

PERIODO DE EJECUCION

Entre el 1 de abril y el 17 de mayo de 2022, se realizó auditoría a los Controles Generales de TI para el Sistema de Información de Gestión Contractual, de acuerdo con lo aprobado en el Plan Anual de Auditoría para el 2022.

OBJETIVO GENERAL

Establecer la existencia y aplicabilidad de los controles generales automáticos y manuales implementados para el Sistema de Gestión Contractual (SGC) de acuerdo con los cinco (5) aspectos objeto de evaluación, que permitan asegurar la confidencialidad, integridad y disponibilidad de la información. Así como, la gestión de riesgos adelantada por las dependencias involucradas en este sistema.

ALCANCE

Evaluación de la aplicación de controles de los siguientes procesos tecnológicos, para el periodo de evaluación comprendido entre el 1 de abril 2021 a 31 de marzo 2022:

- Administración de Usuarios: creación, eliminación y modificación de perfiles de acceso.
- Configuración de parámetros de contraseña.
- Cambios a programas (ajustes y/o cambios de software normales y de emergencia)
- Ajuste a información directamente en la base de datos, gestión de casos de soporte.
- Copias de respaldo y plan de contingencia.

EQUIPO AUDITOR

Jorge Eliecer Gómez Quintero - Jefe Oficina de Control Interno.
Constanza Cárdenas Aguirre – Auditora de Sistemas.

METODOLOGIA APLICADA

Para el desarrollo de las pruebas de auditoría sobre los controles generales automáticos y manuales para el Sistema de Información de Gestión Contractual, se aplicaron las técnicas de auditoría internacionalmente aceptadas tales como indagación, observación, inspección y comprobación selectiva a través de muestreo, entre otros.

MARCO NORMATIVO:

- Manual de Políticas y Controles de Seguridad y Privacidad de la Información (4204000-MA-031 Versión 3 del 23 dic 2021) de la OTIC Secretaria General.
- Procedimiento Gestión de Incidentes y Requerimientos Tecnológicos (2213200-PR-101 vs. 13)
- Guía Sistema de Gestión de Servicios (2211700-GS-044 vs. 07 del 23 diciembre 2021)
- Procedimiento Análisis, diseño, desarrollo e implementación de soluciones (2213200-PR-106 vs. 14)

**AUDITORIA DE GESTION CONTROLES GENERALES DEL
SISTEMA DE INFORMACIÓN CONTRACTUAL (SGC)**

- Guía Gestión de Usuarios (Correo Electrónico, Directorio Activo y Portales web) (2213200-GS-038 vs.06)
- Plan de Contingencia TI – DRP (2213200-OT-020 vs. 06)
- Metodología para el desarrollo y mantenimiento de soluciones (2213200-OT-006 vs.05)
- Guía de gestión y administración de copias de respaldo (2211700-GS-036 vs 06)
- Decreto 1499 de 2017 – MIPG

CONCLUSION

Como resultado del proceso de auditoría realizado a los Controles Generales de Tecnología para el Sistema de Información de Gestión Contractual (SGC), transversal a la organización a través de varias dependencias responsables de su funcionalidad y administración, sistema que soporta toda la operación del proceso de planeación, programación y ejecución contractual, entre otras funcionalidades, se estableció que en términos generales se ajusta a las necesidades funcionales de la entidad.

No obstante, algunos de los controles generales tecnológicos no son efectivos, ya que no vienen operando de forma adecuada que permitan obtener una seguridad razonable para garantizar confidencialidad e integridad de la información administrada. Esto se presenta porque el sistema de información no cuenta con funcionalidades robustas para la administración de usuarios y para la realización de ajustes por errores de registro de información por parte de los usuarios finales, y como consecuencia hay labores que se realizan desde la OTIC y no por los usuarios finales como procede según las mejores prácticas de seguridad de la información.

A continuación, se relacionan algunas de las situaciones observadas:

- Controles no efectivos para el bloqueo e inactivación de usuarios.
- Alto volumen de soportes en la mesa de servicio asociados a cambios directos sobre la base de datos.
- En la matriz de Activos de Información y valoración de riesgos, no se han gestionado riesgos y controles asociados al software ni a la base de datos que soportan el Sistema de Gestión Contractual.

