RESOLUCIÓN RECTORAL No. 062

(09 de septiembre de 2020)

"Por medio de la cual se deroga la Resolución Rectoral No. 001 del 15 de enero de 2018 y se aprueba la nueva Política General de Seguridad de la Información"

EL RECTOR DE LA UNIVERSIDAD CATÓLICA DE PEREIRA, en uso de sus atribuciones legales, y especialmente en lo dispuesto en la Ley 30 de 1992, en el Acuerdo No. 07 del 7 de septiembre de 2010, y

CONSIDERANDO:

Que la Universidad Católica de Pereira, como institución de educación superior, recolecta, consulta y trata la información de todos los inscritos, estudiantes, egresados, graduados, docentes, administrativos y terceros con los que tiene vínculo la Universidad.

Que en cumplimiento a la Ley 1581 de 2012 por medio de la cual se dictaron disposiciones generales para la protección de datos personales y del Decreto 1377 de 2013 por medio del cual se reglamentó parcialmente la Ley 1581 de 2012, la Universidad Católica de Pereira adoptó la Política General de Seguridad de la Información.

Que la Universidad Católica de Pereira cumpliendo con lo dispuesto en la legislación vigente y con el fin de proteger la información que maneja, adoptó la Política General de Seguridad de la Información mediante Resolución Rectoral Nº 001 del 15 de enero de 2018.

Que el Comité Técnico de Archivo de la Universidad ha revisado y ajustado la Política de Seguridad de la información adoptada mediante Resolución Rectoral Nº 001 del 15 de enero de 2018, lo cual se hace necesario modificar aspectos con el fin de implementar nuevas medidas de seguridad de la información de la Institución.

En mérito de lo expuesto, el Rector de la Universidad Católica de Pereira,

RESUELVE:

ARTÍCULO 1: Derogar la Resolución Rectoral No. 001 del 15 de enero de 2018 y aprobar la nueva Política General de Seguridad de la Información en los siguientes términos:

1. INTRODUCCIÓN

El crecimiento de las nuevas tecnologías en el mundo y el intercambio constante de información ha permitido un avance exponencial en el diseño y estructura de las organizaciones, también ha traído consigo ataques externos a través de internet y desde el mismo interior de la organización.

Por esto la Universidad Católica de Pereira, para efectos de la presente política, cuenta con una infraestructura informática robusta para el suministro de los servicios tecnológicos a todas las dependencias y usuarios de la organización; y con el fin de poder preservar la confidencialidad, la integridad y la disponibilidad de la información, establece una Política de Seguridad de la Información, buscando niveles adecuados de protección y resguardo de la información y minimizando así los riesgos asociados.

2. OBJETIVO

Formalizar el compromiso de la Rectoría de la UNIVERSIDAD CATÓLICA DE PEREIRA en la implementación, gestión y mejoramiento continuo de las políticas de seguridad de la información, proporcionando un marco de referencia ligado a todos los activos de información de la Alma Máter, los cuales están en constante evolución de acuerdo con el avance de la tecnología y los requerimientos de la institución.

3. ALCANCE

El documento "Política de Seguridad de la Información" reglamenta la protección y uso de los activos de información de la UNIVERSIDAD CATÓLICA DE PEREIRA.

La gestión de seguridad de la información será administrada a través de los activos de información de la Universidad, definidos en la norma NTC-1S0/IEC 27001 como cualquier bien que tiene valor para la Institución que genera, procesa, almacena o transmite información. Los activos están conformados por:

Localización física: La Universidad Católica Pereira está ubicada en la Carrera 21 No. 49-95 Av. de las Américas en Pereira Risaralda, conformada por siete (07) edificios:

- Buena Nueva
- Dabar
- Kabai
- Aletheia
- Biblioteca
- Humanitas
- Posgrados

- Las actividades de las diferentes áreas que soportan los procesos de generación, almacenamiento y transmisión de información de la UNIVERSIDAD CATÓLICA DE PEREIRA.

- La tecnología utilizada, hace referencia a todos los elementos generados por parte de la UNIVERSIDAD CATÓLICA DE PEREIRA y por quienes la conforman; dichos componentes pueden ser tangibles y digitales.

- Los usuarios internos y externos que interactúan con los activos de información de la Alma Máter.

4. REQUISITOS LEGALES Y REGLAMENTARIOS

Las normas establecidas en este documento son de obligatorio cumplimiento y se complementarán con las demás políticas establecidas en el marco legal de la UNIVERSIDAD CATÓLICA DE PEREIRA.

5. DEFINICIONES

- **Activo:** Cualquier objeto que tiene valor para la organización. NTC-ISO /IEC 27001.

- **Activo de información:** Es una pieza de información definible e identificable, almacenada en cualquier tipo de medio que tiene valor para la Universidad.

- **Acuerdo de Confidencialidad:** Documento que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

- **Auditoría:** Verificación a intervalos planificados para determinar los objetivos de control, controles, procesos y procedimientos del SGSI de la UNIVERSIDAD CATÓLICA DE PEREIRA.

- **Backup:** Copia y archivo de datos de los medios de almacenamiento de la UNIVERSIDAD CATÓLICA DE PEREIRA de modo que se pueda utilizar para restaurar la información original después de una eventual pérdida de datos.

- **Baja cautelar:** Cuando el retiro de un trabajador se produce en circunstancias normales, pero hay que tener un control especial con los accesos y documentación que obran en poder del empleado.

- **Baja crítica:** Cuando el retiro de un trabajador se produce en circunstancias especiales: despidos o conflictos con el empleado.

- **Baja normal:** Cuando el retiro de un trabajador se produce en circunstancias normales y sin conflictos.

- **Contraseña:** Serie secreta de caracteres que permite a un usuario tener acceso a un archivo, ordenador o programa.

- **Control:** Medio para gestionar el riesgo que puede sufrir un activo, en este incluyen políticas, procedimientos y directrices de la organización y pueden ser de naturaleza administrativa, técnica o legal.

- **Disponibilidad:** Se define como el acceso de los usuarios a los datos con los que se trabaja. Los interesados que estén autorizados a acceder a esta información deben poder hacerlo de forma segura y sencilla.

- **Firewall:** Es un dispositivo de seguridad de red que supervisa el tráfico de red entrante y saliente que permite o bloquea el tráfico específico en función de un conjunto definido por reglas de seguridad.

