PERIODO DE EJECUCION

Entre el 19 de agosto y el 17 de septiembre de 2021, se llevó a cabo evaluación del proceso de Gestión, Administración y Soporte de Infraestructura y Recursos Tecnológicos de la Secretaría General, de acuerdo con lo programado en el Plan Anual de Auditoría aprobado para el año 2021.

OBJETIVO GENERAL

Evaluar la aplicación adecuada de los controles claves a los procedimientos que conforman el Proceso Gestión, Administración y Soporte de Infraestructura y Recursos Tecnológicos que, tuvieron modificaciones entre agosto 2020 y julio 2021.

Así mismo, establecer el cumplimiento de directrices y lineamientos relacionados con el Sistema de Gestión de Servicios, Borrado Seguro de la Información y Gestión de Usuarios, documentos contentivos del proceso de apoyo a cargo de la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC.

ALCANCE

Verificar la adecuada aplicación de los controles establecidos por la OTIC de los procedimientos que conforman el proceso Gestión, Administración y Soporte de Infraestructura y Recursos Tecnológicos, correspondiente al periodo comprendido entre agosto 2020 y julio 2021, con base en muestreo aleatorio y las directrices emitidas en las guías: Sistema de Gestión de Servicios, Borrado Seguro de la Información y Gestión de Usuarios (Correo Electrónico, Directorio Activo y Portales Web), aplicables en la materia de acuerdo con las pruebas practicadas.

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 al proceso Gestión, Administración y Soporte de Infraestructura y Recursos Tecnológicos, se aplicaron las técnicas de auditoría internacionalmente aceptadas tales como indagación, observación, inspección y comprobación selectiva a través de muestreo, entre otros.

MARCO NORMATIVO:

- Caracterización del Proceso Gestión, Administración y Soporte de Infraestructura y Recursos Tecnológicos (2213200-PO-036 versión 13 del 19 de octubre 2020).

- Procedimiento Gestión de Incidentes y requerimientos tecnológicos (2213200-PR-101 versión 12 del 18 diciembre 2020)
- Procedimiento Mantenimiento de la Infraestructura Tecnológica (2213200-PR-104 versión 10 del 14 de mayo de 2021)
- Guía Sistema de Gestión de Servicios (2211700-GS-044 versión 5 del 22 de junio 2018)
- Guía Gestión de Usuarios (2211700-GS-038 versión 5 del 28 diciembre 2020)
- Guía Borrado Seguro de Información (4204000-GS-089 versión 1 del 14 julio 2020)
- Guía para el mantenimiento de la infraestructura tecnológica (2211700-GS-052 versión 3 del 14 de julio 2020)
- Mapa de riesgos del proceso con fecha de actualización al 30/04/2021.

CONCLUSION

Como resultado de las pruebas de auditoría practicadas al proceso de Gestión, Administración y Soporte de Infraestructura y Recursos Tecnológicos para el período comprendido entre agosto de 2020 y julio de 2021, proceso a cargo de la OTIC, con el cual se mantiene la disponibilidad de los recursos de tecnología de información y comunicaciones y permite atender oportunamente los requerimientos de soporte tecnológico de usuarios internos y externos, se concluyó que se encuentran implementados y operando algunos de los controles asociados a la actualización de documentación contentiva del proceso, solución adecuada a los requerimientos de soporte puestos en la mesa de servicio, remisión periódica la OAP de soportes y tareas que dan cuenta de la ejecución de los controles definidos en los procedimientos, ejecución de mantenimientos preventivos de equipos de cómputo (impresoras, video beams, escáneres, aires acondicionados).

Se observó que los documentos contentivos del proceso fueron analizados por la OTIC y como resultado se identificaron los que requerían actualización, tarea que está siendo adelantada como parte de la implementación de planes de mejoramiento del proceso.

No obstante, se observaron situaciones para las que se requieren acciones correctivas inmediatas y otras susceptibles de mejora, relacionadas con:

- La Guía Borrado Seguro de Información (4204000-GS-089 versión 1) fue generada y publicada en julio de 2020; sin embargo, se encuentra en la etapa inicial de implementación sin contar con evidencias soporte suficientes que permitan dar cuenta de la ejecución y cumplimiento de los lineamientos y controles allí establecidos.