Referente a los controles existentes, se encontró que se tienen implementado y funcionando adecuadamente los siguientes:

- Administración y depuración de usuarios en el aplicativo, de manera centralizada a través de la Oficina Asesora de Planeación.
- El área de tecnología realiza el bloqueo de usuarios en la base de datos para los usuarios que no registran acceso por un periodo mayor a 90 días.
- Se cuenta con programación de copias de respaldo diarias, semanales y mensuales según lo parametrizado en la herramienta Data Protector.
- A través de los lineamientos dados en procedimiento Gestión de Incidentes y requerimientos Tecnológicos (420400-GS-044 V07), la OTIC realiza el soporte ajustes a la funcionalidad del aplicativo (nuevos desarrollos/mantenimientos) y cambios de información sobre la base de datos solicitados por las dependencias usuarias del Sistema.
- Existencia de manuales funcionales y técnico del Sistema de Información.

En lo concerniente a la evaluación de los controles para la gestión de nuevos desarrollos y mantenimiento del aplicativo, debido a que el procedimiento de Análisis, Diseño, Desarrollo e Implementación de Soluciones (4204000-OT-006 V5) es reciente de acuerdo con su publicación de fecha 21/03/2022, en la actualidad todavía no se cuenta con soportes suficientes que permitan concluir respecto al cumplimiento o efectividad de estos.

OBSERVACIONES Y RECOMENDACIONES

Para la evaluación de Controles Generales de TI del Sistema de Información de Gestión Contractual (SGC), se realizaron pruebas a los controles implementados por la Entidad para la Administración de Usuarios, Gestión de Cambios a Programas, Cambio a datos, atención de requerimientos e incidencias a través de la Mesa de Servicio, Copias de Respaldo y Plan de Contingencia.

A continuación, se describen los principales aspectos observados y las recomendaciones formuladas como resultado de las pruebas practicadas:

1. Administración y Gestión de Usuarios

Observación No. 1

Usuarios asignados a funcionarios retirados y/o sin vínculo laboral identificado

Realizado el cruce de funcionarios retirados de la entidad durante el periodo de evaluación (del 1 de abril 2021 a 31 de marzo 2022) vs los usuarios activos en el sistema (identificados en el archivo de usuarios de la base de datos con el campo account_status = open y el campo Activo = S), se evidenciaron las siguientes situaciones:

- Quince (15) funcionarios retirados y bloqueados (sin acceso) en la fecha de auditoría, sin embargo, para ocho (8) de ellos, el bloqueo se realizó entre 23 y 102 días calendarios posteriores a su retiro, lo cual genera riesgos de uso de usuarios en cabeza de otros funcionarios y accesos no autorizados. Los **ocho (8)** usuarios son: ALCAMARGO, ALEVACA, CEVELEZR, CSANDOVAL, GAMANCERA, LHENAO, LMSANCHEZR, OJASPRILLA

Es de anotar que la labor de inactivación de usuarios a través del aplicativo está a cargo de la Oficina Asesora de Planeación, y el bloqueo a través de la base de datos está a cargo de la OTIC; para el caso de la prueba y de acuerdo con la información de trazabilidad de la base de datos, la fecha de bloqueo corresponde a la ejecución del control realizada por la OTIC.

La situación encontrada, incumple los lineamientos dados en la guía GS-058 –Administración de Base de datos, que en la página 8 dice: “*Se debe realizar este procedimiento una vez al mes para ser informado en el Subcomité de Autocontrol, informando cuantos usuarios fueron bloqueados durante este periodo*” o la guía GS-038 – Gestión de Usuarios que en su numeral 9. Deshabilitación de usuarios, dice: “*...cuando las cuentas son deshabilitadas, inmediatamente se retiran los accesos de: directorio activo, correo electrónico, bases de datos de SI CAPITAL y sistemas de información asociados*”.

**AUDITORIA DE GESTION CONTROLES GENERALES DEL
SISTEMA DE INFORMACIÓN CONTRACTUAL (SGC)**

- Un (1) usuario activo con acceso al Sistema de Información que se encuentra retirado desde el 14/01/2022, generando riesgo de uso indebido o no autorizado y utilización de este en cabeza de otros funcionarios. El usuario es FEJIMENEZ - FELIPE EDGARDO JIMÉNEZ ANGEL.
- Un (1) usuario activo con acceso al Sistema de Información asignado a un funcionario que no corresponde con el estándar de su nombre, y de acuerdo con lo indicado por dicho funcionario, el usuario no es utilizado por él y no conoce a quien pueda pertenecer, generando riesgos de realización de transacciones no autorizadas o erradas en nombre del funcionario responsable del usuario, según lo registrado en la base de datos de usuarios. El usuario es ELPINZONM - FIDEL QUIROGA TRIANA