- **Incidente de seguridad de la información:** Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

- **Información pública:** Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal. Que ha sido declarada legalmente o por su propietario, de conocimiento público y accesible a cualquier persona. Ej. Rendición de cuentas presentada por la entidad, Plan de acción de la Entidad, Convocatorias, estructura orgánica, horarios de atención al público, directorio de dependencias, entre otros. **Ley 1712 de 2014.**

- **Información reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados la **Ley 1712 de 2014. Ejemplo:** La información que sirva para la prevención, investigación y persecución de los delitos y las faltas disciplinarias, mientras que no se haga efectiva la medida de aseguramiento o se formule pliego de cargos, según el caso.

- **Información Clasificada**: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en la **Ley 1712 de 2014. Ejemplo:** hojas de vida, historia laboral, expedientes pensionales, historial académico.

- **Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos.

- **LAN:** Es una red que conecta los ordenadores en un área relativamente pequeña y predeterminada de la Universidad.

- **Licencia de Software:** Es la autorización que el autor, que es quien ostenta el derecho intelectual exclusivo del programa computacional, concede a la UNIVERSIDAD CATÓLICA DE PEREIRA para utilizar el software.

- **Módem:** Es un periférico utilizado para transferir información entre varios equipos a través de un medio de transmisión por cable.

- **OTP (One Time Password):** Es una contraseña válida sólo para una autentificación. Se suele utilizar para que el usuario ingrese por primera vez y luego pueda cambiar su contraseña.

- **Protector de pantalla:** Es un programa informático.

- **Proxy:** Ordenador intermedio que se usa en la comunicación de otros dos.

- **Red privada virtual (VPN):** Método que permite a los empleados remotos acceder a su red de forma segura.

- **Router:** Se utilizan para conectar varias redes. El router actuará como distribuidor, seleccionando la mejor ruta de desplazamiento de la información para que la reciba rápidamente.

- **Seguridad de la Información**: Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras

propiedades tales como: autenticidad, trazabilidad no repudio y fiabilidad. Incluye la seguridad informática, la seguridad TIC y la seguridad de los datos.

- **Seguridad Informática:** Es la seguridad enfocada en los aspectos técnicos de un sistema, como lo son los equipos computacionales.

- **Seguridad TIC:** Abarca la seguridad en cuanto a la tecnología de la información y las comunicaciones que se involucran en el área donde se implementará el sistema de seguridad.

- **Sistema de control de acceso:** Es un mecanismo que en función de la identificación ya autentificada permite el ingreso de los usuarios de la Universidad a datos o recursos, que pueden acceder según sus privilegios.

- **SGSI:** Sistema de Gestión de la Seguridad de la Información.

- **Sistema operativo:** Es el conjunto de programas informáticos que permite la administración eficaz de los recursos de una computadora.

- **Sistema sensible:** Es aquel que administra información confidencial o de uso interno que no debe ser conocida por el público en general.

- **Switches:** Se utilizan para conectar varios dispositivos a través de la misma red dentro de un edificio u oficina de la UNIVERSIDAD CATÓLICA DE PEREIRA. Actuaría de controlador, permitiendo a los diferentes dispositivos compartir información y comunicarse entre sí.

- **Usuario:** Toda persona que pueda tener acceso a un recurso informático de la UNIVERSIDAD CATÓLICA DE PEREIRA.

- **Usuarios externos:** Son aquellos clientes externos que utilizan los recursos informáticos de la UNIVERSIDAD CATÓLICA DE PEREIRA a través de Internet o de otros medios y tienen acceso únicamente a información clasificada como pública.

- **Usuarios de red y correo:** Usuarios a los cuales la UNIVERSIDAD CATÓLICA DE PEREIRA les hace entrega de un correo institucional para el acceso a sus recursos informáticos.

- **Vulnerabilidad:** Debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas.

6. RESPONSABILIDADES

El Señor Rector como representante legal de la UNIVERSIDAD CATÓLICA DE PEREIRA, con el fin de asegurar la integración y el cumplimiento de los requisitos de la Política de Seguridad de la Información en los procesos de la Universidad; define las siguientes responsabilidades.

Dirección de Planeación y Calidad y Gestión Tecnológica

Con el fin de dar continuidad a todos los servicios que presta la Alma Máter con base en la Política de Seguridad de la Información, la Dirección de Planeación y Calidad a través del área de Gestión Tecnológica se encargará de:

- ✓ Coordinar la elaboración de un plan de continuidad de la gestión de seguridad de la información.
- ✓ Coordinar la revisión del plan de continuidad con ejercicios y pruebas.

- ✓ Verificar que los planes de recuperación después de incidentes sean eficientes.

Secretaría General

Se encargará de identificar y atender los requisitos legales y reglamentarios, así como las obligaciones contractuales de seguridad.

Gestión Tecnológica

Como la Coordinación encargada de todos los recursos tecnológicos de la Universidad, nombrará un ingeniero CISO (chief information security officer), cuya función principal sea apoyar las tareas de gestión de seguridad de la información en toda la UNIVERSIDAD CATÓLICA DE PEREIRA tales como:

- ✓ Realizar y mantener el inventario de Activos de la Información.
- ✓ Proponer objetivos de Seguridad de la Información.
- ✓ Informar a la Coordinación de Gestión Tecnológica los resultados de los indicadores medibles.
- ✓ Proponer mejoras en la Seguridad de la Información.
- ✓ Evaluar los recursos necesarios para la Seguridad de la Información.
- ✓ Aprobar los métodos adecuados para la protección de los dispositivos móviles, redes informáticas y otros canales de comunicación.
- ✓ Elaborar los planes, políticas y metodologías necesarias para el cumplimiento de la Política General de Seguridad de la Información.
- ✓ Apoyar a todas áreas y usuarios de la UNIVERSIDAD CATÓLICA DE PEREIRA en todos los procesos que involucren seguridad de la información.

