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

AD-ATIC-0022-2023
2 de marzo de 2023

Licenciado
Walter Campos Paniagua, director
DIRECCIÓN DE ADMINISTRACION Y GESTIÓN DE PERSONAL - 1131

Estimado señor:

ASUNTO:	**Oficio de Advertencia referente al acceso para registro de información al Sistema Nacional para el Reporte de Funcionarios en Huelga.**

En cumplimiento de las actividades preventivas consignadas en el Plan Anual Operativo 2023 y con fundamento en los artículos 21 y 22 de la Ley General de Control Interno, se informa sobre los posibles riesgos generados con la creación (de forma temporal) de credenciales genéricas para realizar reportes en el Sistema Nacional para el Reporte de Funcionarios en Huelga, a fin de que sea valorado para la toma de decisiones y acciones que compete a esa administración activa.

Al respecto, los resultados obtenidos son los siguientes:

I. ANTECEDENTES

El 22 de febrero de 2023, mediante comunicado efectuado por el Área de Información en Recursos Humanos, de la Dirección de Administración y Gestión de Personal a las diferentes unidades institucionales, con personal encargado de realizar reportes en el Sistema Nacional para el Reporte de Funcionarios en Huelga, se indicó, lo siguiente:

> *"Con motivo de agilizar el acceso al Sistema Nacional para el Reporte de Funcionarios en Huelga se ha generado de forma temporal un usuario de uso general para ser suministrado a los funcionarios encargados de realizar el respectivo reporte,* ***este usuario deberá ser comunicado LO ANTES POSIBLE a su vez a las diferentes jefaturas de cada centro de trabajo.***
>
> ***Usuario: ushuelga***
> ***Contraseña: usgeneral***
>
> *Es de suma importancia indicar a las jefaturas, que al momento de ingresar al sistema deben seleccionar de forma correcta el centro de trabajo y el servicio al cual corresponde el reporte, y que* ***por ningún motivo debe realizar el proceso de actualización de contraseña".***

II. RESULTADOS OBTENIDOS

La digitalización del sector de la salud sigue avanzando y dependiendo cada vez más de sistemas de información para llevar a cabo los procesos administrativos, clínicos y diagnósticos.

Si bien esta transformación digital conduce a mejores resultados en la atención y administración de los servicios de salud, también existe el potencial de aumentar los riesgos de seguridad. Toda esta red de equipos y sistemas conforman un entorno crítico y complejo de controlar, generando una oportunidad para el acceso de ciberdelincuentes a la información confidencial o critica de la institución.

Asimismo, en el contexto del presente oficio, es importante señalar que, para una institución como la Caja Costarricense de Seguro Social las credenciales de acceso se constituyen en una de las primeras líneas de

defensa a la hora de administrar la seguridad de los sistemas y redes empresariales. Una contraseña es tan importante como la información que protege, por ello, si éstas no son lo suficientemente fuertes y seguras se conseguirá dificultar en gran medida el trabajo de aquellos que traten de realizar un ataque para obtener datos.

En relación con lo anterior, a través del tiempo, se ha observado la necesidad de que algunas organizaciones compartan, de manera excepcional, con carácter de urgencia o de forma temporal, entre dos o más de sus funcionarios determinadas contraseñas y credenciales para el acceso a sus sistemas de información. Sin embargo, en esta práctica, hay diversos riesgos o factores que se deben tener en cuenta:

Uno de los riesgos más importantes, es el medio por el cual se van a enviar las credenciales de acceso a los diversos involucrados, ya que esto puede generar filtraciones, y esas contraseñas terminen en manos equivocadas. Por tal motivo, es esencial el cumplimiento de normativa y pautas a seguir establecidas por la unidad rectora de TI, con la finalidad de disminuir el riesgo de que colaboradores compartan esos datos de forma poco segura: enviando la información por correo, mensaje de texto, WhatsApp o documentos compartidos.

Además, compartir un usuario y contraseña única para el acceso a un sistema de información podría ser un riesgo de ciberseguridad, ya que limita al equipo de TI el poder establecer de manera segura quién o quiénes tienen acceso a dicho sistema, así como, a quiénes se les comparte este acceso. Esto imposibilita la asignación de responsabilidades individuales y, por tanto, no pueden atribuirse a personas concretas accesos no autorizados. No hay forma de saber si alguien que ha salido de la organización o ya no labora en el mismo servicio sigue teniendo acceso a una contraseña compartida, lo cual, supone un riesgo para la seguridad de la institución, especialmente si parte de su plantilla trabaja a distancia (modalidad de teletrabajo).