Las situaciones mencionadas anteriormente, se presentan debido a;

- ✓ Se continúa utilizando el usuario por otros funcionarios posterior a la fecha de retiro del dueño de la cuenta de usuario.
- ✓ El control actual de depuración anual que realiza la OAP, no es efectivo.
- ✓ El control defectivo de bloqueo realizado por la OTIC cada 90 día, no es oportuno.
- ✓ No se ha implementado un control integral con las áreas de Talento Humano y Contratación para que se realice el bloqueo de usuarios inmediatamente o con una diferencia de máximo una (1) semana posterior al retiro o desvinculación laboral o contractual del funcionario.

Recomendación

Con el objetivo de fortalecer el control de acceso al sistema, es necesario analizar el procedimiento actual de bloqueo/inactivación de usuarios y realizar los ajustes que se consideren necesarios, encaminados a contar con un control integrado con las Direcciones de Talento Humano y Contratación para que se inhabiliten las cuentas de usuario inmediatamente el funcionario se retire o finalice su vinculación contractual con la entidad.

Asimismo, asegurar que el control de bloqueo que realiza la OTIC en la base de datos se realice trimestralmente, sin excepción, con el objetivo de mejorar y controlar los tiempos de inactivación entre la fecha de retiro de un funcionario y la fecha de bloqueo/inactivación del acceso en el Sistema de Información o Base de Datos.

Para el usuario que aún se encuentra en uso (FEJIMENEZ), identificar las causas de la situación para tenerlas en cuenta en el fortalecimiento del control y sin excepción, realizar de inmediato el bloqueo respectivo.

Implementar desde la OAP un control de monitoreo de usuarios periódico de forma que, obteniendo la relación de usuarios con el apoyo de la OTIC, se realice el bloqueo o inactivación de usuarios según resultados del mencionado monitoreo.

De igual forma, desde la OTIC implementar un control de forma integral con las áreas de Talento Humano y Contratación para que se bloqueen de forma inmediata los usuarios asignados a los funcionarios retirados o contratistas que terminan su relación contractual con la Entidad.

Se sugiere a la OAP con el apoyo de la OTIC, identificar las operaciones realizadas en las fechas posterior al retiro de los usuarios mencionados y confirmar con las dependencias a las que pertenecían los funcionarios si corresponden a operaciones y acciones debidamente autorizadas, con el fin de identificar oportunamente si se materializó o no el riesgo.

Oportunidad de Mejora No. 1

Usuarios Genéricos, duplicados y no identificados en el registro de control de la OAP

Usuarios Genéricos

Analizada la relación de usuarios con acceso al Sistema de Información de Gestión Contractual (archivo recibido de la OTIC (Archivo: usuarios_sgc_20220404_3.xls), se identificaron cuatro (4) usuarios genéricos sin un responsable asignado, incumpliendo lo definido en el Manual de Políticas y Controles de Seguridad y Privacidad de la Información y Políticas de TI (MA031 V4) numeral 10.4.5 Control de Acceso. Los usuarios genéricos encontrados son: INFAGO, PRESUPUESTO, SGCONSULTA, VBPLANEA.

Usuarios Duplicados


Se identificaron dos (2) funcionarios con usuarios duplicados con dos (2) y cuatro (4) id de usuarios asociados, así: A nombre de CINDY LORENA RODRÍGUEZ PARRA los usuarios: CLRODRIGUEZ y CLRODRIGUEZP y a nombre de PATRICIA RINCON MAZO los usuarios: PARINCONM, PRINCON, PRINCONM, PRINCONMA

Al respecto, la OAP realizó la revisión de los usuarios, informando a esta Oficina, las razones y soportes respecto a la necesidad de contar con varios usuarios asignados a un mismo funcionario debido a los proyectos que tiene a cargo de diferentes dependencias, como es el caso de las funcionarias: Cindy Lorena Rodríguez Parra y Patricia Rincón Mazo, generando posibles riesgos de ejecución de operaciones por la misma persona pero que requieran estar segregadas. Situación que no es factible determinar debido a que no se cuenta con un análisis de riesgo y una matriz de cargos vs roles/perfiles (ver oportunidad de mejora No. 4).

