CONSEJO DE RECTORÍA
ACUERDO No. 027
25 DE MAYO DE 2018

Por medio del cual se aprueba
La Política Informática de la Universidad Católica de Manizales

El Consejo de Rectoría de la Universidad Católica de Manizales, en ejercicio de las facultades estatutarias y

CONSIDERANDO:

a. Que en el marco de las Políticas de la Universidad Católica de Manizales "La gestión de las actividades de apoyo administrativo y financiero en la UCM, responderá a los criterios de sostenibilidad y conservación del patrimonio institucional; propiciará el control y la protección de los recursos económicos que hacen parte del capital de trabajo y promoverá la transparencia y efectividad de los procesos y la racionalización en el uso de los recursos humanos, materiales, físicos, tecnológicos y económicos".

b. Que la Universidad Católica de Manizales establece en el Plan de Desarrollo 2018-2025 Mega 4: "Contar con un sistema efectivo de gobierno y gestión universitaria"

c. Que la Política de Seguridad contempla un conjunto de buenas prácticas y lineamientos para concientizar y sensibilizar a integrantes de la comunidad universitaria con respecto al uso correcto de información y herramientas asociadas a Tecnologías de Información, impulsando la consecución de objetivos organizacionales en ambientes seguros.

d. Que el Consejo de Rectoría, en sesión del 10 de abril de 2018, aprobó la propuesta de Política Informática presentada por la Vicerrectoría Administrativa y Financiera y la unidad de Sistemas de Información.

ACUERDA:

Artículo primero: Aprobar la Política Informática de la Universidad Católica de Manizales de acuerdo a documento adjunto que hace parte integral del presente Acuerdo.

Comuníquese y cúmplase.

Manizales, 28 de mayo 2018

Hna. MARIA ELIZABETH CAICEDO CAICEDO O.P
Rectora

Mgr. CATALINA TRIANA NAVAS
Secretaria General

Contenido

POLÍTICA INFORMÁTICA

El presente documento describe la política de informática para la UCM, estableciendo un conjunto de buenas prácticas y lineamientos los cuales permiten concientizar y sensibilizar a integrantes de la comunidad universitaria con respecto al uso correcto de información y herramientas asociadas a Tecnologías de Información, impulsando la consecución de objetivos organizacionales en ambientes seguros.
Las prácticas y lineamientos aquí estipulados deben ser aplicados para salvaguardar la información y mantener los atributos de confidencialidad, integridad y disponibilidad de la misma, minimizando los riesgos asociados a la información e infraestructura Tecnológica en general.

CONSIDERANDO

- Que las herramientas TIC se incorporan en la consecución de objetivos institucionales, realización de actividades y procesos.

- Que, para la UCM, la información representa un activo estratégico para el cumplimiento de sus funciones misionales, estratégicas y de apoyo.

- Que las cambiantes condiciones y nuevas plataformas tecnológicas disponibles las cuales son aplicables a la UCM requieren condiciones de seguridad.

- Que existencia de amenazas y riesgos son fuente o causa potencial de eventos o incidentes no deseados y pueden ser causantes de daños a los recursos informáticos de la UCM.

RESUELVE

- La presente política debe incluirse y hacer parte de la documentación del Sistema Integrado de Gestión y políticas de la Universidad Católica de Manizales.

- **Alcance.** Este manual define los lineamientos y procedimientos asociados a seguridad informática, sistemas de información, servicios web, servicios de red y servidores alojados en la institución, aplica para todos y cada uno de los estamentos universitarios;

estudiantes, docentes y administrativos que empleen herramientas TI y sistemas de información para el ejercicio de sus funciones dentro de la institución universitaria.

- **Responsables y Divulgación del documento.** Es responsabilidad los directivos y su personal a cargo, velar por el cumplimiento de lo estipulado en este documento, y de la Unidad de Sistemas la correspondiente divulgación, compartiendo la información a través de los diferentes recursos asociados para una correcta difusión, entre los cuales se destacan; correo institucional, página oficial de la UCM, intranet y otros que los responsables tengan a consideración.

- **Vigencia.** La presente política entra en vigencia a partir de su fecha de expedición, anulando aquellas políticas que le sean contrarias.

1. OBJETIVOS

1.1. Objetivo general

Brindar altos niveles de seguridad, consiguiendo que cada uno de los servicios asociados a TI se realicen de forma eficaz y eficiente, garantizando su correcta funcionalidad y continuidad en la normal operación de sus funciones tanto administrativas como académicas.

Controlar actividades que permitan garantizar la integridad física y lógica de la infraestructura TI de la Universidad Católica de Manizales.

1.2. Objetivos específicos

- Proporcionar a la comunidad universitaria lineamientos que son necesarios para que la información que se administra en la universidad permanezca segura.
- Reducir las amenazas y riesgos que se asocian a la seguridad de la información, sistemas de información y datos en general.
- Establecer un esquema de seguridad de la información con claridad y transparencia en administración del riesgo.
- Garantizar que la prestación de cada uno de los servicios se realice con altos niveles de seguridad.
- Evitar actividades y comportamientos no deseados en relación al uso de recursos TI.
- Sensibilizar a la comunidad universitaria sobre la importancia del uso adecuado de información, sistemas de información, redes, canales de comunicación y otros activos asociados a TI.

- Contar con lineamientos para la planeación, diseño e implementación de un sistema de gestión de seguridad de la información (SGSI).