En publicación “El verdadero valor de tener contraseñas realmente seguras” efectuada por Lisa Institute, se indica un comentario para reflexionar:

> *“(…) Por ello, al igual que tomamos precauciones en la vida cotidiana cerrando la puerta de nuestra casa y no compartiendo la clave de nuestra tarjeta bancaria, debemos ser conscientes de la importante información que protegen las contraseñas en nuestra vida online, asegurándonos de que sean lo más seguras y complejas posible (…)”.*

Actualmente existen muchos riesgos acechándonos, donde ciberdelincuentes sin escrúpulos intentan acceder a los datos críticos de las empresas, razón por la cual, día con día se requiere aumentar las medidas de seguridad para mantener la información confidencial bajo control. Para esto lo más importante y recomendable es crear contraseñas seguras y robustas, así como, evitar por todos los medios un uso y resguardo inadecuado de las credenciales de acceso.

Las Normas de Control Interno para el Sector Público, en el inciso 1.4.5 sobre el control de Accesos, refieren:

> *“La organización debe proteger la información de accesos no autorizados. Para dicho propósito debe:*
> *a. Establecer un conjunto de políticas, reglas y procedimientos relacionados con el acceso a la información, al software de base y de aplicación, a las bases de datos y a las terminales y otros recursos de comunicación (…)*
> *c. Establecer procedimientos para la definición de perfiles, roles y niveles de privilegio, y para la identificación y autenticación para el acceso a la información, tanto para usuarios como para recursos de TI (…)*
> *i. Establecer controles de acceso a la información impresa, visible en pantallas o almacenada en medios físicos y proteger adecuadamente dichos medios (…)*
> *e. Asignar los derechos de acceso a los usuarios de los recursos de TI, de conformidad con las políticas de la organización bajo el principio de necesidad de saber o menor privilegio.*

Los propietarios de la información son responsables de definir quiénes tienen acceso a la información y con qué limitaciones o restricciones".

Las Normas técnicas para la gestión y el control de las Tecnologías de Información emitidas por el Ministerio de Ciencia, Tecnología y Telecomunicaciones, MICITT, señala en el apartado XI. 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.

La Unidad de TI, basado en la Política de seguridad de información / ciberseguridad, debe establecer los mecanismos necesarios para asegurar una protección razonable de los activos tecnológicos, activos de información institucionales, dando énfasis en su clasificación como elemento definitorio para establecer los requerimientos de preservación de la confidencialidad, integridad y disponibilidad de la información (…)".

Las Políticas Institucionales de Seguridad Informática TIC-Seguridad-001, en su numeral 9.2. PSI-CAR-002 Política para la administración de contraseñas por parte de los administradores del directorio activo (active directory) y administradores de aplicaciones, se indica:

"La correcta administración de las contraseñas generadas para los usuarios de la red y aplicaciones de la CCSS, es de vital importancia en la seguridad de toda la información institucional, por lo tanto deben cumplirse lineamientos básicos de configuración de la seguridad que deberán ser aplicados por los administradores de red y de aplicaciones. La administración correcta de las contraseñas incluye entre otros aspectos, velar porque los usuarios usen contraseñas seguras, configurar el plazo de vencimiento de las mismas, así como requerimientos de identificación y robustez (…)".

Las Normas Institucionales de Seguridad Informática TIC-ASC-SEG-0002, en su numeral 6.2. Normas para la política de administración de contraseñas por parte de los administradores del directorio activo (active directory) y administradores de aplicaciones, se indica:

***"(…) Responsabilidad:** Será responsabilidad de los administradores de la plataforma institucional, de los administradores de los Centros de Gestión Informática, que cuenten con permisos para administración de cuentas del Directorio Activo (Active Directory), de los desarrolladores y administradores de aplicaciones, implementar las normas que se detallan.*

Normas

Los administradores de las cuentas de usuario del directorio activo (active directory), desarrolladores y administradores de aplicaciones, deberán configurar y aplicar las siguientes normas, ajustables a todas las contraseñas de red y/o aplicaciones. En el mediano plazo se buscará la forma de utilizar una única cuenta, y el cumplimiento de lo normado en el presente documento será la base para el éxito de dicha implementación.

