CORPORACIÓN UNIVERSITARIA
AUTÓNOMA
DEL CAUCA

RESOLUCIÓN No. 0187

(26 SET. 2018)

POR LA CUAL SE APRUEBA EN PRIMERA INSTANCIA LA POLÍTICA DE SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN DE LA CORPORACIÓN UNIVERSITARIA AUTÓNOMA DEL CAUCA

El Consejo Administrativo de la Corporación Universitaria Autónoma del Cauca, en uso de sus facultades legales y estatutarias, conferida en los estatutos vigentes, y en desarrollo del artículo 55, literal a) y,

CONSIDERANDO:

1. Que la Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la alta dirección de La Corporación Universitaria Autónoma Del Cauca con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros. la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Institución;

2. Que la Política de Seguridad y Privacidad de la Información servirá como base para la creación de otras políticas que estén orientadas al tratamiento de la información, por medio de la generación y publicación de sus lineamientos, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información;

3. Que la creación de las políticas dentro del contexto de la seguridad de la información guiará el comportamiento personal y profesional de los funcionarios, contratistas o terceros sobre la información obtenida, generada o procesada por la entidad, así mismo las políticas permitirán que la Institución trabaje bajo las mejores prácticas de seguridad y cumpla con los requisitos legales a los cuales esté obligada a cumplir;

4. Que, para la Corporación Universitaria Autónoma del Cauca, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la

disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados;

5. Que en reunión ordinaria de Consejo Administrativo realizada el día miércoles veintiséis (26) de septiembre de 2018, se analizó y debatió la propuesta presentada por la división de Tecnologías y Medio Educativos;

RESUELVE:

ARTÍCULO PRIMERO: Aprobar la política de seguridad y privacidad de la información de la Corporación Universitaria Autónoma del Cauca así:

1. INTRODUCCIÓN Y OBJETIVOS

Para asegurar la dirección estratégica de la Entidad, la Corporación Universitaria Autónoma del Cauca establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

a) Minimizar el riesgo de los procesos misionales de la entidad.
b) Cumplir con los principios de seguridad de la información.
c) Cumplir con los principios de la función administrativa.
d) Mantener la confianza de los funcionarios, contratistas y terceros.
e) Apoyar la innovación tecnológica.
f) Implementar el sistema de gestión de seguridad de la información.
g) Proteger los activos de información.
h) Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
i) Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de la Corporación Universitaria Autónoma del Cauca.
j) Garantizar la continuidad del negocio frente a incidentes.

2. ALCANCE/APLICABILIDAD

Esta política aplica a todo el personal con un vínculo laboral o comercial con LA CORPORACIÓN UNIVERSITARIA AUTÓNOMA DEL CAUCA y a todos los otros usuarios externos autorizados a acceder a los recursos de Información de la organización.

3. DEFINICIONES

Activo (asset): Todo lo que tiene valor para la Organización. Hay varios tipos de activos entre los que se incluyen:

a) Información
b) Software, como un programa de cómputo.
c) Físico, como un computador
d) Servicios
e) Personas, sus calificaciones, habilidades y experiencia.
f) Intangibles, tales como la reputación y la imagen.

Clave: contraseña, clave o password es una forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña debe mantenerse en secreto ante aquellos a quien no se le permite el acceso. A aquellos que desean acceder a la información se les solicita una clave; si conocen o no conocen la contraseña, se concede o se niega el acceso a la información según sea el caso. En ocasiones clave y contraseña se usan indistintamente. (Asimismo llamado PIN - Personal Identification Number).

Confidencial: significa que la información no esté disponible o revelada a individuos, entidades o procesos no autorizados.

Correo Electrónico Institucional: Es el servicio basado en el intercambio de información a través de la red y el cual es provisto por la Institución, para los funcionarios, contratistas y practicantes autorizados para su acceso. El propósito principal es compartir información de forma rápida, sencilla y segura. El sistema de correo electrónico puede ser utilizado para el intercambio de información, administración de libreta de direcciones, manejo de contactos, administración de agenda y el envío y recepción de documentos, relacionados con las responsabilidades institucionales.