2. DOCUMENTOS DE REFERENCIA

- Requisitos para los sistemas de gestión de calidad ISO 9001.
- Estándar de seguridad de la información ISO 27001.
- Estándar para la seguridad de la información ISO/IEC 27002.
- Objetivos de Control para Información y Tecnologías, guía de mejores prácticas COBIT.
- Protección de datos personales, Ley 1581 de 2012 Habeas Data.
- Ley Estatutaria 1266 de 2008 por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales.
- Decreto 1377 de 2013 Por el cual se reglamenta parcialmente la Ley 1581 de 2012
- Resolución 3564 de 2015 Anexo 1 Estándares para publicación y divulgación de información

3. TÉRMINOS Y DEFINICIONES

Para efectos de este instrumento se entenderá por:

- **Comité de sistemas:** Equipo conformado por colaboradores de la unidad de sistemas(de acuerdo al tema a revisar), dirección administrativa e invitado con formación en Tecnologías de la Información y la comunicación.
-

  Este equipo analizará e implementará actividades relacionadas con.
  - Adquisición de infraestructura TI que se alinea a las necesidades del negocio.
  - Establecimiento de normas de la UCM relacionado a usos de hardware y software.
  - Establecimiento de lineamientos para selección de proveedores de recursos TI.
  - Velar por el cumplimiento de normas, políticas, estatutos y lineamientos de la UCM

- **Unidad de sistemas:** es el área encargada de:

  - Velar por el buen funcionamiento de la infraestructura tecnológica que se utilice en las diferentes dependencias de la universidad.
  - Determinar y concretar estrategias y objetivos a corto, mediano y largo plazo para la buena administración de la infraestructura tecnológica.
  - Velar y mantener la estabilidad de la infraestructura TI.

- Supervisar el cumplimiento de los requisitos estatuarios y normativos de la UCM.
- Verificar que los servicios ofrecidos en la universidad se realicen bajo estándares de calidad y seguridad.
- Actualizar los requerimientos en términos de TI para las diferentes dependencias de la UCM, manteniendo un inventario actualizado y verificando las necesidades que se presenten día a día.

- **Política en informática:** Para efectos del documento la política representa un conjunto de prácticas y lineamientos, adoptados por toda la comunidad universitaria y entes externos a la universidad (personal que ejerza actividades contratadas por la UCM), tomando medidas adecuadas para que estas se cumplan.

- **Consejo de Rectoría: Instancia encargada de hacer que lo estipulado** en este documento se cumpla.

- **Software:** Conjunto de herramientas lógicas que permiten el funcionamiento de equipos, realizando tareas específicas.

- **Hardware:** Representa máquinas y equipos (físicos) configurables y en este caso adaptables al cumplimiento de objetivos organizacionales de la UCM.

- **Servidor:** Lugar de almacenamiento y procesamiento de información.

- **Backup:** copias de seguridad o de respaldo, las cuales se utilizan en caso de pérdida de información de la fuente principal (servidores locales).

- **Acceso lógico:** Acceso en red mediante los servicios de intranet o internet de la UCM, a través de los cuales se puede acceder a los archivos, navegar en el servidor, enviar un correo electrónico, transferir archivos y/o administrar sistemas de información.

- **Acceso físico:** ingreso de personas a las instalaciones de la universidad.

- **Control:** Mecanismo preventivo y correctivo adoptado por la UCM para la oportuna detección y corrección de errores y riesgos a los cuales se encuentra expuesta la infraestructura TI de la universidad.

- **Comunidad universitaria:** la integran estudiantes, docentes, investigadores, contratistas y administrativos los cuales tienen relación directa o indirecta con las Institución.

Los lineamientos contenidos en este documento, representan obligaciones necesarias para ejercer procesos de evaluación y adquisición de infraestructura tecnológica, el incumplimiento de dichos lineamientos recae en la responsabilidad administrativa.

LA UCM deberá contar con un Coordinador de sistemas, responsable de la administración de los Bienes y Servicios TI, quien realizará las actividades acordes a la vigilancia y aplicación de los lineamientos establecidos por el comité de sistemas.

4. LINEAMIENTOS PARA LA ADQUISICIÓN DE INFRAESTRUCTURA TECNOLÓGICA

Adquirir una nueva tecnología en la UCM representa un factor clave de estrategia tecnológica que involucra no únicamente al área de sistemas, sino que también se convierte en un apoyo a los procesos, estratégicos, misionales, de apoyo, de evaluación y control que se encuentran inmersos en el sistema integrado de gestión de la universidad. Se definen los siguientes lineamientos.

- ✓ La obtención de infraestructura tecnológica, queda sujeta a los lineamientos estipulados en este documento.

- ✓ El comité de sistemas debe establecer periodos y frecuencia de actualización de recursos TI en los que se procederá a verificar necesidades tecnológicas en la UCM.

- ✓ Toda adquisición de tecnología informática debe pasar por procesos de análisis, aprobación y autorización del comité de sistemas.

- ✓ Los equipos que se vayan a adquirir deben estar registrados bajo una marca que cuente con permanencia y reconocimiento en el mercado nacional e internacional.

- ✓ Toda adquisición TI debe contar con tecnología de punta vigente, además la selección debe realizarse teniendo en cuenta velocidad de transferencia de información y de procesamiento.

- ✓ Para garantizar el correcto funcionamiento de las impresoras, estas se deben adquirir teniendo en cuenta las características (hardware y software) de los equipos a las cuales se conectarán.

- ✓ Todos los equipos de operación crítica deben contar con un programa de mantenimiento preventivo y correctivo por parte del proveedor, verificando además que exista

disponibilidad de repuestos por lo menos durante su vida útil (dependiendo del equipo), con esto se busca garantizar la continuidad y funcionamiento de dichos equipos.

