciones de la Universidad Militar Nueva Granada deben bloquear la pantalla de su computador, en los momentos que no esté utilizando el equipo de cómputo o cuando por cualquier motivo deba dejar su puesto de trabajo.

Los usuarios de los sistemas de información y comunicaciones de la Universidad deben cerrar las aplicaciones y servicios de red cuando no necesite de su utilización o se retire del puesto de trabajo.

Al imprimir documentos con información pública reservada o pública clasificada, deben ser retirados del equipo multifuncional una vez sean impresos y no se deben dejar en el escritorio sin custodia.

4.15. POLÍTICA DE SEGURIDAD DE LAS OPERACIONES.

4.15.1. SEGURIDAD DEL CABLEADO

Los cableados deben estar claramente marcados para identificar fácilmente los elementos conectados y evitar desconexiones erróneas en los cuartos técnicos en las tomas de conexión en los puestos de trabajo.

Deben existir planos que describan las conexiones del cableado y se deben exigir para las nuevas construcciones que se realicen o para las adecuaciones en áreas existentes.

El acceso a los centros de cableado (Racks), debe estar protegido.

La Oficina Asesora de Tecnologías de la Información y las Comunicaciones establece un programa de revisiones o inspecciones físicas al cableado, con el fin de detectar dispositivos no autorizados.

4.15.2. MANTENIMIENTO DE LOS EQUIPOS

La Universidad Militar Nueva Granada debe mantener contratos de soporte y mantenimiento de los equipos críticos, y es responsable de renovar o de contratar el mantenimiento el área encargada del equipo.

Las actividades de mantenimiento tanto preventivo como correctivo deben registrarse para cada elemento. Las actividades de mantenimiento de los servidores, elementos de comunicaciones, energía o cualquiera que pueda ocasionar una suspensión en el servicio, deben ser programadas y realizadas por personal autorizadas por la Vicerrectoría Administrativa, Vicerrectoría Académica y la Oficina Asesora de Tecnologías de la Información y las Comunicaciones para la Sede Bogotá y por la Vicerrectoría del Campus Nueva Granada, Vicerrectoría Académica y la Oficina Asesora de Tecnologías de la Información y las Comunicaciones para la Sede Campus Nueva Granada.

Los equipos que requieran salir de las instalaciones de la universidad para reparación o mantenimiento, deben estar debidamente autorizados con el Formato Salidas Transitorias; se debe garantizar que dichos elementos no se encuentra información clasificada de acuerdo a los niveles de clasificación de la información pública reservada o información pública clasificada (privada o semiprivada).

Cuando un equipo de cómputo vaya a ser reasignado o retirado de servicio debe diligenciar el formato de Reintegro de Elementos o de Traspasos, así mismo debe garantizarse la eliminación de toda información existente en los equipos. El traslado entre dependencias de la Universidad de un equipo de cómputo, está a cargo de la División de Servicios Generales, para el control de inventarios.

4.16. POLÍTICA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.

En caso de desarrollos propios la Oficina Asesora de Tecnologías de la Información y las Comunicaciones debe separar los ambientes de prueba y producción, esto con el fin de evitar problemas con los sistemas de información existentes.

La Oficina Asesora de Tecnologías de la Información y las Comunicaciones debe coordinar con los usuarios funcionales de las aplicaciones las pruebas de

funcionamiento y de seguridad a los nuevos sistemas, actualizaciones o aplicaciones en ambiente de pruebas, para validar la operatividad de estos, previo a la aprobación e implementación.

La Oficina Asesora de Tecnologías de la Información y las Comunicaciones desarrollara o adquirirá el software requerido por la Universidad de manera coordinada con él o las áreas que manifieste la necesidad del software, la Oficina Asesora de Tecnologías de la Información y las Comunicaciones establecerá claramente los requerimientos funcionales, operacionales y especificaciones técnicas para la adquisición o desarrollo de sistemas de información y comunicaciones, contemplando requerimientos de seguridad de la información.

Todo nuevo hardware y software que se vaya a adquirir y conectar a la plataforma tecnológica de la Universidad, por cualquier área de la Universidad, deberá ser autorizado por la Oficina Asesora de Tecnologías de la Información y las Comunicaciones para su correcto funcionamiento.

Cualquier copia de un programa original será considerada como una copia no autorizada y su utilización conlleva a las sanciones administrativas y legales pertinentes.

La instalación del software en los equipos de cómputo de la Universidad, se realizará únicamente a través de solicitud en la Mesa de Servicios, previa verificación del licenciamiento.

La Oficina Asesora de Tecnologías de la Información y las Comunicaciones implementará reglas y herramientas que restrinjan la instalación de software no autorizado en los equipos de cómputo.

El software proporcionado por la Universidad no puede ser copiado o suministrado a terceros.

En los equipos cómputo de la Universidad solo podrá utilizar el software licenciado y adquirido en concordancia con el proceso de Contratación y Adquisiciones de la Universidad.

Para la adquisición y actualización de software, es necesario tener visto bueno de la Oficina Asesora de Tecnologías de la Información y las Comunicaciones con su

justificación, quien analizará las propuestas presentadas para su evaluación y aprobación.

En los equipos de cómputo que cumplan funciones Administrativas se encuentra prohibido el uso e instalación de juegos. En los equipos de cómputo que brindan apoyo a funciones de docencia, investigación, y extensión se instalara previa autorización del Jefe del área.

La Oficina Asesora de Tecnologías de la Información y las Comunicaciones debe implementar actividades para la protección contra códigos maliciosos.

La Sección de Sistemas de Información de la Oficina Asesora de Tecnologías de la Información y las Comunicaciones debe implementar métodos o técnicas para el desarrollo de software seguro, estas deben incluir definiciones y requerimientos de seguridad, que le permita a los desarrolladores aplicarlas de manera clara y eficiente.

La Oficina Asesora de Tecnologías de la Información y las Comunicaciones debe implementar y aplicar metodologías que permitan proteger las transacciones de los servicios de aplicaciones de la Universidad.

Se debe gestionar el control de cambios de las aplicaciones, basados en el ciclo de vida, asegurando la integridad desde las primeras etapas de diseño, pasando por mantenimiento.

4.17. POLÍTICA DE RESPALDO Y RESTAURACIÓN DE INFORMACIÓN.

El Objetivo de este aparte es proporcionar medios de respaldo adecuados para asegurar que toda la información esencial y el software, se pueda recuperar después de una falla, garantizando que la información y la infraestructura de software crítica de la entidad, sean respaldadas y puedan ser restauradas en caso de una falla o desastre natural.

La restauración de copias de respaldo en ambientes de producción debe estar debidamente aprobada por el dueño de la información, solicitadas a través mesa de servicios y se deben realizar de acuerdo con las tablas de retención documental vigentes para la Universidad.

Semanalmente el líder de la Sección de Servicios Tecnológicos y el administrador de plataforma de copias de seguridad, verificarán la correcta ejecución de estos procesos de copias de respaldo, suministrando los medios requeridos y controlando la vida útil de cada medio empleado.

Los medios que vayan a ser eliminados o que cumplan el periodo de retención deben surtir un proceso de borrado seguro y posteriormente serán eliminados o destruidos de forma adecuada.

El administrador de la plataforma de copias de seguridad de la Universidad, debe generar tareas de restauración aleatorias de la información y deben ser documentadas.

La información a la cual se le debe realizar respaldo, los tiempos de retención, proceso de restauración y la custodia de la información se definen en el Procedimiento de Respaldo, Custodia y Recuperación de la Información.

4.18. POLÍTICA PARA REALIZACIÓN DE COPIAS EN LOS EQUIPOS DE COMPUTO.

El uso de dispositivos de almacenamiento externo, pueden ocasionalmente generar riesgos para la Universidad al ser conectados a los computadores, ya que son susceptibles de transmisión de virus informáticos o pueden ser utilizados para la extracción de información. Para utilizar dispositivos de almacenamiento externo se debe obtener aprobación formal de la Sección de Análisis y Seguridad de la Información de la Oficina Asesora de Tecnologías de la Información y las Comunicaciones y la Oficina de Protección al Patrimonio.

