INFORME EJECUTIVO

Auditoría de Gestión - Procedimiento Gestión de Incidentes, Requerimientos y Problemas Tecnológicos PR-101

PERIODO DE EJECUCION

Entre el 4 y el 30 de septiembre de 2023, se realizó auditoría de gestión al Procedimiento Gestión de incidentes, requerimientos y problemas tecnológicos, de acuerdo con lo aprobado en el Plan Anual de Auditoría para el 2023.

OBJETIVO GENERAL

Establecer la adecuada aplicación y efectividad de los controles claves definidos en las guías que conforman el procedimiento PR-101 Gestión de Incidentes, Requerimientos y Problemas Tecnológicos, cuyo objetivo es: "*Gestionar las solicitudes de apoyo a los usuarios de las diferentes dependencias de la Secretaria General con el fin de atender y/o solucionar incidentes y requerimientos presentados a nivel de recursos informáticos: hardware, software, seguridad informática y comunicaciones de voz y datos. Adicionalmente analizar y determinar la causa raíz de los problemas tecnológicos proponiendo soluciones permanentes o temporales que sirvan de soporte al proceso de Gestión de Incidentes tecnológicos con el fin de prestar un mejor servicio*"

ALCANCE

Verificar la adecuada aplicación de controles establecidos por la OTIC, según directrices y lineamientos señalados en los siguientes documentos del Sistema Integrado de Gestión, para el periodo de evaluación comprendido entre el 1 de septiembre de 2022 y el 31 agosto de 2023:

- Guía Sistema de Gestión de Servicios (GS-044) V8
- Guía Incidentes de Seguridad (GS-042) V4

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 se aplicaron las técnicas de auditoría internacionalmente aceptadas tales como indagación, observación, inspección y comprobación selectiva a través de muestreo, entre otros.

De acuerdo con la población, para cada prueba se genera la muestra aleatoria objeto de evaluación con el P/T del Excel respectivo para el periodo de evaluación definido.

MARCO NORMATIVO:

1. Procedimientos y Guías SIG:

   - Caracterización del Proceso Gestión de servicios administrativos y tecnológicos (4233100-CR-033) V10
   - Gestión de Incidentes, Requerimientos y Problemas Tecnológicos (2213200-PR-101) V14
   - Guía Sistema de Gestión de Servicios (4204000-GS-044) V8
   - Guía de gestión de incidentes de seguridad, privacidad y seguridad digital y vulnerabilidades (4204000-GS-042) V4

2. Manual de Políticas y Controles de Seguridad y Privacidad de la Información y Políticas de TI (4204000-MA-031) V5

   - Numeral 10.4.8.12 Gestión de Vulnerabilidades Técnicas
   - Numeral 10.4.12 Gestión de Incidentes de Seguridad de la Información

3. ISO 27001:2013:

   - Numeral 7.5. Información Documentada
   - Anexo A - Objetivos de Control y Controles de Referencia: A.12.6 Gestión de la Vulnerabilidad Técnica, A.16 Gestión de incidentes y mejoras en la seguridad de la información

CONCLUSION

Como resultado de la evaluación de auditoría realizada al procedimiento de Gestión de incidentes, requerimientos y problemas tecnológicos, para el periodo objeto de evaluación comprendido entre el 1 de septiembre 2022 y el 31 de agosto 2023, se estableció que en términos generales se viene cumpliendo con los lineamientos definidos en las guías contentivas del proceso y se ajustan a las necesidades de la entidad.

Se encontró que, a través de los lineamientos dados en las guías evaluadas (GS042 - Guía Sistema de Gestión de Servicios y Guía Incidentes de Seguridad y GS044 - Guía de gestión de incidentes de seguridad, privacidad y seguridad digital y vulnerabilidades), se está dando cumplimiento en su mayoría a lo allí establecido, resaltando los siguientes aspectos:

- El documento del procedimiento PR 101 y las guías GS-044 y GS-042, se encuentran vigentes y publicados en el nuevo aplicativo Daruma.

- En la matriz de riesgos de la entidad, se observó que se tiene identificado el riesgo *"Posibilidad de afectación reputacional por baja disponibilidad de los servicios tecnológicos, debido a errores (Fallas o Deficiencias) en la administración y gestión de los recursos de infraestructura tecnológica".* , para el cual se han definido controles preventivos y detectivos definidos en el procedimiento Gestión de incidentes, requerimientos y problemas tecnológicos (PR-101)- y en la Guía Sistema de Gestión de Servicios 2211700-GS-044.