- No se evidenciaron algunos soportes que den cuenta del cumplimiento de lineamientos definidos en la Guía GS052 para el mantenimiento de la Infraestructura Tecnológica versión 3 del 14 de julio 2020, como son: El Plan Anual de Mantenimiento preparado en el último trimestre del año inmediatamente anterior, soportes de aprobación y socialización del plan de mantenimiento preventivo, y relación de activos de fuente de información del mencionado plan.

- Para algunos casos de soporte de una muestra seleccionada, se observó que los tiempos de atención superan los establecidos en los Acuerdos de Niveles de Servicio, según las categorías de los servicios a los que se da soporte desde la Mesa de Servicio de la OTIC.

- Incumplimiento de requisitos exigidos para la creación de cuentas de usuario, específicamente en el diligenciamiento del formato FT1000 y la firma de los usuarios y de los jefes aprobadores.

- Falta de monitoreo de usuarios con acceso a la red de la entidad (Directorio Activo), encontrando usuarios activos que no cuentan con un soporte de tener relación laboral o contractual vigente con la entidad, y usuarios ya retirados con acceso e incluso con registro de fecha de ingreso posterior a la fecha de retiro de la entidad.

- Actualización de los documentos: Guía Sistema de Gestión de Servicios (2211700-GS-044), Guía Incidentes de Seguridad (2211700-GS-042) y Guía para la configuración de perfiles en el Sistema de control de acceso manzana Liévano 2211700-GS-039.

- Actualizar el mapa de riesgos acorde con los controles definidos en los procedimientos contentivos del proceso. Así como, fortalecer el proceso de monitoreo sobre la ejecución y la evaluación de la efectividad de los controles, de tal manera que se detecten oportunamente desviaciones desde un proceso de autoevaluación del área y no solo ante visitas de los entes de control.

OBSERVACIONES Y RECOMENDACIONES PRODUCTO DE LA EVALUACIÓN

Para evaluar el Proceso de Gestión, administración y soporte de infraestructura y recursos tecnológicos, se realizaron pruebas a los controles implementados por la Entidad para atender oportunamente los requerimientos de soporte tecnológico de la entidad, gestionar los usuarios con acceso a la red y al correo electrónico, la gestión del borrado seguro de información sobre los equipos de cómputo y el mantenimiento de la infraestructura tecnológica.

En tal sentido a continuación, se describen los principales aspectos observados y las recomendaciones formuladas como resultado de las pruebas practicadas:

1. Documentación del Proceso en el Sistema Integrado de Gestión (caracterización, procedimientos, guías, manuales y otros procedimientos)

Oportunidad de Mejora No. 1:

Analizados los documentos establecidos en el Sistema Integrado Gestión que hacen parte integral del proceso evaluado, se observó que la mayoría se encuentran vigentes y que varios fueron actualizados entre junio 2020 y agosto 2021, en atención a las recomendaciones formuladas por esta Oficina en la evaluación anterior.

De acuerdo con lo informado por la OTIC, respecto a la actualización de los documentos contentivos del proceso cuya fecha de actualización fue anterior al año 2018, indicó que algunos serán actualizados durante el año 2021 y otros no requieren actualización debido a que el documento continúa vigente.

De otra parte, existen documentos contentivos del proceso (marcados en las tablas siguientes con asterisco (*)) socializados que no están referenciados en los procedimientos ni en los documentos contentivos del proceso.

A continuación, se relaciona el detalle de lo mencionado:

1. Documentos actualizados y publicados entre julio 2020 y agosto 2021:
   - Caracterización del Proceso (2213200-PO-036)
   - Plan de Contingencia TI – DRP (2213200-OT-020)
   - Gestión de Incidentes y requerimientos tecnológicos (2213200-PR-101)
   - Guía Borrado Seguro de Información (4204000-GS-089)
   - Guía para el mantenimiento de la infraestructura tecnológica (2211700-GS-052)
   - Guía para la Administración de Redes (4204000-GS-091)
   - Mantenimiento preventivo de recursos informáticos (2213200-PR-104)
   - Guía de gestión y administración de copias de respaldo (4204000-GS-036)
   - Guía para la Administración de Bases de Datos (4204000-GS-058)
   - Guía Gestión de Usuarios (Correo Electrónico, Directorio Activo y Portales web) (2211700-GS-038).