(…) Sobre la seguridad de las contraseñas:

- *Se debe incluir la respectiva configuración, en las aplicaciones y/o políticas del directorio activo, para que se guarde un histórico de al menos las últimas seis contraseñas usadas por el usuario, para prevenir su reutilización.*
- *El usuario administrador no realizará cambios a las cuentas o contraseñas que sean solicitados vía telefónica, estos deben ser solicitados por el usuario personalmente, debe aportar algún documento que lo identifique y que indique que pertenece al lugar de trabajo que dice provenir,*

o por otra parte debe enviar una nota o formulario previamente diseñado para esta labor, con la firma y sello por parte de la jefatura correspondiente (…)".

Sobre la duración de la contraseña:

- *Toda contraseña tendrá una duración máxima de tres meses, terminado dicho período el usuario de la cuenta deberá renovarla, conforme las restricciones y recomendaciones indicadas.*

Sobre la longitud de la contraseña:

- *La longitud de toda contraseña deberá ser igual o mayor a ocho caracteres*

Sobre la robustez de la contraseña:

- *Ninguna contraseña podrá ser igual o similar a su respectivo nombre de usuario ni podrá quedar en blanco. Las contraseñas deben contener caracteres de al menos 3 de las siguientes 4 clases:*

Clase	Descripción de la clase
Letras mayúsculas	A, B, C, . . . Z.
Letras minúsculas	A,b,c, . . . z.
Números	0,1,2, . . . 9.
Caracteres especiales	Por ejemplo: Símbolos puntuación ú otros como % & ¡ @ ( ) .

Sobre los requerimientos de "logueo":

- *Requerir automáticamente el cambio de contraseña la primera vez que el usuario solicita su ingreso a la red o aplicación.*
- *Se debe incluir la respectiva configuración para que después de 3 intentos fallidos de logueo, la cuenta sea bloqueada y se requiera intervención del administrador para desbloquearla.*

Mediante oficio GG-DTIC-2315-2022 del 03 de mayo del 2022, la Dirección de Tecnologías de Información y Comunicaciones solicitó a los jefes de Centros de Gestión Informática gerenciales, hospitales nacionales, hospitales nacionales especializados, áreas de salud tipo 3, Direcciones de Redes Integradas de Prestación Servicios de Salud, Direcciones de Sucursales, coordinadores Gestión Informática áreas de salud tipo 1 y 2, así como, a los miembros del Consejo Institucional de Centros de Gestión Informática, lo siguiente:

"De acuerdo con el Manual de Organización de la Dirección de Tecnologías de Información y Comunicaciones, y los Lineamientos en Comunicaciones y Redes Informáticas en la CCSS DTI-N-CO-0002; se les recuerda a los niveles locales que administran sus equipos de comunicaciones, la aplicación en todo momento de la normativa.

Adicionalmente, el Presidente de la República, la Ministra de la Presidencia y la Ministra de Ciencia, Innovación, Tecnología y Telecomunicaciones hace extensiva la "DIRECTRIZ N° 133-MP-MICITT, DIRIGIDA A LA ADMINISTRACIÓN PÚBLICA CENTRAL Y DESCENTRALIZADA SOBRE LAS MEJORAS EN MATERIA DE CIBERSEGURIDAD PARA EL SECTOR PÚBLICO DEL ESTADO", la cual nos instruye a "cumplir las recomendaciones y medidas técnicas que emanen del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, por medio de la Dirección de Gobernanza Digital y el Centro de Respuesta de Incidentes de Seguridad Informática (en adelante CSIRT-CR), como ente coordinador de la ciberseguridad nacional, referentes a ciberseguridad y seguridad de la información, con el fin de mejorar las capacidades técnicas, de atención y de gestión de la ciberseguridad y seguridad de la información en las instituciones."

