INFORME FINAL
SEGUIMIENTO AL CUMPLIMIENTO DE LAS POLÍTICAS Y PROTOCOLOS DE SEGURIDAD EN LA INSTALACIÓN, OPERACIÓN Y MANTENIMIENTO DEL APLICATIVO CHIP LOCAL

Fecha del Informe: 2024-10-11
Nombre Auditor: Andrés Mauricio Cruz Vargas
No. Informe: OCI-26-2024

1. OBJETIVO Y ALCANCE.

Evaluar el cumplimiento de las políticas, protocolos de seguridad en la instalación, operación y mantenimiento del aplicativo CHIP local, así como el cumplimiento de las guías establecidas por la Contaduría General de la Nación – CGN en relación a "Instalación y Operación del CHIP local y manejo de parámetros de seguridad CHIP".

El presente seguimiento abarca lo trascurrido de la vigencia 2024, y fue realizado del 2 al 30 de septiembre de este año. Las áreas que cubrió este seguimiento fueron la Unidad de Recursos Financieros y el Grupo de Trabajo Gestión de Plataforma de Tecnologías de Información.

2. CRITERIOS DE AUDITORÍA / SEGUIMIENTO.

- Ley 87 de 1993, por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado.
- Decreto 4131 de 2011, por el cual se cambia la Naturaleza Jurídica del Instituto Colombiano de Geología y Minería (Ingeominas).
- Resolución 0177 de 29 de febrero de 2024, se le asignan funciones a los Grupos de Trabajo del Servicio Geológico Colombiano.
- Documentación publicada en ISOLUCION, Sistema Integral de Gestión.
- Guía para Instalación y Operación del Chip Local, abril 2018, Versión 4.0.
- Guía para el Manejo de Parámetros de Seguridad en el CHIP LOCAL
- Información publicada en las páginas web https://www.chip.gov.co/ y http://www.contaduria.gov.co/

Vale la pena mencionar que el resultado de esta revisión fue remitido en versión Preliminar a la Unidad de Recursos Financieros y al Grupo de Trabajo de Tecnologías de la Información, mediante radicado No. SGC-3-2024-004946 del 30 de septiembre de 2024, con el fin de conocer los comentarios que consideraran respecto a su contenido. Dado que no se recibió respuesta, y tal como se mencionó en el envío, se considera su aceptación con el contenido del mismo, por lo que se procede a emitir el presente informe final en los mismos términos que el informe preliminar.

3. ANÁLISIS, OBSERVACIONES Y RECOMENDACIONES.

El Consolidador de Hacienda e Información Pública (CHIP) es un sistema creado por la Contaduría General de la Nación (CGN) y el Ministerio de Hacienda, para facilitar el registro, validación y difusión

de información desde entidades públicas hacia el Gobierno General y la ciudadanía. Su objetivo es fortalecer el seguimiento fiscal y financiero, homogenizar fuentes de información y simplificar flujos de datos, siendo el único canal para enviar información pública al gobierno nacional.

En la validación efectuada por esta oficina se determinó que:

- La guía para la Instalación y Operación del CHIP Local de la Contaduría General de la Nación (CGN), indica que el perfil de ***Administración de Seguridad***, permite *"(…) al Administrador de Seguridad, tener el control y seguridad del sistema a partir del mantenimiento de usuarios y perfiles, así como la creación y definición de permisos para acceder a las diferentes opciones, o a los objetos de la base de datos, además, el control de las bitácoras para logs de auditoría*."
- El instructivo IN-FIN-CTA-015 "INSTALACION CHIP LOCAL CONTADURIA GENERAL DE LA NACION", indica: "a). La descarga e instalación del aplicativo corre por parte del área de TIC´s, debido a que son ellos quienes tienen los privilegios sobre la red de computadores de la entidad. b). Las claves de acceso al CHIP estarán en cabeza del área de TIC´s. Y por tal motivo, la información será enviada por la misma área. c). El Grupo de TI, verificará los días 25 de cada mes si existe una actualización disponible del aplicativo en la página web www.chip.gov.co"
- El artículo 2 de la Resolución 0177 de 2024 "*Por el cual se le asignan funciones a los Grupos de Trabajo del Servicio Geológico Colombiano*", el Grupo de Trabajo Tecnologías de la Información es el encargado de "*Realizar y mantener actualizado el inventario de la información de plataforma e infraestructura tecnológica, software, aplicaciones y sistemas de información de apoyo a la gestió*n".

Con el objeto de cumplimiento de lo mencionado anteriormente, la OCI solicitó el 2 de septiembre de 2024 al Grupo de Trabajo de Tecnologías de la Información el inventario sobre los equipos del SGC que tienen instalado el aplicativo CHIP Local de la CGN (Ubicación física del activo, Área, Nombre de la máquina y usuario asignado).