- A través de la Mesa de Servicios de Tecnología se da soporte para todo lo relacionado con temas tecnológicos dejando registro y trazabilidad desde la apertura hasta el cierre de los casos en la herramienta GLPI diseñada para tal fin. Estos casos se atienden cumpliendo con unos ANS (Acuerdos de Niveles de Servicio) claramente diseñados y establecidos como parte del procedimiento.

- Se cuenta con un Plan de Seguridad y Privacidad de la Información vigencia 2023 debidamente aprobado por el Comité Institucional de Gestión y Desempeño y, se realizan análisis de vulnerabilidades técnicas a los servidores y sistemas de información, de acuerdo con un cronograma establecido para la vigencia.

Sin perjuicio de lo anterior, se identificó una (1) observación, siete (7) oportunidades de mejora y se formula recomendación que al ser gestionadas propenderán por fortalecer y mejorar la efectividad de los controles y la dinámica de la operación del procedimiento auditado. A continuación, se relaciona la observación identificada y las situaciones objeto de mejora:

Observación:

- Se observó que los tiempos de atención de los casos de soporte atendidos en la Mesa de Servicio GLPI, superan los tiempos establecidos en los Acuerdos de Niveles de Servicio para su solución, al igual que casos que superaron los dos (2) días establecidos para el cierre posterior a la solución que se realiza de manera semanal (cierre mayor a 7 días), según lo definido en el control No. 9 – Aprobar el cierre de la solicitud del procedimiento PR-101 Gestión de incidentes, requerimientos y problemas tecnológicos.

  Recomendación

  En tal sentido, es importante 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 oportunamente 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.

Oportunidades de Mejora:

- La guía GS-042 para la gestión de incidentes de seguridad, privacidad y seguridad digital y vulnerabilidades, se encuentra asociada al procedimiento 4204000-PR-187-Activos de información, en el cual la guía GS-042 únicamente está como documento referenciado pero no como guía de aplicación como si ocurre en el procedimiento PR-101 Gestión de incidentes, requerimientos y problemas tecnológicos.

  El documento FT-006 Acta Chequeo de Inventario préstamo sala de capacitación Archivo de Bogotá, no se encuentra publicado en Daruma. Adicionalmente, se evidenciaron documentos de fechas antiguas (2010, 2013 y 2015).

En tal sentido, es importante revisar y actualizar la documentación en el Sistema de Gestión Daruma para los procedimientos PR-101 Gestión de incidentes, requerimientos y problemas tecnológicos y PR-187 Activos de Información, en lo relacionado a la guía GS-042, así como eliminar de la guía el formato FT-006 en caso de que no se esté utilizando o incluirlo en el aplicativo Daruma.

Asimismo, se recomienda realizar revisión periódica de toda la documentación asociada al procedimiento evaluado con el fin de mantenerla debidamente actualizada, especialmente para asegurar que los documentos antiguos siguen vigentes y aplicándose en la dinámica de la operación.

- Como resultado del seguimiento realizado a los planes de mejoramiento de auditorías de vigencias 2021 y 2022, se encontró que dos (2) acciones fueron efectivas y dos (2) acciones no efectivas. En consecuencia, es necesario fortalecer el proceso de autocontrol y el seguimiento a la efectividad de los controles, para que las medidas correctivas implementadas se mantengan en el tiempo y se detecten oportunamente las desviaciones en la aplicación de los controles y el desempeño del procedimiento que puedan ocurrir por la degradación de los controles.

- Dos (2) categorías definidas para la tipificación de los casos de soporte que se atienden en la Mesa de Servicio GLPI, no tienen definidos ANS (Acuerdos de Nivel de Servicio), seis (6) no tienen su equivalencia en la Guía Sistema de Gestión de Servicios GS-044 y catorce (14) descritos en la Guía no tienen un ANS asignado para su atención. De igual forma, no se observaron categorías definidas en GLPI para la ejecución de análisis de vulnerabilidades tecnológicas.

  Para estas situaciones, es importante alinear las categorías de atención de los casos de soporte GLPI que están parametrizadas en la herramienta GLPI con las definidas en la guía GS-044; así como, definir tiempos de atención (ANS) para las categorías que aún no cuentan con un acuerdo de nivel de servicio establecido.

- Se evidenciaron tres (3) de una muestra de nueve (9) casos de soporte en estado “En espera y No resueltos” que no cuentan con la documentación o reporte al usuario sobre las razones de la no solución del caso. Adicionalmente, se evidenció que los casos asignados a otras dependencias diferentes a la OTIC no cuentan con un control de seguimiento y monitoreo que permita identificar de manera oportuna demoras en la atención de los casos de soporte asignados.