Gestión del Talento Humano

Teniendo en cuenta que es la Coordinación es la encargada de mantener, mejorar y aplicar los diferentes procesos relacionados con la selección, vinculación, inducción, desarrollo y evaluación del desempeño de todas las personas que trabajan en la Universidad, es fundamental su participación en los lineamientos transversales que incluye la presente política, desarrollando labores como:

- ✓ Diseñar e implementar la formación interna de los empleados para que apoyen en la evaluación de riesgos que afecten la integridad, disponibilidad y confidencialidad de la información reservada.
- ✓ Realizar actividades continuas de sensibilización a todos los usuarios de la UNIVERSIDAD CATÓLICA DE PEREIRA referentes a la Seguridad de la Información.
- ✓ Planificar cursos de Seguridad de Información para nuevos empleados.
- ✓ Planear las medidas disciplinarias frente a las violaciones a la Seguridad de la Información que se puedan presentar.
- ✓ Verificar que en la Universidad se estén evitando los riesgos de las actividades subcontratadas identificadas en la matriz de Riesgos de la Información de la UNIVERSIDAD CATÓLICA DE PEREIRA, o disminuyendo a riesgos residuales.
- ✓ Definir las cláusulas de Seguridad de la Información que se deben anexar en la contratación de todas las personas que trabajan para la Universidad.

7. POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN EN LA UNIVERSIDAD CATÓLICA DE PEREIRA

Las normas establecidas en el presente documento son de obligatorio cumplimiento y se han clasificado en:

7.1.Política para el uso de dispositivos móviles

Objetivo:

Evitar el alto grado de exposición que tiene la información tanto clasificada como privada.

Aplicabilidad:

Estas políticas aplican a los miembros de los Consejos, personal administrativo, directivo, docentes, colaboradores, contratistas, y en general a todos los usuarios de la información que deben cumplir con los propósitos generales de la UNIVERSIDAD CATÓLICA DE PEREIRA.

Normatividad:

- Los dispositivos móviles proporcionados por la UNIVERSIDAD CATÓLICA DE PEREIRA (teléfonos móviles, teléfonos inteligentes, tabletas, entre otros), son una herramienta de trabajo que se debe utilizar únicamente para el ejercicio de su labor.
- Todo usuario debe pedir autorización por escrito para instalar o desinstalar aplicaciones en los dispositivos móviles que sean de propiedad de la Universidad y no se permite acceder a las aplicaciones de los equipos.
- En caso de pérdida del equipo, ya sea por sustracción o extravío, deberá dar cuenta de forma inmediata a la Dirección Administrativa y Financiera y a la Coordinación de Gestión Tecnológica.
- Los dispositivos móviles que sean propiedad de la UNIVERSIDAD CATÓLICA DE PEREIRA deben tener configurada únicamente la cuenta de correo electrónico de la Universidad.

- No se permite el acceso a los enlaces de dudosa procedencia solicitados a través de SMS/MMS/Email/Redes sociales, estos podrían ser la fuente de códigos maliciosos.
- Gestión Tecnológica es la única área autorizada para la configuración, modificación o eliminación de aplicativos sobre los dispositivos móviles pertenecientes a la UNIVERSIDAD CATÓLICA DEPEREIRA.
- Los dispositivos móviles, deben permanecer encendidos y cargados durante las horas laborales o de acuerdo con la responsabilidad y requerimientos propios del cargo.
- Es responsabilidad del usuario hacer buen uso del dispositivo suministrado por la UNIVERSIDAD CATÓLICA DE PEREIRA al realizar las actividades propias de su cargo o las funciones asignadas por la Universidad.

7.2. Política para el trabajo fuera del Campus Universitario

Objetivo:

Proteger la información de la UNIVERSIDAD CATÓLICA DE PEREIRA clasificada como privada-reservada que es procesada o almacenada fuera de las instalaciones de la Alma Máter.

Aplicabilidad:

Estas políticas aplican a los miembros de los Consejos, personal administrativo, directivo, docentes, colaboradores, contratistas, y en general a todos los usuarios de la información que deben cumplir con los propósitos generales de la UNIVERSIDAD CATÓLICA DE PEREIRA.

Normatividad:

- Siendo internet el medio de comunicación entre el usuario y la UNIVERSIDAD CATÓLICA DE PEREIRA, es fundamental que los usuarios tomen conciencia de los riesgos y eviten que terceros puedan acceder a recursos sensibles de la Universidad.
- Todo usuario debe reportar la salida o ingreso de la Universidad del equipo que le fue asignado.
- Todo usuario que desee conectarse a las redes privadas de la UNIVERSIDAD CATÓLICA DE PEREIRA deberá solicitar por correo a la Coordinación de Gestión Tecnológica un acceso especial.
- Es responsabilidad de la Coordinación de Gestión Tecnológica dar respuesta a las solicitudes de conexión por fuera de la sede de la Universidad a la red privada de la Alma Máter a usuarios que la soliciten, además establecer y configurar una red VPN con las características de seguridad especiales dependiendo de los privilegios con los que cuente cada usuario, procurando evitar a toda costa la pérdida de información.

7.3.Política para nuevos empleados y contratistas

Objetivo:

Formalizar con los colaboradores, contratistas y demás colaboradores de la UNIVERSIDAD CATÓLICA DE PEREIRA, sus responsabilidades y las funciones de sus roles, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información y de las instalaciones.

Aplicabilidad:

Estas políticas aplican a los miembros de los Consejos, personal administrativo, directivo, docentes, colaboradores, contratistas, y en general a todos los usuarios

de la información que cumplan con los propósitos generales de la UNIVERSIDAD CATÓLICA DE PEREIRA.

Normatividad:

- La dependencia que solicite nuevo personal debe definir la criticidad del puesto a cubrir en colaboración con la Coordinación de Gestión Humana, según la responsabilidad e información que se maneje en el puesto.
- En la selección de candidatos a puestos críticos la Coordinación de Gestión Humana debe comprobar las referencias laborales y académicas de cada aspirante al cargo.
- Cuando se contrate un nuevo empleado o el servicio de un tercero este debe ser comunicado por Gestión Humana sobre las implicaciones de seguridad de la información en relación a las responsabilidades de su trabajo.
- Al momento de firmar el contrato, la Coordinación de Gestión Humana deberá entregar al nuevo funcionario o contratista, los acuerdos de confidencialidad, propiedad intelectual y protección de datos establecidos por la UNIVERSIDAD CATÓLICA DE PEREIRA.
- Al firmar el contrato el nuevo funcionario o contratista se compromete a cumplir con la normatividad establecida dentro de la Política General de seguridad de la información de la UNIVERSIDAD CATÓLICA DE PEREIRA. Este trámite establece formalmente las normas internas y garantiza que el empleado conoce la normativa existente.
- La Coordinación de Gestión Tecnológica impartirá sesiones de formación donde se socialice a los trabajadores o contratistas la normatividad interna y de seguridad de la información de la UNIVERSIDAD CATÓLICA DE PEREIRA. De este modo todos los vinculados conocerán sus obligaciones de seguridad tales como la protección de sus claves de acceso, el uso adecuado del e-mail e internet, la clasificación de la información, entre otros.

