INFORME EJECUTIVO

Auditoría de Gestión - Procedimiento Activos de Información PR-187

PERIODO DE EJECUCION

Entre el 5 y el 31 de octubre de 2023, se realizó auditoría de gestión al Procedimiento Activos de Información, de acuerdo con lo aprobado en el Plan Anual de Auditoría para el 2023.

OBJETIVO GENERAL

Establecer la efectividad de los controles claves definidos en las guías que conforman el procedimiento PR-187 Activos de Información, cuyo objetivo es: "*Proporcionar los criterios y respectivas recomendaciones a los dueños y/o responsables de los procesos para identificar y/o actualizar el inventario de activos de información, la respectiva valoración de los riesgos sobre los activos de información identificados y la generación de planes de mejora a los riesgos identificados acorde al apetito de riesgo de la Secretaría General, a fin de verificar y mantener los niveles de protección requeridos y acorde al cumplimiento de la Ley Nacional y Normativa Técnica Colombiana - NTC* " para el periodo comprendido entre el 1 de octubre de 2022 y el 30 septiembre de 2023.

ALCANCE

Verificar la adecuada aplicación de controles establecidos por la OTIC, según directrices y lineamientos señalados en el procedimiento PR-187 Activos de Información y en la guía GS 004 Guía para la gestión y clasificación de activos de información, para el periodo de evaluación comprendido entre el 1 de octubre de 2022 y el 30 septiembre de 2023.

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, revisión de registros 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 Fortalecimiento Institucional (4202000-CR-052) V 01
- Procedimiento Activos de Información (PR-187) V12
- Guía para la Gestión y Clasificación de Activos de Información (GS-004) V11

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

- Numeral 10.4.4 Gestión de Activos
- Numeral 10.4.4.1. Responsabilidad por los activos de información

3. ISO 27001:2013:

- 8. Control Operacional
- 8.1 Planificación y Control Operacional
- 8.2 Valoración de Riesgos de la Seguridad de la Información
- 8.3 Tratamiento de Riesgos de la Seguridad de la Información
- Anexo A:
- A.5.1 Orientación de la Dirección para la Gestión de la Seguridad de la Información
- A.8.2 Clasificación de la Información

CONCLUSION

Como resultado de la evaluación de auditoría realizada al procedimiento de Activos de Información, para el periodo objeto de evaluación comprendido entre el 1 de octubre 2022 y el 30 de septiembre 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 del procedimiento PR-187 Activos de Información y los lineamientos dados en la guía GS004 - Guía para la Gestión y Clasificación de Activos de Información, se está dando cumplimiento en su mayoría a lo allí establecido, resaltando los siguientes aspectos:

- El documento del procedimiento PR-187 Activos de Información y las guías contentivas del procedimiento, se encuentran vigentes y publicados en el nuevo aplicativo Daruma.

- El procedimiento PR-187-Activos de Información y las Guías asociadas no hacen parte de los controles identificados en la matriz de riesgos integral de la entidad. Al respecto, y de acuerdo con lo informado por la OTIC, los riesgos y controles asociados a Activos de Información se soportan en la matriz FT-367- Identificación, Valoración y Planes de Tratamiento a los Activos de Información.

- Referente a la definición de planes de mejoramiento de las dos (2) vigencias anteriores (2021 y 2022) para el procedimiento PR-187-Activos de Información y las guías asociadas, no se generaron planes de acción para las vigencias indicadas. Referente a planes de acción asociados a “Activos de Información”, se implementó y cerró el plan de acción No. PA220-042-09 referente a la inclusión de la Base de Datos del Sistema de Gestión Contractual en la matriz de Activos de Información de la Dirección de Contratación y de la Subdirección Financiera, concluyendo que la misma es efectiva.

- Se encontró que todas las dependencias de la entidad han identificado sus Activos de información y han valorado los riesgos asociados, excepto la Subsecretaria Distrital de Fortalecimiento Institucional que tiene identificados Activos para las áreas que dependen de esta Subsecretaría, pero no han identificado ni valorado Activos propios de la Subsecretaría.

- A través del procedimiento PR-187 Activos de Información y los lineamientos de la Guía GS 004, las dependencias gestionaron sus activos de información y realizaron la valoración de los riesgos e identificación de controles para su mitigación. Como resultado de la labor realizada, se observó que ninguna dependencia generó planes de tratamiento para sus activos de información en las vigencias 2022 y 2023.