- ✓ El comité de sistemas en sus actividades relativas a planeación y adquisición de infraestructura tecnológica debe establecer criterios de evaluación y selección de proveedores de infraestructura TI, para ello se debe tener en cuenta:

  Para **la UCM**: tipo de necesidad a suplir, estudio de mercado, factibilidad financiera, estudio ambiental, proveedores, análisis de riesgo y plan de mitigación, entendiéndose por:

  Necesidad a suplir: El comité de sistemas debe realizar análisis de situaciones que se presenten en las diferentes dependencias de la UCM, que finalmente requieran de la adquisición de infraestructura TI.

  Revisión de propuestas: Análisis de posibles productos y sus proveedores.

  Factibilidad financiera: Se debe cuantificar ingresos y egresos que generará la adquisición de la infraestructura, para ello se debe tener en cuenta que una infraestructura TI no necesariamente tiene que generar ingresos, sino que estos valores pueden estar inmersos en ahorro de capital financiero y minimización de costos de procesamiento.

  Análisis de riesgo: se debe establecer técnicas de identificación de riesgos, plan de gestión, análisis cualitativo, análisis cuantitativo, aplicación de controles y verificación de riesgos residuales.

  Para **selección del proveedor:** Calidad del producto o servicio, precio, reconocimiento de la empresa (proveedor), cumplimiento de especificaciones técnicas, experiencia en el sector TI, experiencia en soporte técnico, estándares y capacidades, capacitación y certificación de productos y/o servicios, entendiéndose por:

  Calidad (producto o servicio): Parámetro que permite cualificar características del producto o servicio.

  Precio: Costos asociados a la obtención del producto o servicio, en caso de ser un producto deben incluirse costos de administración y mantenimiento.

  Reconocimiento de la empresa (Proveedor): análisis de información de otras organizaciones y su percepción sobre el proveedor.

Especificaciones técnicas: Que se cumpla con todas y cada una de las especificaciones requeridas, además verificar que no sean productos obsoletos y/o con poca permanencia en el mercado.

Experiencia en el sector TI: Presencia en el mercado nacional e internacional teniendo en cuenta, percepción de otras organizaciones sobre el proveedor, calidad del producto o servicio y confiabilidad.

Estándares: Que cumpla con estándares de calidad y que no vayan en contra de la normativa vigente de la UCM.

Capacidades: En caso de requerir un producto en gran cantidad, se debe verificar que el proveedor se encuentre en capacidad de abastecer la demanda.

Capacitación y certificación: El proveedor debe presentar la idoneidad en el conocimiento para garantizar procesos de capacitación y certificación del personal de los productos y/o servicios adquiridos.

- ✓ Para la adquisición de Hardware se tendrá en cuenta:

  - El/ los equipo(s), que se vaya a adquirir deben cubrir con las especificaciones establecidas.

  - El equipo debe estar dentro de la lista de equipos vigentes del proveedor y debe cumplir con las normativas asociadas a recursos TI de la UCM.

  - Los equipos adquiridos deben tener garantía con vigencia mínima de un año y además se debe tener el soporte técnico adecuado del proveedor.

  - Es recomendable la adquisición de equipos que representen el uso de las últimas tecnologías en el mercado.

  - Todos los equipos de una referencia diferente deben contar con sus respectivos manuales y soporte técnico para la instalación (en caso de ser requerido).

  - El software que se requiera utilizar en los equipos debe contar con sus respectivas licencias de uso actualizadas.

5. LINEAMIENTOS DE CONTROL DE ACCESO

Mantener la integridad de la información en la UCM, representa conservar con exactitud la información que ha sido suministrada o generada dentro de la universidad, la cual no podrá ser modificada ni alterada por personas que no cuenten con un perfil de usuario con privilegios asociados al uso de los sistemas de información de la UCM, de igual manera se debe controlar el acceso físico a instalaciones de la universidad para prevenir riesgos asociados a la infraestructura física de TI. Para ello se definen los siguientes lineamientos.

5.1. Identificadores de usuario y contraseñas:

- ✓ Todos los usuarios con acceso a un sistema de información o a una red informática, deben disponer de un usuario y una contraseña de usuario asociada.

- ✓ Ningún usuario recibirá un identificador de acceso a la Red de Comunicaciones, Recursos Informáticos o Aplicaciones hasta que no acepte formalmente la Política de Seguridad vigente.

- ✓ Los administradores de sistemas de información deben encargarse de dar privilegios a usuarios que requieran el acceso a dichos sistemas, dependiendo de los módulos y actividades que el usuario vaya a utilizar o realizar.

- ✓ Se debe verificar que no exista software o programas que permitan el acceso remoto de agentes no autorizados a los sistemas de información y recursos de red.

El control de acceso queda sujeto a los siguientes lineamientos

5.2. Del acceso lógico

- ✓ El acceso a redes lógicas de la UCM deberá realizarse mediante métodos de autenticación segura que permita proporcionar el acceso a personas autorizadas y negar dicho acceso a no autorizadas.

- ✓ El comité de sistemas es el encargado de definir quién o quienes serán responsables de la consulta y/o modificación de la información, de acuerdo a los procesos institucionales

- ✓ La información contenida en dispositivos de almacenamiento externo de propiedad de la UCM, debe estar resguardada en lugares con acceso restringido.

- ✓ El acceso a recursos de red, se administra bajo las políticas de acceso a internet

- ✓ Desvincular roles asignados a uso de sistemas de información y servicios de red en cuanto existan terminaciones de contrato o procesos de desvinculación de personal.

- ✓ En cuanto a la información que tiene acceso cada persona de la UCM, se ratifica que esta no se utilizará para fines que no se encuentren ligados a las actividades de la universidad.