El 3 de septiembre de 2024 fue remitió a esta Oficina un archivo en Excel que incluyó entre otros, los siguientes campos (ver tabla 1): Usuario, Nombre completo, Ubicación física, Cédula, Dirección IP, Hostname, Estado de instalación, Estado de actualización, Fecha de instalación, Fecha de actualización, Clave de ADMIN, Observaciones, Acción y Caso en ITOP, donde fueron determinados cinco equipos, de los cuales uno no tenía instalado el chip:

USUARIO	UBICACIÓN FISICA	HOSTNAME	INSTALADO
YGUACANEME	ADMINITRATIVA	BG-CON-071440	SI
LPACHECO	URF	BG-RFI-055684	SI
LSBORDA	TALENTO HUMANO	BG-COC-046675	SI
HERODRIGUEZ	URF	BG-URF-071356	SI
MOVALLE	CONTROL INTERNO	BG-OCI-055990	NO*

Tabla 1 - Campos del archivo en Excel

* Según las observaciones indicadas en el archivo Excel, el equipo se habría dañado y fue necesaria reinstalar el sistema operativo., por lo que a la fecha está pendiente una nueva instalación.

De acuerdo con lo anterior, esta Oficina realizó una prueba de recorrido en cada uno de los equipos indicados, con el fin de:

- Verificar que el inventario suministrado se ajuste a la realidad de la entidad.
- Verificar que el perfil ***Administración de Seguridad*** se encuentre configurado.

En nuestra prueba de recorrido encontramos las siguientes situaciones:

3.1 DESACTUALIZACIÓN DEL INVENTARIO DE EQUIPOS DONDE ESTÁ INSTALADO EL CHIP

De los cuatro equipos de cómputo de los usuarios descritos en la tabla 1, el equipo asignado al usuario YGUACANEME no coincide con los datos proporcionados en el inventario[1] (ver *Imagen 1*):

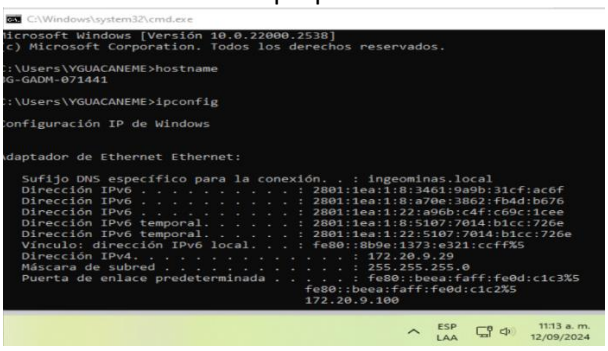

Imagen 1 - Nombre de equipo YGUACANEME

3.2 VERSIÓN DESACTUALIZADA DEL CHIP

Se identificó que dos equipos de cómputo, el BG-RFI-055684 (ver Imagen 2) y el BG-COC-046675 (ver Imagen 3), no tienen instalada la última versión del aplicativo CHIP local, correspondiente a la versión 24.13.0.

Imagen 2 - Versión del aplicativo CHIP local en equipo BG-RFI-055684

Imagen 3 - Versión del aplicativo CHIP local en equipo BG-COC-046675

[1] El artículo 2 de la Resolución 0177 de 2024 "Por el cual se le asignan funciones a los Grupos de Trabajo del Servicio Geológico Colombiano", indica que el Grupo de Trabajo Tecnologías de la Información es el encargado de "Realizar y mantener actualizado el inventario de la información de plataforma e infraestructura tecnológica, software, aplicaciones y sistemas de información de apoyo a la gestión".

3.3 VALIDACIÓN DE PERFILES CREADOS EN CHIP

La OCI solicitó apoyo al personal de la Mesa de Ayuda, encargados de la clave de ADM_GENERAL para validar los perfiles creados (ADM_SEGURIDAD, REGISTRO, REGISTRO Y ENVIO) en el aplicativo CHIP local del equipo actual, pero esta validación no pudo realizarse porque la clave que gestionan para dicho perfil no era correcta[2].

Dado lo anterior, *se* identificó *que* tres *equipos de cómputo, el BG-RFI-055684, BG-COC-046675 y BG-URF-071356, no tienen creado el usuario ADM_SEGURIDAD* (ver Imagen 4). *Esto implica que no cumplen* con los parámetros recomendados de seguridad, conforme el numeral 2.2 "Cambios de clave" de la "Guía Manejo Parámetros Seguridad CHIP versión 3.0 de 2018, "*(…) es recomendable que el responsable de la clave cree un usuario con el perfil de administrador de seguridad y siga los procedimientos de su entidad en políticas de seguridad informática (…)*".