2. Documentos que requieren actualización rápida antes del cierre de año 2021:

   - Guía Sistema de Gestión de Servicios (2211700-GS-044)
   - Guía Incidentes de Seguridad (2211700-GS-042)
   - Guía para la configuración de perfiles en el Sistema de control de acceso manzana Liévano (2211700-GS-039)

3. Documentos que no requieren actualización, de acuerdo con lo indicado por la OTIC, continúan vigentes:

   - Guía de acceso a data center, cuartos técnicos y cuartos de almacenamiento de medios (4204000-GS-037).
   - Lista de chequeo impresoras y otros elementos (2213200-FT-724)*
   - Lista de chequeo PC de escritorio y portátiles (2213200-FT-725)*
   - Lista de instalación / desinstalación de software (2213200-FT-722)
   - Mantenimiento preventivo (2213200-FT-259)
   - Plan Anual de Mantenimiento Infraestructura Tecnológica (2211700-FT-940) **
   - Solicitud de préstamo de equipos (2211700-FT-858)*
   - Solicitud de servicios TIC Secretaría General (4204000-FT-1000).
   - Estándares de nomenclatura para desarrollo de aplicaciones en ambientes de bases de datos (4204000-OT-047)

- Actualización de elementos informáticos (2213200-FT-518).
- Clasificación y preevaluación solicitud de requerimientos (2213200-FT-519) *
- Bitácora de acceso a centros de cómputo y cuarto de comunicaciones (2213200-FT-267)

Nota: * Documento sin referencia ni llamado desde los procedimientos, guías u otros documentos contentivos del proceso
** Documento sin versionamiento en el interior del documento

De otra parte, se observó que en la Caracterización del Proceso (2213200-PO-036 versión 13) se referencian los siguientes dos documentos que no hacen parte de este proceso, sino del proceso estratégico denominado “Estrategia de Tecnología de la Información y las Comunicaciones”. Los documentos son:

- Lineamientos para la implementación y sostenibilidad del sistema de gestión de seguridad de la información (4204000-OT-048).
- Manual del SubSistema de Seguridad de la Información (4204000-MA-031). El nombre del este documento no corresponde con el documento que actualmente se encuentra vigente y que hace parte del proceso “Estrategia de Tecnología de la Información y las Comunicaciones”

Continuar con el proceso de revisión y actualización tanto de la Caracterización del proceso como de los documentos contentivos del mismo que así lo requieren, y confirmar que estén debidamente referenciados en los procedimientos o guías según aplique y se requiera para su entendimiento y ejecución en la dinámica diaria de la operación.

Producto de la recomendación realizada en la auditoría de la vigencia anterior, actualmente se cuenta con el Planes de Acción No. 242-241 encaminados a la implementación de un control de monitoreo periódico de usuarios de Directorio Activo.

Oportunidad de Mejora No. 2:

Para algunos de los documentos actualizados durante el periodo evaluado (agosto 2020 a julio 2021), no se encontró evidencia de socialización de los mismos en el Subcomité de Autocontrol del área, y aunque para algunos se evidencian pantallas de citación a reunión por Teams o pantalla del informe presentado en subcomité de autocontrol por la Ingeniera a cargo del tema, con estas evidencias no es factible concluir si se realizó o no la presentación en el Subcomité. Tampoco se cuenta con listas de asistencia que permitan confirmar la participación de los funcionarios en las sesiones de socialización programadas por Teams, aspecto importante para conocer los cambios en actividades y aplicación adecuada de estos.

A continuación, se relacionan los documentos bajo la circunstancia mencionada:

- Caracterización del Proceso (2213200-PO-036)
- Guía Borrado Seguro de Información (4204000-GS-089)
- Gestión de Incidentes y requerimientos tecnológicos (2213200-PR-101)
- Mantenimiento preventivo de recursos informáticos (2213200-PR-104)

- Guía de gestión y administración de copias de respaldo (4204000-GS-036)
- Guía Gestión de Usuarios (Correo Electrónico, Directorio Activo y Portales web) (4204000-GS-038).

Se sugiere fortalecer la labor de socialización de las actividades actualizadas en los documentos contentivos del proceso Gestión, Administración y Soporte de Infraestructura y Recursos Tecnológicos, y realizar las socializaciones correspondientes con el equipo de trabajo y funcionarios dejando soporte idóneo de la tarea realizada, como lista de asistencia, fecha de la reunión, temas tratados; así como, realizar las socializaciones oportunamente en un período no mayor a un mes luego de la oficialización y publicación de los documentos, obteniendo utilidad y control en la ejecución de actividades del proceso.