- ✓ Garantizar que el acceso a redes de la universidad, no altere procesos misionales e institucionales.

- ✓ El acceso a sistemas de información será controlado por el/los administradores del sistema.

- ✓ La contraseña de acceso a los diferentes sistemas de información y otros servicios de red debe tener combinaciones alfanuméricas con una cantidad mínima de ocho caracteres.

- ✓ El usuario que administre información a través de los sistemas de información de la universidad asegurará que dicha información sea precisa, completa y que no sea divulgada innecesariamente.

- ✓ Se deberá realizar un análisis completo y confiable de entes externos a la UCM para proporcionar acceso a sistemas y servicios de red de la institución.

- ✓ Los administradores de los sistemas de información deben monitorear periódicamente los perfiles definidos para el acceso a dichos sistemas.

5.3. Del acceso físico

- ✓ Debe restringirse el acceso a información alojada en dispositivos de almacenamiento externo (USB, CDS, discos duros externos y otro tipo de almacenamiento).

- ✓ Sólo al personal autorizado le está permitido el acceso a las instalaciones en donde se almacena la información que se considera confidencial para la UCM.

- ✓ El acceso de personal externo a la universidad, será controlado y monitoreado por la unidad que requiera el ingreso de dicho personal.

- ✓ Se debe negar el acceso de la comunidad estudiantil a sitios que el comité de sistemas considere prioritarios de proteger.

- ✓ El acceso a la información de la institución por parte de docentes y administrativos debe estar limitado por las funciones asignadas en el contrato de acuerdo al manual de funciones y manual de convivencia.

5.4. Responsabilidades personales

- ✓ Todas y cada una de las personas pertenecientes a la comunidad universitaria, son responsables de las actividades relacionadas con el uso de su acceso autorizado a los diferentes sistemas de información y servicios tecnológicos.

- ✓ Bajo ningún criterio se deberá utilizar las credenciales de acceso de otro usuario que se encuentre autorizado.

- ✓ Cada usuario es responsable de cuidar de sus credenciales de acceso, este no debe compartirlas con otras personas, ni mantenerlas a la vista.

- ✓ Dado el caso de que un usuario tenga sospechas de que sus credenciales de acceso (usuario y clave de usuario), son usadas por otra persona, debe proceder a modificar su contraseña e informar al área de redes y/o al jefe inmediato.

- ✓ En lo posible evitar el uso de contraseñas que se consideran no seguras o fáciles de descifrar.

- ✓ Cumplir con normas jurídicas que afirmen los derechos patrimoniales que la ley concede a los autores.

- ✓ Los usuarios sólo podrán crear archivos que contengan datos personales para uso temporal y siempre que sus funcionalidades así lo requieran. Estos archivos deben ser destruidos cuando hayan dejado de ser útiles para la finalidad para la que fueron creados.

- ✓ Los usuarios deben informar a su jefe inmediato cualquier evento que pueda afectar a la seguridad de los datos personales, pérdida de dispositivos de almacenamiento, sospechas de uso indebido del acceso autorizado por otras personas.

5.5. De los datos personales

- ✓ Gestionar la aplicación del "MANUAL DE PRIVACIDAD Y TRATAMIENTO DE DATOS PERSONALES DE LA UNIVERSIDAD CATÓLICA DE MANIZALES" y guardar evidencias de aceptación de dicho manual.

- ✓ No se deberá almacenar información de datos personales en los equipos de la UCM, o si se requiere deberá tener aprobación de los jefes de dependencias.

- ✓ No se permitirá el uso de datos personales para fines comerciales, políticos, religiosos y/o publicitarios.

5.6. Salida de información

- ✓ Asegurar que la información que representa datos personales, no sea divulgada y usada para fines no institucionales.

- ✓ La información proveniente de los diferentes sistemas de información, únicamente debe ser utilizada para la ejecución de procesos institucionales.

- ✓ Toda información resultante de procesos institucionales debe ser debidamente almacenada y protegida de riesgos asociados a la misma.

6. LINEAMIENTOS PARA EL MANEJO DE LA INFORMACIÓN

El manejo de la información en diferentes activos asociados a tratamiento de información de la UCM tanto externos como internos debe ser debidamente controlado, para ello se toma como guía la norma ISO 27000 y la LEY ESTATUTARIA 1266 DE 2008 de la constitución política de Colombia, que permiten tener un conocimiento preciso sobre los activos que posee la Universidad como factor clave de administración de riesgos, de igual forma el uso adecuado de la información**.**

Se debe cumplir con los siguientes lineamientos.

- ✓ Es responsabilidad del comité de sistemas divulgar la existencia de lineamientos para el uso del correo electrónico en la UCM.

- ✓ El usuario de una cuenta de correo electrónico con dominio @ucm.edu.co, es responsable de conocer, aceptar y aplicar los lineamientos que se asocian al uso del correo electrónico.

- ✓ Asegurar que la información se encuentre debidamente respaldada y protegida.

- ✓ Los datos resultantes de procesos realizados con sistemas de información deben contar con procedimientos de respaldo, teniendo en cuenta la actualización de los datos y asegurando que los lugares en los que se respalda la información cuentan con niveles de seguridad adecuados.

- ✓ Para los usuarios que tengan a disposición equipos personales se recomienda que cada usuario ejecute su propio respaldo de información, en dispositivos de almacenamiento que consideren convenientes.

- ✓ Todas y cada una de las dependencias de la UCM son garantes de que los procesos de recolección y administración de la información, se realicen para la efectiva operación de los sistemas de información inmersos en procesos institucionales.

- ✓ El comité de sistemas debe establecer la periodicidad con la que se realice procesos de eliminación de duplicidad de información.