  Por estas situaciones encontradas, es importante 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.

- El 100% de la muestra de los casos (11) de eventos/incidentes de Seguridad Informática fueron catalogados con prioridad “mediana”, sin evidenciar una catalogación diferente de prioridad como lo establece la guía GS-042 en el numeral 7.3.2 Tiempos de respuesta; y el 27% (3 casos) tuvieron un tiempo de respuesta superior al ANS establecido.

De otra parte, se observó que en la guía GS-042 no existe diferenciación de tareas y/o documentación a llevar a cabo cuando el caso de soporte corresponde a un evento o a un incidente de seguridad.

Si bien las diecisiete (17) categorías clasificadas en GLPI como “Seguridad Informática” tienen asignado un ANS, los mismos difieren de lo definido en el numeral 7.3.2 – Tiempos de respuesta de la guía GS-042.

En consecuencia, es necesario ajustar la guía GS042 para atender los casos de soporte de seguridad informática según lo definido en el numeral 7.3.2, revisar y ajustar el diseño del control de los ANS con el fin de alinear los tiempos de atención según lo definido en la guía GS-042.

- Para una muestra de cinco (5) Sistemas de Información críticos, se observó que los servidores que soportan uno (1) de ellos (Portal Secretaría General Producción – SECGEN) no ha sido objeto de análisis de vulnerabilidad debido a que la herramienta actual con la que se realiza la actividad no permite realizar el escaneo desde el exterior.

  Es necesario revisar y asegurar que los servidores que soportan la aplicación y base de datos de los Sistemas Críticos de la entidad sean objeto de análisis de vulnerabilidades periódicamente (mínimo 2 veces al año) y asegurar que se realice la remediación de las vulnerabilidades encontradas.

Recomendación

- Para una muestra de nueve (9) casos de soporte clasificados, se observaron tres (3) clasificados en una categoría diferente a la que le correspondía según la descripción del caso, uno (1) sin formato FT-1000, uno (1) sin registro de aprobación del cierre. De otra parte, se observaron 65 de 228 casos de soporte correspondientes a eventos de seguridad que no se encuentran clasificados en las categorías de Seguridad Informática.

  Por lo anterior, es importante identificar las causas asociadas a las situaciones aquí presentadas y reforzar la capacitación de los colaboradores que atienden los casos de soporte y que realizan la clasificación y cierre de los soportes GLPI.

OBSERVACIONES, OPORTUNIDADES DE MEJORA Y RECOMENDACIONES PRODUCTO DE LAS PRUEBAS PRACTICADAS

Para el desarrollo de la evaluación de los controles claves y el cumplimiento de lineamientos establecidos en los documentos contentivos del procedimiento Gestión de incidentes, requerimientos y problemas tecnológicos, en lo que respecta a la guía del Sistema de Gestión de Servicios y la guía de gestión de incidentes de seguridad, privacidad y seguridad digital y vulnerabilidades, se realizaron verificaciones de informes de mantenimiento y pruebas en línea relacionadas con la atención oportuna y solución de los casos de soporte recibidos en la mesa de servicio, asociados a casos tecnológicos y de incidentes de seguridad de la información.

A continuación, se describen los principales aspectos identificados como observaciones, oportunidades de mejora y las recomendaciones formuladas como resultado de las pruebas practicadas:

1. Procedimiento PR-101 - Gestión de Incidentes, Requerimientos y Problemas Tecnológicos

Oportunidad de Mejora No. 1 – Actualización y publicación de Normatividad del Proceso

Se observó que las dos (2) guías evaluadas en este proceso auditor y los documentos relacionados se encuentran vigentes y debidamente publicados en la herramienta Daruma con fechas de actualización entre julio 2022 y enero 2023. El formato 2211600-FT-006 - Acta Chequeo de Inventario préstamo sala de capacitación Archivo de Bogotá no se encuentra publicado

Se observó que la guía GS-042 V4 - Guía de gestión de incidentes de seguridad, privacidad y seguridad digital y vulnerabilidades, que hace parte de los documentos contentivos del procedimiento evaluado PR-101 gestión de incidentes, requerimientos y problemas tecnológicos - V14, en el Sistema de Gestión Daruma se encuentra asociada al procedimiento 4204000-PR-187-Activos de información, en el cual la guía GS-042 únicamente está como documento referenciado pero no como guía de aplicación como si ocurre en el procedimiento PR-101 Gestión de incidentes, requerimientos y problemas tecnológicos - V14.