Los equipos de cómputo destinado que brindan apoyo a funciones de docencia, investigación, y extensión se les permite tener acceso a la utilización de dispositivos de almacenamiento externo.

4.19. POLÍTICA DE GESTIÓN DE VULNERABILIDADES

La Oficina Asesora de Tecnologías de la Información y las Comunicaciones de Información en coordinación con el CSIRT de la Universidad, realizará pruebas técnicas de vulnerabilidad a la plataforma tecnológica por lo menos una vez al año.

La Oficina Asesora de Tecnologías de la Información y las Comunicaciones implementará un programa de gestión de vulnerabilidades técnicas que incluya el plan de tratamiento de las mismas, el cual deberá ser aprobado por el Comité de Gestión de Desempeño Institucional.

4.20. POLÍTICA DE SEGURIDAD DE LAS COMUNICACIONES.

La Oficina Asesora de Tecnologías de la Información y las Comunicaciones debe interconectar las diferentes sedes de la Universidad indicando los estándares técnicos de configuración de red y de seguridad de la información

La Oficina Asesora de Tecnologías de la Información y las Comunicaciones debe implementar sistemas de protección entre las diferentes redes de la Universidad. Identificar y documentar los servicios, protocolos y puertos autorizados en las redes de datos e inhabilitar o eliminar los servicios, protocolos y puertos no utilizados.

La Oficina Asesora de Tecnologías de la Información y las Comunicaciones debe segmentar la red, de modo que permita separar los grupos de servicios de información

4.21. POLÍTICA PARA LA TRANSFERENCIA DE INFORMACIÓN.

Los lineamientos para la transferencia de datos se rigen por el Manual Integrado de Protección de Datos Personales de la Universidad Militar Nueva Granada.

4.22. POLÍTICA DE USO DE LOS SISTEMAS DE INFORMACIÓN

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.

Los sistemas de información y las herramientas asociadas a estos sólo podrán ser utilizados por personal debidamente autorizado y será responsabilidad de cada jefe de área definir las tareas que conllevan el acceso a estos.

Cada usuario será individualmente responsable por el manejo adecuado de las claves de acceso o contraseñas asignadas y de la información registrada en los sistemas.

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 Gestión 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.

El uso de los recursos de sistemas de información o equipo que tenga como objetivo cualquier tipo de ganancia económica personal está prohibido.

El acceso no autorizado a los sistemas de información de la Universidad está prohibido y es considerada una falta grave, esto de acuerdo con la Ley 734 de 2002,

Artículo 50. Faltas graves y leves “Constituye falta disciplinaria grave o leve, el incumplimiento de los deberes, el abuso de los derechos, la extralimitación de las funciones, o la violación al régimen de prohibiciones, impedimentos, inhabilidades, incompatibilidades o conflicto de intereses consagrados en la Constitución o en la ley”, Acuerdo 2 de 2015, Artículo 107. Faltas Disciplinarias “b) Faltas graves: 1. Actuar contrariamente a los estatutos, reglamentos y normas internas de la Universidad u obstaculizar o impedir la aplicación de los mismos.” para estudiantes de pregrado y Acuerdo 2 de 2017, Artículo 75. Faltas Disciplinarias “b) Faltas graves: 1. Actuar contrariamente a los estatutos, reglamentos y normas internas de la Universidad u obstaculizar o impedir la aplicación de los mismos.” para estudiantes de posgrado.

Ningún funcionario debe usar la clave o contraseña de otro funcionario, y de la misma manera ninguno debe dar a conocer su clave 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 que destine el ente de control de seguridad de la información de la Universidad a realizar esta labor, previa firma de acta de confidencialidad, y este debe generar el procedimiento de cambio de contraseña una vez termine la labor.

La información que reposa en las bases de datos 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.

La información almacenada en las bases de datos 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.

4.22.1. USO INDEBIDO DE LOS SISTEMA DE INFORMACIÓN POR PARTE DE UN FUNCIONARIO:

El uso indebido demostrado los Sistemas de Información por parte de un funcionario es considerada una falta grave, esto de acuerdo con la Ley 734 de 2002, Artículo 50. Faltas graves y leves “Constituye falta disciplinaria grave o leve, el incumplimiento de los deberes, el abuso de los derechos, la extralimitación de las funciones, o la violación al régimen de prohibiciones, impedimentos, inhabilidades, incompatibilidades o conflicto de intereses consagrados en la Constitución o en la ley”

4.22.2. USO INDEBIDO DE LOS SISTEMA DE INFORMACIÓN POR PARTE DE UN ESTUDIANTE:

El uso indebido demostrado los Sistemas de Información por parte de un estudiante es considerada una falta grave, esto de acuerdo con la Acuerdo 2 de 2015, Artículo 107. Faltas Disciplinarias “b) Faltas graves: 1. Actuar contrariamente a los estatutos, reglamentos y normas internas de la Universidad u obstaculizar o impedir la aplicación de los mismos.” para estudiantes de pregrado y Acuerdo 2 de 2017, Artículo 75. Faltas Disciplinarias “b) Faltas graves: 1. Actuar contrariamente a los estatutos, reglamentos y normas internas de la Universidad u obstaculizar o impedir la aplicación de los mismos.” para estudiantes de posgrado.

4.23. POLÍTICA DE USO DE CORREO ELECTRÓNICO.

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
Vicerrectoría	Siglas de la Vicerrectoría	@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 Jefatura	@unimilitar.edu.co	Oficina o dependencia
Correos especiales	Nombre del correo. Ejemplo: protecciondedatos	@unimilitar.edu.co	Personal
Funcionario, Estudiante de Pregrado o Posgrado	Nombre.Apellido + Condicional *	@unimilitar.edu.co	Personal

* Si algún funcionario tiene alguna coincidencia con otro en su nombre y apellido al momento de crear el correo electrónico, se adicionará un condicional el cual será la inicial del segundo apellido y si también coinciden la letra del segundo apellido se adicionará un número consecutivo.

La creación de los buzones de correo electrónico de los estudiantes de la Universidad Militar Nueva Granada, se realiza en un periodo de 5 días hábiles después de haber legalizado la matrícula.

La creación de los buzones de correo electrónico de los funcionarios de la Universidad Militar Nueva Granada, se realiza en un periodo de 5 días hábiles, una vez sea notificado por resolución el funcionario por la División de Gestión de Talento Humano.

La creación de los buzones de correo electrónico de Dependencias de la Universidad Militar Nueva Granada, se realiza en un periodo de 5 días hábiles después de haber recibido la aprobación de creación por parte de la Vicerrectoría u Oficina a la que pertenece la Dependencia. Todo se cree a una dependencia debe tener un funcionario de planta responsable, esto con el fin de garantizar su correcta utilización.

Todos los usuarios del sistema de correos de la Universidad aceptan los Términos y Condiciones de Uso del Correo Electrónico Universidad Militar Nueva Granada, el cual se anexa al presente manual.

Los comunicados internos de la Universidad Militar deben ser dirigidos a los correos de tipo personal.

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.

El correo electrónico institucional debe ser usado únicamente para propósitos concernientes a las funciones de su cargo.

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.

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.

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 de 1999

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.

Los usuarios de correo electrónico institucional que identifique en su correo contenido sospechoso o con posibles virus, deben notificarlo a la Oficina Asesora de Tecnologías de la Información y las Comunicaciones, y al correo electrónico tic.seguridad@unimilitar.edu.co.