7.4.Política para terminación o cambio de empleo para los empleados o servicios de terceros

Objetivo:

Propender que los colaboradores, contratistas y demás colaboradores de la UNIVERSIDAD CATÓLICA DE PEREIRA, entiendan las responsabilidades y los deberes que permanecen validos durante la terminación o cambio de empleo.

Aplicabilidad:

Estas políticas aplican al personal administrativo, directivo, colaboradores, profesores, contratistas, y en general a todos los usuarios de la información que tengan un vínculo contractual con la UNIVERSIDAD CATÓLICA DE PEREIRA.

Normatividad:

- El Coordinador del área a la cual pertenece el funcionario, junto con la coordinación de Gestión Humana, deben clasificar la desvinculación según las circunstancias que la rodean como, normal, cautelar o critica.
- La Coordinación de Gestión Humana debe:
  - ✓ Comunicar el cambio o terminación de contrato de un empleado por medio de correo electrónico al área de soporte de Gestión Tecnológica. En la comunicación se debe indicar el nombre, la fecha efectiva del cambio o desvinculación del empleado, su clasificación y cualquier medida o control especial que sea necesario realizar.
  - ✓ El retiro de accesos físicos, tales como: llaves, cajas fuertes, carné de la Universidad, etc.

- La Coordinación de Gestión Tecnológica debe coordinar que la desvinculación se produzca en el plazo adecuado dependiendo de la clasificación y efectuando los siguientes lineamientos:
  - ✓ Bloquear o inactivar los accesos lógicos, tales como: email cuando aplique, acceso a la intranet y servidores, etc.
  - ✓ El retiro de recursos electrónicos de material privativo de la Universidad, como computador, dispositivos móviles, entre otros.
  - ✓ La realización de copias de seguridad de la información sensible antes del retiro o cambio de cargo.
  - ✓ La supervisión de todos los accesos hasta el día de la desvinculación del empleado.

7.5.Política para procesos disciplinarios por incumplimiento de una política de seguridad de la información

Objetivo General:

Describir las actuaciones que implican la violación de la seguridad de la información.

Objetivos Específicos:

- Establecer el proceso disciplinario por el incumplimiento de la Política general de seguridad de la información de la UNIVERSIDAD CATÓLICA DE PEREIRA con el fin de aplicar medidas correctivas conforme a los niveles de clasificación definidos y mitigar posibles afectaciones contra la seguridad de la información.
- Evitar que los colaboradores, contratistas y otros usuarios de la UNIVERSIDAD CATÓLICA DE PEREIRA vulneren las políticas y los procedimientos de seguridad de la información.

Aplicabilidad:

Estas políticas aplican al personal administrativo, directivo, colaboradores, docentes, estudiantes, contratistas, y en general a todos los usuarios de la información de la UNIVERSIDAD CATÓLICA DE PEREIRA.

La Secretaría General y el área de Gestión Humana será la encargada de realizar las investigaciones disciplinarias siguiendo el proceso establecido por el incumplimiento de la Política General de seguridad de la información en la UNIVERSIDAD CATÓLICA DE PEREIRA.

Normatividad:

Las acciones que implican el incumplimiento de la Política General de Seguridad de la Información establecida por la UNIVERSIDAD CATÓLICA DE PEREIRA son:

- Siendo usuario activo, no firmar los acuerdos de confidencialidad o de entrega de información o de activos de información.
- Ingresar a documentos o información de otros procesos, dependencias o áreas, sin previa autorización de la coordinación del proceso o de Gestión Tecnológica.
- No reportar las violaciones a la Política General de la información, cuando se tenga conocimiento de ello.
- Clasificar y registrar de manera inadecuada la información en los aplicativos de la Universidad.
- Impedir u obstaculizar el funcionamiento o el acceso normal al sistema académico, ERP, intranet, otros sistemas o programas de la Universidad, datos informáticos o las redes de telecomunicaciones de la UNIVERSIDAD CATÓLICA DE PEREIRA.

- Destruir, dañar, borrar, deteriorar o suprimir datos informáticos o un sistema de tratamiento de información de la UNIVERSIDAD CATÓLICA DE PEREIRA.
- Distribuir, enviar, introducir software malicioso u otros programas de computación de efectos dañinos en las carpetas compartidas, almacenamiento en la nube y dispositivos pertenecientes a la UNIVERSIDAD CATÓLICA DE PEREIRA.
- Destruir, dañar, borrar, deteriorar o suprimir datos personales de las bases de datos de la UNIVERSIDAD CATÓLICA DE PEREIRA.
- Suplantar un usuario ante los sistemas de autenticación y autorización establecidos por la UNIVERSIDAD CATÓLICA DE PEREIRA, superando las medidas de seguridad informática.
- No mantener la confidencialidad de las contraseñas de acceso a la red de datos, los recursos tecnológicos o los sistemas de información de la UNIVERSIDAD CATÓLICA DE PEREIRA o permitir que otras personas accedan con el usuario y clave del titular a éstos.
- Permitir el acceso u otorgar privilegios de acceso a las redes de datos de la UNIVERSIDAD CATÓLICA DE PEREIRA a personas no autorizadas o sin previa autorización del jefe inmediato.
- Llevar a cabo actividades fraudulentas o ilegales.
- Intentar acceder sin autorización a cualquier computador de la UNIVERSIDAD CATÓLICA DE PEREIRA.
- Sustraer de las instalaciones de la UNIVERSIDAD CATÓLICA DE PEREIRA, documentos con información institucional calificada como información reservada o clasificada de acuerdo con las tablas de control de acceso del Sistema de Gestión Documental de la institución.
- Entregar, enseñar y divulgar información institucional, calificada como información pública reservada: a personas o entidades no autorizadas.
- Realizar cambios no autorizados en el sistema académico, ERP, intranet, entre otros sistemas de información de la UNIVERSIDAD CATÓLICA DE PEREIRA.