Se encontró que el documento 2211600-FT-006 Acta Chequeo de Inventario préstamo sala de capacitación Archivo de Bogotá, aun cuando se menciona en el numeral 6.8 de la Guía GS-044 no se encuentra publicado en Daruma. Asimismo, se evidenciaron documentos de fechas antiguas (2010, 2013 y 2015).

En tal sentido, es importante revisar y actualizar la documentación en el Sistema de Gestión Daruma para los procedimientos PR-101 Gestión de incidentes, requerimientos y problemas tecnológicos y PR-187 Activos de Información, en lo relacionado a la guía GS-042, así como eliminar de la guía el formato FT-006 en caso de que no se esté utilizando o incluirlo en el aplicativo Daruma.

Asimismo, se recomienda realizar revisión periódica de toda la documentación asociada al procedimiento evaluado con el fin de mantenerla debidamente actualizada, especialmente para asegurar que los documentos antiguos siguen vigentes y aplicándose en la dinámica de la operación.

2. Seguimiento Planes de Mejoramiento Establecidos como resultado de la Auditoría Realizada en la Vigencia Anterior

Oportunidad de Mejora No. 2 – Efectividad de los Controles

Revisados los Planes de Mejoramiento generados como resultado de las Auditorías vigencias 2021 y 2022, se observó que para el procedimiento y las guías en evaluación (PR-101, GS-044 y GS-042), acciones de mejora definidas fueron finalizadas y cerradas. Analizada la efectividad de las mismas, se presentaron las siguientes situaciones:

- Dos (2) acciones fueron efectivas de acuerdo con las pruebas de auditoría realizadas, correspondiente a las acciones PA220-093 Acción 368 y PA230-001 Acción 435 asociada a la actualización de la guía GS-044.

- Dos (2) acciones, aunque fueron atendidas en su momento para la implementación de la acción durante la vigencia respectiva, como resultado de las pruebas realizadas en esta auditoría se observó que nuevamente se presentan la situación reportada en vigencias anteriores. Las dos (2) acciones no efectivas son: PA220-042 Acción 157 y Accion_963.

Es necesario fortalecer el proceso de autocontrol y el seguimiento a la efectividad de los controles, para que las medidas correctivas implementadas se mantengan en el tiempo y se detecten oportunamente las desviaciones en la aplicación de los controles y el desempeño del procedimiento que puedan ocurrir por la degradación de los controles.

3. Gestión de Riesgos Incidentes, Requerimientos y Problemas Tecnológicos

Analizado el Mapa de Riesgos Institucional de fecha 30/06/2023, se observa que el procedimiento PR-101 y la Guía GS-044 son los controles preventivos y detectivos definidos para el riesgo No.148 (FT-G005 en Daruma) que dice: "*Posibilidad de afectación reputacional por baja disponibilidad de los servicios tecnológicos, debido a errores (Fallas o Deficiencias) en la administración y gestión de los recursos de infraestructura tecnológica"*.

Por lo tanto, se concluye que se tiene identificado el riesgo del proceso con asociación de los controles definidos en el procedimiento PR-101y la guía GS-044.

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

Oportunidad de Mejora No. 3 – Acuerdos de Nivel de Servicio vs categorización de los casos de soporte

Revisados los casos de soporte GLPI con relación al cumplimiento de los ANS establecidos para las categorías del sistema de gestión de servicios GLPI, según la guía 4204000-GS-044 Guía Sistema de Gestión de Servicios versión 8- numeral 4.1 Objetivos específicos "*Cumplir con los niveles de servicio (ANS) acordados.*", se observaron las siguientes situaciones:

1. En el archivo "Categorías y ANS 30-01-2023.xls", existen catorce (14) grupos con 345 registros, de los cuales dos (2) no tiene asignado tiempo del ANS. Las dos categorías de Protección de Datos Personales sin ANS son: solicitud Asesoría en Gestión Datos Personales y solicitud Aviso de privacidad y autorización de tratamiento.

   De otro lado, al validar los 345 registros de las categorías definidas con ANS vs las categorías definidas en la Guía Sistema de Gestión de Servicios versión 8 (GS-044), se observó que seis (6) no tienen su equivalencia en la guía.

2. Se observó en la Guía Sistema de Gestión de Servicios versión 8, la definición de catorce (14) categorías con 82 subcategorías, de las cuales tres (3) no tienen asignación de ANS en el archivo "Categorías y ANS 30-01-2023.xls".