4.23.1. USO INDEBIDO DEL CORREO ELECTRÓNICO POR PARTE DE UN FUNCIONARIO:

El uso indebido demostrado de correo electrónico por parte de un funcionario o la utilización demostrada sin autorización del correo electrónico de otro funcionario o estudiante es considerado una falta grave, esto de acuerdo con la Ley 734 de 2002, Artículo 50. Faltas graves y leves "Constituye falta disciplinaria grave o leve, el incumplimiento de los deberes, el abuso de los derechos, la extralimitación de las funciones, o la violación al régimen de prohibiciones, impedimentos, inhabilidades, incompatibilidades o conflicto de intereses consagrados en la Constitución o en la ley"

4.23.2. USO INDEBIDO DEL CORREO ELECTRÓNICO POR PARTE DE UN ESTUDIANTE:

El uso indebido demostrado de correo electrónico por parte de un estudiante la utilización sin autorización demostrada del correo electrónico de otro funcionario o estudiante es considerada una falta grave, esto de acuerdo con la Acuerdo 2 de 2015, Artículo 107. Faltas Disciplinarias "b) Faltas graves: 1. Actuar contrariamente a los estatutos, reglamentos y normas internas de la Universidad u obstaculizar o impedir la aplicación de los mismos." para estudiantes de pregrado y Acuerdo 2 de 2017, Artículo 75. Faltas Disciplinarias "b) Faltas graves: 1. Actuar contrariamente a los estatutos, reglamentos y normas internas de la Universidad u obstaculizar o impedir la aplicación de los mismos." para estudiantes de posgrado.

4.24. POLÍTICA DE GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN

La Universidad establece como responsable al Líder de la Sección de Análisis y Seguridad de la Información de la Oficina Asesora de Tecnologías de los procedimientos de gestión para el tratamiento de incidentes de seguridad de la información asegurando una respuesta rápida, eficaz y eficiente, quienes investigarán y solucionarán los incidentes presentados, implementando las acciones necesarias para evitar que vuelvan a suceder, así mismo debe escalar los incidentes de acuerdo con la criticidad del mismo.

El único canal acreditado para reportar incidentes de seguridad ante las autoridades y hacer el pronunciamiento oficial ante entidades externas es el Jefe de la Oficina Asesora de Tecnologías de la Información y las Comunicaciones o el funcionario que sea delegado por el Rector de la Universidad.

La Universidad designa la Oficina Asesora de Tecnologías de la Información y las Comunicaciones para responder a los eventos o incidentes de seguridad informática, de acuerdo a las sugerencias, recomendaciones y/o acompañamiento del CSIRT generando el procedimiento de respuesta.

Se debe establecer la implementación de lecciones aprendidas al término del análisis y solución de incidentes de seguridad de la información, estos deben ser socializados a los interesados conservando la confidencialidad de las mismas, de igual manera, serán utilizadas como herramienta para la toma de decisiones y revisiones de la política de seguridad.

El CSIRT debe establecer el procedimiento para la recolección de evidencia digital, siguiendo los lineamientos jurídicos vigentes en Colombia y estándares internacionales.

En el caso que se presente un evento de vulneración a la Seguridad de la Información en el cual se vea involucrada la participación de algún funcionario la Universidad Militar Nueva Granada, debe darse traslado a la Oficina de Control Interno Disciplinario, mediante comunicación remitida por el Sistema de Gestión Documental. Si lo requiere, la Oficina de Control Interno Disciplinario, puede solicitar el apoyo al CSIRT, de la Oficina Asesora de Tecnologías de la Información y las Comunicaciones o de cualquier otra área funcional de la Universidad.

4.25. POLÍTICA DE REVISIONES DE SEGURIDAD DE LA INFORMACIÓN

La Universidad podrá realizar auditorías con personal externo a la entidad al sistema de gestión de seguridad de la información, para la verificación y cumplimiento de objetivos, controles, políticas y procedimientos de seguridad de la Información.

Los Directivos y Jefes de División de la Universidad, deben verificar y supervisar el cumplimiento de las políticas de seguridad de la información en su área de responsabilidad.

La Universidad asigna un funcionario para realizar revisiones esporádicas no programadas con el fin verificar el cumplimiento de las políticas de seguridad de la información en las instalaciones de gobierno

La Oficina de Protección al Patrimonio con apoyo de Oficina Asesora de Tecnologías de la Información y las Comunicaciones debe establecer el procedimiento para revisar periódicamente los sistemas de información con el herramientas automáticas y especialistas técnicos.

4.26. POLÍTICA DE RETENCIÓN Y ARCHIVO DE DATOS.

Las reglas y los principios generales que regulan la función archivística del Estado, se encuentran definidos por la Ley 594 de 2000, la cual es aplicable a la administración pública en sus diferentes niveles producidos en función de su misión y naturaleza.

La ley prevé el uso de las tecnologías de la información y las comunicaciones en la administración, conservación de archivos y en la elaboración e implantación de programas de gestión de documentos.

5. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

Es el conjunto de procedimientos y estrategias definidos para contrarrestar las interrupciones en las actividades misionales de la Universidad, para asegurar sus procesos críticos contra fallas mayores en los sistemas de información o contra desastres y asegurar que las operaciones se recuperen oportuna y ordenadamente, generando un impacto mínimo o nulo ante una contingencia.

Prevenir interrupciones en las actividades de la plataforma tecnológica que van en detrimento de los procesos críticos de tecnología afectados por situaciones no previstas o desastres.

Se debe desarrollar e implantar un Plan de Continuidad del Negocio para asegurar que los procesos misionales de tecnología de la Universidad sean restaurados dentro de escalas de tiempo razonables.

La Universidad deberá tener definido un plan de acción que permita mantener la Continuidad del Negocio teniendo en cuenta los siguientes aspectos:

- Identificación y asignación de prioridades a los procesos críticos de tecnología del Universidad de acuerdo con su impacto en el cumplimiento de la misión de la entidad.
- Documentación de la estrategia de continuidad del negocio.
- Documentación del plan de recuperación del negocio de acuerdo con la estrategia definida anteriormente.
- Plan de pruebas de la estrategia de continuidad del negocio.

La continuidad del negocio deberá ser gestionada por la Oficina de Direccionamiento Estratégico e Inteligencia Competitiva con apoyo de la Oficina Asesora de Tecnologías de la Información y las Comunicaciones.

La alta dirección será la responsable de velar por la implantación de las medidas relativas a la Continuidad del Negocio. Igualmente, de desarrollar las tareas necesarias para el mantenimiento de estas medidas. Se encargará de la definición y actualización de las normas, políticas, procedimientos y estándares relacionados con la Continuidad del Negocio, igualmente velará por la implantación y cumplimiento de las mismas.

6. CUMPLIMIENTO

Los diferentes aspectos contemplados en este Manual son de obligatorio cumplimiento por toda la Comunidad Universitaria. En caso de que se violen las políticas de seguridad ya sea de forma intencional o por negligencia, se tomará las acciones disciplinarias y legales correspondientes, por parte de la Universidad.

El Manual de la Política de Seguridad de la Información debe prevenir el incumplimiento de las leyes, estatutos, regulaciones u obligaciones contractuales que se relacionen con los controles de seguridad.

7. CONTROLES

El Manual de la Política de Seguridad de la Información está soportado en un conjunto de procedimientos que se encuentran documentados en archivos complementarios a este manual. Los usuarios de los servicios y recursos de tecnología pueden consultar los procedimientos en la Intranet o en la página Web de la Universidad.

MARCO LEGAL

- Constitución Política de Colombia 1991.
  - Artículo 15. Reconoce como Derecho Fundamental el Habeas Data.
  - Artículo 20. Libertad de Información.
- Ley 87 de 1993, por la cual se dictan Normas para el ejercicio de control interno en las entidades y organismos del Estado, y demás normas que la modifiquen.
- Ley 734 de 2002, del Congreso de la República de Colombia, Código Disciplinario Único.
- Ley 23 de 1982 de Propiedad Intelectual - Derechos de Autor. Modificada por la 1385 de 2017
- Ley 594 de 2000 - Ley General de Archivos.