- Instalar programas o software no autorizados en las estaciones de trabajo o equipos portátiles institucionales, los únicos autorizados para realizar este tipo de acciones son los colaboradores de la Coordinación de Gestión Tecnológica.
- Copiar sin autorización los programas informáticos de la UNIVERSIDAD CATÓLICA DE PEREIRA, o violar los derechos de autor o acuerdos de licenciamiento.
- No guardar de forma segura la información cuando se ausenta de su puesto de trabajo o al terminar la jornada laboral, (documentos impresos que contengan información clasificada o reservada)
- No hacer el uso adecuado de las carpetas compartidas en los servidores para el almacenamiento de la información perteneciente a la UNIVERSIDAD CATÓLICA DE PEREIRA.
- Dejar información reservada, en carpetas compartidas o en lugares distintos al servidor de archivos, obviando las medidas de seguridad.
- Permitir que personas ajenas a la UNIVERSIDAD CATÓLICA DE PEREIRA, deambulen sin acompañamiento, al interior de las instalaciones, en áreas no destinadas al público que puedan poner en riesgo los bienes y la continuidad de los servicios en la Universidad.
- Almacenar en los computadores personales de los usuarios o en cualquier tipo de medio de almacenamiento removible, información de la UNIVERSIDAD CATÓLICA DE PEREIRA.
- Hacer uso de la red de internet de la Universidad, para obtener, mantener o difundir en los equipos de sistemas, material ofensivo, cadenas de correos y correos masivos no autorizados.
- Recibir o enviar información institucional a través de correos electrónicos personales, diferentes a los asignados por la institución.
- Enviar información reservada o información clasificada por correo, copia impresa o electrónica sin la debida autorización de los protocolos establecidos para la divulgación.

- Usar dispositivos de almacenamiento externo cuya autorización no haya sido otorgada por la coordinación de Gestión Tecnológica de la UNIVERSIDAD CATÓLICA DE PEREIRA.
- Permitir el acceso de personal externo, a la VLAN administrativa, sin la autorización de la coordinación de Gestión Tecnológica de la UNIVERSIDAD CATÓLICA DE PEREIRA.
- Ser negligente en el cuidado de los equipos, dispositivos portátiles o móviles, entregados para actividades propias de la UNIVERSIDAD CATÓLICA DE PEREIRA.
- Descuidar documentación con información reservada o clasificada, de la institución, sin las medidas apropiadas de seguridad, que garanticen su protección.
- Registrar información reservada o clasificada, en apuntes, agendas, libretas. Sin el debido cuidado. Ejemplo: resultado de pruebas psicológicas, información de historias laborales, información de procesos disciplinarios etc.
- Archivar información pública reservada o clasificada, sin claves de seguridad o cifrado de datos.
- Utilizar los recursos tecnológicos de la UNIVERSIDAD CATÓLICA DE PEREIRA para beneficio personal.
- Acceder en todo o parte del sistema de información o permanecer dentro del mismo utilizando técnicas de hacking (no ético) en contra de la voluntad de los controles de seguridad de la información de la UNIVERSIDAD CATÓLICA DE PEREIRA.

7.6.Política para el uso del computador de escritorio o portátil

Objetivo:

Difundir las normas para el buen funcionamiento y mantenimiento de los equipos de cómputo, portátil o de escritorio suministrados por la UNIVERSIDAD CATÓLICA DE PEREIRA a los usuarios internos.

Aplicabilidad:

Estas políticas aplican al personal administrativo, directivo, profesores y colaboradores, que tengan un vínculo contractual con la UNIVERSIDAD CATÓLICA DE PEREIRA y tengan asignado un equipo de cómputo de escritorio o portátil.

Normatividad:

- Gestión Tecnológica es el área encargada de solicitar la compra de equipos nuevos luego de haber realizado el estudio técnico y verificar la necesidad de cambiar o renovar los computadores.
- Gestión Tecnológica debe establecer una configuración adecuada para los computadores, de escritorio o portátiles, de los colaboradores antes de su primer uso.
- El área de soporte de Gestión Tecnológica es la responsable brindar mantenimiento y soporte a todos los equipos asignados a los colaboradores pertenecientes a la Alma Máter.
- El área de soporte de Gestión Tecnológica es la responsable de recibir los equipos nuevos (de escritorio o portátiles) tan pronto ingresen por primera vez a la UNIVERSIDAD CATÓLICA DE PEREIRA, los deben registrar en el sistema como activos fijos o elementos de control verificando que estén completos y en perfectas condiciones de funcionamiento.
- La Coordinación de Gestión Tecnológica es la responsable de autorizar la entrega del equipo nuevo de cómputo, portátil o de escritorio, a los colaboradores de la Universidad, y hacer firmar el documento de recepción de equipo.
- Todos los requerimientos de aplicativos y equipos informáticos deben ser solicitados a través de la mesa de ayuda de Gestión Tecnológica con su correspondiente justificación para su respectiva viabilidad.

- Los colaboradores de la UNIVERSIDAD CATÓLICA DE PEREIRA que, por las funciones de su cargo, por disposiciones médicas, o para atender reglamentaciones gubernamentales del orden nacional o local, requieran retirar de las instalaciones de la Universidad, equipos de cómputo (escritorio o portátil), impresoras, escáner, video-proyectores, entre otros, deben solicitar autorización a la coordinación de Gestión Tecnológica y a la Dirección Administrativa y Financiera y en algunos casos, se requerirá la autorización del respectivo jefe inmediato
- Los equipos de cómputo, portátiles o de escritorio, asignados a cada uno de los usuarios de la UNIVERSIDAD CATÓLICA DE PEREIRA, son propiedad de la Institución y, por lo tanto, esta es la encargada de definir las aplicaciones que se han de manejar en cada equipo. La instalación o desinstalación de aplicaciones de software por parte de los usuarios queda restringida.
- El uso de los equipos de cómputo, portátiles o de escritorio, debe limitarse única y exclusivamente a fines institucionales y deben ser validadas por un dominio.
- La Coordinación de Gestión Humana, deberá mantener informada a la Coordinación de Gestión Tecnológica de la rotación o desvinculación de los colaboradores o contratistas con el fin de recibir los equipos que se encontraban a cargo de estos usuarios.
- Los usuarios no deben realizar actos que impliquen un mal uso de los recursos tecnológicos. Estos actos incluyen, pero no se limitan, a: envió de correo electrónico masivo con fines no institucionales y práctica de juegos en línea, entre otros.
- Estarán bajo custodia de la Coordinación de Gestión Tecnológica los medios electrónicos que vengan originalmente con el software de los equipos de cómputo y sus respectivos manuales y licencias de uso, adicionalmente las claves para descargar el software de fabricantes de sus páginas web o sitios en internet y los passwords de administración de los equipos informáticos, sistemas de información o aplicativos.