Las categorías son: Restauración de cintas de seguridad*, Incremento de tamaño de disco de un server, incremento en la RAM en un Server Windows y Cambio de nombre para el teléfono*. De acuerdo con lo informado por la OTIC, las dos (2) categorías marcadas con asterisco (*), fueron deshabilitadas en la herramienta GLPI según el número de servicio 185290; por lo tanto, se confirma la necesidad de actualizar las categorías en la guía GS-044.

3. No se observaron categorías definidas en GLPI para la ejecución de análisis de vulnerabilidades Tecnológicas. Una vez analizada la fuente de información recibida de la OTIC, con los casos registrados en la herramienta para el tema de "Análisis de Vulnerabilidades", se observa que no se tiene definida una categoría adecuada para tipificar este tipo de servicio, puesto que se incluye bajo la categorización genérica de: "INFRAESTRUCTURA > Otros Servicios de Infraestructura".

   De otra parte, en el archivo mencionado, se incluyeron cuatro (4) casos GLPI con Información de casos de vulnerabilidad de Victimas (SISTEMAS DE INFORMACIÓN > Sistema de Información SIVIC > Modificación de Servicios y SISTEMAS DE INFORMACIÓN > Sistema de Información SIVIC > Nuevos Desarrollos (Actualizaciones), esto debido a que la consulta para identificar este tipo de casos de servicio debe realizarse manual por no tener definida una categorización.

Las situaciones mencionadas, generan posibles riesgos de integridad de información, inoportunidad en la atención de los casos de servicio y demoras en la atención y solución de los casos de servicio.

Acciones para adoptar para su mejoramiento

En tal sentido, es importante definir los tiempos de Acuerdos de Niveles de Servicio para las tipologías que aún no lo tienen, con el fin de contar con el criterio de atención en caso de presentarse un requerimiento, así mismo, fortalecer los controles con el fin de asegurar la equivalencia de las categorías definidas en la Guía Sistema de Gestión de Servicios y el archivo de registro de los ANS.

Adicionalmente, si bien los Acuerdos de Nivel de Servicio para la gestión de casos de soporte tecnológico se tienen establecidos en la guía GS-044; se recomienda que la política para la definición y actualización de los ANS haga parte integral de la documentación del procedimiento objeto de auditoría.

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 – Cumplimiento de ANS y oportunidad en la atención de los casos de soporte

Se llevó a cabo seguimiento al cumplimiento de los ANS para la atención de los casos de soporte atendidos por la Mesa de Servicio, acorde con los lineamientos establecidos en la guía GS-044, obteniendo los siguientes resultados:

1. De un total de 33.952 casos reportados, se evaluaron 25.912 (25.767 cerrados y 145 resueltos), de los cuales es evidenció que el 54% (14.118) fueron atendidos dentro de los ANS establecidos, el restante 46% (11.794) excedieron el tiempo de atención de acuerdo con los ANS.

   En atención a la respuesta al informe preliminar, recibida de la OTIC, se adjuntó en el informe final el archivo en Excel con el detalle de los 11.794 casos de soporte que, se identificaron con tiempo de atención mayor a los ANS establecidos.

2. Verificados los 25.767 en estado cerrado, se identificó que el 71% (18.221) fueron cerrados dentro del término establecido y el restante 29% (7.546) registraron el cierre con posterioridad a los dos (2) días establecidos. Situación no acorde con lo definido en el numeral 8.2 Cierre de una solicitud de servicio de la Guía Sistema de Gestión de Servicios GS-044 que dice: "…*recuerde que transcurridos dos (02) días de resuelta su solicitud, se procederá con el cierre de la misma "a satisfacción", si usted no manifiesta lo contrario*" y con lo definido en el control No. 9 – Aprobar el cierre de la solicitud de PR-101 Gestión de incidentes, requerimientos y problemas tecnológicos, que dice: "*El profesional o técnico autorizado por el jefe de la Oficina TIC, semanalmente verifica los casos que han sido resueltos con dos días de anterioridad para proceder con el cierre de la solicitud, conforme la Guía Sistema de Gestión de Servicios 2211700-GS-044".*

   Adicionalmente, para una muestra de nueve (9) casos de soporte identificados bajo esta situación, se solicitó soporte de la verificación semanal realizada para aprobar el cierre de la solicitud (actividad 9 del procedimiento PR-101 que dice: "El profesional o técnico autorizado por el jefe de la Oficina TIC, semanalmente verifica los casos que han sido resueltos con dos días de anterioridad para proceder con el cierre de la solicitud", sin recibir respuesta a la solicitud. Por lo tanto, se concluye que el control de verificación de la actividad 9 – aprobar el cierre de la solicitud no es efectivo.