2. Guía Sistema de Gestión de Servicios (2211700-GS-044)

Oportunidad de Mejora No. 3

Analizado el archivo con los ANS recibido (Categorías GLPI 20-07-21 ANS.xlsx) y los casos de soporte de GLPI abiertos durante el periodo de evaluación, se evidenció que existen categorías en GLPI que no cuentan con un Acuerdo de Nivel de Servicio definido. Adicionalmente, no se refleja que exista relación directa entre la descripción de las categorías de GLPI vs los nombres establecidos en los ANS (Acuerdos de Nivel de Servicio). A continuación, se detallan las situaciones identificadas:

1. Se evidenciaron quince (15) categorías (campo: Categoría del archivo: Punto 4-solicitudes-cerradas-agosto 1-2020-a-julio-31-2021.xls) de los registros GLPI que, no tienen un ANS definido o no tienen un tiempo establecido para la atención respectiva. Algunos ejemplos bajo esta situación son:

   - Sin tiempo de ANS definido: Cuentas de Usuario\Creación o Modificación de cuenta de red, Cuentas de Usuario\Desbloqueo y/o restablecimiento de cuenta, Cuentas de Usuario\ Creación de cuenta de correo electrónico, INFRAESTRUCTURA\Nube\Despliegue Aplicaciones, entre otros.

   - Sin ANS definido: TECNOLOGICO\SAT\Gestion de Usuarios SAT, TECNOLOGICO\ EQUIPOS\Solicitud CCTV, Telefonía\Asistencia en Telefonía y Capacitación.

2. Dieciséis (16) categorías en GLPI (según los casos de soporte registrados en GLPI, archivo: Punto 4-solicitudes-cerradas-agosto 1-2020-a-julio-31-2021.xls) que pertenecen a una categoría diferente a la existente en los ANS (Categorías GLPI 20-07-21 ANS.xls). Mencionamos algunos ejemplos a continuación:

   - INFRAESTRUCTURA > Seguridad Informática > Habilitar VPN vs INFRAESTRUCTURA - Seguridad Informática - Habilitar o Deshabilitar VPN (ajustar por: Habilitación de VPN)

   - MESA DE SERVICIOS > Usuario Final > Asistencia y/o Capacitación Sistemas Operativos vs Software y/o Archivos de Usuario Final - Asistencia y/o Capacitación Sistemas Operativos-

– Telefonía > Asignación, Reasignación o Traslado de extensión y/o línea telefónica vs INFRAESTRUCTURA - Usuario Final - Asignación, Reasignación o Traslado de extensión y/o línea telefónica

3. Revisadas las categorías de servicio definidas en la guía GS044-Guía Sistema Gestión de Servicios, numeral 3.2 – Categorización de la solicitud de Servicio, se observó que no hay relación entre la descripción de las categorías vs los nombres establecidos en GLPI. Algunos ejemplos a continuación:

Al respecto, es necesario revisar las categorías parametrizadas en la herramienta GLPI de la Mesa de Servicio vs la clasificación definida en la Guía Sistema de Gestión de Servicios, y realizar los ajustes a que haya lugar, ya sea la parametrización en la herramienta de Mesa de Servicio o evaluar si se requiere actualizar la Guía mencionada.

Observación No. 1

De 22.671 casos de soporte de la Mesa de Servicio en estado cerrado y registrados entre agosto 2020 y julio 2021, para una muestra de nueve (9) registros se identifican dos (2), equivalente al 22%, cuya categoría no tiene definido un ANS (correspondiente al 22% de la muestra) y cinco (5) (correspondiente al 56% de la muestra) que no fueron resueltos dentro de los tiempos establecidos en los ANS, generando inoportunidad en la atención del servicio (tiempo transcurrido entre la fecha de registro y la fecha de solución). Los casos evidenciados bajo la situación mencionada son: 178533, 178916, 180515, 187819, 189850, 200970 y 222607, con diferencia de días en su solución con respecto a los ANS establecidos de entre 8 y 70 días.

De igual forma, se identifica que en el numeral 3.2.9 – Sistemas de Información de la guía GS044- Guía Sistema de Gestión de Servicios no se detalla bajo esta categoría los casos de soporte relacionados con Gestión de Usuarios de Aplicaciones. Para la muestra seleccionada se observaron los siguientes casos: 187819 y 209444.

Asimismo, según la guía GS-044 numeral 3.2.8, el control de componentes debe categorizarse en “Servicios Especiales”, sin embargo, se encontraron dos (2) casos de soporte categorizados de manera diferente. Los casos de soporte: 189850 y 200970.

