CAJA COSTARRICENSE DE SEGURO SOCIAL
Auditoría Interna
Teléfono: 2539-0821 ext. 2000-7468
Correo electrónico: coinccss@ccss.sa.cr

Al contestar refiérase a: **ID-108624**
CONFIDENCIAL

AS-ASALUD-0018-2024
12 de marzo de 2024

Doctora
Nuria Marín Monge, directora medica

Licenciada
Madelin Porras Arguedas, administradora
ÁREA DE SALUD GUÁPILES-2634

Estimadas señoras:

ASUNTO: Oficio de Asesoría sobre la utilización de contraseñas para ingreso a computadoras y sistemas institucionales.

Esta Auditoría, en cumplimiento del Programa de Actividades Especiales, consignadas en el Plan Anual Operativo 2024 y con fundamento en los artículos 21 y 22 de la Ley General de Control Interno, emite asesoría, en cuanto al uso de contraseñas de ingreso a computadoras institucionales.

En relación con este asunto, mediante visita realizada el 24 de enero 2024, se detectó en esa área de salud, que la funcionaria G.J.C.P, accedió a la sesión de una computadora utilizando las credenciales del usuario OMVALERI perteneciente a la misma unidad.

Esta Auditoría le consulta a la funcionaria G.J.C.P, del por qué utiliza el usuario y clave de OMVALERI para el ingreso a la computadora y los datos de ésta, y responde que él le presta las claves cuando ella lo sustituye.

En ese sentido, es importante indicar que, el compartir contraseñas, conlleva riesgos significativos para la seguridad cibernética. Este acto puede comprometer la privacidad y permitir el acceso indebido a nuestros sistemas informáticos.

Aunado a lo anterior, las Normas Técnicas para la Gestión y Control de las Tecnologías de Información y Comunicaciones del Ministerio de Ciencia, Innovación, Tecnologías y Telecomunicaciones, establecen el su apartado XI. Sobre seguridad y ciberseguridad lo siguiente:

> *"La institución debe tener y aplicar en forma consistente una estructura formal al nivel institucional, que permita establecer las acciones para administrar la seguridad de la información, ciberseguridad debidamente respaldada con la política de seguridad de la información / ciberseguridad y que oriente la disponibilidad de niveles de protección y salvaguarda razonables en atención a requerimientos técnicos, contractuales, legales y regulatorios asociados (…)".*

Por su parte, las Normas de control interno para el Sector Público señalan en el inciso 5.7.4 Seguridad que:

> *"Deben instaurarse los controles que aseguren que la información que se comunica resguarde sus características propias de calidad, y sea trasladada bajo las condiciones de protección apropiadas, según su grado de sensibilidad y confidencialidad. Así también, que garanticen razonablemente su disponibilidad y acceso por parte de los distintos usuarios en la oportunidad y con la prontitud que la requieran."*

Finalmente, las Normas Institucionales de Seguridad Informática TIC-ASC-SEG-0002 establecen en su inciso "6.1. **NORMAS PARA LA POLÍTICA CORRECTO USO DE CONTRASEÑAS DE PARTE DE LOS USUARIOS DE RED Y APLICACIONES**" que:

> *"(…) Alcance: Esta norma aplica a todos los funcionarios de la Institución, que posean cuentas de red aplicaciones, para el cumplimiento de sus respectivas funciones.*
>
> *Responsabilidad: Será responsabilidad de todos los usuarios de la red y aplicaciones de la Institución acatar las normas establecidas en este documento.*
>
> *Todo funcionario de la red institucional y de aplicaciones, que posea una o varias cuentas creadas a su nombre, deberá cumplir con las siguientes normas, que constituyen las mejores prácticas para la manipulación de las contraseñas personales y lo protegerán del hurto y modificación de la información institucional que administra (…).*
>
> *2. La contraseña no deberá compartirse, sin excepción con ninguna otra persona (aunque se trate de la jefatura, un soportista, o compañeros de trabajo), ya que el dueño de la cuenta será el responsable por el uso que se le dé a la misma".*
>
> *El Código Penal Costarricense refiere en su artículo "230 - Suplantación de identidad" que:*
>
> *"Será sancionado con pena de prisión de uno a tres años quien suplante la identidad de una persona física, jurídica o de una marca comercial en cualquiera red social, sitio de Internet, medio electrónico o tecnológico de información."*

CONSIDERACIONES FINALES

En virtud de lo analizado en el presente documento, es importante señalar la necesidad de revisar, monitorear y controlar el uso de claves de acceso a sistemas institucionales y computadoras propiedad de la Caja, con el fin de prevenir eventuales actividades delictivas por medio de herramientas informáticas que puedan comprometer la continuidad de los servicios y el patrimonio institucional, efectuando para ello, un análisis de riesgos para la identificación de áreas críticas.

Es importante brindar continuidad a la implementación del marco regulatorio relacionado con las Tecnologías de la Información y Comunicación (TIC), asegurando su acatamiento de manera efectiva. En concordancia con las capacidades institucionales, es necesario planificar y ejecutar acciones destinadas a robustecer la infraestructura tecnológica, con el propósito de evitar posibles responsabilidades de índole administrativo, civil o penal.

Asimismo, resulta esencial llevar a cabo de manera periódica procesos de concientización a los usuarios sobre el riesgo del tema analizado. Este enfoque tiene como objetivo, minimizar los riesgos identificados los cuales, de no ser abordados, podrían generar inconsistencias en la prestación de los servicios institucionales. La administración eficiente y eficaz de los recursos a través de las Tecnologías de la Información y Comunicación (TIC) representa un componente clave para mitigar los riesgos.

Con el propósito de fortalecer la seguridad y proteger la integridad de la información, es necesario hacer una revisión general a todos los usuarios sobre el acceso a los sistemas institucionales y computadoras a las cuales tienen acceso, y efectuar un recordatorio de la importancia de realizar el cambio de las contraseñas periódicamente al menos cada 3 meses, de conformidad con lo establecido en el manual de Normas Institucionales de Seguridad Informática TIC-ASC-SEG-0002, como una medida preventiva fundamental. Este proceso no solo contribuye a salvaguardar la confidencialidad de los datos, sino también fortalece el sistema institucional frente a posibles amenazas cibernéticas.

De conformidad con lo anterior, esta auditoría informa a esa área de salud de Guápiles, sobre la situación evidenciada en el presente documento, con el propósito de que se impulsen las acciones que correspondan, para que se haga un uso adecuado de las contraseñas institucionales otorgadas a los funcionarios.

Al respecto, se deberá informar a esta Auditoría Interna de forma escrita las acciones realizadas para la gestión de lo indicado y atención de la situación comunicada, en el plazo de 1 mes a partir del recibido de este documento.

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2024.03.12 12:07:08 -06'00'

M.S c. Olger Sánchez Carrillo
Auditor

OSC/RJS/EAM/RMJM//WGC/lbc

C. Doctora Carla Teresa Alfaro Fajardo, directora, Dirección de Red Integrada para la Prestación de Servicios de Salud Huetar Atlántica-2699.
Auditoría-1111

Referencia: ID-108624