Usuarios existentes en la Base de Datos no identificados en el registro de control de la OAP

Se identificaron doce (12) usuarios activos en la Base de Datos que no cuentan con un registro en el archivo de control que administra la OAP para el control de accesos al Sistema de Información Contractual, lo que implica la existencia de posibles usuarios con acceso no requerido o no necesario con sus funciones. Los usuarios son: AMFARFAN, DACAVANZO, DIR_MANRIQUE, ELPINZONM, JBORRAYB, JGFERNANDEZ, JGMOLANO, JORGEADE, MESOCHA, SCSEGURA, SGCONSULTA, SLAVILAA.

De acuerdo con lo encontrado anteriormente, se hace necesario fortalecer el control actual de depuración de usuarios que realiza anualmente la OAP, para que en complemento al memorando que se remite a todas las dependencias de la Entidad, y en coordinación con la OTIC, se realice un cruce de usuarios en estado activo en la Base de Datos vs el control de usuarios que lleva la OAP, de tal forma que, se identifiquen las diferencias, se revise las causas de la situación y se realicen los correctivos a que haya

	OFICINA DE CONTROL INTERNO
	INFORME EJECUTIVO
AUDITORIA DE GESTION CONTROLES GENERALES DEL SISTEMA DE INFORMACIÓN CONTRACTUAL (SGC)	

lugar. Inicialmente, se sugiere implementar el control trimestral y posteriormente cuando se encuentre estable, se puede ampliar el periodo a semestral.

Es importante que, desde la OTIC se evalúe la posibilidad de realizar nuevos desarrollos al aplicativo que permitan contar con funcionalidades ágiles y dinámicas para la administración de usuarios, logrando así la administración total de usuarios desde el área funcional OAP, lo cual trae como beneficio la eliminación de tareas operativas en la OTIC y fortaleciendo los controles en el proceso de administración de usuarios desde la OAP.

Oportunidad de Mejora No. 2

Estado del Usuario registrado por el aplicativo diferente al estado del usuario actualizado en la base de datos

Analizada la base de datos de usuarios (archivo: usuarios_sgc_20220404_3.xls recibido de la OTIC), se observó que se manejan dos estados de usuario, uno activo o inactivo en el aplicativo (campo “activo” = S o N) y un estado de cuenta de la base de datos (campo “account_status” = open o blocked), con lo cual se puede concluir una falta de alineación entre la activación e inactivación de las cuentas de usuario, que se realiza a través de la Base de Datos y la que se realizan a través de la aplicación, generando falta de integridad o inconsistencia del estado del usuario entre ambas fuentes de información.

Es de señalar que, este asunto no genera riesgo de accesos no autorizados puesto que, al ingresar con un usuario activo en la base de datos, pero inactivo en el aplicativo no se le presentan opciones para realizar acciones en el sistema, y al encontrarse bloqueado en la base de datos desde el inicio no permite su ingreso al aplicativo.

Al respecto, se evidenciaron setenta (70), es decir, el 31 % de doscientos veintisiete (227) usuarios bajo la condición mencionada. Algunos ejemplos de usuarios bajo esta condición son: ALAVERDE, CSANDOVAL, HRINCON, MLMUNOZ, P_RIVERA, entre otros.


Al respecto, es conveniente identificar las causas de la situación mencionada, con el propósito que técnicamente desde la OTIC, se integre el proceso de inactivación de usuarios a nivel de base de datos vs el aplicativo, de tal forma que, el bloqueo de usuario se realice de manera oportuna e integralmente.

Oportunidad de Mejora No. 3

Definición de roles en los Manuales del Sistema de Información vs los configurados en el aplicativo

Los roles existentes en el aplicativo y definidos en el Manual Funcional del Sistema de Gestión Contractual de programación y ejecución del Plan Contractual (Archivo: MANUAL SGC V5.pdf) son:

- Rol Planeación: Permisos para crear y modificar los parámetros de la programación y consultar los diferentes reportes del plan contractual.
- Responsable de rubros: Permisos para crear, modificar y consultar el plan contractual de los rubros y proyectos asignados. Así como registrar, modificar y consultar la ejecución del plan contractual.
- Rol Contratos: Permisos para crear, modificar y consultar el módulo de procesos contractuales.

	OFICINA DE CONTROL INTERNO
	INFORME EJECUTIVO
AUDITORIA DE GESTION CONTROLES GENERALES DEL SISTEMA DE INFORMACIÓN CONTRACTUAL (SGC)	

- Interventor normal: Permisos para crear, modificar y consultar, a partir de los contratos.
- Interventor (no programación, no PAC): Igual al interventor normal, más solicitar disponibilidades y contratos.
- Rol Consulta: Permisos a consultar los diferentes reportes del sistema.
- Corporativa: Permisos para aprobar y consultar el plan contractual.