Dicha aplicación es indispensable ante la situación que se está experimentando a nivel nacional de ataques cibernéticos, que, con el objetivo de minimizar la probabilidad de eventuales ataques en equipos de comunicaciones, y en vista que los equipos de comunicaciones de sus Unidades son administrados

localmente; se solicita su colaboración para que con carácter de urgencia verifiquen, que cuentan con al menos las siguientes condiciones, a nivel de todos los equipos de comunicaciones:

1. Tener instalada la versión del sistema operativo recomendada por el fabricante.
2. Usar cuentas diferentes para la administración de cada equipo de comunicaciones.
3. Usar contraseñas robustas para la administración de equipos, según lo establecido por el Area de Seguridad y Calidad de la Información, en las Normas Institucionales de Seguridad Informática TIC-ASC-SEG-0002.
4. Dar mantenimiento preventivo y correctivo.
5. Establecer Listas de Control de Acceso que permitan restringir el acceso remoto, solo a las direcciones IP que asignen los encargados de la unidad (CGIs, administradores de red, responsables de los equipos de comunicaciones).
6. Utilizar solamente SSH v2 para el acceso remoto a los equipos.
7. Habilitar NTP y syslog, que permita auditar para el manejo de incidentes.
8. Asegurar el acceso mediante puertos de consola y aux, realizando la autenticación ya sea a nivel local, o Radius o TACACS+.
9. Cualquier otra consideración que apliquen, de acuerdo con el criterio y experiencia local.

Adicionalmente, en atención a la Directriz N° 133-MP-MICITT, mediante alerta técnica MICITT-DGD-DRII-AT-127-2022 Medidas técnicas ante la situación nacional de ciberseguridad, se solicita implementar las siguientes medidas técnicas:

1. Implementar en la institución sistemas de protección y seguridad DNS: mismo que ya se encuentra implementado por la Dirección de Tecnologías de Información y Comunicaciones a nivel institucional desde el pasado 27 de abril 2022.

2. Cambio de contraseñas para todos los usuarios de todas las plataformas informáticas: se solicita su aplicación inmediata a más tardar el 05 de mayo, y comunicar al correo Grupo ASC-Subárea de Seguridad en TIC gsaseg@ccss.sa.cr el cumplimiento de la medida. Deben utilizar al menos 10 caracteres, que contengan mayúsculas, minúsculas, números y signos especiales, salvo que el sistema no permita esta definición, para lo cual deberá definir la mayor seguridad posible bajo las limitaciones del sistema.

3. Implementar el doble factor de autenticación en todos los sistemas que ofrezcan esta medida de seguridad: esta valoración la está realizando la Dirección de Tecnologías de Información y Comunicaciones.

4. Realizar una revisión completa de los usuarios creados para cada uno de los sistemas informáticos y de comunicación, y el Active Directory (para las instituciones que lo utilicen), se debe verificar que sean usuarios válidos y reconocidos por la institución. En caso de detectar usuarios que no corresponda como válido o reconocido por la institución, proceder con su eliminación de forma inmediata (no inactivar, hay que eliminar): y comunicar al correo Grupo ASC-Subárea de Seguridad en TIC gsaseg@ccss.sa.cr el cumplimiento de la medida.

5. Realizar una revisión de la salida de internet de todos los servidores de la institución. Los servidores que no requieran salida a internet, proceder a deshabilitarla: Esta medida se está valorando a nivel de la Dirección de Tecnologías de Información y Comunicaciones, para su aplicación inmediata. Informar si existen equipos que necesariamente requieren salida a internet al correo Grupo ASC-Subárea de Seguridad en TIC gsaseg@ccss.sa.cr

6. Iniciar la implementación como medida preventiva de la aplicación de protección contra el malware tipo Ransomware, para equipos con sistema operativo Microsoft, que el CSIRT-CR estará coordinando directamente con su institución: esta medida ya está siendo implementada a nivel de la Dirección de Tecnologías de Información y Comunicaciones, en conjunto con los Ingenieros

Microsoft, Equipo DART. Por lo que se los solicita brindar cualquier apoyo que pudiera solicitarse a los Centros de Gestión Informática.

7. Implementar en la institución sistemas de protección de tipo EDR: dado que no contamos con una solución de este tipo, esta medida está en coordinaciones con el CSIRT-CR MICITT, dado que cuenta con licencias temporales ante esta situación de ciberseguridad nacional para las instituciones públicas por medio de cooperación público-privado. El equipo técnico está haciendo valoraciones costo-beneficio y tomando en cuenta nuestra infraestructura para la selección de la solución.

8. Definir una política de seguridad en la institución o agregarla a alguna política existente, la cual indique que todas las cuentas de usuario, para cada uno de los sistemas que no cuente con alguna actividad en un periodo de un mes, se deberá proceder con su eliminación de forma inmediata (no inactivar, hay que eliminar). No aplica para el usuario del correo electrónico: Es importante la aplicación inmediata en los sistemas institucionales.