   Respecto a esta situación, y luego de analizar la respuesta recibida de la OTIC al informe preliminar, se ajusta la prueba de revisión semanal validando cierres posteriores a 7 días (la prueba se había realizado con cierre posterior a 5 días hábiles), ajustando valores y porcentajes; sin embargo, la situación que mostramos en el informe preliminar se mantiene. En el archivo final, se adjuntó archivo Excel con el detalle de los 7.546 casos de soporte que no cumplen con el cierre semanal.

   Recibida la respuesta de a OTIC donde menciona que: "*El procedimiento fue modificado en el 2022 y describe que el cierre de los servicios se realiza semanal para todos los casos cuya fecha de solución sea mayor a dos días de resuelto y se procederá a cambiar el estado de la solicitud a "Cerrado". Por lo anterior no es viable la observación en cuanto al cierre posterior de servicio";* se aclara que la prueba fue realizada teniendo en cuenta la periodicidad semanal para el cierre.

Las dos situaciones mencionadas anteriormente, evidencian un incumplimiento de los ANS establecidos para la atención oportuna de los requerimientos tecnológico, al igual que inoportunidad en el tiempo de dos (2) días definido para el cierre de las solicitudes posterior a su solución, ocasionando una mala imagen sobre el servicio ofrecido por la OTIC en la atención a las demás dependencias.

En tal sentido, es importante 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.

Oportunidad de Mejora No. 4 – Casos de soporte no resueltos

Para una muestra de nueve (9) casos de soporte en estado “En espera y No resueltos”, se observaron tres (3), correspondientes al 33% de la muestra, que no cuentan con la documentación o reporte al usuario sobre las razones de la no solución del caso, incumpliendo lo establecido en la guía GS-044 numeral 8-Solución de una solicitud de Servicio que dice: *“se debe registrar cómo efectivamente se solucionó el servicio, bien sea “resuelto” es decir cumpliendo las expectativas del usuario, o “no resuelto” es decir no se pudo cumplir con el requerimiento”.* Los casos de soporte son: 297332 - SIAB cargue de descripciones, 302241 - Cambiar plantilla notificación GLPI en el árbol SDQS y 303957 - SOLICITUD MANTENIMIENTO DE EDIFICACIONES- ACTIVACION PUERTA PLANOTECA Y ENTRADA ADMINISTRACION.

A partir de la situación presentada con el caso de soporte No. 303957, se evidenció que los casos asignados a otras dependencias diferentes a la OTIC, en este caso a la Dirección Administrativa y Financiera y a la Dirección del Sistema Distrital de Servicio a la Ciudadanía, no cuentan con un control de seguimiento y monitoreo que permita identificar de manera oportuna demoras en la atención de los casos de soporte GLPI asignados, como ocurrió con el caso No. 303957*.

En consecuencia, se recomienda fortalecer los controles de seguimiento para los casos “no resueltos”, con el fin de asegurar que se dé una solución adecuada y oportuna a los usuarios y queden correctamente documentados en la herramienta GLPI.

Igualmente, es necesario que desde las dependencias DAF y DSDSC, se implemente un control de monitoreo similar al que se tiene en la OTIC, que permita identificar cumplimiento de tiempos en la solución de los casos, detectar y corregir la inoportunidad en la atención de los casos de servicio asignados a esas dependencias.

Revisión de la Documentación de la solución de los casos de Soporte

Una vez verificada la documentación del punto de control No 8 del procedimiento 2213200-PR-101 Gestión de incidentes, requerimientos y problemas tecnológicos V 14 "*la Oficina TIC, mensualmente verifica la documentación del 5% de las solicitudes en estado Resuelto,* y para una muestra de cuatro (4) meses del periodo evaluado, se observó que:

- En los cuatro (4) meses se verificó el 5% de los casos según lo establecido en Actividad 8 y el punto de control del procedimiento.
- Se generaron los "INFORME ESTADÍSTICO DE LA GESTIÓN DE INCIDENTES Y REQUERIMIENTOS", para cada uno de los cuatro meses, adicionalmente se evidenció la fuente de datos donde se llevó a cabo el análisis de la información.