Recomendación

Fortalecer el proceso de monitoreo, seguimiento y medición de los tiempos de cumplimiento para la solución de los casos de la mesa de servicio de acuerdo con los ANS definidos, de manera que se detecten oportunamente desviaciones y se tomen las acciones correctivas y preventivas necesarias encaminadas a dar cumplimiento a los ANS y prestar un servicio oportuno al usuario en cumplimiento a los Acuerdos de Nivel de Servicio establecidos con el proveedor de la Mesa de Servicio.

Observación No. 2

Analizada una muestra de diez (10) casos de soporte GLPI de los 2.607 registrados en las categorías creación o modificación de cuenta, creación o modificación de cuenta de red o creación de cuenta de correo, se observó que para uno (1) de ellos, correspondiente al 10% de la muestra, no se cuenta con soporte del FT1000 y, para los otros cinco (5) restantes, correspondientes al 50%, no se cuenta con firma del jefe en señal de aprobación; ni se encontró un soporte complementario entendiendo la situación de la emergencia sanitaria y el teletrabajo.

Esta situación genera riesgos de usuarios con acceso a la red de la entidad sin autorización y/o sin conocimiento de parte de los niveles aprobadores autorizados.

Los VPN vs seis (6) casos de la muestra de diez (10), representan el 60% que, no cumplen con los requisitos establecidos en el numeral 3. Realizar, evaluar, categorizar solicitud de servicio del procedimiento PR-101- Gestión de Incidentes y requerimientos tecnológicos, ni con los lineamientos dados en el numeral 3. Gestión de Usuarios de la guía GS038-Guia Gestión de usuarios, son: 196297, 196758, 198701, 207521, 208856 y 211353.

Recomendación

Es importante que la OTIC, de cumplimiento estricto al procedimiento PR-101- Gestión de Incidentes y requerimientos tecnológicos, y a los lineamientos establecidos en la guía GS-038- Guía Gestión de Usuarios.

Adicionalmente, es recomendable implementar pronto un control de revisión por muestreo, para asegurar que todos los usuarios creados tengan un caso de soporte en GLPI (Mesa de Servicios) y el formato FT-1000 debidamente firmado y diligenciado. Esto debido a que, en la auditoría del año anterior, se evidenció la misma situación y al realizar seguimiento de la acción No. 247 ya finalizada se evidencia que la acción no fue efectiva, por tanto, no se ha subsanado esta debilidad de control, con vertiéndose en una situación recurrente, generando riesgos.

Asimismo, se considera necesario definir un campo en la herramienta GLPI de la Mesa de Servicios, para incluir el código de usuario y responsable, con que se crean los usuarios en los sistemas de información.

Observación No. 3

En el numeral 3.3 Mantenimiento Preventivo de la guía GS044 – Guía Sistema Gestión de Servicios, se hace referencia al documento “Guía de Cumplimiento del Plan Anual de Mantenimientos Preventivos”, sin embargo, el mismo no se encuentra publicado en el SIG. El documento que se evidenció publicado en el SIG corresponde a la guía GS052-Guía para el mantenimiento de la Infraestructura Tecnológica versión 3 del 14 de julio 2020.

No se evidenciaron soportes según lineamientos establecidos en la Guía GS052, así:

- ✓ Plan anual de mantenimiento año 2021 preparado el último trimestre del año 2020 (FT940) de acuerdo con lo definido en los numeral 4.1, 5.1, 5.2 de la guía mencionada.

- ✓ Soporte de aprobación y socialización del plan de mantenimiento preventivo, según numerales 5.2 y 5.3 de la guía mencionada.

- ✓ Relación de activos fuente de información para la preparación del plan de mantenimiento anual, según se encuentra definido en el numeral 4.2 de la misma guía.

Recomendación

Es necesario realizar sensibilización a los funcionarios sobre los lineamientos definidos en la guía GS-Guía para el mantenimiento de la Infraestructura Tecnológica, con el fin de dar cumplimiento a los controles y lineamientos allí definidos.

3. Guía Borrado Seguro de Información (4204000-GS-089)

Observación No. 4

Analizados los casos GLPI recibidos (Archivo: Punto 9 -solicitudes-cerradas-agosto 1-2020-a-julio-31-2021-que incluyen la palabra -BORRAR-.xlsx), se observó que existen treinta y siete (37) casos y ninguno corresponde a solicitudes de borrado seguro de información, lo que significa que no se han registrado solicitudes de este tipo en la mesa de servicio según lo establecido en la guía GS089- Borrado Seguro de Información. Por lo tanto, no es factible concluir sobre la aplicabilidad de la guía y de los mecanismos de destrucción mencionados en el mismo documento.