- ✓ Propender por tener sistemas de información auditables y acorde a las nuevas tecnologías en aras de su buen funcionamiento.

- ✓ Promover procesos de mejora continua de la política de seguridad de la información.

- ✓ Promulgar que el uso de la información realizada por administrativos y contratistas sea bajo responsabilidad de los mismos.

- ✓ La información obtenida mediante sistemas de información de la UCM es considerada de propiedad de la Universidad y además se encuentra sujeta a consideraciones expuestas en este documento.

- ✓ La información que se considere eventual no representa un valor significativo para la UCM, por lo tanto, el respaldo de la misma queda a consideración de cada dependencia.

- ✓ En términos de no renovación de contrato, la persona que finaliza su periodo laboral con la institución debe proporcionar la información necesaria a quien le suceda en el cargo o en su defecto a su jefe inmediato.

- ✓ Toda información contenida en medios de almacenamiento externos (discos duros, CDS, USB) que se considere importante para la institución debe estar alojada en lugares con altos niveles de seguridad.

- ✓ Ningún colaborador en proyectos de software y/o trabajos específicos, debe poseer material o información confidencial de la UCM.

- ✓ Adoptar guías para la implementación de controles de seguridad de la información como, ISO 27001, ISO 27002 y COBIT.

- ✓ Asegurar que los desarrollos internos se realicen bajo normas estrictas de seguridad de la información.

- ✓ Establecer límites en cuanto a personal autorizado que requiera consultar, modificar o eliminar información, para ello se deben tomar medidas que el comité de sistemas considere pertinentes.

- ✓ Las personas que ejerzan actividades en relación a tratamiento de información, deben firmar un acuerdo de confidencialidad de la misma.

- ✓ Todo el personal que tenga a disposición un computador personal para desarrollo de actividades intrínsecas de la UCM, debe ser consiente que la información obtenida mediante procesos de manipulación del equipo para actividades que se relacionen directa

o indirectamente con la universidad, le pertenece a la UCM y esta se reserva el derecho de manipulación, divulgación y administración.

7. COPIAS DE SEGURIDAD DE LA INFORMACIÓN

Con el fin de mantener la información protegida contra la pérdida o daño, accidental o intencional, se han definido los siguientes lineamientos:

- ✓ Los líderes de proceso con el apoyo de la Unidad de Sistemas definirán la periodicidad de copias de seguridad y los períodos de retención para el respaldo y almacenamiento de la información.

- ✓ De acuerdo a la criticidad de los datos y a la periodicidad con la que se realizan procesos transaccionales de la información, se definirá la programación de copias de seguridad tanto de bases de datos como de la información que los usuarios poseen en sus equipos de cómputo.

- ✓ La Universidad Católica de Manizales proporcionará los recursos necesarios para disponer de un medio de almacenamiento externo (Cloud Backup), con el fin de tener contingencia ante la pérdida de la información.

- ✓ Cada administrador de sistemas en conjunto con el coordinador de sistemas, debe establecer periodos de recuperación y verificación de las copias de respaldo, estableciendo además una estructura documental que permita la verificación de copias de seguridad de usuarios finales, facilitando el conocimiento sobre la estructura de información.

- ✓ Se debe realizar el respaldo de la información de los equipos personales empleados para la ejecución de actividades de la UCM, este respaldo se realizará de acuerdo a los lineamientos definidos por el comité de sistemas. Se debe tener en cuenta la criticidad de la información para definir la periodicidad con que se realizarán dichos respaldos.

- ✓ Asegurar que los dispositivos de almacenamiento de información se mantengan en áreas seguras, las cuales deben contar con; controles de acceso y seguridad física, detectores de incendio y sistemas de extinción de fuego, sistemas eléctricos regulados, controles adecuados de humedad y temperatura.

- ✓ Los lineamientos para las copias de seguridad de los equipos en los cuales se genera grandes cantidades de información y que no se encuentran registrados en la red bajo la cual se administran copias de seguridad, serán

definidos por el comité de sistemas, los cuales deben establecer el lugar y capacidad de almacenamiento de dicha información.

8. GESTION DE COMUNICACIONES Y OPERACIONES

Con el fin de asegurar la operación correcta y segura de los recursos de la información se debe:

- ✓ Tomar medidas correspondientes para la minimización de riesgos de fallos en los diferentes sistemas de información de la UCM.

- ✓ Asegurar la protección de la información y software, manteniendo atributos de integridad y disponibilidad de los servicios de tratamiento de información.

- ✓ Asegurar el buen manejo de la información, mediante la documentación de control de cambios realizados.

- ✓ Establecer criterios de aprobación en cuanto se requiera realizar modificaciones en la seguridad de la información, el cual lleve consigo modificaciones de accesos, modificación y/o mantenimiento de software.

- ✓ Garantizar la documentación y actualización de los procedimientos relacionados con la administración de las diferentes plataformas tecnológicas que soportan los procesos de negocio de la universidad.

- ✓ Segregar funciones y procedimientos necesarios para monitorear todas las actividades de seguridad de la información.

- ✓ Establecer adecuados niveles de soporte a los sistemas de información.

- ✓ Las personas encargadas de manipular software y servicios de procesamiento de información deben ser conscientes de los peligros de los códigos maliciosos y los jefes de dependencias (especialmente unidad de sistemas), deben implementar los controles necesarios para evitar, detectar y eliminar dichos posibles códigos maliciosos.

9. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

Mantener la estabilidad de los procesos de negocio de la UCM, en caso que se realice interrupción de las actividades que generalmente se ejecutan en la institución.