- Ley 80 de 1993, Ley 1150 de 2007 y decretos reglamentarios.
- Ley 527 de 1999, por 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.
- Directiva presidencial 02 del año 2000, Presidencia de la República de Colombia, Gobierno en línea.
- Ley 1032 de 2006, por el cual se dictan disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en base de datos personales.
- Ley 1266 de 2007, por la cual se dictan disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en base de datos personales.
- Ley 1273 de 2009, "Delitos Informáticos" protección de la información y los datos.
- Ley 1437 de 2011, "Código de procedimiento administrativo y de lo contencioso administrativo".
- Ley 1581 de 2012, "Protección de Datos personales".
- Ley 1712 de 2014, “De transparencia y del derecho de acceso a la información pública nacional”.
- Ley 962 de 2005. “Simplificación y Racionalización de Trámite. Atributos de seguridad en la Información electrónica de entidades públicas;”
- Ley 1150 de 2007. “Seguridad de la información electrónica en contratación en línea”
- Ley 1341 de 2009. “Tecnologías de la Información y aplicación de seguridad”.
- Decreto 1599 de 2005, por el cual se adopta el Modelo Estándar de Control Interno MECI para el Estado Colombiano.
- Código Penal Colombiano - Decreto 599 de 2000
- Decreto 2609 de 2012, por la cual se reglamenta la ley 594 de 200 y ley 1437 de 2011.
- Decreto 1377 de 2013, por la cual se reglamenta la ley 1581 de 2012.
- Decreto 2952 de 2010. “Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008”.
- Decreto 886 de 2014. “Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012”.
- Decreto 1083 de 2015. “Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012”.
- Decreto 1080 de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del sector cultura”
- CONPES 3701 de 2011 Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 3854 de 2016 Política Nacional de Seguridad digital.

- Acuerdo 2 de 2015 Reglamento General Estudiantil de Pregrado Universidad Militar Nueva Granada.
- Acuerdo 6 de 2018 Reglamento General Estudiantil de Posgrados Universidad Militar Nueva Granada.

REQUISITOS TÉCNICOS

- Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de la seguridad de la información.
- Norma Técnica Colombiana NTC/ISO 17799 Código de práctica para la gestión de la seguridad de la información.
- ISO/IEC 27005 Information technology Systems- Security techniques- information security risk management.
- Modelo Estándar de Control Interno MECI 1000 2da versión "Subsistema: Control de Gestión; Componente: Actividades de Control; Elemento: Monitoreo y Revisión e Información".
- Norma Técnica Colombiana NTC - ISO 19011 "Directrices para la Auditoría de los Sistemas de Gestión de la Calidad y/o Ambiental".

ANEXOS

ANEXO 1. TÉRMINOS Y CONDICIONES DE USO DEL CORREO ELECTRÓNICO

El objeto de estas condiciones de uso del correo electrónico es garantizar la calidad del servicio, así como un uso de acuerdo con las funciones de la Universidad, docencia, investigación, y extensión; sin menoscabar los derechos individuales y las libertades de los usuarios del servicio.

1. ACEPTACIÓN DE LAS CONDICIONES DE USO

Todos los estudiantes, egresados, funcionarios y/o dependencias (a través de un responsable) de la Universidad que utilice este servicio adquiere la condición de usuario del servicio.

La utilización del servicio de correo electrónico de la Universidad Militar Nueva Granada, implica el conocimiento y plena aceptación de las advertencias legales y condiciones que a continuación se especifican:

a. Aceptación, sin reservas, de la Política de Seguridad de la Información de la Universidad Militar Nueva Granada y cualesquiera otras disposiciones o condiciones que la Universidad pueda imponer.
b. Aceptación, sin reservas, de las presentes condiciones de uso y de que estas quedan completadas por cualesquiera disposiciones legales de ámbito nacional que sean de aplicación al uso del correo electrónico.

2. CONDICIONES DE ACCESO

a. La utilización del servicio de correo electrónico de la Universidad Militar Nueva Granada es carácter gratuito.
b. Los usuarios se comprometen a usar sus claves de acceso (nombre y contraseña) de acuerdo con las siguientes restricciones:
   - La contraseña no puede, de ningún modo, infringir los derechos de propiedad industrial e intelectual ni atentar contra el honor y a la propia imagen de terceros.
   - Las claves de acceso son para uso exclusivo del usuario titular, su custodia y correcta utilización son de su responsabilidad. Queda prohibido permitir su utilización a personas no autorizadas.
   - Los usuarios del servicio procederán al cambio de contraseña al ingresar por primera vez, cada vez que se solicite el restablecimiento de esta al administrador, cuando sea requerido por el sistema o cuando considere que pueda ser conocida por un tercero.

3. CONDICIONES DE USO

Cumplimiento de las normas establecidas

a. La utilización del servicio de correo electrónico de la Universidad Militar Nueva Granada no puede transgredir las normas legales vigentes
b. Los comunicados internos de la Universidad Militar deben ser dirigidos a los correos de tipo personal.
c. Los correos que se definen como oficina o dependencia, son correos que se utilizan como medios de comunicación entre la comunidad en general y la Universidad.
d. El correo electrónico institucional debe ser usado únicamente para propósitos concernientes a las funciones del cargo.
e. 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 o de alguna persona en particular.
f. 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.
g. 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.
h. Los usuarios de correo electrónico institucional, que identifique contenido sospechoso o con posibles virus en el correo, deben notificarlo a la Oficina Asesora de Tecnologías de la Información y las Comunicaciones, y/o al correo electrónico tic.seguridad@unimilitar.edu.co
i. 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.

Uso para fines profesionales o académicos

Las cuentas de correo electrónico de la Universidad Militar Nueva Granada no deben ser, utilizadas con fines privados o comerciales, ya que constituye una herramienta de trabajo.

Canal de comunicación Institucional

La Universidad Militar Nueva Granada, podrá hacer uso de este servicio para hacer llegar a los usuarios cualquier información que considere relevante. La recepción de estos mensajes no es opcional.

Prohibición de abuso en el correo electrónico:

- Por contenido: queda prohibido enviar, almacenar o distribuir mensajes cuyo contenido atente contra las leyes nacionales existente vigentes o contra los tratados internacionales suscritos por Colombia, o promueva actuaciones que vayan en contra de la ley.
- Por suplantación: queda prohibido el envío de correo utilizando la suplantación de identidad.
- Por Cadenas (Spam): queda prohibido el envío de comunicaciones electrónicas con finalidad comercial a una pluralidad de receptores que no las hayan solicitado.
- Por su finalidad: queda prohibido el envío de mensajes de correo electrónico cuyo único propósito sea el de sobrecargar, paralizar o de cualquier otro modo, perjudicar el normal funcionamiento del servicio.

Propiedad intelectual

La condición de usuario del servicio de correo electrónico de la Universidad Militar Nueva Granada no implica, en ningún caso, una autorización de uso de los derechos de propiedad intelectual titularidad de la Universidad.

En consecuencia, el Usuario de este servicio se compromete a respetar los derechos enunciados y a evitar cualquier actuación que los pudiera perjudicar.

La utilización no autorizada de los derechos de propiedad intelectual de la Universidad Militar Nueva Granada, en general, cualquier vulneración de la posesión y titularidad de los derechos será puesta en conocimiento de las autoridades, con el fin de realizar las investigaciones correspondientes y aplicar las sanciones que den a lugar.

Mantenimiento de cuentas de correo

Con objeto de optimizar los recursos empleados en la prestación del servicio de correo electrónico, las cuentas de correo electrónico:

a. Serán suspendidas si no registran acceso durante un periodo de 2 años si no se mantiene vinculación laboral, como estudiantes o egresado de la Universidad.
b. Las cuentas de los funcionarios que se desvinculen de la Universidad serán suspendidas una vez llegue el formato de paz y salvo emitido por la División de Gestión del Talento Humano y serán eliminadas, en un periodo de 3 años después de la desvinculación.

