CIRCULAR No. 1591

DE: DIRECTOR INSTITUTO DEPARTAMENTAL DE SALUD DE NORTE DE SANTANDER

PARA: COORDINADORES DE DEPENDENCIAS, GRUPOS Y SUBGRUPOS DEL INSTITUTO DEPARTAMENTAL DE SALUD

FECHA: 04 DE ABRIL DE 2022

ASUNTO: SEGURIDAD PARA EL USO Y ACCESO A LAS CUENTAS DE CORREO ELECTRÓNICO INSTITUCIONAL.

De acuerdo a lo dispuesto en las Políticas de Seguridad y Privacidad de la Información del Instituto Departamental de Salud de Norte de Santander establecidas mediante Resolución N° 1017 del 25 Marzo de 2021, y que se encuentran publicadas en la página web institucional, se establece que el manejo de las claves institucionales debe ser personal y confidencial.

En el numeral 5.4 **POLÍTICA DE CONTROL DE ACCESO (página 20 de 38)** se encuentra la sección **Sistema Gestión de contraseñas.** Donde se establece lo siguiente: **"***Los usuarios deben cumplir las prácticas de la entidad para el uso de información de contraseñas que se relacionan a continuación: a) Mantener la confidencialidad de la información de contraseña, asegurándose de que no sea divulgada a ninguna otra parte, incluidas personas externas a la entidad y personal de otras dependencias de la institución no autorizadas. b) Evitar llevar un registro (en papel, en un archivo de software o en un dispositivo portátil) de contraseña. c) cambiar la información de contraseña siempre que haya cualquier indicio de que se pueda comprometer la información…* e) No compartir información de contraseña del usuario individual".

De acuerdo a lo anterior, el lineamiento recomendado desde la oficina de sistemas de información es, que desde la coordinación de cada una de las Áreas el manejo de las contraseñas sea confidencial, dando acceso únicamente al coordinador y en caso de ser necesario por quién él considere de su entera confianza, preferiblemente que sea una sola persona quien utilice responsablemente las credenciales de acceso. Por otra parte, al requerirse el iniciar sesión en un equipo diferente al de la coordinación, las claves no deben ser socializadas, en este caso la persona de confianza debe ser quien realice esta acción. A su vez se recomienda hacer periódicamente cambio de la contraseña del correo institucional, para mitigar el riesgo de que personas mal intencionadas ingresen, alteren o borren información institucional.

De igual manera se establece dentro de la Resolución N° 1017 de 2021, las repercusiones que un funcionario puede tener al estar ingresando sin autorización a un correo institucional, borrando o modificando información de la entidad. Indicándose que por el incumplimiento de las políticas de Seguridad y Privacidad de la Información se podrá incurrir en una falta disciplinaria grave.

Se deben aplicar los controles para mitigar el manejo de los riesgos inherentes a la situación que se está presentando en la actualidad, donde se han evidenciado acciones de borrado de información institucional con intencionalidad y no un borrado accidental. Por lo anteriormente mencionado, se recuerda que es de obligatorio cumplimiento para los funcionarios y contratistas, aplicar lo estipulado en el anexo técnico de la Resolución N° 1017 de 2021 donde se establecen las Políticas de Seguridad y Privacidad de la Información de la entidad.

CARLOS ARTURO MARTINEZ GARCIA

Proyecto y Revisó: Armando Rojas C.
Elaboró: Yaruth Núñez S. Yaruth N.