Custodio de la información: es el encargado de la administración de seguridad de información. Dentro de sus responsabilidades se encuentra la gestión del Plan de Seguridad de Información, así como la coordinación de esfuerzos entre el personal de sistemas y los responsables de las otras áreas de la Entidad, siendo estos últimos los responsables de la información que utilizan. Asimismo, es el responsable de promover la seguridad de información en todo el Instituto con el fin de incluirla en el planteamiento y ejecución de los objetivos institucionales.

Disponibilidad de la información: La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. A groso modo, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

Hardware: Conjunto de los componentes que integran la parte material de una computadora.

Integridad: Propiedad de salvaguardar la exactitud de la información y sus métodos de procesamiento los cuales deben ser exactos.

Información: Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.

Internet: Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación.

Intranet: Una intranet es una red informática que utiliza la tecnología del Protocolo de Internet para compartir información, sistemas operativos o servicios de computación dentro de una organización.

Malware: El malware es la descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras. El malware a menudo utiliza herramientas de comunicación populares, como el correo electrónico y la mensajería instantánea, y medios magnéticos extraíbles, como dispositivos USB, para difundirse. También se propaga a través de descargas inadvertidas y ataques a las vulnerabilidades de seguridad en el software. La mayoría del malware peligroso actualmente busca robar información personal que pueda ser utilizada por los atacantes para cometer fechorías.

Mecanismos de bloqueo: son los mecanismos necesarios para impedir que los usuarios, tanto de los sistemas de información como de los servicios, tengan acceso a estos sin previa autorización, ya sea por razones de seguridad, falta de permisos, intentos malintencionados o solicitud de los propietarios de la información. Los bloqueos pueden ser temporales o definitivos dependiendo del tipo de situación presentada.

Memoria USB: La memoria USB (Universal Serial Bus) es un tipo de dispositivo de almacenamiento de datos que utiliza memoria flash para guardar datos e información. Se le denomina también lápiz de memoria, lápiz USB o memoria externa, siendo innecesaria la voz inglesa pen drive o pendrive.

Mensajería Instantánea Institucional: Comúnmente conocido como "Chat", es un canal de comunicación provisto por la Institución para facilitar una forma de comunicación en tiempo real entre los funcionarios, contratistas y practicantes autorizados creando un espacio virtual de encuentro específico.

Phishing (cosecha y pesca de contraseñas): Es un delito cibernético con el que por medio del envío de correos se engaña a las personas invitándoles a que visiten páginas web falsas de entidades bancarias o comerciales. Allí se solicita que verifique o actualice sus datos con el fin de robarle sus nombres de usuarios, claves personales y demás información confidencial.

Política: Declaración general de principios que presenta la posición de la administración para un área de control definida. Las políticas se elaboran con el fin de que tengan aplicación a largo plazo y guíen el desarrollo de reglas y criterios más específicos que aborden situaciones concretas. Las políticas son desplegadas y soportadas por

estándares, mejores prácticas, procedimientos y guías, las políticas deben ser pocas (es decir un número pequeño), deben ser apoyadas y aprobadas por las directivas de la Institución y deben ofrecer direccionamientos a toda la Entidad o a un conjunto importante de dependencias. Por definición, las políticas son obligatorias y la incapacidad o imposibilidad para cumplir una política exige que se apruebe una excepción.

Propietario de la información: En tecnologías de la información y la comunicación (TIC) es el responsable de preservar y disponer de la información de acuerdo a los lineamientos de la Entidad. El término tecnologías de la información se usa a menudo para referirse a cualquier forma de hacer cómputo. Como nombre de un programa de licenciatura, se refiere a la preparación que tienen estudiantes para satisfacer las necesidades de tecnologías en cómputo y comunicación de gobiernos, seguridad social, escuelas y cualquier tipo de organización.

Puntos de entrada y salida: Cualquier dispositivo (distinto de la memoria RAM) que intercambie datos con el sistema lo hace a través de un "puerto", por esto se denominan también puertos de E/S ("I/O ports"). Desde el punto de vista del software, un puerto es una interfaz con ciertas características; se trata por tanto de una abstracción (no nos referimos al enchufe con el que se conecta físicamente un dispositivo al sistema), aunque desde el punto de vista del hardware, esta abstracción se corresponde con un dispositivo físico capaz de intercambiar información (E/S) con el bus de datos.