Funcionamiento anormal de una cuenta de correo

En caso de detectarse un funcionamiento anormal de una cuenta de correo, bien mediante procedimientos automatizados de seguridad o bien mediante denuncias, los administradores del servicio de correo realizarán los correctivos para restablecer la normalidad. El usuario será informado de la situación presentada en un periodo de 5 días hábiles, a través del mismo correo.

Medidas contra el correo basura (spam)
Para eliminar la recepción de mensajes no solicitados se utilizará un sistema basado en listas negras. Las listas negras a considerar serán las propuestas a la Universidad Militar Nueva Granada a través del área encargada de administrar el servicio. Adicionalmente, mediante el sistema de seguridad que tiene el proveedor del servicio se permite identificar un correo como posible correo basura (spam), este mensaje se etiqueta spam y se dejará al usuario la decisión final de qué hacer con el mensaje.

La Oficina Asesora de Tecnologías de la Información podrá adoptar cualquier otra medida técnica que permita mejorar la calidad del servicio.

Medidas con relación al Malware
El proveedor del servicio utiliza sistemas de antivirus en sus servidores de correo que permite marcar los mensajes de correo que incorporen malware y es responsabilidad del usuario si abre el correo que es marcado.

COMPROMISO DE CONFIDENCIALIDAD CON RELACIÓN AL SERVICIO DE CORREO ELECTRÓNICO
Los funcionarios de la Universidad Militar Nueva Granada que por su trabajo tenga acceso a la administración del correo electrónico se compromete a cumplir con la obligación de secreto y confidencialidad respecto del contenido de los correos, para lo cual debe firmar el compromiso de confidencialidad.

La confidencialidad de contenidos y contraseñas a las que se refiere este apartado no excluye la posibilidad de que, en estricto cumplimiento de los requerimientos judiciales o, en su caso, autoridad legalmente autorizada, deban revelarse los contenidos de los mensajes, así como la identidad de los autores.

Para acceder al correo electrónico se facilitará una dirección electrónica y una contraseña inicial que deberá ser cambiada inmediatamente una vez recibida para mantener la confidencialidad de la misma. Los usuarios tomarán todas las medidas para mantener la confidencialidad de la misma.

Cualquier solicitud posterior de correo de cambio de contraseña dirigida a los administradores del servicio deberá realizarse previa identificación del titular de la

cuenta y sólo al titular se le podrá facilitar dicha contraseña. Se dispondrá de un mecanismo de recuperación automatizado de contraseñas que podrá ser utilizado si el usuario ha facilitado una dirección de correo alternativa.

Los funcionarios que por razones del servicio conozca o pueda tener acceso a una contraseña de un correo electrónico del que no es titular, se compromete a no divulgar y no hacer uso inadecuado de esta.

EXCEPCIÓN DE RESPONSABILIDAD
Por el funcionamiento del servicio:

- Privacidad: la Universidad Militar Nueva Granada no garantiza privacidad absoluta en la utilización del servicio.
- La Universidad Militar Nueva Granada queda eximida de cualquier responsabilidad por los daños y perjuicios que pudieran derivarse del acceso y eventual manipulación de los mensajes electrónicos gestionados mediante este servicio.
- Problemas técnicos: la Universidad Militar Nueva Granada, no puede garantizar el buen funcionamiento en todo momento. Las interrupciones de funcionamiento serán previamente advertidas sólo si ello es racionalmente posible.
- La Universidad Militar Nueva Granada queda eximida de cualquier responsabilidad derivada del mal funcionamiento del servicio que tenga su origen en una circunstancia accidental, fuerza mayor, trabajos necesarios de mantenimiento o cualquier otra causa no imputable a la misma.
- El único responsable por el buen uso de la cuenta de correo electrónico asignada por la Universidad Militar Nueva Granada es el usuario responsable de esta.
- La Universidad Militar Nueva Granada no ejerce control alguno sobre dicha utilización ni sobre el contenido de los mensajes enviados por los usuarios.
- Los usuarios deberán actuar siempre con la debida diligencia, lo que supone, entre otras cosas, tomar todas las precauciones razonables para evitar el envío, la recepción y el almacenamiento de mensajes de correo electrónico con adjuntos que contengan virus.

POLÍTICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL
La Universidad Militar Nueva Granada pone en conocimiento de los usuarios del servicio que sus datos personales van ser tratados por la Universidad, única y exclusivamente para asuntos institucionales.

- En cumplimiento de lo dispuesto en la Ley 1581 de 2012, los usuarios podrán ejerce el derecho de conocer, actualizar y rectificar sus datos personales frente a los Responsables del Tratamiento o Encargados del Tratamiento.
- Los datos de carácter personal facilitados por los usuarios podrán ser comunicados a un tercero sólo para el cumplimiento de los fines de la Universidad.

TERMINACIÓN

Si bien, en principio el servicio para los estudiante o egresados tiene una duración indefinida, la Universidad tiene derecho a suspenderlo o darlo por terminado, si no se utiliza el servicio por un periodo de 2 años una vez graduado o cancelado sus estudios. Para los funcionarios de la Universidad la duración del servicio es por el tiempo que dure el contrato con la Universidad.

LEY Y JURISDICCIÓN APLICABLE

Las presentes condiciones de uso se rigen por las leyes nacionales vigentes y se somete los usuarios a las mismas.

ANEXO 2. TÉRMINOS Y CONDICIONES PARA LOS PAGOS POR MEDIOS ELECTRÓNICOS

En el presente documento encontrará los términos y condiciones del servicio de recaudo de la oferta institucional de servicios de la Universidad Militar Nueva Granada.

Al ingresar a este sitio y al utilizar cualquiera de sus servicios, el **USUARIO** está aceptando los términos y condiciones establecidos en esta página**. LA UNIVERSIDAD MILITAR NUEVA GRANADA** (en adelante **LA UNIVERSIDAD**) podrá modificar estos términos y condiciones en cualquier momento, asunto que se notificará oportunamente a los usuarios.

LA UNIVERSIDAD ha puesto a disposición la plataforma E-collect, implementada por la empresa Avisor Technologies S.A.S, con el fin de prestar a la comunidad el servicio de recaudo de la oferta institucional de **LA UNIVERSIDAD**. Por favor lea atentamente las condiciones de uso antes de utilizar este sitio. Al entrar y utilizar los servicios ofrecidos por **LA UNIVERSIDAD**, usted declara expresamente su aceptación a las siguientes condiciones:

- **SERVICIOS Y USUARIOS.** Estos términos y condiciones aplican a todos los usuarios de los servicios que se recaudan mediante esta plataforma, incluyendo la comunidad universitaria, aspirantes, representantes y/o acudientes de los estudiantes.

  El término servicios hace referencia a todos los contenidos y funcionalidades específicas tales como pago de servicios académicos habilitados por el sitio web de **LA UNIVERSIDAD**.

- **REGISTRO Y CONTRASEÑA. EL USUARIO** que desee hacer uso de los servicios de recaudo que ofrece la plataforma, deberá registrarse y diligenciar todos los campos siguiendo las instrucciones que se le indiquen, siendo el único responsable por la veracidad de la información.

  Al ingresar la información, el **USUARIO** autoriza a **LA UNIVERSIDAD** a realizar el tratamiento de su información con las entidades u operadores financieros para la formalización de la transacción financiera. La identificación y la clave de acceso son personales e intransferibles y el **USUARIO** será el único responsable por su uso adecuado.

  El **USUARIO** es responsable del uso de los servicios en línea del sitio web. Ello implica, utilizarlos de manera ágil, eficiente, racional y, además, cumplir con las normas establecidas para su uso y para preservar la seguridad del sistema.