- ✓ Se debe definir e implementar los controles necesarios para poder identificar y minimizar los posibles riesgos asociados a la continuidad del negocio.

- ✓ Asegurar que la continuidad de los servicios asociados a TI no sea interrumpida y en caso de suceder, se debe asegurar que dichos servicios puedan ser recuperados en la menor cantidad de tiempo posible.

- ✓ Definir estrategias de prevención y recuperación de servicios ofrecidos por la UCM, siendo necesario asignar y organizar los recursos necesarios.

- ✓ La gestión y operación de recursos asociados a tratamiento de información deberá realizarse bajo responsabilidades y procedimientos adecuados.

- ✓ Se deberá realizar presupuestos y cronogramas que soporten la estabilidad de los procesos de negocios dado el caso de presentarse eventos que impidan la continuidad del negocio.

- ✓ La administración de informática debe definir y establecer un plan de continuidad del negocio, orientado a la recuperación y restauración de las funciones críticas de la UCM en caso de presentarse interrupciones no deseadas, para ello se debe tener en cuenta:

    - Fase de análisis y evaluación de riesgos.
    - Desarrollo del plan de mitigación de riesgos.
    - Ejecución del plan de mitigación de riesgos.
    - Pruebas y mantenimiento del plan.

10. DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Para la prestación del servicio de desarrollo o construcción de Software aplicativo, se debe seguir los siguientes lineamientos.

- ✓ Todo proyecto de contratación de desarrollo o construcción de software requiere de un estudio de factibilidad que permita establecer la rentabilidad del proyecto, así como los beneficios que se obtendrán del mismo.

- ✓ Todo desarrollo de software que se realice dentro de la Universidad Católica de Manizales, tiene que estar ligado necesariamente a las actividades intrínsecas de la universidad.

- ✓ El comité de sistemas decidirá si aprobará o no la solicitud de desarrollo de software, bajo un estricto análisis con la unidad de sistemas y dependencias asociadas, teniendo en cuenta análisis de factibilidad realizado.

- ✓ La información contenida en las bases de datos deberá ser administrada de forma tal que los datos contenidos se encuentren protegidos, cumpliendo con la Ley Estatutaria 1266 de 2008 de la constitución política de Colombia, “Por la cual se dictan las disposiciones generales de hábeas data y se regula el manejo de la información contenida en bases de datos personales”.

- ✓ Si, para ejecutar un nuevo desarrollo de software se requiere de un tipo de contratación externa a la universidad, esta contratación deberá sujetarse a los lineamientos de adquisición de infraestructura tecnológica que se encuentran en este documento y sometido a interventoría. Los costos de contratación, compra de software y hardware se especificarán en un documento que realice la universidad en conjunto con el agente externo y deberán ser cubiertos según el tipo de contratación que se vaya a realizar.

- ✓ Todos los sistemas o desarrollos de software que sean realizados por personal de la Universidad Católica de Manizales son propiedad de esta, por consiguiente, la Universidad tendrá los derechos de autor y está en facultad de utilizar dichos desarrollos en áreas y/o actividades que requiera sin ningún tipo de restricción.

- ✓ En caso de que los desarrollos realizados, se hagan en conjunto con personal ajeno a la universidad, esta solicitará a dicho personal, firmar los derechos de cesión a la UCM, otorgando también el reconocimiento al trabajo realizado por dicho personal.

- ✓ Finalizado el proyecto de desarrollo de software, el personal o equipo de trabajo entregará; código fuente, ejecutable, manual técnico, manual de usuario y demás documentos que hayan surgido durante el desarrollo del software.

- ✓ Los sistemas de información de la UCM que se encuentren en ejecución deben contar con sus respectivos manuales, técnico y de usuario.

- ✓ Los sistemas de información deben integrar módulos de auditoría de registro de Logs de usuario, que permita verificar las acciones ejecutadas en el sistema.

11. SEGURIDAD FÍSICA Y DEL ENTORNO

Con el objetivo de mantener la seguridad de la información de la Universidad católica de Manizales, se define:

Área segura: Espacio físico en el cual se aloja y/o procesa información crítica de la UCM.
Consideraciones de áreas seguras: Data center, centro de monitoreo por cámaras, salas de computo, áreas de gestión documental.

Perímetro de seguridad física: La UCM cuenta con un área de recepción y entrada a las instalaciones mediante el cual se impide el acceso a personal no autorizado, mediante el uso de torniquetes que permiten movimientos de acceso cuando se accede mediante tarjeta de proximidad (tarjeta tipo visitante cuanto se trate de una persona no perteneciente a la comunidad universitaria).

Del acceso físico: Los perímetros de seguridad se utilizarán para proteger las áreas que contenga información transaccional y recursos asociados a su procesamiento.

Se definen los siguientes lineamientos:

- ✓ Todas las personas pertenecientes a la comunidad universitaria deben poseer un carnet (tarjeta de proximidad) de acceso a las instalaciones de la UCM, las personas que no posean dicho carnet deben realizar la solicitud (de acceso) en el primer puesto de control de acceso (portería), entregando un documento el cual se regresará al propietario en cuanto realice la devolución del carnet correspondiente.

- ✓ El propietario del carnet o tarjeta de proximidad se hace responsable del uso adecuado del mismo.

- ✓ El uso del carnet únicamente debe realizarlo el propietario y queda prohibido prestar dicho carnet.

- ✓ La pérdida del carnet de acceso se debe reportar al UMA para que se tomen medidas correspondientes.

- ✓ Asegurar que las puertas de acceso a las oficinas y centro de datos se encuentre en perfecto estado.

- ✓ Los derechos de acceso a las áreas seguras deben ser revisadas con una frecuencia determinada por el comité de sistemas.