- Periódicamente, la Coordinación de Gestión Tecnológica efectuará la revisión de los programas utilizados en cada dependencia. La descarga, instalación o uso de aplicativos o programas informáticos no autorizados será considerada como una infracción a la Política General de Seguridad de la Información de la UNIVERSIDAD CATÓLICA DE PEREIRA.

7.7.Política para el uso de las salas de sistemas y laboratorios.

Objetivo:

Garantizar y establecer reglas para el cuidado de los recursos institucionales y el buen funcionamiento de las salas de sistemas y laboratorios.

Aplicabilidad:

Estas políticas aplican al personal administrativo, directivo, docentes, estudiantes con matrícula académica y/o financiera vigente y graduados de los programas de la Universidad.

Normatividad:

- La administración de los recursos y funcionamiento de las salas de cómputo es responsabilidad de la Coordinación de Gestión Tecnológica a través del área de soporte.
- La administración de los recursos y funcionamiento de los diferentes laboratorios es responsabilidad de Gestión Tecnológica en conjunto con los directores de programa y/o coordinadores del laboratorio.
- La Coordinación de Gestión Tecnológica debe establecer una configuración adecuada de software y hardware para los equipos de cómputo que son parte de la infraestructura de las salas de sistemas de la

UNIVERSIDAD CATÓLICA DE PEREIRA de acuerdo con los requerimientos de cada sala.

- Los servicios de cómputo ofrecidos por las salas de sistemas de la Universidad se refieren al préstamo de los computadores con el software necesario para el desarrollo de clases o trabajos académicos y el acceso a Internet.
- El mantenimiento preventivo y correctivo de hardware y software de las salas de sistemas es deber de Gestión Tecnológica y se debe de realizar en los momentos que no se vean afectadas las labores académicas y/o administrativas programadas en ellas.
- La programación de horarios de clases en las salas será asignada las direcciones de programa y validadas con Gestión Tecnológica la disponibilidad a través del área de soporte técnico al inicio del semestre académico de la UNIVERSIDAD CATÓLICA DE PEREIRA.
- El servicio de las salas de sistemas será suspendido en caso de mantenimiento de emergencia, siniestro, o cuando las condiciones lo ameriten, a consideración de Gestión Tecnológica.
- Para las reservas extraordinarias durante el semestre, se deberá presentar la solicitud por medio de la mesa de ayuda de la UNIVERSIDAD CATÓLICA DE PEREIRA con al menos tres días hábiles de anticipación, especificando la fecha y hora, las aplicaciones (software) y el uso para el que requiere la sala. Esta reserva estará sujeta a la disponibilidad de las salas.
- Es deber del usuario que hace uso de la sala de cómputo entregarla en perfecto orden al finalizar su préstamo.
- Si durante la utilización de la sala de sistemas el usuario encuentra una falla física o lógica de cualquiera de los equipos de cómputo, debe informar a Gestión Tecnológica.
- Los usuarios no podrán efectuar ninguna de las siguientes labores sin autorización previa de la Coordinación de Gestión Tecnológica:

- ✓ Instalar software en cualquier equipo de cómputo de la sala.
- ✓ Bajar o descargar software de Internet u otro servicio en línea en cualquier equipo de cómputo de la sala.
- ✓ Modificar, revisar, transformar o adaptar cualquier software propiedad de la UNIVERSIDAD CATÓLICA DE PEREIRA.
- ✓ Descompilar o realizar ingeniería inversa en cualquier software de propiedad de la UNIVERSIDAD CATÓLICA DE PEREIRA.

7.8.Política para el manejo de la documentación física

Objetivo:

Mantener la integridad y disponibilidad del archivo de los documentos producidos en la ejecución de los procesos de la UNIVERSIDAD CATÓLICA DE PEREIRA, el cual se efectuará de conformidad con los instrumentos archivísticos aprobados.

Aplicabilidad:

Estas políticas aplican al personal administrativo, directivo, docentes, colaboradores, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales de la UNIVERSIDAD CATÓLICA DE PEREIRA.

Normatividad:

- Las tablas de retención documental establecen cuánto tiempo se deben mantener almacenados los archivos de acuerdo en cada una de las etapas de su ciclo vital.
- Las tablas de control de acceso establecen el tipo de información que se maneja en cada una de las series y subseries documentales y así mismo

establece el tipo de acceso a las mismas (acceso público, clasificado o reservado).

- Las reglas y los principios generales que regulan la función archivística de la UNIVERSIDAD CATÓLICA DE PEREJRA, se encuentran definidos por el Comité de Archivo y el Plan de Gestión Documental, siguiendo los lineamientos emitidos por el Archivo General de la Nación.
- La UNIVERSIDAD CATÓLICA DE PEREIRA promueve el uso de las tecnologías de la información y las comunicaciones en la administración, conservación de archivos por medio de la intranet.
- Mediante el uso de la plataforma Sevenet - Gestión Documental se conformarán expedientes virtuales de conformidad con las Tablas de Retención y Valoración Documental aprobadas.

7.9.Política para la seguridad en las redes de datos

Objetivo:

Propender por la protección de la información en las redes y de la infraestructura de soporte, además de la operación correcta y segura de los puntos de red.

Aplicabilidad:

Estas políticas aplican a los miembros de los consejos, administrativos, directivos, docentes, colaboradores, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales de la UNIVERSIDAD CATÓLICA DE PEREIRA

Normatividad:

- Los usuarios deberán emplear los puntos de red, para la conexión de equipos informáticos propiedad de la UNIVERSIDAD CATÓLICA DE PEREIRA.
- La activación y gestión de los puntos de red es responsabilidad de Gestión Tecnológica, la instalación de puntos de red se hará a través de Gestión del Campus.
- Las configuraciones de enrutadores, switches, firewalls, sistemas de detección de intrusos y otros dispositivos de seguridad de red, deben ser documentadas y mantenidas por la Gestión Tecnológica.
- Todo equipo tecnológico debe ser revisado, registrado y aprobado por la Coordinación de Gestión Tecnológica antes de conectarse a cualquier nodo de la Red de comunicaciones y datos institucional.
- Gestión Tecnológica debe desconectar aquellos dispositivos tecnológicos que no estén aprobados para estar conectados a los puntos de red de la Alma Máter y reportar tal conexión como un incidente de seguridad.
- Los colaboradores y personal provisto por terceras partes, antes de contar con acceso lógico por primera vez a la red de datos de la UNIVERSIDAD CATÓLICA DE PEREIRA, deben, contar con el formato de creación de cuentas de usuario debidamente autorizado y el Acuerdo de Confidencialidad firmado previamente.
- No se permite el ingreso al centro de datos, al personal que no esté expresamente autorizado. La Coordinación de Gestión Tecnológica debe llevar un control de ingreso y salida del personal que visita el centro de datos. En el centro de datos debe disponerse de una planilla para el registro, la cual debe ser diligenciada en lapicero de tinta al iniciar y finalizar la actividad a realizar.