9. Se les recuerda el cumplimiento del siguiente artículo de la Directriz 133 MPMICITT:
Artículo 4 - Se instruye a la Administración Pública Central y se insta a la Administración Pública Descentralizada a informar al Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR) de Costa Rica sobre los incidentes que ocurran en sus instituciones que afecten la confidencialidad, disponibilidad e integridad de servicios disponibles al público, o la continuidad de las funciones institucionales, o la suplantación de identidad de la institución en redes sociales, incluso aquellos incidentes que a lo interno de la institución se consideren bajo control.

Dichos incidentes se deberán informar a la dirección csirt@micit.go.cr proporcionando, al menos, los siguientes datos: nombre, vía de contacto, institución del estado afecta y descripción del problema. Adicionalmente, se instruye a la Administración Pública Central y se insta a la Administración Pública Descentralizada a respaldar la información referente al incidente acontecido, para las investigaciones correspondientes. El resaltado y el subrayado no son partes del original.

En relación con esta instrucción, las notificaciones al CSIRT del MICITT está bajo la gobernanza de la Dirección de Tecnologías de Información y Comunicaciones, por lo que es imprescindible recordarle a los usuarios que ante cualquier sospecha de ataque o malware debe reportarlo de inmediato al teléfono: 2539-1000, correo servicios-tic@ccss.sa.cr, en TEAMS como Mesa de Servicios TIC o con su CGI respectivo, para cualquier atención inmediata del incidente". El subrayado y resaltado no corresponden al original".

III. CONSIDERACIONES

Los constantes ciberataques efectuados en el sector salud e instituciones gubernamentales, a nivel mundial, no deben ser un elemento que frene el imparable y necesario proceso de digitalización, al contrario, la mejor manera de controlar y proteger la información e infraestructuras tecnológicas críticas es con el uso de herramientas y tecnologías existentes que permiten controlar accesos no permitidos, bloquear virus y ataques varios, registrar cada uno de los accesos a información protegida y controlar otras vulnerabilidades de la evolución tecnológica.

Por lo anterior, es prioritario que las organizaciones fortalezcan las medidas de seguridad y acceso a los sistemas, así como, disminuir cualquier oportunidad que facilite a los ciberdelicuentes la intrusión a sus plataformas tecnológicas, es por ello que las debilidades de control en la administración de credenciales para el acceso a los sistemas de información, disminuyen la posibilidad de garantizar la integridad, disponibilidad, confiabilidad y calidad de la información, ya que la misma se encuentra expuesta a eventuales accesos no autorizados, modificación, sustracciones o pérdidas, así como transacciones no autorizadas que podrían generar el uso, modificación y divulgación de datos sensibles.
En relación con lo anterior, es importante señalar como antecedente que, el 31 de mayo de 2022, se registró en horas de la madrugada un ciberataque contra los servidores de la C.C.S.S., el cual obligó, en ese momento,

a realizar una desactivación controlada de los servicios TI institucionales, generando una afectación en la oportunidad y calidad de los servicios brindados a los usuarios internos y externos, situación que pudo haberse generado por vulnerabilidades en el uso y resguardo de credenciales para el acceso a los sistemas institucionales, motivo por el cual, se debe considerar los riesgos en que podría estar expuesta la institución con la utilización de una cuenta genérica para el acceso de información al Sistema Nacional para el Reporte de Funcionarios en Huelga.

De conformidad con lo expuesto, se advierte a esa Administración Activa sobre las debilidades identificadas en relación con el uso de credenciales genéricas para el acceso al Sistema Nacional para el Reporte de Funcionarios en Huelga, a fin de que se adopten las acciones que sean pertinentes y se establezcan las medidas de control necesarias para garantizar razonablemente el cumplimiento normativo, así como, la integridad, disponibilidad, confiabilidad, calidad y seguridad de la información crítica institucional.

De lo anterior, informar -en el **plazo 8 días** - a esta Auditoría sobre las acciones ejecutadas en atención de lo descrito.

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)
Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2023.03.02 18:06:26 -06'00'

M. S.c. Olger Sánchez Carrillo
Auditor Interno

OSC/RJS/RAHM/AEBB/jfrc

C. Doctora. Karla Solano Durán, jefe, Despacho Gerencia General -1100.
Máster. Eithel Geovanni Corea Baltodano, subgerente a.i, Dirección de Tecnologías de Información y Comunicaciones -1150.
Auditoría

Referencia-ID-83691