- Al corte diciembre 2022, se cuenta con 2.153 Activos de información identificados por 33 dependencias de la Entidad. Observando que algunas dependencias identificaron entre 1 y 50 Activos de Información y otras entre 50 y 100, y algunas cuentan con más de 200 Activos de Información.

Sin perjuicio de lo anterior, se identificó una (1) observación, cuatro (4) oportunidades de mejora y se formulan algunas recomendaciones 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:

- Si bien se observó la participación del funcionario de la Subdirección de Gestión Documental, en la reunión inicial para la actualización de los Activos de Información vigencia 2023, no se contó con su participación en las posteriores reuniones, que diera cuenta del cumplimiento de la actividad 5 del procedimiento que dice: "*Una vez se encuentren programadas las reuniones el gestor documental asignado, el gestor designado por cada dependencia, el Oficial de seguridad de la información y/o oficial de protección de datos personales asistirán para verificar y validar la clasificación de Tablas de Retención Documental de los activos de información.*

  Para una muestra de ocho (8) dependencias, se evidenció que el 87% (7) cuentan con la asociación de las TRD que les aplique a los activos de información, excepto la Subdirección Financiera cuya matriz no cuenta con esta información y en los campos denominados “TABLAS DE RETENCIÓN DOCUMENTAL (versión 3), se diligenció “Sin definir”.

Recomendación

En tal sentido, es importante dar cumplimiento a la actividad No. 5 del procedimiento PR-187, en la ejecución de la función de la Subdirección de Gestión Documental, en lo referente a verificar y validar la clasificación de las TRD de los Activos de Información, y en los casos en que aplique realizar la actualización de las matrices de Activos de Información, como ejemplo citamos: la Subdirección Financiera que tiene “sin definir” las TRD asociadas a los Activos de Información identificados.

Adicionalmente, evaluar la necesidad de contar con la participación del colaborador de Gestión Documental, en todas las sesiones que se realizan con las dependencias o definir su participación puntual verificando las TRD asociadas a los Activos de Información, posterior al trabajo que realiza cada una de las dependencias en la identificación y valoración de sus Activos de Información.

Oportunidades de Mejora:

- Se observó que el documento OT-084 Política de gobierno digital, fue eliminado de la normatividad interna (aplicativo Daruma). Sin embargo, en la guía GS 107 continúa como parte del alcance y se menciona en el numeral 7.2 - Ejecución de los controles de seguridad definidos para la preservación y disponibilidad de la “Información Pública, la igual que, en el procedimiento PR-187 Activos de Información también se encuentra referenciado en la sección 8. Documentos de referencia., Por lo tanto, es importante que la documentación en el Sistema de Gestión Daruma para el procedimiento PR-187 Activos de Información sea revisada y actualizada, al igual que, las guías contentivas del procedimiento.

  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 se encuentra acorde con la dinámica de la operación.

- En el formato FT-1137 Consolidado Identificación, valoración y matriz de Riesgos de los Activos de Información (matriz vigencia 2022), se identificó una diferencia de 37 activos de información que no tienen registro de la valoración correspondiente, al igual que, una diferencia de 35 activos de información que tienen valoración de riesgos sin su respectivo registro en la hoja de identificación de los activos de información. Situaciones que evidencian debilidad de control al llevar a cabo la actividad No.18 del procedimiento PR-187 Activos de Información.

- Para una muestra de controles que mitigan los riesgos asociados a los activos de información, para las tres (3) dependencias de la muestra, se evidenciaron situaciones como:

  - Un control que no está descrito como tal, ni mitiga el riesgo valorado de pérdida de disponibilidad de la información: Activo de información SID207 con el control: software licenciado, de la Subdirección de Imprenta Distrital.

- Activos de información con riesgos identificados, pero sin un control definido para su mitigación: DDDI-011 Oficios y DDDI-012 Correos electrónicos enviados a las entidades distritales u otras instancias externas.
- Frecuencia semanal para el control de acceso únicamente a personal autorizado, entendiendo que el control de accesos se realiza por demanda y los usuarios, se depuran con una periodicidad mayor a una semana. Los activos son STDI-093, STDI 099 y STDI 100.
- Un control definido como documentación que se encuentra registrada en SECOPII; sin embargo, al ser un "acta" no es un activo que haga parte de los documentos que se cargan en SECOPII de los contratos: DCMPR-002 Acta del subcomité de autocontrol.