- **DEVOLUCIONES, RETIROS Y OTROS. EL USUARIO** acepta, declara y reconoce que las operaciones financieras realizadas en esta plataforma estarán sometidas a la normativa de **LA UNIVERSIDAD**, quien será la única competente para definir, aprobar, establecer y analizar si los valores económicos pagados referentes a los servicios académicos son susceptibles de devolución de conformidad con su Calendario Académico, Acuerdo Anual de Derechos Pecuniarios, Reglamento Estudiantil y la demás normatividad vigente en **LA UNIVERSIDAD**.

  EL USUARIO acepta, declara y reconoce expresamente que las operaciones financieras correspondientes con devoluciones, retiros y cancelaciones deberán ser tramitados única y exclusivamente con **LA UNIVERSIDAD**, quien en cada caso concreto realizará el contacto con la entidad financiera para verificar y conceptuar sobre la viabilidad de la solicitud en consideración a la operación financiera realizada por **EL USUARIO**.

- **PROCESAMIENTO DE TRANSACCIONES.** Teniendo en cuenta que durante el proceso de validación de una transacción puede haber, a discreción de **LA UNIVERSIDAD**, una sospecha de fraude o de otras conductas sospechosas, que den inicio a los mecanismos de verificación adicional o presentarse situaciones por fuera del control de **LA UNIVERSIDAD**, tales como intermitencias o caídas en las redes de procesamiento de pagos de las entidades financieras, **LA UNIVERSIDAD** no garantiza un plazo específico para la realización de las transacciones de **EL USUARIO**.

  Por lo tanto, **LA UNIVERSIDAD** no se responsabiliza por los inconvenientes o daños económicos sufridos por **EL USUARIO** debido a: atrasos o problemas derivados de la tardanza en la aprobación y/o finalización de la transacción y/o transacciones rechazadas por el sistema o por las entidades financieras, por cualquier razón.

  Así mismo, en caso de imposibilidad de llevar a cabo una transacción o rechazo de la misma, **LA UNIVERSIDAD** informará a **EL USUARIO** la novedad presentada sin detallar las causas de la imposibilidad o del rechazo.

  En el caso en que se evidencie un fraude por los pagos realizados con tarjetas débito o crédito, el pago realizado por esta modalidad será reversado de los sistemas académicos y financieros de **LA UNIVERSIDAD** pues se da por entendido que los recursos no ingresaron a sus cuentas bancarias. Los casos de fraude por pagos electrónicos serán notificados al respectivo programa académico quien realizará los procesos disciplinarios que correspondan. En estos casos no se otorgarán prórrogas adicionales a las ya establecidas por **LA UNIVERSIDAD**, así la

notificación del fraude sea posterior al comienzo de la actividad académica que se ha pagado por esta vía.

LA UNIVERSIDAD no se responsabiliza por las actuaciones de terceros intermediarios a quienes se les confíen claves de acceso o se les entregue dinero para el pago de los diferentes servicios académicos que ofrece. Los únicos medios autorizados para pago son los Bancos y entidades financieras autorizadas por la División Financiera, así como los servicios web ofrecidos en esta plataforma. En ningún caso relacionado con estas operaciones fraudulentas se realizará reintegro de recursos.

En caso de presentarse, reporte de transacciones sospechosas por parte de las entidades bancarias, **EL USUARIO** autoriza de manera voluntaria y expresa a **LA UNIVERSIDAD** para poner en conocimiento de las autoridades correspondientes cualquier información, hechos o conductas del **USUARIO** que puedan constituir delito, dar lugar a responsabilidad civil o violación de cualquier norma de carácter municipal, departamental, nacional o internacional.

- **RESPONSABILIDAD. LA UNIVERSIDAD** no será responsable por daños que los programas sobre los cuales corre la plataforma ni por los archivos que baje del mismo, ocasionen en el equipo o los archivos de **EL USUARIO**, incluyendo virus. **LA UNIVERSIDAD** no será responsable por los perjuicios que **EL USUARIO** pueda causar a terceros en la utilización de la plataforma de servicios de recaudo. **EL USUARIO** asume todos los riesgos asociados con tratar con otros usuarios con los cuales entre en contacto a través de la plataforma de servicios de recaudo. En caso de que **EL USUARIO** tenga alguna disputa con otros usuarios este libera a **LA UNIVERSIDAD** de cualquier reclamación, demanda o daño de cualquier naturaleza, que llegue a ocurrir o que de cualquier otra forma se relacione con dicho conflicto.

  LA UNIVERSIDAD no se responsabiliza por transferencias de dinero erróneos que resulten del ingreso incorrecto de la información por parte de **EL USUARIO** o equivocaciones derivadas del ingreso incorrecto del monto a transferir por parte de **EL USUARIO**.

- **RESTRICCIONES. EL USUARIO** únicamente podrá ingresar a las secciones de la plataforma de servicios de recaudo que le sean autorizadas por **LA UNIVERSIDAD**, por tanto, se abstendrá de utilizar cualquier medio para violar la seguridad y restricciones de la plataforma de servicios de recaudo y la sola intención de hacerlo evidenciada por **LA UNIVERSIDAD** será causal para dar por terminada su transacción e informar a las autoridades correspondientes de este hecho. **EL USUARIO** no podrá enviar correos electrónicos no solicitados, incluyendo promociones y/o publicidad de productos y servicios. No podrá incluir en la

plataforma de servicios de recaudo cualquier derecho de franquicia, esquema de pirámide, membresía a un club o grupo, representación de ventas, agencia comercial o cualquier oportunidad de negocios que requiera pago anticipado o pagos periódicos, solicitando el reclutamiento de otros miembros, sub-distribuidores o sub-agentes. Tampoco podrá incluir, colocar o enviar cadenas de cartas, virus, caballos de troya, bombas de tiempo o cualquier programa de computador o herramienta con la intención de dañar, interferir, interceptar o apropiarse de cualquier sistema, datos o información. **EL USUARIO** no podrá ni permitirá que otras personas o instituciones publiquen o transmitan en la plataforma de servicios de recaudo información o textos ilegales, dañinos, amenazantes, injuriosos, calumniosos, hostigantes, vulgares, obscenos, odiosos, discriminatorios o cualquier otro material de cualquier clase o asuman conductas que puedan constituir delitos, dar lugar a responsabilidad civil o violar cualquier disposición legal.

EL USUARIO defenderá a su costa a **LA UNIVERSIDAD** frente a cualquier reclamación penal, civil, laboral y principalmente por competencia desleal, prácticas restrictivas, violación de marcas o nombres registrados, violación de derechos individuales o de autor, responsabilidad civil, etc., originada por el mal uso de la plataforma de servicios de recaudo. En todo caso **EL USUARIO** pagará a **LA UNIVERSIDAD** todos los costos legales que este tipo de reclamaciones le originen, sin perjuicio de las indemnizaciones a que haya lugar por estos hechos.

- **USOS PROHIBIDOS DEL SISTEMA.** La plataforma de servicios de recaudo puede ser usada únicamente para propósitos legales. **LA UNIVERSIDAD** prohíbe el uso del sitio web en cualquiera de las siguientes formas:
  - **a.** Incluir cualquier información biográfica incompleta, falsa o inexacta o información que no corresponda a la verdadera.
  - **b.** Borrar o revisar cualquier material incluido en la plataforma por cualquiera otra persona o entidad, sin la debida autorización.
  - **c.** Usar cualquier elemento, diseño, software o rutina para interferir o intentar interferir con el funcionamiento adecuado de la plataforma o cualquier actividad que sea llevada a cabo en la misma.
  - **d.** Intentar descifrar, descompilar o desensamblar cualquier software comprendido en el sitio web o que de cualquier manera haga parte de la plataforma.
  - **e.** En general, incluir o colocar en sitio web información falsa, inexacta, incompleta o engañosa. Si usted tiene un password o contraseña que le permita el acceso a un área no pública de la plataforma, no podrá revelar o compartir ese password o contraseña con terceras personas o usar el password o contraseña para propósitos no autorizados.
  - **f.** Ocultar la identidad propia o la de otros al usar los servicios.
  - **g.** Deshabilitar, sobrecargar o deteriorar los servicios.

h. Interferir con el uso y provecho de los servicios.
i. Usar los servicios para realizar conductas discriminatorias actividades ilícitas o que atenten contra los derechos de las personas en forma difamatoria, obscena, amenazante o abusiva.