RSS (Really Simple Syndication): RSS son las siglas de Really Simple Syndication, un formato XML para sindicar o compartir contenido en la web. Se utiliza para difundir información actualizada frecuentemente a usuarios que se han suscrito a la fuente de contenidos. El formato permite distribuir contenidos sin necesidad de un navegador, utilizando un software diseñado para leer estos contenidos RSS tales como Internet Explorer, entre otros (agregador).

Scanner: Es un periférico que permite transferir una imagen desde un papel o superficie y transformarlos en gráficos digital (proceso también llamado digitalización). Existen actualmente escáneres que capturan objetos en tres dimensiones. Suelen utilizar un haz de luz o láser para realizar el proceso. Los escáneres no distinguen el texto de los gráficos, por lo tanto, debe existir un procesamiento de la imagen escaneada para generar texto editable. Este proceso es llamado OCR, y existen múltiples aplicaciones para tal fin. La resolución de los escáneres se mide en DPI.

Seguridad de la información: Hace referencia a la preservación de la confidencialidad (propiedad de que la información, significa que no esté disponible o revelada a individuos no autorizados, entidades o procesos.), integridad (protección de la exactitud e integridad de los activos) y disponibilidad (propiedad de ser accesibles y utilizables a la demanda por una entidad autorizada) de la información.

Servicio: Es el conjunto de acciones o actividades de carácter misional diseñadas para incrementar la satisfacción del usuario, dándole valor agregado a las funciones de la entidad.

Servicios de almacenamiento de archivos "On line": Un servicio de alojamiento de archivos, servicio de almacenamiento de archivos online, o centro de medios online es un servicio de alojamiento de Internet diseñado específicamente para alojar contenido estático, mayormente archivos grandes que no son páginas web. En general estos servicios permiten acceso web y FTP. Pueden estar optimizados para servir a muchos usuarios (como se indica con el término "alojamiento") o estar optimizados para el almacenamiento de usuario único (como se indica con el término "almacenamiento"). Algunos servicios relacionados con el alojamiento de vídeos, alojamiento de imágenes, el almacenamiento virtual y el copiado de seguridad remoto.

SGSI: Sistema de Gestión de Seguridad de la Información: Es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System. En el contexto, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración. La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

Sistemas de Información: Un sistema de información es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo. Habitualmente el término se usa de manera errónea como sinónimo de sistema de información informático, en parte porque en la mayoría de los casos los recursos materiales de un sistema de información están constituidos casi en su totalidad por sistemas informáticos. Estrictamente hablando, un sistema de información no tiene por qué disponer de dichos recursos (aunque en la práctica esto no suela ocurrir). Se podría decir entonces que los sistemas de información informáticos son una subclase o un subconjunto de los sistemas de información en general.

Smartphone: El teléfono inteligente (en inglés: smartphone) es un tipo teléfono móvil construido sobre una plataforma informática móvil, con una mayor capacidad de almacenar datos y realizar actividades, semejante a la de una minicomputadora, y con una mayor conectividad que un teléfono móvil convencional. El término «inteligente», que se utiliza con fines comerciales, hace referencia a la capacidad de usarse como un computador de bolsillo, y llega incluso a reemplazar a una computadora personal en algunos casos.

Software: Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora.

Spam: También conocido como correo basura, el spam es correo electrónico que involucra mensajes casi idénticos enviados a numerosos destinatarios. Un sinónimo

común de spam es correo electrónico comercial no solicitado (UCE). El malware se utiliza a menudo para propagar mensajes de spam al infectar un equipo, buscar direcciones de correo electrónico y luego utilizar esa máquina para enviar mensajes de spam. Los mensajes de spam generalmente se utilizan como un método de propagación de los ataques de phishing.

Tecnología de la información T.I.: Hace referencia a las aplicaciones, información e infraestructura requerida por una entidad para apoyar el funcionamiento de los procesos y estrategia de negocio.

