RESOLUCIÓN 125 DE 2020
(2 DE ABRIL)

"Por la cual se adoptan protocolos de Seguridad y Privacidad de la Información y Protección de Datos Personales en la Universidad Surcolombiana"

EL RECTOR (E) DE LA UNIVERSIDAD SURCOLOMBIANA

En uso de sus atribuciones legales y reglamentarias, en especial las conferidas en el numeral 18 del artículo 31 del Acuerdo 075 de 1994-Estatuto General de la Universidad Surcolombiana- y;

CONSIDERANDO:

Que, en cumplimiento de su misión, la Universidad Surcolombiana debe impulsar y materializar los cambios que demandan los tiempos modernos, para mantener el posicionamiento y el liderazgo en la formación de talento humano al servicio de la Región Surcolombiana y del país.

Que mediante Resolución 385 del 12 de marzo de 2020, el Ministro de Salud y Protección Social, de acuerdo con lo establecido en el Artículo 69 de la Ley 1753 del 9 de junio de 2015- Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 "Todos por un nuevo país", declaró el estado de emergencia sanitaria por causa del nuevo Coronavirus COVID-19 en todo el territorio nacional hasta el 30 de mayo de 2020 y, en virtud de la misma, adoptó una serie de medidas con el objeto de prevenir y controlar la propagación del COVID-19 y mitigar sus efectos.

Que la Universidad Surcolombiana expidió la Circular 009 de 2020, donde suspendió la atención al público desde el 16 de marzo 2020 hasta nueva orden.

Que mediante Resolución 118 del 16 de marzo de 2020 el Rector (E) suspendió los términos procesales de todas las actuaciones administrativas; igualmente el Consejo Académico expide los comunicados 001, 002, 003 de 2020, donde se suspenden las clases presenciales en las diferentes sedes de la Universidad, prácticas estudiantiles y salidas extramuros y se conmina a la comunidad académica y administrativa a trabajar desde la casa utilizando medios electrónicos y virtuales en aras de mitigar los riesgos de propagación del COVID -19.

Que mediante Resolución 079B del 17 de febrero de 2020, se creó el Comité de Seguridad de la Información de la Universidad Surcolombiana, como órgano responsable de la implementación, aplicabilidad y funcionalidad de la Política de Seguridad de la Información, Política de Protección de Datos Personales y del Plan de Contingencia y Continuidad Informático.

Que mediante la Resolución 289 de 2019 se adopta la Política General del Modelo de Seguridad y Privacidad de la Información y el Manual de la Política Seguridad y Privacidad de la Información de la Universidad Surcolombiana.

Que la Resolución 290 de 2019 adopta la Política de tratamiento y Protección de datos personales de la Universidad Surcolombiana, la Resolución 056 de 2020, adopta el Plan de Seguridad y Privacidad de la Información vigencia 2020 y la Resolución 057 de 2020, adopta el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información vigencia 2020.

RESOLUCIÓN 125 DE 2020
(2 DE ABRIL)

Que atendiendo las recomendaciones del Gobierno Nacional, Local e Institucional respecto a la declaratoria de emergencia sanitaria del país por los casos presentados de COVID-19 se hace necesario implementar estrategias tecnológicas seguras que permitan continuar con el desarrollo de las actividades administrativas y académicas de la Universidad las cuales el Comité de Seguridad de la Información en reunión extraordinaria aprobó.

Que, en mérito de lo expuesto,

RESUELVE

ARTICULO 1. Adoptar los protocolos de Seguridad de la Información y Protección de Datos Personales en la Universidad Surcolombiana, así:

1. La Seguridad Informática de la Universidad es responsabilidad del Centro de Información, Tecnología y Control Documental. La instalación de VPN, software de acceso remoto y todo lo relacionado con instalación de software o hardware a los equipos de cómputo de la Universidad, será realizado por personal de las áreas de soporte técnico, área de desarrollo de software y área de comunicaciones o redes. Para esto, en los casos necesarios debe haber presencia del Usuario dueño del equipo para que proceda a cambiar clave inmediatamente se realice cualquier instalación y/o configuración en el equipo.

2. Si se hace necesario activar algún servicio de cara a Internet, primero de debe evaluar el riesgo antes de realizar la actividad. Que estas acciones de contingencia no afecten la seguridad de los datos.

3. Es responsabilidad del Centro de Información, Tecnología y Control Documental (CITCD) mantener actualizado el sistema operativo con los últimos parches de seguridad liberados por el fabricante en todos sus dispositivos.

4. El personal de soporte técnico configurará los equipos de los usuarios que necesiten acceder de manera remota, con el fin de que éstos no se bloqueen y el usuario pueda tener conectividad continua. (No contempla problemas energía o casos de fuerza mayor).

5. Una vez realizado el análisis de criticidad entre el Centro de Información, Tecnologías Control Documental y el Jefe de la dependencia, el Centro de Información, Tecnología y Control Documental (CITCD) definirá y configurará el tipo de herramienta para acceso remoto a ser instalado en los equipos de los usuarios.

6. Se debe realizar capacitación, acompañamiento e implementación de tutoriales para todos los funcionarios y contratistas que realizarán trabajo en casa, indicando las medidas y políticas de seguridad que deben tener con el uso de las aplicaciones y equipos que pongan en riesgo la seguridad de la Información. (No dejar sesiones activas en las aplicaciones,

cerrar la sesión del Windows con el fin de dejar bloqueado el computador una vez finalice su trabajo).

7. Se deben establecer cláusulas de confidencialidad y responsabilidad con aquellas personas ajenas a las dependencias y que por alguna razón deban ingresar a alguna de ellas por una urgencia.

8. Teniendo en cuenta que la Universidad debe garantizar la disponibilidad de la plataforma Tecnológica para el trabajo en casa se deben definir los agentes responsables que tendrán ingreso sin restricción a las instalaciones de la Universidad en caso de una contingencia. (Personal del Centro de Información, Tecnología y Control Documental (CITCD), Servicios Generales y usuarios).

9. La comunicación institucional se debe realizar utilizando el correo institucional (@usco.edu.co) y no correos personales.

10. Con el propósito de que toda la comunicación de la Universidad sea manejada por el Sistema de Gestión Documental, se hace necesario que el Centro de Información, Tecnología y Control Documental (CITCD)programe una inducción a todo el personal en cuanto a la utilización y parametrización del mismo y la Oficina de Talento Humano continúe el proceso de actualización de la información del aplicativo de Personal, con las correspondientes novedades (vinculaciones, traslados entre otros) de manera que se garantice la integridad y veracidad de la información.

11. Se debe iniciar el proceso de actualización de los procedimientos del Sistema de Gestión de calidad incluyendo la modalidad de trabajo en casa.

ARTICULO 2. La presente Resolución rige a partir de la fecha de su expedición.

PUBLIQUESE Y CÚMPLASE

Dada en Neiva, a los dos (2) días del mes de abril del año 2020.

(Original Firmado)
PABLO EMILIO CERQUERA BAHAMON
Rector (e)

(Original Firmado)
SHIRLEY MILENA BOHÓRQUEZ CARRILLO
Secretaria General.

Revisó: Secretaria General

Proyectó: Martha Liliana Hermosa
Profesional Especializado Centro e Información, Tecnologías y Control Documental