- **MARCAS Y PROPIEDAD INTELECTUAL. LA UNIVERSIDAD** es el legítimo propietario de la marca **UNIVERSIDAD MILITAR NUEVA GRANADA,** y otras que aparezcan en la plataforma de servicios de recaudo que estén identificadas como de propiedad de los proveedores de información y servicios o de terceros. Las marcas que aparezcan a nombre de los proveedores de información y servicios o de terceros son de su propiedad. La información que aparece en la plataforma, el diseño gráfico, la presentación y la compilación de la información, son propiedad exclusiva de **LA UNIVERSIDAD** y están protegidos por las normas sobre propiedad intelectual y por los tratados internacionales que sobre la materia ha suscrito y ratificado la República de Colombia.

- **TERMINACIÓN**. **LA UNIVERSIDAD** se reserva el derecho unilateral de restringir el acceso en caso de detectar cualquier uso no permitido del Sitio Web y tomar las acciones legales correspondientes.

- **SOLUCIÓN DE CONTROVERSIAS.** Cualquier conflicto, controversia o diferencia que surja en relación con alguna o algunas de las estipulaciones y que ocurra en desarrollo de estos Términos, podrá ser resuelta, en primera instancia, en forma directa por las partes, cada una de las cuales designará para el efecto un representante, quienes se reunirán para discutir, en arreglo directo, la diferencia o conflicto presentado, dentro de los cinco (5) días hábiles siguientes a su ocurrencia. Las decisiones adoptadas en desarrollo de esta etapa, cualesquiera que ellas sean, deberán constar en acta suscrita por las partes.

  En el evento de que la etapa anterior se hubiere agotado sin llegarse a un acuerdo, las partes acudirán al mecanismo de conciliación en derecho en un centro de conciliación legalmente habilitado; en el evento que no se logre un acuerdo bajo este mecanismo, se deberá acudir ante la jurisdicción ordinaria.

  LA UNIVERSIDAD no garantiza que el sitio WEB opere libre de errores o que el sitio WEB y su servidor se encuentre libre de virus de computadores u otros mecanismos dañinos. Si el uso del sitio web o del material resulta en la necesidad de prestar servicio de reparación o mantenimiento a sus equipos o información o de reemplazar sus equipos o información, **LA UNIVERSIDAD** no es responsable por los costos que ello implique. La plataforma se pone a disposición en el estado en que se encuentre. La plataforma no otorga garantía alguna sobre la exactitud, confiabilidad u oportunidad del material, los servicios, los textos, el software, las

gráficas y los links o vínculos. En ningún caso la universidad, sus proveedores o cualquier persona mencionada en el sitio web será responsable por daños de cualquier naturaleza, resultantes del uso o la imposibilidad de usar el sitio web o el material. Links a otros sitios web. **LA UNIVERSIDAD** no será responsable, contractual o extracontractualmente, por ningún daño indirecto, especial, incidental, punitivo, lucro cesante, pérdida de oportunidad, entre otros daños consecuenciales, ya sea que su posibilidad de ocurrencia haya sido prevista o no, previamente por **LA UNIVERSIDAD** resultantes de la indisponibilidad del servicio, de la demora en el procesamiento del pago, del fraude por suplantación de identidad del pagador o del comercio, o de cualquier otro daño indirectamente relacionado con la prestación de los servicios de **LA UNIVERSIDAD**.

- **EFECTOS DEL ACUERDO Y LEY APLICABLE.** Este acuerdo es el único vigente que existe entre las partes, y sus efectos se producen desde el momento en que **EL USUARIO** acepta sus términos y condiciones conforme se indica en las cláusulas anteriores.

El presente acuerdo se rige por las leyes de Colombia.

NOTIFICACIONES. EL USUARIO acepta que toda comunicación y/o modificación en relación con este acuerdo se efectuará a través del sitio web de **LA UNIVERSIDAD**.

Por lo tanto, **LA UNIVERSIDAD** no tiene la obligación de enviar a **EL USUARIO** ningún tipo de aviso por correo físico y/o certificado ni por correo electrónico.

EL USUARIO es responsable de ingresar al sitio web de **LA UNIVERSIDAD** para consultar y mantenerse informado de los cambios en el Acuerdo.

- Acepto Términos y Condiciones
- Autorizo el Tratamiento de Datos Personales

ANEXO 3. TÉRMINOS Y CONDICIONES PARA USO DE LOS SISTEMAS DE INFORMACIÓN

El administrador de los sistemas de información advierte que la responsabilidad frente a la veracidad y exactitud de la información que se reporta, es exclusiva del usuario que ingresa la información al sistema, por tanto, a este le corresponde garantizar que la misma refleje la situación real en los aspectos informados.

AVISO ACCESO INICIAL AL SISTEMA DE INFORMACIÓN

Los Sistemas de Información de la Universidad Militar Nueva Granada, tienen por objeto, administrar la información de los procesos de la Universidad. El acceso y el uso de información en él contenida, es exclusiva responsabilidad del usuario. El administrador del sistema no se responsabiliza por daños o perjuicios derivados del acceso, uso o mala utilización de la información.

TÉRMINOS Y CONDICIONES DE USO

- El tratamiento de la información contenida en los Sistemas de la Universidad, es exclusivo para la realización de sus funciones.
- Los Sistemas de Información, contiene la información reportada por los estudiantes, proveedores y funcionarios de la Universidad. Es administrado por la Oficina Asesora de Tecnologías de la Información y las Comunicaciones, tiene por objeto facilitar el conocimiento de la información relacionada con los diferentes procesos de la Universidad; el acceso al mismo y el uso de información en él contenida, es exclusiva responsabilidad del usuario.
- La Oficina Asesora de Tecnologías de la Información y las Comunicaciones, como administrador de los Sistemas de Información, no persigue ningún lucro, ganancia o interés comercial con la Información contenida en estos.
- El usuario será responsable de todas las transacciones o acciones efectuadas con su cuenta de usuario asignada por la Universidad.
- Ningún usuario deberá acceder a los Sistemas de Información de la universidad, utilizando una cuenta de usuario o clave de otro usuario.
- Los datos ingresados por los usuarios de los Sistemas de Información deben dar cumplimiento a lo dispuesto en la Ley 1581 de 2012.
- En el caso que se presente un evento de Seguridad de la Información en el cual se vea involucrado un usuario de los sistemas de Información de la Universidad Militar Nueva Granada, debe ser reportado a la Oficina de Control Interno Disciplinario, para realizar las respectivas investigaciones y se realice el debido proceso.
- Los perfiles de acceso a los sistemas de información son definidos por las funciones que el usuario desempeña en la oficina o dependencia. El acceso a los sistemas de información, solamente debe ser usado únicamente para propósitos concernientes a las funciones del cargo.

- Los usuarios, que identifiquen usos indebidos del sistema de información, deben notificar a la Oficina Asesara de Tecnologías de la Información y las Comunicaciones o al correo electrónico tic.seguridad@unimilitar.edu.co
- La información contenida en los sistemas de Información 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.

LEY Y JURISDICCIÓN APLICABLE

Las presentes condiciones de uso se rigen por las leyes nacionales vigentes y se somete los usuarios a las mismas.