Sin embargo, se observó que en el manual técnico no se encuentran definidos los roles Consulta y Corporativa, al igual que se encuentran definidos roles adicionales a los mencionados, como los siguientes:


- Administrador: Este usuario es el encargado de administrar los Sistemas de Gestión Contractual, SIPRES y Facturación.
- Planeación: Estos usuarios son los encargados de administrar el módulo de anteproyecto de presupuesto en el Sistema de Gestión Contractual. Encargado además de la parametrización de las tablas del anteproyecto de presupuesto.
- Aprueba Plan Contractual: Este usuario es el encargado de realizar las aprobaciones al Plan Contractual.
- Contratación: Estos usuarios son los encargados de administrar y registrar el módulo de procesos contractuales. Encargados además de la parametrización de las tablas y de registrar la información contractual en el módulo de procesos contractuales.
- Responsable de Rubro: Estos usuarios son los encargados de alimentar en el sistema, la información acerca de la programación presupuestal. (anteproyecto, modificaciones al plan contractual, programación del PAC, etc.). A demás pueden registrar la información sobre la ejecución de los contratos. (actas de inicio, de terminación anticipada, de suspensión, de liquidación, solicitud de contratos, delegaciones de interventoría, solicitudes de pagos, etc.
- Interventoría: Estos usuarios son los encargados de registrar la información sobre la ejecución de los contratos. (actas de inicio, de terminación anticipada, de suspensión, de liquidación, solicitud de contratos, delegaciones de interventoría, solicitudes de pagos, etc.
- Vo.bo. Solicitud Disponibilidades Inversión: Este usuario es el encargado de asignar el visto bueno a la solicitud de disponibilidades de inversión.
- Facturación: Este usuario es el encargado de administrar y registrar la información en el sistema de facturación.
- Presupuesto: Estos usuarios son los encargados de administrar y registrar la información en el SIPRES.

En razón de los anterior, es importante revisar y realizar lo más pronto posible los ajustes a que haya lugar, de los roles y perfiles de acceso existentes en el aplicativo vs base de datos y manuales del sistema de información como son: el manual funcional y el manual técnico.

Oportunidad de Mejora No. 4

Parámetros de configuración de contraseña

Como medida de seguridad todo aplicativo exige el registro de credenciales (usuario y contraseña) robustas para un ingreso seguro, sin embargo, para el caso específico de este aplicativo observamos que

	OFICINA DE CONTROL INTERNO
	INFORME EJECUTIVO
AUDITORIA DE GESTION CONTROLES GENERALES DEL SISTEMA DE INFORMACIÓN CONTRACTUAL (SGC)	

la exigencia de contraseña es básica y no cuenta con parámetros de configuración de contraseña robustos, generando riesgos de acceso no autorizado y posibles modificaciones de la información por utilización de usuarios no autorizados.

A continuación, se relacionan los parámetros de configuración de la contraseña procedente según las mejores prácticas establecidas de seguridad de acceso al sistema de información:

- Tamaño mínimo de 8 caracteres
- Una minúscula y una mayúscula
- Un carácter especial
- Vencimiento de contraseña los 30 días
- Bloqueo por intentos de acceso fallidos
- Exigencia de cambio de contraseña al primer ingreso del usuario.

Asimismo, la identificación del usuario y contraseña son independientes al usuario de la red, lo cual facilita el ingreso al aplicativo con usuarios no activos en la red de la Entidad, vulnerando el control de acceso. Al igual que las contraseñas construidas y asignadas corresponden al mismo id de usuario y no se cambian periódicamente.

Debido a que el aplicativo no tiene la posibilidad de cambio de contraseña por parte del usuario final, no es posible cumplir con los lineamientos definidos en el Manual de Políticas y Controles y Privacidad de la Información Versión 4, que en su numeral 10.3.3.2 Responsabilidades de los Usuarios indica lo que se debe cumplir en cuento a la configuración de contraseña de acceso a los sistemas de información.

Al respecto, se evidenció que las contraseñas son asignadas por el área de Tecnología, sin conservar el lineamiento antes mencionado, con una clave fácil de conocer y que posibilita los accesos no autorizados al aplicativo y en cabeza de funcionarios diferentes al responsable del usuario.

