INSTITUCIÓN TECNOLÓGICA
COLEGIO MAYOR DE BOLÍVAR

RESOLUCION No. 310
(01 de julio de 2020)

POR MEDIO DE LA CUAL SE IMPLEMENTA LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN LA INSTITUCIÓN, CON MOTIVO DE LA SITUACION DE EMERGENCIA SANITARIA, PRODUCIDA POR EL VIRUS CORONAVIRUS - COVID 19.

El RECTOR DE LA INSTITUCION TECNOLOGICA COLEGIO MAYOR DE BOLIVAR, en uso de sus facultades legales y estatutarias y

CONSIDERANDO

Que las normas ISO, son un conjunto de normas orientadas a ordenar la gestión de una empresa en sus distintos ámbitos, con el fin de asegurar la calidad, seguridad y eficiencia de productos y servicios.

Que la institución se encuentra certificada bajo la norma ISO 9001:2015 la cual establece que se deberá controlar la información documentada para así asegurarse de que se encuentra disponible cuando sea necesario y que esto es adecuado para su utilización, así mismo determinará cómo será la distribución, el acceso, la recuperación y la utilización de dicha información.

Que en aras de mantener y mejorar continuamente los procesos de la institución debemos salvaguardar toda la información documentada generada en el ejercicio de las labores de cada uno de los procesos

Que la ITCM cuenta con un Sistema de Gestión de Seguridad y Salud en el Trabajo para prevenir accidentes y enfermedades laborales de acuerdo con el Decreto10172 de 2015, dando cumplimiento a las disposiciones del Misterio del Trabajo.

Que, atendiendo a la emergencia sanitaria producida por el Covid-19, el personal de la institución ITCMB se encuentra laborando de manera remota en casa, se hace necesario asegurar la conservación de los documentos generados durante el desarrollo de sus labores.

Que el Decreto 1072 de 2015, establece que es necesario conservar la documentación como medida preventiva para asegurar la integridad física y funcional de los documentos del Sistema de Gestión de Seguridad y Salud en el Trabajo, asegurando la legibilidad, identificación, acceso y protección contra daños o perdida de los documentos. La información podrá ser guardada de forma electrónica garantizando su preservación.

Que, por lo anteriormente expuesto,

RESUELVE

ARTICULO PRIMERO. Implementar en la Institución una estrategia que permita salvaguardar la información, permitiendo así acceder cuando se requiera, a través de canales adecuados y siguiendo los procesos correctos, por lo cual toda la

Escaneado con CamScanner

información generada durante el ejercicio de las labores asignadas al personal de la institución deberá ser guardada de forma digital y cargada en la nube Google Drive del correo institucional, de tal manera que en cualquier eventualidad que surja, la institución pueda de forma ágil y rápida acceder a dicha información así:

PARAGRAFO. Para el caso de los funcionarios que se le suministraron equipos para conexiones de escritorio remoto y VPN deben cumplir con estas medidas de seguridad:

- No compartir ni prestar las credenciales de acceso (Sesión de Windows y VPN) con segundas personas.
- Mantener el equipo conectado a internet, para que este reciba actualizaciones diarias del antivirus y sistema operativo.
- No conectarse a redes inalámbricas de dudosa procedencia.
- No guardar datos en el equipo físico, recuerde que lo está usando de puente para conectarse a su equipo Institucional por tal motivo está prohibido guardar datos institucionales en las estaciones físicas.
- No insertar medios extraíbles memorias USB, Discos externos, unidades de CD, DVD.
- Si necesitas salir de tu hogar por suministros u otras razones, asegúrate de que los dispositivos de trabajo estén apagados o bloqueados y en un lugar seguro.
- Si necesitas trasladarte con el equipo recuerda:
- Es caso de que tengas carro no dejarlo visible.
- Usar un bolso donde quepa totalmente el equipo.

ARTICULO SEGUNDO. Toda la información que se genere y derive de su labor como funcionario o contratista de la institución tiene carácter sensible y confidencial es por eso que no está permitido el uso de memorias USB, Discos externos, unidades de CD, DVD u otros mecanismos para extraer la información del disco duro del computador, de tal manera que deberá salvaguardar la información institucional en el drive de su cuenta de correo Institucional y esta corresponderá ser guardada estableciendo el siguiente orden:

- Tema o Proceso desarrollado
- Año
- Mes > Nombre de subcarpetas (Si es necesario)
- Ejemplo: EVIDENCIAS PLAN DE ACCIÓN / 2020/ ABRIL / Factor 1.

PARAGRAFO. Esta información debe ser original y correcta, por lo cual no debe ser modificada, manteniendo sus datos exactamente tal cual fueron generados, sin manipulaciones ni alteraciones por parte de terceros, por lo que se recomienda que aquellos documentos que no pueden ser modificados por otras personas se guarden en archivo PDF o se le asigne clave de seguridad.

ARTICULO TERCERO. En el caso de uso de dispositivos de propiedad de los funcionarios o contratistas (BYOD) deberán trabajar con el equipo conectado al drive de la cuenta Institucional para salvaguardar los datos en la nube y seguir el orden mencionado, en ningún momento la información podrá ser copiada al disco duro de la máquina del funcionario, para ello dispondrá del software File Stream de Drive que se descarga de la

Escaneado con CamScanner

página oficial de google https://dl.google.com/drive-file-stream/GoogleDriveFSSetup.exe y este permite acceder a la información Institucional sin ocupar espacio en tu disco.

ARTICULO CUARTO. Los canales institucionales para emitir información veraz son la página web institucional "colmayorbolivar.edu.co" y las redes sociales Institucionales, Facebook "Mayor de Bolívar", Twitter "colmayorbolivar", YouTube "colmayorbolivar". Instagram "colmayorbolivar".

ARTICULO QUINTO. Abstenerse de usar, compartir y difundir su correo personal para compartir, generar información Institucional. No abrir archivos adjuntos a menos que sean de una fuente conocida y confiable Se ha detectado la difusión de páginas web falsas creadas para vender productos sanitarios. No abrir correos electrónicos masivos (spam), con contenidos relacionados con el COVID-19 y que llevan adjuntos archivos que ejecutan malware tipo ransomware o troyanos bancarios o webs oficiales (phising) como entidades Gubernamentales, Cruz Roja, hospitales y otros similares, solicitando contribuir económicamente a campañas solidarias inexistentes.

PARAGRAFO. Consultar siempre con el Coordinador de Soporte y Desarrollo Tecnológico sobre correos sospechosos o alertas en tú equipo informático.

ARTICULO SEXTO. El Proceso de Soporte y Desarrollo Tecnológico verificará semanalmente por áreas la disposición y el acatamiento de las medidas de seguridad informática y el resultado de las mismas será informado a las directivas.

ARTICULO SEPTIMO. Esta estrategia de seguridad de la información, deberá implementarse de forma inmediata, al momento de expedirse y entrar a regir esta resolución.

ARTICULO OCTAVO. La presente resolución rige a partir de su expedición.

PUBLIQUESE, NOTIFIQUESE Y CUMPLASE
Dada en Cartagena de Indias, a los 01 día del mes de julio de 2020

JAIRO MENDOZA ALVAREZ
Rector

RAFAEL HERAZO BELTRAN
Secretario General

Escaneado con CamScanner