- ✓ Los recursos de información más críticos deben estar localizados en lugares a los cuales el acceso sea restringido.

12. INSTALACIÓN Y PROTECCIÓN DE EQUIPOS

Propender por la correcta instalación de los recursos informáticos de la UCM, de sus supervisiones y la periodicidad de sus mantenimientos, se tienen los siguientes lineamientos.

12.1. De la instalación

- ✓ Los equipos de la UCM se deben instalar y proteger de riesgos, amenazas, peligros ambientales y accesos no autorizados.

- ✓ Los siguientes lineamientos deben aplicarse para la correcta instalación y protección de equipos de la UCM:

  - Mantener un registro actualizado y con información verificable, sobre la cantidad de equipos que son propiedad de la universidad.

  - Los equipos (sin excepción alguna) que son propiedad de la UCM deben ajustarse a los lineamientos planteados en este documento y otras normas, políticas y procedimientos que se establecen en el Sistema Integrado de Gestión de la institución.

  - El usuario que requiera que un equipo sea removido de su lugar, debe registrar la solicitud en la mesa de ayuda y estará sujeto a la viabilidad o no de la adecuación del equipo a un nuevo lugar.

  - El usuario del equipo se hace responsable del hardware y software del equipo que se le haya asignado.

  - Los equipos que son propiedad de la UCM, deben tener instalado software de antivirus licenciado y adoptado por la universidad.

  - Asegurar la disponibilidad y ejecución de los sistemas de firewall y antivirus, estos deben estar funcionando constantemente.

  - Todo software instalado en los equipos de cómputo debe contar con su respectiva licencia de uso.

- No se debe realizar modificaciones a la configuración de equipo por parte de la comunidad universitaria, este proceso solo puede realizarse por personal idóneo proporcionado por la institución.

- Todo equipo se entrega con el software y hardware necesario según el cargo o función que ejerza la persona.

- Todo equipo de cómputo asignado al cargo o función de una persona, debe ser apagado correctamente, para evitar deterioro o daños en los mismos por caídas del fluido eléctrico.

- Para mantener recursos informáticos seguros se debe establecer; controles para sistema operativo, software, bases de datos, aplicaciones, procesos y comunicaciones manteniendo para cada uno de ellos; claves de acceso únicas que permitan el acceso únicamente a personal autorizado, verificar información proveniente de fuentes externas a la universidad corroborando que se encuentre libre de cualquier agente contaminante o perjudicial para el funcionamiento de los equipos, mantener pólizas de seguros de los recursos TI actualizadas y en funcionamiento.

12.2. Del mantenimiento

✓ Se deberá seguir los siguientes lineamientos para el adecuado mantenimiento de equipos:

- Verificar el estado de los equipos en relación a su vida útil, se debe planear y ejecutar revisiones periódicas para comprobar su estado y realizar mantenimiento.

- Generar reportes sobre el estado de los equipos, problemas encontrados, mantenimiento realizado y posible ingreso de equipos nuevos.

- Clasificar los equipos para su respectivo mantenimiento y especificar si el proceso se realiza en las instalaciones de la universidad o se contrata.

- Los equipos que no sean propiedad de la universidad sino de funcionarios externos, no serán revisados y no se les realizará mantenimiento.

- Se debe realizar procesos de dada de baja, destinación final o reutilización de equipos. Teniendo en cuenta su funcionamiento y vida útil y, analizando la información que puede estar contenida en sus medios de almacenamiento.

- El comité de sistemas debe velar porque se realicen actualizaciones y aplicación de parches de seguridad en los equipos administrados en la UCM.

12.3. Uso apropiado de los recursos

✓ Los Recursos Informáticos, Datos, Software, Red Corporativa y Sistemas de información están disponibles exclusivamente para cumplir con las obligaciones y propósitos operativos para los que fueron implantados. Todo el personal usuario de dichos recursos debe ser consciente de los derechos de confidencialidad asociados a su uso.

13. LINEAMIENTOS USO DE DISPOSITIVOS MÓVILES (SMARPHONES Y TABLETAS)

Existe un auge y una gran aceptación de dispositivos inteligentes por parte de la comunidad universitaria, es posible que con el uso inadecuado de estos, la UCM se encuentre expuesta a riesgos asociados a tratamiento de información, para prevenir y contrarrestar dichos riesgos se definen los siguientes lineamientos:

✓ La persona encargada del área de redes debe proporcionar información a quién solicite acceso a los servicios de internet que posee la UCM.

✓ El acceso a servicios de red e internet a través de dispositivos móviles debe restringirse a personas no pertenecientes a la comunidad universitaria, en caso contrario se debe solicitar autorización para el uso de dichos servicios.

- ✓ Los usuarios deben verificar que no se emita o realice difusión de información confidencial a través de dichos dispositivos.

14. PROHIBICIONES

Queda prohibido:

- Alterar o intento de alteración de la información.
- La creación excesiva de usuarios para el acceso a equipos de cómputo de la UCM.
- Almacenar datos personales en equipos en los que se limita el acceso a esta información.
- Intentar alterar la información contenida en las diferentes bases de datos de la universidad, este proceso únicamente lo puede realizar personal altamente capacitado y permitido por la UCM.
- Introducción de contenidos amenazantes, inmorales, obscenos a la red de la universidad.
- Proliferación intencional o no intencional de código malicioso a la red corporativa de la UCM.
- Instalación de software no permitido por la UCM, en los diferentes equipos.
- Alterar funcionamiento de programas antivirus y sus actualizaciones, dejando vulnerables a los sistemas de cualquier elemento destinado a destruir o corromper los datos informáticos.
- Incumplir los lineamientos estipulados en este documento, interfiriendo en el adecuado funcionamiento de los sistemas de la UCM en general.

