ACUERDO 018
DEL 12 DE OCTUBRE DE 2022

POR MEDIO DEL CUAL SE EMITE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El Consejo Superior de la Universitaria del Chicamocha en ejercicio de sus atribuciones legales, estatutarias y

CONSIDERANDO:

Que la Universitaria del Chicamocha es una institución de Educación Superior de naturaleza jurídica de utilidad común, sin ánimo de lucro, de derecho privado y constituida como corporación, que desarrolla programas de formación profesional en los niveles académicos de pregrado y posgrado y en las modalidades de formación presencial, distancia y virtual, y educación continuada; con sede principal en la ciudad de Bucaramanga y sujeta a inspección y vigilancia por el Ministerio de Educación Nacional, de acuerdo con lo estipulado en la Ley 30 de 1992.

Que la Ley 30 de 1992, en el capítulo IV, artículo 29, reconoce a las instituciones universitarias el derecho a darse y modificar sus estatutos, adoptar sus correspondientes regímenes, establecer, arbitrar y aplicar sus recursos para el cumplimiento de su misión social y de su función institucional.

Que el artículo 65 de la Ley 30 de 1992, faculta a las Instituciones de Educación Superior, para definir las políticas académicas y administrativas y la planeación institucional en desarrollo del principio constitucional de autonomía universitaria.

Que el artículo 26, literal d. del Estatuto General establece como función del Consejo Superior “aprobar los reglamentos estudiantiles, investigación, extensión, profesoral, prácticas, internacionalización, de bienestar universitario, así como los demás que resulten necesarios para el buen funcionamiento de la Institución”.

Que el Decreto 1330 de 25 de julio de 2019 expedido por el Ministerio de Educación Nacional, en el artículo 2.5.3.2.3.1.3. literal b. establece que las políticas institucionales “son el conjunto de directrices establecidas por la institución con el fin de orientar y facilitar el logro de sus objetivos por parte de los diferentes estamentos, en los

distintos niveles formativos y modalidades en coherencia con su naturaleza jurídica, tipología, identidad y misión institucional".

Que el Decreto 1008 de 2018 establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones", determina en el artículo 2.2.9.1.2.1 como componente de política digital los habilitadores transversales como elementos fundamentales de la Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital.

Que en reunión realizada por el Consejo Superior celebrada el día 12 de octubre de 2022 la presidenta y representante legal de la entidad, presenta la Política de Seguridad de la Información de la Universitaria del Chicamocha.

Que estando presente el cien por ciento (100%) del quórum estatutario con voz y voto para deliberar y decidir en la reunión mencionada en el punto que antecede, se analizó la Política de Seguridad de la Información de la Universitaria del Chicamocha siendo esta aprobada por unanimidad.

En mérito de lo expuesto el Consejo Superior de la Corporación Universitaria del Chicamocha,

ACUERDA:

ARTÍCULO PRIMERO. Aprobar la Política de Seguridad de la Información de la Universitaria del Chicamocha, conforme al proyecto presentado a consideración en la parte motiva del presente acuerdo y relacionado a continuación:

CAPITULO I
DEFINICIÓN Y PROPÓSITOS

ARTÍCULO 1. DEFINICIÓN. La política de seguridad de la información está orientada a proteger los activos de datos de la Universitaria del Chicamocha con el ánimo de mitigar los riesgos en la perdida de información vital para el desarrollo institucional.

ARTÍCULO 2. PROPÓSITOS. Son propósitos de la política:

a) Monitorear las alteraciones de seguridad de la información
b) Identificar y evaluar los riesgos de seguridad de la información a los cuales están expuestos los activos de la Institución.
c) Consolidar la cultura de seguridad de la información.

ARTÍCULO 3. RIESGOS. El gestor de infraestructura, realiza el análisis de riesgos de seguridad de la información con el objetivo de identificar las posibles vulnerabilidades y mitigar o eliminar su ocurrencia.

ARTÍCULO 4. SEGURIDAD EN EL TRABAJO EN CASA. La Universitaria del Chicamocha, instituye los requisitos para el establecimiento de conexiones remotas a la plataforma tecnológica de la Institución; así mismo, suministra las herramientas y controles necesarios para que dichas conexiones se realicen de manera segura.

ARTÍCULO 5. CONTROL Y ADMINISTRACIÓN DE ACCESOS. La Universitaria del Chicamocha, tendrá la obligación de controlar el acceso de la información y posteriormente restringirla solo al personal autorizado conforme el perfil de acceso, teniendo en cuenta mecanismos de protección para la red y la información, así mismo garantizar la implementación de controle a perímetros de seguridad para la protección de áreas.

ARTÍCULO 6. SEGURIDAD PARA EL INTERNET El acceso a Internet deberá ser utilizado con el objetivo para el cual fue provisto. Igualmente, los funcionarios deberán atender las siguientes recomendaciones:

a) Los funcionarios deberán abstenerse de navegar en sitios de juegos en línea, pornografía, terrorismo, activismo y cualquier categoría que esté fuera del contexto laboral y/o que infrinja la normatividad aplicable.
b) Las conexiones directas desde equipos institucionales con salida a internet no están permitidas.
c) Adicionalmente, el área de infraestructura como administrador de la red de Internet, podrá deshabilitar los permisos de acceso a Internet en el momento en que lo considere necesario y más aún cuando la seguridad de la información haya sido comprometida.
d) El área de infraestructura podrá monitorear el correcto uso de los recursos de acceso a internet cuando lo considere necesario.