Tipos de información: cualquier tipo de información producida y/o recibida en la Institución, sus dependencias y funcionarios y en general por cualquier persona que desarrolle actividades inherentes a la función de dicha entidad o que hayan sido delegados por esta, independientemente del soporte y medio de registro (análogo o digital) en que se produzcan, y que se conservan en:

a) Documentos de Archivo (físicos y electrónicos).
b) Archivos institucionales (físicos y electrónicos).
c) Sistemas de Información Corporativos.
d) Sistemas de Trabajo Colaborativo.
e) Sistemas de Administración de Documentos.
f) Sistemas de Mensajería Electrónica.
g) Portales, Intranet y Extranet.
h) Sistemas de Bases de Datos.
i) Discos duros, servidores, discos o medios portables, cintas o medios de video y audio (análogo o digital), etc.
j) Cintas y medios de soporte (back up o contingencia).
k) Uso de tecnologías en la nube.

Usuario de la información: Para la informática es un usuario aquella persona que utiliza un dispositivo o un ordenador y realiza múltiples operaciones con distintos propósitos. A menudo es un usuario aquel que adquiere una computadora o dispositivo electrónico y que lo emplea para comunicarse con otros usuarios, generar contenido y documentos, utilizar software de diverso tipo y muchas otras acciones posibles. El usuario no es necesariamente uno en particular instruido o entrenado en el uso de nuevas tecnologías, ni en programación o desarrollo, por lo cual la interfaz del dispositivo en cuestión debe ser sencilla y fácil de aprender. Sin embargo, cada tipo de desarrollo tiene su propio usuario modelo y para algunas compañías el parámetro de cada usuario es distinto.

Webcam: Cámara Web: Una cámara web o cámara de red (en inglés: webcam) es una pequeña cámara digital conectada a una computadora la cual puede capturar imágenes y transmitirlas a través de Internet, ya sea a una página web o a otra u otras computadoras de forma privada. Las cámaras web necesitan una computadora para transmitir las imágenes. Sin embargo, existen otras cámaras autónomas que tan sólo necesitan un punto de acceso a la red informática, bien sea ethernet o inalámbrico. Para diferenciarlas de las cámaras web se las denomina cámaras de red.

4. MARCO LEGAL Y NORMATIVO

LEY 23 DE 1982 sobre Derechos de Autor. Congreso de la República. Disponible en Línea http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=3431 [Recuperado en enero de 2017]

CONSTITUCIÓN POLÍTICA DE COLOMBIA 1991; Artículo 15. "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. Disponible en Línea: http://www.constitucioncolombia.com/titulo-2/capitulo-1/articulo-15 [Recuperado en enero de 2017]

LEY 527 DE 1999; por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276 [Recuperado en enero de 2017]

LEY 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, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488 [Recuperado en enero de 2017]

LEY 1273 DE 2009, Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492 [Recuperado en enero de 2017]

LEY 1474 DE 2011 Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=43292 [Recuperado en enero de 2017]

DECRETO 4632 DE 2011 Por medio del cual se reglamenta parcialmente la Ley 1474 de 2011 en lo que se refiere a la Comisión Nacional para la Moralización y la Comisión Nacional Ciudadana para la Lucha contra la Corrupción y se dictan otras disposiciones. Disponible en Línea: http://wsp.presidencia.gov.co/Normativa/Decretos/2011/Documents/Diciembre/09/dec463209122011.pdf [Recuperado en enero de 2017]

LEY ESTATUTARIA 1581 DE 2012, Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981. [Recuperado en enero de 2017]

DECRETO 1377 DE 2013 Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646 [Recuperado en enero de 2017]

NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC colombiana 27001:20013. 2013-12-11. Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.

MANUAL GOBIERNO EN LÍNEA 3.1 Ver 2014-06-12. Para la Implementación de la Estrategia de Gobierno en Línea, entidades del orden nacional; Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea; Formato Política SGSI - Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea.