Es importante que, desde la OTIC se realicen sesiones de capacitación y revisión con las diferentes dependencias, con el objetivo de evaluar y actualizar los controles definidos para la mitigación de los riesgos asociados a los Activos de Información en lo referente a la descripción del control, frecuencia y evidencia de su aplicación y de ser necesario actualizar y ajustar la matriz consolidada de Activos de Información, que se está trabajando para su publicación con vigencia 2023.

Recomendaciones:

- Revisar y ajustar la funcionalidad de "previsualización" en la página web cuando se consulta el Inventario de Activos de Información, con el fin de asegurar que la información se encuentra disponible para su consulta, puesto que al verificar el contenido de la publicación, se observaron dos bases de datos Excel, para las cuales se han dispuesto las opciones de previsualización y descarga; y al efectuar la consulta por la opción de previsualización, se evidenció que en la consulta de ambos archivos se genera el mensaje "Esta vista de recurso no está disponible al momento".

- Es necesario realizar la revisión de los lineamientos establecidos en las guías GS-004 - Guía para la gestión y clasificación de activos de información y GS-096 - Guía metodológica, para la gestión de riesgos de seguridad digital, con el fin de ajustar la normatividad acorde con la operatividad actual del procedimiento, así como tener en cuenta esta situación para corregir como parte del proceso de revisión y ajuste anual que se está haciendo a las Matrices de Activos de Información de la Entidad. Adicionalmente, evaluar los criterios establecidos para la generación de Planes de Tratamiento con el fin de asegurar que los Activos están siendo valorados y tratados de forma adecuada.

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 Activos de Información, se realizaron verificaciones de la normatividad, la actualización de la matriz de Activos de Información por las Dependencias de la Entidad, su publicación en la página Web y, la aplicación de controles para una muestra de dependencias.

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

1. Normatividad del procedimiento PR-187 – Activos de Información

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

Se observó que el procedimiento cuenta con tres (3) guías, un (1) instructivo, tres (3) formatos y un (1) documento denominado "Otro Documento", documentos que se encuentran vigentes y debidamente publicados en la herramienta Daruma con fechas de actualización entre julio 2022 y enero 2023. Los principales documentos identificados como parte del proceso corresponden a: PR-187 Procedimiento Activos de Información, GS004 Guía de Inventario y clasificación de activos de información, GS107 Guía para el manejo de activos y requerimientos de seguridad para los activos de información, GS096 Guía Metodológica para la Gestión de Riesgos de Seguridad Digital, entre otros.

Se observó que el procedimiento PR-187 Activos de Información - V12, se encuentra vigente desde el 05 de enero 2023, hace parte del proceso: "Fortalecimiento Institucional", y cuenta con tres (3) guías para su aplicación, y que todos los documentos contentivos del procedimiento, tienen fechas actualizadas desde abril 2022 hasta junio 2023.

Se encontró que el documento OT-084 Política de gobierno digital, fue eliminado de la normatividad interna (aplicativo Daruma). Sin embargo, en la guía GS 107 continúa como parte del alcance y se menciona en el numeral 7.2 - Ejecución de los controles de seguridad definidos para la preservación y disponibilidad de la "Información Pública, la igual que en el procedimiento PR-187 Activos de Información también se encuentra referenciado en la sección 8. Documentos de referencia.

En tal sentido, es importante revisar y actualizar la documentación en el Sistema de Gestión Daruma para el procedimiento PR-187 Activos de Información sea revisado y actualizado, al igual que las guías contentivas del procedimiento.

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 se encuentra acorde con la dinámica de la operación.

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

Revisados los Planes de Mejoramiento generados como resultado de las Auditorías vigencias 2021 y 2022, se observó que para el procedimiento (PR-187) y las guías en evaluación (GS-004 y GS-107), no existen acciones de mejora.

Se consultaron los planes de acción relacionados con Activos de Información, observando que para la vigencia 2022 se trabajó y cerró el plan de acción No.PA220-042-09 "Revisar a partir de las orientaciones metodológicas de la OTIC, los ajustes que se requieran a la matriz de activos de información específicamente a los asociados al Sistema de Gestión Contractual" correspondiente a la oportunidad de mejora que dice "…*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".