ANEXO 4. LINEAMIENTOS DE SEGURIDAD PARA LOS EQUIPOS DE CÓMPUTO QUE REALIZAN TRANSACCIONES FINANCIERAS EN LA UNIVERSIDAD MILITAR NUEVA GRANADA

Lineamientos de Seguridad de Operación

Los equipos de cómputo que se destinen a realizar transacciones financieras deben tener las siguientes características de seguridad

a) Requerir clave de autenticación para el ingreso y uso, las cuales deben cambiarse cada tres meses y tener especificaciones
   - Longitud mínima de 10 caracteres
   - La Clave debe contener caracteres alfanuméricos y caracteres especiales
b) Los equipos deben bloquearse por inactividad a los 3 minutos.
c) Se debe limitar los privilegios de la cuenta de usuario utilizada para realizar transacciones financieras, no permitir instalación de ningún software.
d) Restringir en lo posible la ejecución de archivos como (.exe, .vbs, .com .scr, etc.) que no hagan parte de los sistemas necesarios para la elaboración de las actividades propias la transacción financiera.
e) Efectuar el borrado regular de:
   - Archivos temporales del sistema operativo
   - Archivos temporales de Internet, cookies
   - Historial de navegación y descargas
f) Establecer los mecanismos necesarios para que la instalación, actualización o desinstalación de programas o dispositivos en el equipo de cómputo, sea realizada únicamente por los funcionarios de la Oficina Asesora de Tecnologías de la Información y las Comunicaciones, esta actividad deben ser revisadas y aprobadas por el Oficial de Seguridad de la Información o un designado.
g) Restringir la instalación de software que permita conexión remota y restringir el software de acceso remoto que tiene preinstalado el Sistema Operativo.
h) Asegurar que el equipo de cómputo mínimo con antivirus (con módulos de anti - keylogger, firewall personal, antispyware), software licenciado y actualizado de forma automática o supervisada.
i) Restringir los puertos que permitan la conexión y acceso a dispositivos de almacenamiento extraíbles
j) Activa que el sistema operativo y las aplicaciones necesarias para la actividad en el equipo de cómputo pueda recibir las actualizaciones de seguridad de forma automática, cada vez que sean emitidas por el fabricante.
k) El equipo de cómputo debe ser destinado de manera exclusiva para la realización de las transacciones financieras.
l) Apagar el equipo de cómputo cuando no se esté utilizando.

Lineamientos de Seguridad Física

a) Restringir el acceso al área física desde donde se realizan transacciones financieras sólo para personal autorizado.
b) Contar con cámaras de video, las cuales deben cubrir al menos el acceso principal al área y el funcionario que utilice el equipo de cómputo.

Lineamientos de Seguridad De la Red de Datos

a) Restringir el acceso a correos personales, redes sociales y en general a otros sitios no asociados con las funciones.
b) Implementar mecanismos de autenticación que permitan confirmar que el equipo de cómputo es un dispositivo autorizado dentro de la red de la entidad.
c) Debe evitar realizar transacciones financieras desde dispositivos móviles o desde la red WIFI de la Universidad.

ANEXO 5. LINEAMIENTOS DE SEGURIDAD PARA LAS CLAVES DE LOS SERVICIOS INFORMATICOS LA UNIVERSIDAD MILITAR NUEVA GRANADA

Las características que deben tener las claves de los servicios informáticos y de los sistemas de información de la Universidad Militar Nueva Granada son los siguientes.

- Tener mínimo ocho (8) caracteres alfanuméricos
- Se debe realizar el cambio de la contraseña cada 3 meses si el sistema no lo solicita.
- Cada vez que se cambien la contraseña deben ser distintas en por lo menos las 4 anteriores.
- Las contraseñas deben contener los siguientes caracteres:
  - Caracteres en mayúsculas (de la **A** a la **Z**)
  - Caracteres en minúsculas (de la **a** a la **z**)
  - Números (0 1 2 3 4 5 6 7 8 9)
  - Caracteres especiales (¡?!”#$%&/)
- No debe contener partes del nombre de la oficina, Universidad, Militar, UMNG o más de dos caracteres consecutivos

ANEXO 6. MANEJO DE CONTRASEÑAS PARA ADMINISTRADORES DE TECNOLOGÍA DE LOS SERVICIOS INFORMATICOS LA UNIVERSIDAD MILITAR NUEVA GRANADA

1. Manejo de Contraseñas para Administradores de Tecnología

Las contraseñas de ROOT y SA de los servidores y de las Bases de Datos de la Universidad están a cargo de los funcionarios responsables de administrarlos, dichas claves deben quedar en custodia de la Rectoría y la Oficina de Protección al Patrimonio, quienes son encargados de suministrar en caso de ser requeridas por el Plan de Continuidad del Negocio en el cual se consigna los nombres de los usuarios y contraseñas. Las contraseñas tendrán una vigencia de 6 meses, terminado este tiempo deben ser cambiadas.

Se debe garantizar que el ingreso a la administración se realice con la vinculación directamente con las credenciales del directorio activo, para los administradores.

2. Características de las Claves de los Administradores

- Se debe realizar el cambio de la contraseña cada 3 meses si el sistema no lo solicita.
- La clave no debe contener las palabras root, sys, tic, Universidad, Militar, UMNG, partes del nombre de la oficina o más de dos caracteres consecutivos
- Tener una longitud mínima de seis (6) caracteres.
- Tener una longitud máxima de doce (12) caracteres.
- Las contraseñas deben contener los siguientes caracteres:
  - Caracteres en mayúsculas (de la A a la Z)
  - Caracteres en minúsculas (de la a a la z)
  - Números (0 1 2 3 4 5 6 7 8 9)
  - Caracteres especiales (¡?!”#$%&/)
- Cada vez que se cambien la contraseña deben ser distintas en por lo menos las 5 anteriores.
- No puede contener con caracteres y números que no se encuentren en la contraseña anterior.

Las contraseñas referentes a las cuentas “predefinidas” incluidas en los sistemas o aplicaciones adquiridas deben ser desactivadas. De no ser posible su desactivación, las contraseñas deben ser cambiadas después de la instalación del producto.

Los funcionarios de la Oficina Asesora de Tecnologías de la Información y las Comunicaciones no deben dar a conocer sus claves de usuario a terceros de los sistemas de información, sin previa autorización del Jefe de la Oficina, de ser necesario.

Los usuarios y claves de los administradores de los sistemas de información o de servidores son de uso personal e intransferible.

El personal la Oficina Asesora de Tecnologías de la Información y las Comunicaciones debe emplear obligatoriamente las claves o contraseñas con un alto nivel de complejidad.

3. Suministro de las Claves de Administración

De ser requeridas las claves de Administración de los Servidores y de la Bases de Datos por el desarrollo del Plan de Continuidad del Negocio o por simulacro de este, se debe suministrar en sobre sellado al Jefe de la Oficina Asesora de Tecnologías de la Información y la Comunicaciones.

Como constancia de este procedimiento se firmará un acta de reunión en donde se registrará el suministro de las claves. Como veedor del proceso está el Jefe de Oficina de Control Interno de Gestión.

4. Cambio de Claves

Todo cambio de claves ya sea por vencimiento, por utilización en simulacro o por activación del Plan de Cantidad del Negocio debe ser informado por el Jefe de la Oficina Asesora de Tecnologías de la Información y las Comunicaciones al Jefe de la Oficina de Protección al Patrimonio y a la Rectoría. Las claves se deben entregar en sobre sellado.

Una vez se realice el cambio de las claves, se debe realizar su destrucción en presencia Jefe de la Oficina Asesora de Tecnologías de la Información y las Comunicaciones, Jefe de la Oficina de Protección al Patrimonio y el Jefe de Oficina de Control Interno de Gestión.

Como constancia de este procedimiento se firmará un acta de reunión en donde se registrará el procedimiento realizado.