DECRETO 103 DE 2015, por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=60556 [Recuperado en enero de 2017]

DECRETO 1494 DE 2015, Por el cual se corrigen yerros en la Ley 1712 de 2014. Disponible en Línea: http://wp.presidencia.gov.co/sitios/normativa/decretos/2015/Decretos2015/DECRETO%201494%20DEL%2013%20DE%20JULIO%20DE%202015.pdf [Recuperado en enero de 2017]

5. NIVEL DE CUMPLIMIENTO.

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

A continuación, se establecen los lineamientos la Política de Seguridad de la Corporación Universitaria Autónoma del Cauca, que para este efecto se llamará como "Institución".

La Institución ha decidido definir, implementar, operar y mejorar de forma continua una Política de Seguridad y Confidencialidad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.

La Institución protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.

La Institución protegerá la información creada, procesada, transmitida o resguardada por procesos institucionales relacionados la comunidad académica, administrativa y financiera, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

Toda la información que es generada por toda la comunidad académica (administrativos, docentes y estudiantes), contratistas y pasantes de la Institución en beneficio y desarrollo de las actividades propias de entidad es propiedad de la Corporación Universitaria Autónoma del Cauca, a menos que se acuerde lo contrario en los contratos escritos y autorizados. Esto también incluye la información que pueda ser adquirida o cedida a la Institución de parte de entidades o fuentes externas de información que sean contratadas o que tengan alguna relación con la Institución.

La Institución protegerá su información de las amenazas originadas por parte del personal.

La Institución protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

La Institución controlará la operación de sus procesos institucionales relacionados la comunidad académica, administrativa y financiera garantizando la seguridad de los recursos tecnológicos y las redes de datos.

La Institución implementará control de acceso a la información, sistemas y recursos de red.

La Institución garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

La Institución garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

La Institución garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

La Institución garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

Las responsabilidades frente a la seguridad de la información de la Institución serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.

A este documento podrán integrarse en adelante lineamientos o políticas relativas a la seguridad y privacidad de la información siempre y cuando no sea contrario a lo expresado en esta política.

5.1 RESPONSABILIDADES FRENTE A LA POLÍTICA DE SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN.

5.1.1 RESPONSABILIDADES DE LA DIVISIÓN DE TECNOLOGÍA Y MEDIOS EDUCATIVOS

a) Establecer, mantener y divulgar las políticas y procedimientos de servicios de tecnología, incluida esta política de seguridad de la información y todos sus artículos, el uso de los servicios tecnológicos en toda la Institución de acuerdo a las mejores prácticas y lineamientos de la División de Tecnología y Medios Educativos y directrices de la Dirección General Administrativa.

b) Mantener la custodia de la información que reposa en los diferentes sistemas de información, bases de datos y aplicativos de la Institución.

c) La División de Tecnología y Medios Educativos debe aplicar las sanciones pertinentes a la comunidad académico administrativa (Directivos, administrativos, docentes, estudiantes, contratistas y pasantes) de la Institución por los eventos que estén en contra de la seguridad de la información y de la infraestructura tecnológica de la Institución. La sanción debe ser homologada de acuerdo con el reglamento interno de trabajo en el capítulo XIX "Escala de Faltas y Sanciones Disciplinarias" expedido por la Unidad de Talento Humano y Bienestar Institucional. Al respecto para mayor información se describe en el artículo segundo de acciones disciplinarias.

d) Proporcionar medidas de seguridad físicas, lógicas y procedimentales para la protección de la información digital de la Institución.

e) Aplicar y hacer cumplir la Política de Seguridad y Privacidad de la Información y sus componentes.

f) Administrar las reglas y atributos de acceso a los equipos de cómputo, sistemas de información, aplicativos y demás fuentes de información al servicio de la Institución.

g) Analizar, aplicar y mantener los controles de seguridad implementados para asegurar los datos e información gestionados en la Institución.

h) Resolver de común acuerdo con las demás unidades académico administrativas y los propietarios de la información los conflictos que se presenten por la propiedad de la información al interior de la Institución. Esto incluye los posibles medios de acceso a la información, los datos derivados del procesamiento de la información a través de cualquier aplicación o sistema, los datos de entrada a las aplicaciones y los datos que son parte integral del apoyo de la solicitud.

i) Habilitar/Deshabilitar el reconocimiento y operación de Dispositivos de Almacenamiento externo de acuerdo con las directrices emitidas de parte de la División de Tecnología y Medios Educativos y las diferentes direcciones.

j) Implementar los mecanismos de controles necesarios y pertinentes para verificar el cumplimiento de la presente política.