Una vez analizada la efectividad de la acción mencionada (PA220-042-09), se observó que la Base de Datos del SGC se encuentra identificada como Activo de Información en la matriz 2022 de la Dirección de Contratación y en la matriz 2023 de la DC y de la SF, por lo que se concluye la acción de mejora implementada como efectiva. La acción de mejora es la No. PA220-042-09 de la vigencia 2022 que dice: "Accion_1251 Revisar a partir de las orientaciones metodológicas de la OTIC, los ajustes que se requieran a la matriz de activos de información específicamente a los asociados al Sistema de Gestión Contractual."

3. Gestión de Riesgos Activos de Información – Matriz Vigencia 2022

Analizado el Mapa de Riesgos Institucional de fecha 30/06/2023, se observó que el procedimiento PR-187 y las guías asociadas no hacen parte de los controles identificados en la matriz de riesgos integral de la entidad. De acuerdo con lo informado por la OTIC, los riesgos y controles asociados a Activos de Información se soportan en la matriz FT-367- Identificación, Valoración y Planes de Tratamiento a los Activos de Información.

Tomando en consideración lo indicado por la OTIC, sobre el lineamiento de valoración de riesgos e identificación de controles asociados a los Activos de Información, y una vez analizado el formato FT-1137 Consolidado identificación, valoración y matriz de riesgos de los activos de información (matriz vigencia 2022), se obtuvieron los siguientes resultados:

Valoración de Riesgos de los Activos de Información

Oportunidad de Mejora No. 2 – Diferencia de Activos de Información entre la identificación de estos y los registros de los Activos en la matriz de Valoración de Riesgos

Se observó que en el formato "424000-FT-1137 Consolidado Identificación, Valoración Matriz de Riesgos de los Activos de Información" (matriz vigencia 2022), en la hoja "Consolidado Activos" se registraron 2.153 activos de información, de los cuales al verificarlos con el registro de la hoja "Consolidado valoración riesgos", se evidenció que cruzan 2.116 activos, correspondiente al 98%, identificando una diferencia de 37 activos de información que no tienen registro de la valoración correspondiente. Algunos ejemplos de activos de información bajo esta situación son: JG-002, DDCS-001, SSA-221, SF-253, DAF-550, SF-753, SGD760, entre otros.

De igual forma, al cruzar los registros de la hoja "Consolidado valoración riesgos" con la hoja "Consolidado Activos", se evidenció que 35 activos de información tienen valoración de riesgos, sin embargo, no se observó su respectivo registro en el consolidado de activos de información. Citamos algunos ejemplos de activos de información bajo esta situación son: SC-221, SSA.253, DTH-531, SF-552, DAF-612, entre otros.

Las situaciones anteriormente descritas, evidencian debilidad de control al llevar a cabo la actividad No.18 del procedimiento PR-187 Activos de Información, que dice: "*Consolidar información sobre activos de información, valoración de riesgos y planes de tratamiento e Información Pública, Pública Clasificada y*

Pública Reservada", así como falta de integridad de la información en el consolidado de los activos de información y la valoración de los riesgos que son publicados en el botón de transparencia y datos abiertos de la entidad.

Lo anterior, no está acorde con lo establecido en:

- El Procedimiento PR-187 Activos de información, Actividad No. 18 – Consolidar información sobre activos de información, valoración de riesgos y planes de tratamiento e Información Pública, Pública Clasificada y Pública Reservada.
- Guía Riesgos Seguridad GS-096 numeral 6, Valoración de riesgos sobre los activos de información.
- MA-031 Manual de Políticas y controles de Seguridad y privacidad de la Información y políticas de TI, numeral 10.4.4.1. Responsabilidad por los activos de información.
- NTC ISO 9001:2015 numeral 7.5.3.2. literal d) "conservación y disposición." 7.5.3.1 Control de la información documentada a) esté disponible y sea idónea para su uso, donde y cuando se necesite".

En consecuencia, y de acuerdo con lo informado por la OTIC en respuesta al informe preliminar, la información se tendrá en cuenta para ajustar en el nuevo archivo consolidado que se está trabajando actualmente para que todos los activos cuenten con sus respectivos riesgos asociados.