De los 37 casos recibidos, 35 corresponden a solicitudes de borrado de información de las bases de los Sistemas de Información SIVIC, Perno, Facturación, SIGA y Gestión Contractual. Los otros dos (2) casos corresponden a solicitudes de borrado de temporales de un PC y de borrado de archivos del OneDrive; por lo tanto, se confirma que ninguno de los casos recibidos corresponde a los soportes asociados al cumplimiento de la guía 089 – Borrado Seguro de Información.

Al cierre de la auditoría no se recibieron los soportes solicitados que están establecidos en la guía GS-089, para el borrado seguro de información, tales como: mail de solicitud de borrado enviado por el jefe de la dependencia, caso de soporte en GLPI, autorización y aprobación del requerimiento de borrado de información y acta de destrucción para los equipos dados de baja.

Por lo anteriormente enunciado, se concluye que la ejecución de la guía GS-089 de borrado de información se encuentra en proceso de estabilización, al no contar con evidencia suficiente para concluir respecto al cumplimiento de los lineamientos y de los controles allí establecidos.

Recomendación

Es importante llevar a cabo la sensibilización de la guía GS-089 de borrado de seguro de información, involucrando a las diferentes responsables de la ejecución de los controles y lineamientos allí definidos. Además, de asegurar que se deje evidencia soporte del borrado de información realizado a todo equipo de cómputo reintegrado al almacén, reasignado o dado de baja.

4. Guía Gestión de Usuarios (2211700-GS-038)

Observación No. 5

Recibida y analizada la relación de usuarios activos con acceso a la red (Directorio Activo) y al correo electrónico, se observó que no se cuenta con un control periódico de monitoreo sobre los usuarios que tienen acceso al Directorio Activo, que permita controlar efectivamente que los usuarios mantienen relación laboral con la Entidad, ya sea por contratación directa o de servicios profesionales, lo que implica riesgo de posibles accesos no autorizados a la red de la entidad (Directorio Activo) y/o al correo electrónico.

Realizados los cruces de usuarios activos en el Directorio Activo con los funcionarios de la planta de personal vigente y los funcionarios retirados, con base en la información suministrada por la Dirección de Talento Humano, se identificaron las siguientes situaciones:

- Cincuenta y uno (51) usuarios activos con acceso a la red que, de acuerdo con las relaciones de funcionarios recibidas de Talento Humano (archivo: Funcionarios_Activos 082020 - 082021.xlsx) y de Contratación (Archivo: Contratistas_Vigentes agosto 2020 a 2021.xlsx), no se encontró que tengan relación laboral o contractual vigente con la entidad. Ver detalle en el informe final.

- Cuarenta y Siete (47) usuarios en estado activo con accesos a la red (Directorio Activo), que según la relación recibida de Talento Humano al corte 31 de agosto de 2021, son usuarios desvinculados de la entidad con fechas de retiro que oscilan entre el 05/10/2020 y el 31/08/2021, y aún se encuentran activos en el DA, veintidós (22) de ellos, presentan ingreso posterior a la fecha de retiro. Adicionalmente se observa que el funcionario tampoco cuenta con un contrato vigente con la Entidad. Ver detalle en el informe final.

- Doscientos ochenta y uno (281) usuarios con más de 90 días de no ingreso a la red, incumpliendo lo establecido en el numeral 8. Cuentas Deshabilitadas, de la guía GS-038 Guía Gestión de Usuarios de Gestión de Usuarios. Ver detalle en el informe final.

- Cuatrocientos veintiuno (421) usuarios genéricos activos en el DA, sin contar con un usuario responsable, a manera de ejemplo mencionamos los siguientes: aranda@alcaldiabogota.gov.co, parqueadero2@alcaldiabogota.gov.co, sgsi@alcaldiabogota.gov.co, consultoríadddi, redesisab@alcaldiabogota.gov.co, todaslasdependencias@alcaldiabogota.gov.co, sgeneral_ivc@alcaldiabogota.gov.co, management@alcaldiabogota.gov.co.