5.1.2 RESPONSABILIDADES DE LOS PROPIETARIOS DE LA INFORMACIÓN

Son propietarios de la información cada uno de los directores, así como los jefes de las oficinas donde se genera, procesa y mantiene información, en cualquier medio, propia del desarrollo de sus actividades.

a) Valorar y clasificar la información que está bajo su administración y/o generación.
b) Autorizar, restringir y delimitar a los demás usuarios de la institución el acceso a la información de acuerdo a los roles y responsabilidades de los diferentes funcionarios, contratistas o practicantes que por sus actividades requieran acceder a consultar, crear o modificar parte o la totalidad de la información.
c) Determinar los tiempos de retención de la información en conjunto con la unidad de Gestión Documental y Correspondencia y las áreas que se encarguen de su protección y almacenamiento de acuerdo a las determinaciones y políticas de la entidad como de los entes externos y las normas o leyes vigentes.
d) Determinar y evaluar de forma permanente los riesgos asociados a la información, así como los controles implementados para el acceso y gestión de la administración comunicando cualquier anomalía o mejora tanto a los usuarios como a los custodios de la misma.
e) Acoger e informar los requisitos de esta política a todos los funcionarios, contratistas y practicantes en las diferentes dependencias del Instituto.

5.1.3 RESPONSABILIDADES DE LOS FUNCIONARIOS, CONTRATISTAS Y PRACTICANTES USUARIOS DE LA INFORMACIÓN.

a) Utilizar solamente la información necesaria para llevar a cabo las funciones que le fueron asignadas, de acuerdo con los permisos establecidos o aprobados en el Manual de Funciones y el reglamento interno de trabajo, expedido por la División de Talento Humano y Bienestar Institucional.
b) Manejar la Información de la Institución y rendir cuentas por el uso y protección de tal información, mientras que esté bajo su custodia. Esta puede ser física o electrónica e igualmente almacenada en cualquier medio.
c) Proteger la información a la cual acceden y procesen, para evitar su pérdida, alteración, destrucción o uso indebido
d) Evitar la divulgación no autorizada o el uso indebido de la información.
e) Cumplir con todos los controles establecidos por los propietarios de la información y los custodios de la misma.
f) Informar a sus superiores sobre la violación de estas políticas o si conocen de alguna falta a alguna de ellas.
g) Proteger los datos almacenados en los equipos de cómputo y sistemas de información a su disposición de la destrucción o alteración intencional o no justificada y de la divulgación no autorizada.
h) Reportar los Incidentes de seguridad, eventos sospechosos y el mal uso de los recursos que identifique, a la División de Tecnología y Medios Educativos.

i) Proteger los equipos de cómputo, de comunicaciones y demás dispositivos tecnológicos o técnico-científicos designados para el desarrollo de sus funciones. No está permitida la conexión de equipos de cómputo y de comunicaciones ajenos al instituto al a red Institucional ni el uso de dispositivos de acceso externo a Internet o de difusión de señales de red que no hayan sido previamente autorizadas por la División de Tecnología y Medios Educativos.

j) Usar software autorizado que haya sido adquirido legalmente por la Institución. No está permitido la instalación ni uso de software diferente al Institucional sin el consentimiento de la División de Tecnología y Medios Educativos.

k) Justificar el uso de equipos tecnológicos por fuera de los asignados por la Institución que presten cualquier servicio en pro del desarrollo de sus funciones. Se debe tener autorización de la División de Tecnología y Medios Educativos el cual evaluará la viabilidad del uso del equipo.

l) Divulgar, aplicar y el cumplir con la presente Política.