- Se generaron las respectivas observaciones y recomendaciones en cada uno de los informes a partir de la revisión efectuada.
- En el caso del informe del mes de octubre de 2022 en el numeral 9 "Auditoría de la documentación" se indica: "*Para el mes de septiembre se tuvieron 1332 servicios en estado cerrados o resueltos...*", por lo cual, se recomienda revisar y efectuar el ajuste al informe con el fin de garantizar que los resultados tengan la trazabilidad frente al período evaluado el cual corresponde al mes de octubre de 2022.

Lo anterior evidenció cumplimiento en la ejecución del control de verificación de la documentación de la solución y, se recomienda fortalecer el control con el fin de asegurar la trazabilidad de la información registrada en los informes respecto el período que se esté evaluando.

Recomendación No. 1 – Clasificación y documentación para la solución de los casos GLPI

Para una muestra de nueve (9) casos de soporte GLPI, se observaron las siguientes situaciones correspondientes al 55% de la muestra evaluada:

1. Tres (3) no se encuentran clasificados correctamente en la categoría correspondiente:
   - El caso 272790 indica en su descripción “Liberar Sesión Sat Colpensiones” y se encuentran clasificado como gestión de usuarios (categoría de “TECNOLOGICO > SAT > Gestion de Usuarios SAT)
   - El caso 299021 su descripción es “PLANO VICTIMAS OP 3663” para la ejecución de un script y se encuentra clasificado como Asistencia Sistema de Información y Capacitación.
   - El caso 277911 su descripción es WALL PAPER PARA INSTALAR: RESULTADOS: EDUCACIÓN – JÓVENES y está categorizado como "INFRAESTRUCTURA > Otros Servicios de Infraestructura".

2. Uno (1) no tiene anexo el formato FT-1000 para asignación de tarjeta de proximidad. Caso GLPI 281815

3. Uno (1) no cuenta con el registro de aprobación del cierre de la solicitud (actividad 9 del procedimiento). Caso GLPI 279687

De igual forma, para 228 casos de soporte analizados y recibidos de la OTIC como eventos/incidentes de seguridad, se identificaron 65 (28,5%) que no se encuentran clasificados en las categorías de Seguridad informática, sino en categorías como:

- ✓ Equipos de Cómputo > Asistencia equipos de cómputo y capacitación.
- ✓ SISTEMAS DE INFORMACIÓN > Asistencia Sistema de Información y Capacitación
- ✓ INFRAESTRUCTURA > Otros Servicios de Infraestructura,
- ✓ INFRAESTRUCTURA > Correo Electrónico > Solicitud Traza de Correo.

Por lo tanto, se recomienda identificar las causas asociadas a las situaciones aquí presentadas y reforzar la capacitación de los colaboradores que atienden los casos de soporte y que realizan la clasificación y cierre de los soportes GLPI.

5. Guía de gestión de incidentes de seguridad, privacidad y seguridad digital y vulnerabilidades (4204000-GS-042)

Oportunidad de Mejora No. 5 – Cumplimiento de ANS y oportunidad en la atención de los casos de soporte de eventos/incidentes de seguridad

Verificado el cumplimiento de los ANS establecidos para la atención de incidentes, en la Guía 4204000-GS-042 Guía de gestión de incidentes de seguridad, privacidad y seguridad digital y vulnerabilidades V4, en el numeral 7.3.2. Tiempos de respuesta, Tabla 3-Niveles de escalamiento eventos/incidentes.

Para una muestra de once (11) eventos/incidentes, se evidenció que:

- El 100% de los casos se catalogaron con nivel de prioridad “Mediana”, lo cual equivale que su atención debe darse en un lapso de 24 a 48 horas; sin evidenciar una catalogación diferente de prioridad como lo establece la guía.

- De la muestra de once (11) casos, el 73% (8) cumplieron con el ANS establecido según el nivel de prioridad “mediana” y el restante 27% (3) casos tuvieron un tiempo de respuesta por encima del ANS establecido.

Oportunidad de Mejora No. 6 – Guía de gestión de incidentes de seguridad, privacidad y seguridad digital y vulnerabilidades

De acuerdo con el objetivo de la guía que indica: “*Gestionar adecuadamente los incidentes y eventos de seguridad de la información*” y partiendo de los eventos/incidentes recibidos por parte de la OTIC, se observaron las siguientes situaciones:

- En la guía no se tiene diferenciación entre evento e incidente, y de acuerdo con lo informado por la OTIC, son tipificaciones de casos diferentes que deben ser atendidos de manera diferencial.