SOFTWARE

- La instalación de software ilegal y de dudosa procedencia.

- Eliminar licencias de activación de software, se debe tratar con mayor severidad la eliminación de licencias de sistemas operativos y antivirus.

RECURSOS DE RED

Ningún usuario con acceso a los servicios de redes de la universidad debe:

- Configurar enrutadores, switches y otros dispositivos de red sin el debido consentimiento del personal del área de redes.
- Desarrollar o ejecutar programas que interfieran en las actividades de otros usuarios de la UCM.
- Ingresar personal no autorizado a lugares en los que se administren recursos de red.
- Instalar programas no autorizados
- Ingresar a páginas de dudosa procedencia y contenido inadecuado.
- Conectar dispositivos que permitan compartir el acceso a internet a entes externos a la universidad.
- Intentar obtener credenciales de un usuario de la UCM, para acceder a los servicios de red que ofrece la universidad.

CONECTIVIDAD A INTERNET

Queda prohibido:

- El uso del internet para fines no institucionales.
- Compartir usuario y contraseña de usuario para que una persona no autorizada tenga acceso a los servicios de internet ofrecidos por la UCM.

- Incumplir con las restricciones de acceso a Internet, firewall, antivirus y otro tipo de bloqueos de red y sistemas de la universidad.

- Realizar actividades que alteren el funcionamiento de los sistemas de información de la UCM.

- Realizar proselitismo político, religioso e ideológico que vaya en contra de la ideología de la institución.

- El uso de internet para fines no académicos, es decir el uso para propósitos comerciales, publicitarios o propagación de mensajes destructivos u obscenos.

15. ACTUALIZACIONES DE LA POLÍTICA INFORMÁTICA

- Los lineamientos proporcionados en esta política pueden ser modificados dependiendo de las nuevas necesidades, modificaciones a la infraestructura tecnológica, adquisición de TI, desarrollo e implementación de nuevo software y actualización de otras políticas que se puedan adherir al sistema integrado de gestión de la UCM.

- La actualización de lineamientos generará una nueva versión de esta política, por lo tanto, los responsables se encargarán de comunicar a toda la comunidad universitaria, la actualización de esta política.

- Es responsabilidad de la comunidad universitaria la lectura de la actualización de la política informática, la no lectura del documento genera desconocimiento de lineamientos y por ende aplicación de sanciones por el incumplimiento de lo planteado.

- Los jefes de dependencias deben notificar al comité de sistemas los casos en los que las personas no se acojan a la política informática, y estos finalmente deben tomar las medidas necesarias, para que no se altere el cumplimiento de los objetivos planteados en esta política.

16. RESPONSABILIDADES

- Es responsabilidad de cada empleado, el cuidado y la administración de su área de trabajo, debe velar por salvaguardar los activos físicos y lógicos que se le fueron asignados, incluye;

equipos de cómputo, medios de almacenamiento externo, periféricos, activos de información, archivos, sistemas de información y sistemas operativos.

- El personal de la UCM debe notificar al comité de sistemas en caso de ser testigo de violación a la política establecida.

- El encargado administrar sistemas de información de la UCM, debe aplicar cada uno de los lineamientos estipulados en esta política en cuanto a el control de acceso, en caso de realizarse una incorrecta asignación de usuario para el acceso al sistema, la responsabilidad recae sobre el administrador.

- El personal que encuentre falencias en la seguridad de los sistemas de información y/o en el uso de los mismos, está en la obligación de reportar dichas falencias al personal de administración informática o al administrador del sistema.

- Es responsabilidad del comité de sistemas concientizar a la comunidad universitaria acerca de la aceptación y aplicación de la política, sustentando que, si se aplican cada uno de los lineamientos aquí estipulados se pueden eliminar riesgos asociados al tratamiento de información y a la seguridad de TI en general.

17. DISPOSICIONES TRANSITORIAS

1. Las disposiciones aquí enmarcadas, entrarán en vigor a partir de su fecha de expedición.

2. Si se realiza modificaciones a esta política, la vigencia de la misma será definida en el Consejo de Rectoría basado en las recomendaciones del comité de sistemas, los cuales también serán encargados de divulgar la nueva política.

3. El desconocimiento de esta política no libera de responsabilidades a integrantes de la comunidad universitaria.

REFERENCIAS BIBLIOGRÁFICAS

1. Benitez, M. (2013). Políticas de Seguridad Informática. *Gestión Integral*, 5-37.

2. Univesidad Nacional de Colombia. (11 de Octubre de 2015). *Dirección Nacional de Tecnologías de la Información y las Comunicaciones.* Obtenido de: http://www.dntic.unal.edu.co/images/seguridad/PolticadeSeguridadInformaticaydelaInformacion.pdf

3. Universidad Católica de Manizales. (Mayo de 2015). Obtenido de Políticas Institucionales UCM: http://www.ucm.edu.co/wp-content/uploads/docs/normativas/normativas/politicas_institucionales_ucm.pdf

4. Universidad del Valle. (s.f.). *Oficina de Informática y telecomunicaciones*. Obtenido de Políticas para el uso de recursos informáticos: http://www.univalle.edu.co/politicainformatica/

5. Universidad Distrital Francisco José de Caldas. (s.f.). Obtenido de Política para la Seguridad de la información de la Univerisidad Distrital Francisco José de Caldas: https://portalws.udistrital.edu.co/CIT/documentos/NORMATIVIDAD/politica_seguridad/archivos/Politica_para_Seguridad_Informacion_Version_0.0.1.0.pdf