m) Aceptar y reconocer que en cualquier momento y sin previo aviso, la Dirección General o la Representación Legal de la Institución, puede solicitar una inspección de la información a su cargo sin importar su ubicación o medio de almacenamiento. Esto incluye todos los datos y archivos de los correos electrónicos institucionales, sitios web institucionales y redes sociales propiedad del Institución, al igual que las unidades de red institucionales, computadoras, servidores u otros medios de almacenamiento propios de la Institución. Esta revisión puede ser requerida para asegurar el cumplimiento de las políticas internamente definidas, por actividades de auditoría y control interno o en el caso de requerimientos de entes fiscalizadores y de vigilancia externos, legales o gubernamentales.

n) Proteger y resguardar su información personal que no esté relacionada con sus funciones en la Institución. **La Institución** no es responsable por la pérdida de información, desfalco o daño que pueda tener un usuario al brindar información personal como identificación de usuarios, claves, números de cuentas o números de tarjetas débito/crédito.

6 LINEAMIENTOS POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

6.1 Lineamiento 1: Uso de recursos tecnológicos

Expone las condiciones, normas y procedimientos necesarios para la regulación del uso de los recursos informáticos y de servicios de red que la Institución proporciona a la comunidad académica para el óptimo desarrollo de su quehacer Institucional. Este documento reposa en el Manual de Recursos Tecnológicos.

6.2 Lineamiento 2: Uso del servicio de correo electrónico

Reglamenta la gestión sobre las cuentas de los correos electrónicos Institucional, además concientiza a los funcionarios, contratistas o practicantes

de la Institución de los riesgos asociados con el uso de correo electrónico y presenta las normas y protocolos a seguir para el buen uso de este servicio. Este documento reposa en el Manual de Correos Electrónicos.

6.3 Lineamiento 3: Tratamiento y buen uso de datos personales

Se presenta la política para el tratamiento de datos personales, la cual será informada a todos los titulares de los datos recolectados o que en el futuro se obtengan en el ejercicio de las actividades académicas, culturales, comerciales o laborales. Dando cumplimiento a lo dispuesto en la Ley estatutaria 1581 de 2012 y a su Decreto Reglamentario 1377 de 2013. Este documento reposa en la política específica de Tratamiento de protección de datos personales de los titulares de la Corporación Universitaria Autónoma del Cauca. Este lineamiento y sus procedimientos se encuentra en el documento de Política de tratamiento de Datos Personales.

6.4 Lineamiento 4: Acuerdo para el tratamiento de datos personales

Se presenta el documento para que el titular autorice el tratamiento de datos personales, en el cual se expone la responsabilidad de la institución como de los derechos del titular.

6.5 Lineamiento 5: Aviso de privacidad de datos personales

Se presenta el documento donde se le expone al titular los fines para los cuales van a ser utilizados sus datos personales. Esto en cumplimiento de la Ley 1581 de 2012 y demás normas concordantes.

ARTÍCULO SEGUNDO: El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Institución que se consigna en el acuerdo No 002 de 2017 el cual se aprueba el Reglamento Interno del Trabajo, incluyendo lo establecido en las normas que competen a los manuales de convivencia, al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere, la violación de estas Políticas pueden resultar en acciones disciplinarias inmediatas.

ARTÍCULO TERCERO: Establecer como política institucional la aplicación de la Política de Seguridad y Confidencialidad de la Información, en todas las unidades administrativas.

ARTÍCULO CUARTO: Autorizar cambios de forma inherentes al proceso de actualización de la Política de Seguridad y Confidencialidad de la Información, previa presentación por parte del Consejo Administrativo.

ARTÍCULO QUINTO: Cualquier solicitud relacionada con esta política o la aplicación de esta debe ser referida a la División de Tecnología y Medios Educativos.

ARTÍCULO SEXTO: Notificar la presente resolución a toda la comunidad directiva, administrativa, académica y auxiliar.

ARTÍCULO SÉPTIMO: La presente resolución rige a partir de la fecha de su aprobación, y deroga todas aquellas que le sean contrarias.

COMUNÍQUESE, PUBLÍQUESE Y CÚMPLASE

Expedida en Popayán, 26 SET. 2018

MANUEL ANDRÉS BELALCÁZAR SANDOVAL
Presidente Consejo Administrativo

EDUARDO ADOLFO MUÑOZ PORTILLA
Secretario Consejo Administrativo