- Para una muestra de once (11) incidentes de seguridad, no se evidenció documentación soporte según lo definido en la guía GS-042, numerales 7.4 y 7.5.1. Al respecto, la OTIC informó que no se cuenta con esta documentación soporte porque durante el periodo evaluado no se han presentado incidentes de seguridad y que la información entregada a la OCI (casos GLPI) como fuente de información para esta auditoría, corresponde a eventos de seguridad y no a incidentes; en consecuencia, no existen soportes para validar el cumplimiento de las actividades detalladas en la guía puesto que no se han presentado incidentes de seguridad.

- Verificadas las categorías diecisiete (17) categorías para los tipos de soporte de “Seguridad Informática” definidas para la atención de los casos GLPI, se observó que el 100% tienen asignados los ANS; sin embargo, teniendo en cuenta el numeral 7.3.2. Tiempos de respuesta de la guía GS-042

Gestión de incidentes de seguridad, privacidad y seguridad digital y vulnerabilidades, estos pueden cambiar de acuerdo con la prioridad asignada, de manera que no es coherente con los ANS generales establecidos para la atención de casos de soporte (guía GS 044 Guía Sistema de Gestión de Servicios).

Acciones para adoptar que reúnen las Oportunidades de Mejora No. 5 y 6

Es necesario fortalecer los controles con el fin de asegurar que los eventos/incidentes de seguridad sean atendidos dentro de los tiempos establecidos según el nivel de prioridad y según lo establecido en la guía GS-042 numeral 7.3.2 Tiempos de Respuesta.

Ajustar la guía GS042, asegurando que los lineamientos allí definidos se dispongan tanto para “eventos” como para “incidentes” de seguridad, diferenciando claramente las actividades y documentación soporte que se requiere según corresponda, y que los lineamientos allí establecidos estén acordes con la dinámica actual de la operación.
Revisar y ajustar el diseño de control de los ANS definidos para la atención de los casos de soporte de la Mesa de servicio con el fin de alienarlos según lo definido en la guía GS-042 Gestión de incidentes de seguridad, privacidad y seguridad digital y vulnerabilidades de incidentes.

Análisis de Vulnerabilidades

Para tres (3) registros de análisis de vulnerabilidades por demanda se observó su adecuada ejecución, dos de ellos para realizar cierre de vulnerabilidades y el otro corresponde al análisis de vulnerabilidades realizado al nuevo sistema de información SAT Web.

Oportunidad de Mejora No. 7 – Servidores críticos vs Análisis de Vulnerabilidades

De una muestra de cinco (5) Sistemas de información, catalogados como críticos en el PL-020 Plan de Contingencia, se observó que se ejecutó el análisis de vulnerabilidades a cuatro (4) de ellos para la vigencia 2023. El Sistema de Información crítico (1) que no ha sido objeto de análisis de vulnerabilidades es el Portal Secretaría General Producción - SECGEN (servidores srvlnxwebapp01, srvlnxwebapp02, srvlnxwebapp03), correspondiente al 20% de la muestra evaluada.

En atención a la respuesta recibida de la OTIC al informe preliminar, se detallan a continuación los sistemas de la muestra evaluada:

De acuerdo con lo informado por la OTIC, este servicio del Portal Secretaria General, no ha sido objeto de análisis de vulnerabilidades debido a que la herramienta Nexpose con la que se realiza la labor no permite realizar el escaneo desde el exterior; de manera que con la nueva herramienta Tennable ya se tiene programado el análisis para el mes de octubre.

Al respecto, es importante revisar y asegurar que los servidores que soportan la aplicación y base de datos de los Sistemas Críticos de la entidad sean objeto de análisis de vulnerabilidades periódicamente (mínimo 2 veces al año) y asegurar que se realice la remediación de las vulnerabilidades encontradas.

Plan de Seguridad de la Información

Se observó que Plan de Seguridad de la Información para la vigencia 2023 fue debidamente socializado y aprobado en el Comité Institucional de Gestión y Desempeño realizado en la fecha 9/05/2023. Asimismo, se evidenció que la Secretaria General y el Jefe de la Oficina Jurídica realizaron observaciones al Plan que en la misma acta se menciona que estas no afectan la aprobación del Plan.

Debido a que en el acta mencionada no se refleja la relación de los participantes en la sesión del Comité de esa fecha, no fue factible confirmar la asistencia de todos los participantes establecidos según Resolución 494 de 2019; no obstante, el acta está debidamente firmada por la Secretaria General y la Jefe de la OAP.

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