Las situaciones anteriormente mencionadas, están generando constantes riesgos de accesos no autorizados a la red de la entidad (Directorio Activo), dificultad para establecer responsabilidades en caso de uso indebido de estos usuarios, posible ejecución de operaciones en los sistemas de información en cabeza de usuarios que no cuentan con una relación laboral o contractual con la Entidad, así como un incumplimiento al Manual del Sistema de Seguridad de la Información (MA-031 versión 2) en su numeral 10.3.1 – Responsabilidades, en los ítems que se mencionan a continuación:

"…
Tanto el responsable del área restringida como el encargado del manejo del activo de información deberán realizar al menos una revisión anual (o cuando sea requerido) de los derechos de acceso de los usuarios en intervalos regulares, con el fin de mantener un control eficaz de acceso a los datos y a los servicios de información.

Todos los usuarios tendrán un identificador único (ID del usuario) para su uso personal que les permita validar los accesos y verificar el buen uso de la información, sistemas de información e instalaciones.

En caso de que existan identificadores de usuarios genéricos en cualquier sistema operacional, base de datos, o aplicación, deben estar debidamente individualizados los responsables; validados y gestionados los riesgos de seguridad de la información; y aprobados los controles respectivos por la Oficina de Tecnologías de la Información y las Comunicaciones. …"

Recomendación

Es indispensable implementar lo más pronto posible medidas de control y en coordinación con el área de Talento Humano, el monitoreo mensual de usuarios para inactivar inmediatamente aquellos que se han retirado de la entidad, así como con el área de Contratación, los que no cuenten con un contrato vigente.

Con el objetivo de prevenir riesgos es necesario identificar, depurar y actualizar los usuarios genéricos y los que no se encontraron dentro de los funcionarios activos como funcionarios de la Entidad, según registros de Talento Humano, o como contratistas vigentes, asegurando que únicamente se tiene permitido de acceso a usuarios con vínculo contractual vigente con la entidad.

Es preciso revisar, actualizar y divulgar el Manual de Seguridad de la Información estableciendo el tiempo de la revisión de los derechos de acceso de los usuarios, de anual a semestral, teniendo en cuenta que en la actualidad el manual indica que: "*Tanto el responsable del área restringida como el encargado del activo de información deberán realizar* ***al menos una revisión anual*** *(o cuando sea requerido) de los derechos de acceso de los usuarios en intervalos regulares, con el fin de mantener un control eficaz de acceso a los datos y a los servicios de información*." (la negrilla es nuestra).

Consideramos importante incorporar y ajustar lo más pronto posible estas medidas de control en el procedimiento de Administración de Usuarios, incluyendo las actividades de control y responsables de gestionar los usuarios (creación, actualización, bloqueo y/o retiro) para todos los Sistemas de Información existentes en la Entidad, evaluando la posibilidad de implementar un control periódico que, bajo responsabilidad de la OTIC, asegure que las directrices y/o políticas generales aplicables a la

administración de usuarios se cumplan para todos los Sistemas de Información de la Entidad, alineado a lo establecido en el Manual de Seguridad de la Información (4204000-MA031) relacionado con la revisión anual de los derechos de acceso y la desactivación de los mismos una vez terminados los vínculos contractuales con la Entidad, previniendo la exposición del riesgo.

5. Seguimiento Planes de Mejoramiento Vigencias anteriores

Verificados los Planes de Acción resultado de la auditoría realizada en la vigencia anterior al proceso de apoyo Gestión, Administración y Soporte de Infraestructura y Recursos Tecnológicos, se identificaron veintitrés (23) acciones de mejora con el siguiente estado de implementación, al corte julio 2021:

- Diecisiete (17) finalizadas (acciones Nos. 237, 239, 240, 241, 243, 244, 245, 246, 247, 249, 250, 252, 253, 254, 257, 258, 259).

- Seis (6) vencidas, así: La acción No. 238, desde el 28 de febrero de 2021 con un avance del 95%. Y las acciones Nos. 242-241, 248, 251, 255 y 256 desde el 30 de junio 2020 con avances desde el 60% hasta el 96%, situaciones que hacen que no se subsanen efectivamente las debilidades de control, permaneciendo los riesgos latentes.

Realizadas las pruebas para verificar la efectividad de los planes de acción implementadas, se observaron las siguientes situaciones:

1. Doce (12) fueron efectivas y corresponden a la eliminación de algunos procedimientos del proceso y la actualización o creación de guías. Las acciones son: 237, 239, 240, 241, 243, 244, 250, 253, 254, 257, 258, 259.