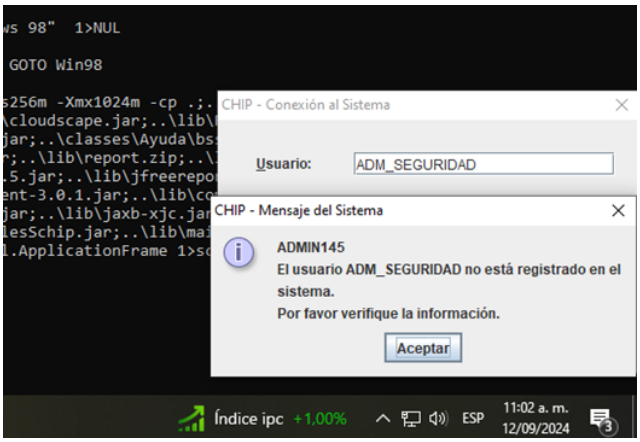

Imagen 4 - Ingreso de Usuario ADM_SEGURIDAD

3.4 OTRAS SITUACIONES EVIDENCIADAS

- Conforme a la solicitud realizada por esta Oficina, en relación al inventario de los equipos del SGC que tienen instalado el aplicativo CHIP Local de la CGN, se constató que el archivo suministrado contenía la clave del usuario ADM_GENERAL. Aunque la clave resultó ser incorrecta, la presencia de datos de acceso en archivos sin cifrado representa una vulnerabilidad crítica. Esto podría facilitar el acceso no autorizado a sistemas sensibles, comprometiendo la confidencialidad de la información.
- Conforme con la prueba de recorrido con cada uno de los equipos, al validar el ingreso al portal www.chip.gov.co, se identificó que los navegadores web permiten el almacenamiento de usuarios y contraseñas. Esta funcionalidad, aunque puede facilitar el acceso a diversas

[2] El instructivo IN-FIN-CTA-015 Instalación Chip Local Contaduría General de la Nación en condiciones generales indica *"b). Las claves de acceso al CHIP estarán en cabeza del área de TIC´s. Y por tal motivo, la información será enviada por la misma área. c). El Grupo de TI, verificará los días 25 de cada mes si existe una actualización disponible del aplicativo en la página web www.chip.gov.co*".

aplicaciones, también representa un riesgo potencial para la seguridad de la información, ya que puede llevar a la exposición de credenciales si no se gestionan adecuadamente.

3.5 RIESGO EVALUADO.

En relación al riesgo evaluado en este seguimiento de la matriz de riesgos del Grupo de Trabajo de Tecnologías de la Información: "*Fallas en hardware y/o software que impiden el correcto funcionamiento de herramientas requeridas para la gestión institucional. Puede suceder que se presenten fallas en el funcionamiento de hardware y/o software que detengan o alteren el funcionamiento normal de los servicios tecnológicos a través de los cuales se desarrolla la operación del proceso*". Y el control asociado al riesgo "*Existe un registro con el inventario de licencias de software, con el objeto de determinar el lugar donde se encuentran instaladas y la cantidad que está instalada respecto a las licencias adquiridas o alquiladas por la entidad*", se recomienda reforzar el control asociado. Es esencial garantizar que este registro no solo esté actualizado, sino que también incluya detalles sobre las fechas de actualización y revisiones periódicas alineadas con el instructivo institucional IN-FIN-CTA-015.

4. RECOMENDACIONES

- Adoptar medidas que garanticen la precisión y actualización de activos de información del aplicativo CHIP como: Controles de verificación, asignar un responsable específico para la gestión del inventario de activos de información, entre otros.
- Evaluar la posibilidad de implementar medidas de seguridad de la información en lo que respecta a la gestión de contraseñas conforme a la norma ISO/IEC 27001.

  - ✓ **Cifrado de Datos Sensibles**: Asegurarse de que cualquier archivo que contenga información crítica, como contraseñas de usuarios, esté cifrado tanto en reposo como en tránsito.
  - ✓ **Política de Almacenamiento Seguro**: Establecer políticas que prohíban el almacenamiento de contraseñas en texto claro y que obliguen a utilizar herramientas de gestión de contraseñas seguras.
  - ✓ **Capacitación Continua**: Proporcionar formación regular al personal sobre las mejores prácticas en seguridad de la información, enfatizando la importancia de la protección de datos sensibles.

- Implementar medidas que mitiguen el riesgo asociado al almacenamiento de credenciales en navegadores web como: Desactivación de almacenamiento automática de contraseñas, y establecer y comunicar políticas claras sobre el uso de contraseñas seguras, entre otras.
- Con el fin de mantener actualizada la última versión del aplicativo CHIP local (según lo indicado en el instructivo IN-FIN-CTA-015), es importante documentar cada revisión y sus resultados para facilitar un seguimiento efectivo. Además, establecer recordatorios y asignar responsabilidades específicas podría contribuir a que esta práctica se realice de manera sistemática y efectiva.

5. CONCLUSIONES.

Existe una debilidad en la gestión del inventario de activos de información con relación al aplicativo CHIP local proporcionado por el Grupo de Trabajo de Gestión de Plataforma de Tecnologías de Información, pues se detectó una discrepancia en la información que incluye registros inexactos en la asignación incorrecta de algunos equipos a usuarios y la administración de la clave del perfil ADM_GENERAL incorrecta; por lo que sugerimos tener en cuenta las recomendaciones presentadas en este informe.

Cordialmente,

Auditor: Andrés Mauricio Cruz Vargas - Contratista

Aprobó: Erika Huari - Jefe de Control Interno