- La Coordinación de Gestión Tecnológica debe garantizar que el control de acceso al centro de datos de la UNIVERSIDAD CATÓLICA DE PEREIRA cuenta con dispositivos electrónicos de autenticación.
- La Coordinación de Gestión Tecnológica deberá garantizar que todos los equipos de los centros de datos cuenten con un sistema alterno de respaldo de energía.
- La limpieza y aseo del centro de datos debe efectuarse en presencia de un funcionario de la Coordinación de Gestión Tecnológica. El personal de limpieza debe ser ilustrado con respecto a las precauciones mínimas a seguir durante el proceso de limpieza.
- En las instalaciones del centro de datos o centros de cableado, está prohibido fumar, comer o beber; de igual forma se debe eliminar la permanencia de papelería y materiales que representen riesgo de propagación de fuego, se debe mantener el orden y limpieza en todos los equipos y elementos que se encuentren en este espacio.
- El cableado de la red debe ser protegido de interferencias por medio de canaletas que lo protejan.
- Los cables de potencia de los equipos de cómputo de la UNIVERSIDAD CATÓLICA DE PEREIRA deben estar separados de los de comunicaciones.
- La toma de fotografías o la grabación de vídeo en las instalaciones del centro de datos debe estar expresamente autorizada por la Coordinación de Gestión Tecnológica y exclusivamente con fines institucionales.
- Las puertas del centro de datos deben permanecer cerradas. Si por alguna circunstancia se requiere ingresar y salir del centro de datos, el funcionario responsable de la actividad se ubicará dentro del centro de datos.
- Mientras no se encuentre personal dentro de las instalaciones del centro de datos, las luces deben permanecer apagadas.
- Los equipos del centro de datos que se requieran deben estar monitoreados, con el fin de poder detectar las fallas que se puedan presentar y llevar una bitácora de seguimiento.

7.10.Política para el uso de contraseñas

Objetivo:

Brindar protección a la información en todos los dispositivos electrónicos pertenecientes a la Alma Máter, por medio del buen uso de las contraseñas de acceso.

Aplicabilidad:

Estas políticas aplican a los miembros de los consejos, administrativos, directivos, docentes, colaboradores, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales de la UNIVERSIDAD CATÓLICA DE PEREIRA.

Normatividad:

- La Coordinación de Gestión Tecnológica deben concienciar y controlar que los usuarios sigan buenas prácticas de seguridad en la selección, uso y protección de claves o contraseñas, las cuales constituyen un medio de validación de la identidad de un usuario y consecuentemente un medio para establecer derechos de acceso a las instalaciones, equipos o servicios informáticos de la UNIVERSIDAD CATÓLICA DE PEREIRA.
- Los usuarios son responsables del uso de las claves o contraseñas de acceso que se le asignen para la utilización de los equipos o servicios informáticos de la UNIVERSIDAD CATÓLICA DE PEREIRA.
- Los accesos a la información y sistemas informáticos deben ser solicitados siempre por el responsable directo del usuario a la Coordinación de Gestión Tecnológica. Dichos accesos deben ser siempre justificables por la labor que se va a realizar.

- El usuario será responsable de todas las transacciones o acciones efectuadas con su "cuenta de usuario".
- Ningún usuario deberá acceder a la red, sistema educativo, ERP, etc., con las credenciales de otro usuario.
- Los usuarios deben tener en cuenta los siguientes aspectos:

  - ✓ El cambio de contraseña sólo podrá ser solicitado por el titular de la cuenta o su jefe inmediato a la Coordinación de Gestión Tecnológica o en su defecto de manera automática con la periodicidad definida por Gestión Tecnológica.
  - ✓ Terminar las sesiones activas cuando finalice, o asegurarlas con el mecanismo de bloqueo cuando no estén en uso.
  - ✓ Se bloqueará el acceso a todo usuario cuando se detecté varios intentos de ingresos sin éxito, a un equipo o sistema informático, en forma consecutiva.

- Las contraseñas deben:

  - ✓ Tener algún grado de complejidad y no deben ser palabras comunes que se puedan encontrar en diccionarios, ni tener información personal, por ejemplo: fechas de cumpleaños, nombre• de los hijos, placas de automóvil, entre otros.
  - ✓ Tener por lo menos un carácter especial, una letra mayúscula, una letra minúscula y un carácter numérico.
  - ✓ Cambiarse obligatoriamente la primera vez que el usuario ingrese al sistema.
  - ✓ Cada vez que se cambien estas deben ser distintas por lo menos de las últimas tres anteriores.
  - ✓ Cambiarse si la contraseña ha estado bajo riesgo o se ha detectado anomalía en la cuenta de usuario.

- ✓ No ser visible en la pantalla, al momento de ser ingresada o mostrarse o compartirse.
- ✓ No ser reveladas a ninguna persona, incluyendo al personal de Gestión Tecnológica.
- ✓ No ser registradas en papel, archivos digitales o dispositivos manuales.
- ✓ Cambiarse la contraseña del directorio activo de la UNIVERSIDAD CATÓLICA DE PEREIRA regularmente cada seis (06) meses.

- En el caso de las tabletas:

  - ✓ Deben evitarse los controles de acceso basados en patrones de puntos, siendo los más deseables el control biométrico o la huella dactilar para aquellos dispositivos que lo soporten.

  - ✓ Debe de estar activado el bloqueo temporal. 'En algunos dispositivos con información muy sensible, podría Activarse incluso el check de borrado completo del dispositivo si hay 10 fallos seguidos en la autenticación.

- Tanto en computadores portátiles como en Smartphone y tablets, habrá de activarse las políticas de bloqueo de sesión (o de apagado de pantalla) solicitando autenticación para volver a interactuar con el dispositivo. El periodo máximo de inactividad antes de, dicho bloqueo debe ser de un (01) minuto para Smartphone y Tablets, así como tres (03) minutos para computadores portátiles.