ARTÍCULO 7. ESCRITORIO LIMPIO. SE debe adoptar por parte de la Institución una política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles y una política de pantallas limpias en las instalaciones

de procesamiento de información, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto y durante el horario normal de trabajo, como fuera del mismo.

a) Al finalizar la jornada de trabajo, los funcionarios de la institución guardan en un lugar seguro los documentos y dispositivos removibles que contengan información clasificada o reservada de la institución.
b) El uso de fotocopias, escáner o cualquier medio en que se puedan generar copias o difundir información hacia afuera de la institución es manejado solamente por los funcionarios, con el fin de proteger del personal externo la información de la institución.
c) Los funcionarios deberán mantener bajo su custodia los documentos enviados a los equipos de impresión, evitando que estos documentos queden sobre la impresora u otro lugar, expuestos a la perdida.
d) Cuando el funcionario de la institución se retire de su sitio de trabajo deberá bloquear su sesión personal evitando comprometer información.

ARTÍCULO 8. CONTROLES CONTRA CÓDIGOS MALICIOSOS. La Universitaria del Chicamocha, tendrá que proporcionar los mecanismos necesarios para promover la protección de la información, y las plataformas tecnológicas esto incluye el procesamiento y almacenamiento de información, minimizando los riesgos asociados, además de evitar divulgación, modificación o daño permanente por la filtración de software malicioso, Así mismo se debe generar conciencia entre los funcionarios contratistas y personal de externo a la Institución sobre la importancia de la seguridad de la información y los ataques por código malicioso.

a. Se deberá contar con una herramienta que permita verificar la presencia de algún virus malicioso en los archivos recibidos de fuentes externas o a través de redes de datos.
b. Actualizar periódicamente el software de detección de amenazas, para el análisis de computadoras, dispositivos móviles, removibles o cualquier otro dispositivo conectado a la red de la institución.
c. Concientizar a los funcionarios de la institución sobre la importancia de verificar el remitente de la información y de los riesgos asociados a los virus informáticos.
d. Los usuarios deberán reportar el área de sistemas cualquier evento sospechoso que pudiese vulnerar la seguridad de la información.

ARTÍCULO 9. RESPALDO DE LA INFORMACIÓN. Para garantizar el respaldo de la información se realizan copias de seguridad de forma mensual y se almacenan en un espacio en la nube con el fin de asegurar la integridad y disponibilidad de la información. Cada respaldo cuenta con la fecha de realización y es almacenado en una carpeta con el nombre de la dependencia a la que pertenece el funcionario sobre el que se realizó la copia.

ARTÍCULO 10. INSTALACIÓN DE SOFTWARE. Los funcionarios de la institución no están facultados para instalar ningún software, por lo tanto, el área de infraestructura es la encargada de garantizar que los equipos se encuentren limitados para la instalación de programas de computación no autorizados.

ARTÍCULO 11. LICENCIAS DE SOFTWARE. La Institución garantiza que el software que adquiera y usa, se encuentra debidamente licenciado, considerando y acatando los derechos de propiedad intelectual.

ARTÍCULO 12. CORREO ELECTRÓNICO. El área de infraestructura establece los siguientes mecanismos para la segura gestión del correo electrónico institucional:

a) La cuenta de correo electrónico institucional asignada a los funcionarios únicamente podrá ser utilizada para finalidades relacionadas con el desarrollo de las funciones correspondientes al cargo o función, quedando limitado el uso de dicha cuenta al ámbito laboral y/o profesional.
b) Los usuarios no deben utilizar una cuenta de correo electrónico institucional que pertenezca a otra persona. En caso de ausencias o vacaciones se debe recurrir a mecanismos alternos como redirección de mensajes.
c) Cualquier correo electrónico sospechoso debe ser reportado al siguiente correo infraestructura@unich.edu.co
d) Toda la información almacenada, gestionada o trasmitida por correo electrónico institucional, es propiedad de la misma.

ARTÍCULO 13. CREACIÓN DE CUENTA DE CORREO. El área de infraestructura es la dependencia encargada de proveer acceso al correo electrónico institucional a los usuarios autorizados. Las cuentas de usuario deben ser creadas basadas en el cargo del funcionario, área o dependencia o nombre del funcionario de la siguiente manera.

a) cargo@unich.edu.co
b) Primernombre.primerapellido@unich.edu.co

ARTÍCULO 14. IMAGEN INSTITUCIONAL: Con el fin de fortalecer la imagen institucional la Entidad determina las siguientes características para los mensajes de correo electrónico:

a) Fuente: Montserrat
b) Tamaño: 12
c) Color de fuente: negro
d) Firma Institucional con los estilos ya establecidos para nuevos correos, respuestas y envíos.

ARTÍCULO 20. VIGENCIA. La política de seguridad de la información, rige desde su expedición

ARTÍCULO SEGUNDO. La política de seguridad de la información aprobada y relacionada en el artículo que antecede es de difusión, aplicación y cumplimiento obligatorio por toda la comunidad universitaria de la entidad.

ARTÍCULO TERCERO. La presente política de seguridad de la información aprobada y relacionada en el ARTÍCULO PRIMERO de la parte resolutiva, rige a partir de la fecha de su expedición y deroga las disposiciones contrarias a lo aquí establecido.

COMUNÍQUESE, PUBLÍQUESE Y CÚMPLASE

Dado en Bucaramanga a los 12 días del mes de octubre de 2022

CLAUDIA HERNÁNDEZ NARANJO
Presidente y Representante Legal

RAFAEL EDUARDO LAMO TRIANA
Secretario General