Es necesario que, la OTIC evalúe y analice la posibilidad de implementar un control de acceso integrado con las credenciales de acceso a la red (Directorio Activo) para que el ingreso al aplicativo SGC sea controlado y administrado con las mismas credenciales con que se ingresa a la red de la entidad o realizar los desarrollos necesarios en el aplicativo o configuración en la base de datos con el fin de contar con contraseñas de acceso seguras y cumpliendo con estándares de seguridad y mejores prácticas, al igual que lograr cumplir con los lineamientos establecidos en el Manual de Políticas y Controles y Privacidad de la Información.

Recomendación No.1 - Definición de roles de acuerdo con el cargo y segregación de funciones

Evaluated los usuarios activos en el sistema y los roles de acceso definidos, se observó que para el proceso de administración de usuarios no se cuenta con una matriz de perfiles por cargo, no se han determinado perfiles incompatibles en el proceso (acciones que por su criticidad no deban ser realizadas por la misma persona, ej.: registro de informe de actividades vs aprobación y envío de cuenta a financiera), ni se cuenta con una matriz de roles y responsabilidades (RACI), donde se establezcan claramente una segregación de funciones y con la cual se pueda determinar la validez de los perfiles actuales del sistema y los responsables de cada acción, con el riesgo de que un usuario pueda ejecutar operaciones no acorde

con su perfil, no autorizadas o sin aprobaciones por los niveles necesarios para acciones sensibles y críticas.

Se sugiere que desde las áreas funcionales (OAP, Contratación y Financiera) en conjunto con la OTIC, se implemente una matriz de usuarios y perfiles integralmente con las actividades definidas en los procesos que involucran al Sistema de Gestión Contractual (SGC) y de acuerdo con las responsabilidades de los funcionarios se definan los perfiles por cargo. De igual forma, analizar las funciones incompatibles dentro del proceso vs los accesos otorgados en el Sistema de Información, mitigando así, el riesgo de accesos no autorizados al sistema de información. Se sugiere apoyarse con la OTIC (Rol Seguridad de la Información) para la definición de estos temas.

Al contar con marcos de referencia (matriz) es factible determinar oportunamente desviaciones en la asignación de perfiles, fortaleciendo el control de acceso a la información e identificando los riesgos correspondientes.

2. Gestión de casos de soporte / cambios a datos por la herramienta GLPI

Observación No. 2

Tiempos de gestión en el cierre de los casos de soporte GLPI

Analizada una muestra de nueve (9) soportes GLPI de una población de 590 casos de soporte para el Sistema de Información Contractual, se evidenció que:

- Los nueve (9) casos de la muestra fueron solucionados en menos de una (1) hora, según fecha y hora registrada en GLPI, siendo oportuna la atención al usuario.
- Respecto a la fecha de cierre del caso de soporte que se realiza posterior a la solución del mismo, se encontró que: dos (2) de los nueve (9) casos, correspondiente al 22%, fueron cerrados en tiempos mayores a dos (2) días entre la fecha de solución y la fecha de cierre, así: Caso **240021** en 3.67 días y Caso **214747** en 7.10 días, incumpliendo el procedimiento PR101 Versión 13, que en la página 16, tarea “cerrar solicitud”, indica que: *“Una vez transcurridos los (02) días de resuelto la solicitud se realizará el cierre de la solicitud, se procede a cambiar el estado de la solicitud a “cerrado”.*

Recomendación

Es importante que la OTIC, realice un análisis de los tiempos transcurridos entre la fecha de solución y la fecha de cierre de los casos de soporte, con el fin de identificar si las situaciones detectadas en esta auditoría son puntuales y excepcionales o, en caso contrario, analizar las causas de la inoportunidad y realizar las acciones correctivas a que haya lugar, fortaleciendo el control de cierre del caso de soporte y prevenir el riesgo de incumplimiento del lineamiento establecido.

Recomendación No. 2 - Cambio Directo a Datos

Consultada una muestra de nueve (9) casos de soporte registrados en la mesa de ayuda (herramienta GLPI) de una población de quinientos noventa (590), se observó que el 100% de los registros de la muestra (9) corresponde a cambio directo a datos; labor que realiza los ingenieros de la OTIC directamente sobre la Base de Datos, generando riesgos importantes de errores de modificaciones no autorizadas, errores o cambios intencionales sobre la información relacionada con presupuesto, planes contractuales e información almacenada en la base de datos sobre contratos en ejecución.

No se refleja que la solicitud para la realización de un cambio directo a datos sea generada y/o aprobada por un nivel jerárquico apropiado o que dicho nivel sea copiado en la solicitud. Se considera necesario contar con un enlace definido y aprobado por cada una de las áreas funcionales/usuarios del sistema de información para la solicitud y aprobación de los cambios directos sobre la base de datos.