Identificación de controles existentes para mitigación del riesgo identificado y asociado al activo de información

Oportunidad de Mejora No.3 – Debilidades en la definición y aplicación de los controles para la mitigación de los riesgos asociados a los Activos de Información

Para una muestra de cuatro (4) dependencias, se evaluó la definición y aplicación de controles para una muestra de los activos de información existentes en la matriz respectiva para la vigencia 2022, encontrando las siguientes situaciones:

Subdirección de Imprenta Distrital

Para una muestra de ocho (8) activos de información, se evidenció lo siguiente:

- ✓ Los activos SID-164 y SID190 cuentan con el esquema de backup diario, semanal y mensual programado por la OTIC para el servidor de base de datos del Sistema de Información del Registro Distrital.
- ✓ El backup para el activo SID-165 y SID-172 lo realiza el proveedor del aplicativo EMLAZE ERP.
- ✓ Conservación del activo SID-168 Cronograma de Mantenimiento y SID-206 Piezas gráficas y audiovisuales de la dependencia, en el equipo del funcionario responsable y en One-drive (por 10 años).
- ✓ Control de acceso físico para resguardo del activo SID-170 Certificado de calibración.

- ✓ Para el activo SID-207 Aplicativos de diseño Suite Adobe se recomienda revisar la descripción del control, porque el software licenciado no es un control para mitigar el riesgo pérdida de disponibilidad de la información (definido en la valoración de riesgos).

Dirección Distrital de Desarrollo Institucional

Para una muestra de cinco (5) activos de información, se evidenció lo siguiente:

- No hay control definido para los riesgos identificados de Pérdida de Disponibilidad y de Integridad de la Información valorados para los Activos de Información DDDI-011 Oficios y DDDI-012 Correos electrónicos enviados a las entidades distritales u otras instancias externas.
- Para los Activos de Información DDDI-016, DDDI-021 y DDDI-029 se evidenció la existencia de control de acceso para la carpeta compartida en One-Drive.

Subdirección Técnica de Desarrollo Institucional

Para tres activos de información, se recomienda revisar la frecuencia definida porque el control de accesos corresponde a cada vez que se requiere un nuevo acceso y a la depuración que se realice con una periodicidad establecida y en la matriz se tiene definida frecuencia de una (1) semana. Los activos de información bajo está circunstancia son: STDI-093, STDI-099 y STDI-100.

Dirección de Contratación

Evaluados nueve (9) activos de información de la Dependencia, se observó que:

- Para el activo DCMPR-002 Acta del Subcomité de autocontrol, se recomienda revisar este control porque las actas del subcomité de autocontrol no se cargan en SECOPII. Aunque este activo fue ajustado en la matriz vigencia 2023, es necesario revisarlo a la luz del nuevo activo de información que corresponde a “ACTAS”.

- Para siete (7) Activos de información, se recomienda revisar en conjunto con la OTIC, la forma de gestionar los controles que son administrados por un tercero, como es el caso de los documentos que se registran en SECOPII, como por ejm. los activos: DSMPR-032, DSMPR-050, DSMPR-069, DSMPR-152, DSMPR-159, DSMPR-196 y DSMPR-197.

- El Activo de Información DCMPR-213 Base de datos Sistema de Gestión Contractual, cuentan con el esquema de backup diario, semanal y mensual programado por la OTIC

Se hace recomendable que, desde la OTIC, se lleven a cabo sesiones periódicas de capacitación y revisión con las diferentes dependencias, con el objetivo de evaluar y actualizar los controles definidos para la mitigación de los riesgos asociados a los Activos de Información en lo referente a la descripción del control, frecuencia y evidencia de su aplicación.

En respuesta recibida de la OTIC al informe preliminar, se informó que el proceso de actualización de las matrices se realiza de manera anual o en caso que se llegue a materializar un riesgo, razón por la cual esta Oficina de Control sugiere evaluar la necesidad de realizar ajustes anticipadamente para dar oportunidad a la acción de mejora o generar un plan de acción específico de revisión y actualización de controles para llevar a cabo durante el proceso de actualización de los activos que se realice en el año 2024.

Definición de los planes de tratamiento de Riesgos de Seguridad Digital, Seguridad y Privacidad de la Información

La Guía Riesgos de Seguridad GS-096 establece en el numeral 6.7. Planes de tratamiento de Riesgos de Seguridad Digital, Seguridad y Privacidad de la Información, que: "*Es importante tener en cuenta que todos los riesgos con evaluación después de controles que se encuentren ubicados en las zonas: "Catastrófico" o "Mayor" deberán contar con definición de un respectivo plan de tratamiento que permita mitigar la probabilidad de ocurrencia e impacto asociados al activo o grupo de activos de información.*", una vez revisados los Planes de Tratamiento detallados en el "Consolidado valoración riesgos" del formato FT-1137 (matriz vigencia 2022), se observaron 2.151 registros de valoración de riesgos de activos de información así: 635 Riesgo Menor, 1.498 Riesgo Bajo, 14 Riesgo Moderado y 4 Riesgo Alto.