7.11. Política para el uso de Internet

Objetivo:

Establecer lineamientos que garanticen la navegación segura en internet, evitando errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información.

Aplicabilidad:

Estas políticas aplican a los miembros de los consejos, administrativos, directivos, docentes, colaboradores, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales de la UNIVERSIDAD CATÓLICA DE PEREIRA.

Normatividad:

- Gestión Tecnológica se encargará de controlar el acceso a sitios web que puedan afectar la confidencialidad, integridad y disponibilidad de la información propia de la Universidad.
- Está permitido a los colaboradores de la UNIVERSIDAD CATÓLICA DE PEREIRA la descarga de archivos de Internet sólo para propósitos institucionales.
- Está permitido el acceso a servicios de mensajería instantánea y redes sociales sólo para los colaboradores de la UNIVERSIDAD CATÓLICA DE PEREIRA que teniendo en cuenta sus funciones deben hacer uso de estos servicios.
- Los usuarios del servicio de internet no deben acceder a páginas relacionadas con pornografía, drogas, hacking o cualquier otro sitio web que vaya en contra de las leyes vigentes o políticas establecidas en este documento.

- Los colaboradores deberán abstenerse de enviar información privada reservada, confidencial o de uso interno de la institución en sitios web que no hagan parte de los procesos establecidos con otras instituciones.
- En caso de ser necesario Gestión Tecnológica, podrá acceder a revisar cualquier tipo de activo de información y material que los usuarios creen, almacenen, envíen o reciban, a través de Internet de cualquier otra red o medio, en los equipos informáticos a su cargo.

7.12. Política para el uso de carpetas virtuales

Objetivo:

Establecer una operación correcta y segura de los discos de red o carpetas virtuales.

Aplicabilidad:

Estas políticas aplican a los miembros de los consejos, administrativos, directivos, docentes, colaboradores, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales de la UNIVERSIDAD CATÓLICA DE PEREIRA.

Normatividad:

- Gestión Tecnológica se encargará de dar acceso a la información ubicada en las carpetas de red. Los usuarios tendrán permisos de escritura, lectura o modificación de información en las carpetas de red, dependiendo de sus funciones y su cargo.
- Gestión Tecnológica se encargará de generar copias de respaldo de la información de las carpetas de red diariamente y de conservar la seguridad, confidencialidad y disponibilidad de estas.

- La información institucional que se trabaje en los computadores personales de cada usuario debe ser trasladada periódicamente a las carpetas de red por ser información institucional.
- La información almacenada en cualquiera de las carpetas de red debe ser de carácter institucional.
- No está permitido extraer, divulgar o publicar información de cualquiera de los discos de red sin expresa autorización del jefe inmediato.

7.13. Política para la adquisición, desarrollo y mantenimiento de software

Objetivo:

Definir la normatividad para la adquisición, desarrollo y mantenimiento de software en la UNIVERSIDAD CATÓLICA DE PEREIRA.

Aplicabilidad:

Estas políticas aplican a los miembros de los consejos, administrativos, directivos, docentes, colaboradores, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales de la UNIVERSIDAD CATÓLICA DE PEREIRA.

Normatividad:

- Gestión Tecnológica es el área encargada de definir la zona de almacenamiento de los aplicativos propios de la Universidad.
- Para el desarrollo de software propio de la Universidad se deben tener tres ambientes: producción, desarrollo y pruebas.

- Los datos en los ambientes de desarrollo y pruebas deben ser diferentes a los de producción, garantizando que los desarrolladores o tester's no conozcan datos reales de la Universidad.
- Todo el software usado en el desarrollo de aplicaciones debe estar licenciado o contar con la debida autorización del proveedor.
- Se deben tener acuerdos de licencias, propiedad de código y derechos de propiedad intelectual con las empresas y personal que desarrollen software para la Universidad.
- La interconexión con sistemas internos o externos deberá cumplir con los criterios de confidencialidad, integridad, disponibilidad, además de definir los niveles de acuerdo del servicio.
- Para la adquisición y actualización de software y/o sistema de información, es necesario efectuar la solicitud a la Coordinación de Gestión Tecnológica con sustentación de un proyecto ante la Dirección de Planeación y Calidad.
- Todo software nuevo que se vaya a adquirir y conectar a la plataforma tecnológica de la UNIVERSIDAD CATÓLICA DE PEREIRÁ, por cualquier dependencia o proyecto de la Universidad, deberá ser gestionado por el Área de Gestión Tecnológica.
- La instalación del software en los equipos de cómputo de la UNIVERSIDAD CATÓLICA DE PEREIRA se realizará únicamente a través del Área de Gestión Tecnológica.
- El software proporcionado por la UNIVERSIDAD CATÓLICA DE PEREIRA a los usuarios no puede ser copiado o suministrado a terceros.
- Para la adquisición y actualización de software, es necesario efectuar la solicitud a la Coordinación e Gestión Tecnológica con su justificación.

7.14. Política para la seguridad física y del entorno

Objetivo:

Asegurar la operación correcta y segura de la información en formato impreso.

Aplicabilidad:

Estas políticas aplican a los miembros de los consejos, administrativos, directivos, docentes, colaboradores, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales de la UNIVERSIDAD CATÓLICA DE PEREIRA.

Normatividad:

- Las oficinas deben contar con restricción de acceso, que impidan la entrada a personas externas o no autorizadas.
- Los equipos de cómputo que estén ubicados cerca a zonas de atención al público deberán ubicarse de tal forma que las pantallas no puedan ser visualizadas por personas no autorizadas.
- Los documentos con información identificada como clasificada o reservada deben ser protegidos de tal forma que no sean de fácil acceso o dejados a la vista. Cuando la persona responsable de la información se ausente de su lugar de trabajo, debe guardar cualquier documento que contenga información sensible.
- Los colaboradores de la UNIVERSIDAD CATÓLICA DE PEREIRA deben conservar su escritorio libre de información, propia de la entidad, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.

- Al imprimir documentos de carácter confidencial, estos deben ser retirados de la impresora inmediatamente y no se deben dejar en el escritorio sin custodia.

ARTÍCULO 2: La presente Resolución rige a partir de la fecha de expedición.

COMUNÍQUESE Y CÚMPLASE

Dado en Pereira a los nueve (09) días del mes de septiembre del dos mil veinte (2020)

BEHITMAN ALBERTO CÉSPEDES DE LOS RÍOS, Pbro.
Rector