2. Dos (2) corresponden a temas de depuración de usuarios de los sistemas de información Contractual y Facturación, que no hacen parte del alcance de esta auditoría y que se realiza seguimiento a su efectividad cuando se auditen esos Sistemas de Información que son administrados por áreas diferentes a la OTIC, dueña del proceso auditado. Las acciones son: 245 y 246.

3. Tres (3) acciones que se consideran no efectivas luego de realizar pruebas de verificación en cuanto a su ejecución durante el periodo evaluado, con los siguientes resultados:

    - Acción 247: Se evidenció capacitación realizada el 7/07/2021 a los funcionarios de la mesa de servicio que atienden casos en nivel 0. Se tomó una muestra de diez (10) casos de soporte de creación/modificación de cuenta y para seis (6) de ellos, se observaron debilidades en el diligenciamiento del formato FT1000. Los casos son: 196297, 196758, 198701, 207521, 208856, 211353. Ver detalle en la observación No.2 arriba en este informe.

    - Acción 249: Al cierre de la auditoria no se obtuvo información que permitiera dar cuenta de la efectividad de la acción. La acción corresponde a: “Actualizar el inventario de bases de datos, con la versión respectiva y el Sistema de Información que soporta”.

- Acción 252: Al cierre de la auditoria no se obtuvo información que permitiera dar cuenta de la efectividad de la acción, relacionada con la actualización del Excel creado cuando se cerró la acción, donde se contaba con el listado de servidores vs activos de información, clasificación de criticidad e identificación y confirmación de la configuración y toma de copias de respaldo.

Oportunidad de Mejora No. 4

Es necesario revisar y actualizar los archivos de bases de datos vs versión vs Sistema de información (acción 249) y de servidores vs activos de información vs backups (acción No. 252). Adicionalmente, definir un responsable quien realice esta labor periódicamente y así garantizar su permanencia en el tiempo.

Oportunidad de Mejora No. 5

Es conveniente realizar nuevamente capacitación a los funcionarios de la mesa se servicio para reforzar el conocimiento en los requisitos obligatorios cuando se reciben casos de soporte de creación/modificación de cuenta de usuario, así como definir lineamientos y controles compensatorios en caso de tener excepciones en el diligenciamiento del formato FT1000 debido a la circunstancia actual de Teletrabajo.

6. Mapa de Riesgos y Controles en el Proceso

Se evidenció que el Mapa de Riesgos del proceso publicado en el SIG con fecha abril 2021, se encontraba desactualizado y el mismo fue ajustado y publicado en el mes de septiembre posterior a la realización de las pruebas de auditoría ejecutadas por esta Oficina de Control, en cumplimiento a los planes de mejoramiento No. 369 y 807.

Oportunidad de Mejora No. 6

No se evidenciaron soportes que den cuenta del seguimiento periódico que se realiza sobre los controles definidos en los procesos, específicamente para el procedimiento PR101 - Gestión de Incidentes y requerimientos tecnológicos, así:

No. Control	Periodo monitoreo sin evidencia
3	enero a abril 2021
5	enero a abril 2021
6	enero a abril 2021
7	enero a abril 2021
8	enero a abril 2021
9	septiembre – diciembre 2020 enero a abril 2021
12	septiembre – diciembre 2020

Solicitados los soportes del monitoreo realizado a los controles definidos en los mapas de riesgo, más no un monitoreo periódico que se realice desde la OTIC para concluir sobre la efectividad de los mismos y la materialización o no de los riesgos.

Por ejemplo, para el control PC#3 del procedimiento PR-104 se cuenta con soportes de algunos mantenimientos realizados, sin embargo, no se evidencia relación entre el cronograma de mantenimiento planeado vs su ejecución, que permita determinar el cumplimiento en frecuencia y en fechas, tal como se indica en la descripción del control.

Por lo anteriormente expuesto, se considera importante que en instancia del subcomité de autocontrol o las actividades cotidianas de seguimiento al proceso, es fundamental evaluar periódicamente la efectividad de los controles implementados para detectar oportunamente las debilidades en su aplicación que pueden permitir la materialización de los riesgos identificados, entre otros como: inoportunidad en la ejecución de los mantenimientos preventivos de los equipos de cómputo, demora en la atención de requerimientos o sin cumplir con los requisitos establecidos en la guía respectiva.

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, definieron acciones de mejora dirigidas a subsanar y prevenir las observaciones identificadas como gestionar las oportunidades de mejora, 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 y 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