Se cumple con el lineamiento dado en la guía GS-058 – Guía para la Administración de Base de Datos Versión 2 que en la página 12 dice: “...se debe verificar que el solicitante es el administrador de la información o quien haga sus veces...”; sin embargo, se considera que el lineamiento es muy genérico y no es factible concluir respecto a si la persona solicitante es o no el administrador de la información, puesto que no se cuenta con un listado de funcionarios y/o cargos definidos como solicitantes o aprobadores de este tipo de cambios sobre la Base de Datos.

Sobre el particular, se recomienda a la OTIC analizar el volumen de cambios de datos que se realizan y evaluar la posibilidad de implementar ajustes funcionales en el aplicativo por medio de opciones para el usuario final, de tal forma que los cambios se realicen a través del aplicativo disminuyendo los requerimientos de cambio directo sobre la base de datos y la carga operativa que esto genera para la OTIC, lo cual se pueda realizar accediendo a realizar ajustes por medio de perfiles de acceso y niveles de aprobación, dejando trazabilidad de dichas operaciones como parte de los registros de log del Sistema de Información.

Recomendación No.3 - Categorización de los casos de soporte

Analizadas las categorías de clasificación de los casos de soporte de la mesa de ayuda (herramienta GLPI), no se identifican categorías que diferencien los tipos de solicitud del SGC entre desarrollos y temas de mantenimientos de la aplicación, cambios a datos, infraestructura, etc.

En tal sentido, se hace conveniente que, dentro de la categoría de sistemas de Información, contar con una categoría específica que permita clasificar los casos correspondientes al Sistema de Gestión Contractual, generando beneficios en identificación fácil y clara de las debilidades del Sistema de Información, mejor administración de los casos de soporte de la mesa de servicio y mayor control en la identificación y análisis de casos de soporte repetitivos que permitan tomar acciones e implementar mejoras en el Sistema de Información.

3. Copias de Respaldo (backups)

Observación No. 3

Tiempos de retención de copias de respaldo

De acuerdo con la reunión realizada con el Administrador de los backups de la OTIC, se identificó que el tiempo de retención de las cintas es de dos semanas para las copias de respaldo con periodicidad diaria y semanal. Al respecto, se observó que no se está cumpliendo en la debida forma, según lo establecido en la guía de Gestión y Administración de copias de Respaldo (4204000-GS-036 V6) en su página 11, donde el lineamiento para la “Planificación de la Copia de Respaldo” indica que:

“... ”

- RespalDOS Diarios: Se sobre escribe la información cada 4 semanas. Con esta información es posible tener la información de cualquier día de la semana de las últimas 3 semanas.
- RespalDOS Semanales: Se sobre escribe la información cada 4 semanas (cada mes). Con esta información es posible tener la información del día Domingo de las últimas 4 semanas.

“... ”

Recomendación

Revisar la periodicidad con que se están tomando las copias de respaldo de la base de datos y del aplicativo que soportan el Sistema de Gestión Contractual con respecto a la guía de Gestión y Administración de Copias de Respaldo (4204000-GS-036 V6), y definir la realización de los ajustes que correspondan, ya sea en la configuración del tiempo definido y parametrizado en la herramienta de toma de copias de respaldo (DataProtector) o ajustando la guía GS-036 que da los lineamientos respecto al tiempo de retención de copias en la herramienta para evitar su incumplimiento.

Gestión de Riesgos

Oportunidad de Mejora No. 5

Identificación de Activos de Información y Riesgos de Seguridad Digital

Analizada la matriz de Activos de Información (Archivo: Activos y Riesgos 2021.xls) se encuentran seis (6) activos de información asociados al Sistema de Gestión Contractual, de los cuales dos (2) corresponden al tipo de activo “software” y los otros cuatro (4) clasificados como tipo de activo “información”, observando que no se cuenta con la identificación del activo de información y valoración de riesgos para la Base de Datos que almacena los registros de la operación del Sistema de Gestión Contractual, de igual forma, las principales dependencias usuarias del SGC como son: Dirección de Contratación, Subdirección Financiera y Oficina Asesora de Planeación no tienen identificado como activo crítico el Sistema de Gestión Contractual.

De otra parte, en la matriz de identificación y valoración de riesgos de los Activos de Información, no se evidencian riesgos y controles asociados a: Pérdida de información, Fraudes o ejecución de operaciones

no autorizadas o no acorde a las responsabilidades, interrupción del servicio u operación del sistema y Fallas en el funcionamiento del Sistema de Información.

Al respecto, es conveniente que la Oficina Asesora de Planeación (OAP) y en coordinación con la OTIC, revisen las matrices de Activos de Información y Valoración de Riesgos asociados al Sistema de Gestión Contractual e incluir la Base de Datos del SGC como activo crítico, puesto que allí, es donde se almacenan los registros de información relacionados con el proceso de gestión contractual de la Entidad.

Así mismo, la OTIC gestione con las principales áreas usuarias del aplicativo la identificación de los activos de información críticos y se valoren los riesgos relacionados con el Sistema de Gestión Contractual y que son soporte de los procesos de la Entidad.

Oportunidad de Mejora No. 6


No se obtuvo evidencia que dé cuenta de la actividad de control de monitoreo para verificar la efectividad de los controles definidos por cada una de las dependencias responsables, con lo cual se confirma y asegura que los activos de información están siendo debidamente protegidos y cuentan con una adecuada gestión del riesgo. Este monitoreo que, se implementó bajo los planes de acción No. 5 (108) y 420, y con lo cual se asegura que los controles definidos en la matriz de activos de información existan y sean efectivos, minimizando así el riesgo descrito en la matriz para los activos de información referente a: “Pérdida de Integridad por falencias en la totalidad de la información descrita en el Sistema de Gestión Contractual”.

En este sentido, es necesario fortalecer el proceso de identificación y valoración de riesgos relacionados con Seguridad Digital, de manera que desde la OTIC se mantenga la tarea de seguimiento de la efectividad de los controles a cargo de las dependencias de la Entidad, de la mano con la actualización de los activos de información que se realiza anualmente.

Plan de Contingencia

Realizada la solicitud de información inicial a la OTIC (radicado No. 3-2022-10845) y una vez recibida la respuesta vía mail donde se indica que: “...a finales del año pasado se revisó lo relacionado con el plan de continuidad de negocio y es claro que la implementación de este depende de temas presupuestales que como es bien sabido corresponden a una órbita superior a la oficina TIC”, se concluye que la situación reportada por esta Oficina con memorando 3-2021-36372 del 23 de diciembre de 2021 continúa vigente y se está gestionando bajo el plan de acción No. 1065 con fecha de finalización planeada para el 30 de julio de 2022, sin producirse gestión de avance al corte de abril 2022.

En la vigencia 2021, emitimos el informe mencionado anteriormente que: “En la actualidad la Entidad no cuenta con un Plan de Contingencia en funcionamiento debidamente aprobado y probado que garantice la continuidad de las operaciones de la Secretaría General en caso de ocurrir eventos inesperados”, lo cual involucra el Sistema de Gestión Contractual, objeto de esta auditoría. Y la acción definida desde la OTIC es: “Definición y Actualización previo a la aprobación de la alta gerencia para su puesta en marcha

	OFICINA DE CONTROL INTERNO
	INFORME EJECUTIVO
AUDITORIA DE GESTION CONTROLES GENERALES DEL SISTEMA DE INFORMACIÓN CONTRACTUAL (SGC)	

en el 2022. En caso de no aprobarse la Secretaría General asumirá el riesgo del no respaldo de la infraestructura tecnológica en caso de la materialización del riesgo.”

Plan de Mejoramiento

Producto de la evaluación practicada y resultado del análisis del informe preliminar, la Oficina de Tecnologías de la Información y las Comunicaciones y la Oficina Asesora de Planeación, definieron acciones de mejora dirigidas a subsanar y prevenir las observaciones identificadas como gestionar las oportunidades de mejora y recomendaciones, las cuales conforman el plan de mejoramiento establecido que hace parte integral del informe final, a efecto de adelantar los respectivos seguimientos por los responsables como por la Oficina de Control Interno para su cumplimiento.

Criterios de clasificación de conceptos derivados de la auditoría.

Tipo de observación	Descripción
Observación	Incumplimiento de normas o procedimientos internos que pueden materializar un riesgo.
Oportunidad de mejora	Sin implicar un incumplimiento normativo o de procedimientos internos, es susceptible de mejora el proceso.

Elaborado por: Constanza Cárdenas Aguirre – Contratista, Auditora de Sistemas
 Revisado y Aprobado por: Jorge Eliecer Gómez Quintero – Jefe Oficina de Control Interno