Lo anterior, evidencia que luego de la aplicación de los controles definidos, ningún activo de información se ubica dentro de las zonas catastrófico o mayor, por lo cual, se concluye que no era pertinente la definición de planes de tratamiento.

De otra parte, de acuerdo con la información registrada en la hoja "Consolidado Planes Tratamiento" de la matriz "4204000-FT-1137 Consolidado identificación, valoración y matriz de riesgos de los activos de información.xlsx" (matriz vigencia 2022), se evidenció que para ninguna dependencia se generaron planes de tratamiento para el año 2022. Asimismo, de acuerdo con lo informado por la OTIC para el año 2023 tampoco se generaron planes de tratamiento para las Dependencias.

Recomendación No. 1 – Tipificación Planes de Tratamiento

Analizada la tipificación evidenciada para cada Activo de Información en la columna "RESULTADO PARA PLAN DE TRATAMIENTO" de la matriz FT-1137 Consolidado Identificación, valoración y matriz de riesgos de los Activos de Información (matriz vigencia 2022), se observó que se tienen dos clasificaciones así:

1. Generar controles al Activo de Información para proteger su Confidencialidad, Integridad y Disponibilidad del Riesgo.

2. Realizar una revisión anual de los controles definidos.

En consecuencia, la tipificación definida como: "*Generar controles al Activo de Información para proteger su Confidencialidad, Integridad y Disponibilidad del Riesgo*", aunque se entiende que requería una acción no es coherente con la no definición de Planes de Tratamiento o acciones para tratar los riesgos de falta

de confidencialidad, integridad o disponibilidad de la información. De otra parte, no se observa que esta tipificación de los resultados para los planes de tratamiento tenga un lineamiento establecido en la guía GS-004 Guía para la gestión y clasificación de activos de información o en la guía GS-096 - Guía metodológica para la gestión de riesgos de seguridad digital.

Debido a lo anterior, es necesario realizar la revisión de los lineamientos establecidos en las guías 004 - Guía para la gestión y clasificación de activos de información y GS-096 Guía metodológica para la gestión de riesgos de seguridad digital, con el fin de ajustar la normatividad acorde con la operatividad actual del procedimiento, así como tener en cuenta esta situación para corregir como parte del proceso de revisión y ajuste anual que se está haciendo a las Matrices de Activos de Información de la Entidad. Adicionalmente, evaluar los criterios establecidos para la generación de Planes de Tratamiento con el propósito de asegurar que los Activos están siendo valorados y tratados de forma adecuada.

4. Procedimiento PR-187 - Activos de Información

4.1 Definición y aprobación del plan de trabajo

Se evidenció cronograma con las actividades programadas entre el 1 de abril de 2023 y el 31 de diciembre 2023 para dar cumplimiento al proceso de actualización de los Activos de Información por cada una de las dependencias de la entidad. Para la ejecución de las actividades de actualización, se programaron las dependencias por grupos para adelantar las tareas de identificación de activos, valoración de riesgos, planes de tratamiento y entrega final de la matriz a la OTIC entre el 2 de mayo y el 31 octubre de 2023, con cronogramas detallados por cada área. Asimismo, se observó mail de aprobación del plan de trabajo (cronograma) enviado por el jefe de la OTIC con fecha 22/03/2023.

4.2 Distribución de los Activos de Información por Tipo de Activo

Analizado el inventario de Activos de Información corte diciembre 2022, se observó en el formato “424000-FT-1137 Consolidado Identificación, Valoración Matriz de Riesgos de los Activos de Información con un total de 2.153 activos de información, de los cuales el 89% (1.925) corresponden a “Datos/Información”, el 10% (217) se encuentra distribuido en: base de datos (66), software/aplicaciones (61), hardware/infraestructura (55), servicios (24), soportes de información/dispositivos móviles (11), y solo el 0.5% (11) corresponden a Recurso Humano (10) e Instalaciones (1).

Recomendación No. 2 – Dependencia sin Activos de Información Identificados y Valorados

Analizada la matriz de Activos de Información con corte diciembre 2022 (4204000-FT-1137 Consolidado identificación, valoración y matriz de riesgos de los activos de información.xlsx), se observó que treinta y tres (33) dependencias de las treinta y cuatro (34) registradas en el organigrama (97%) identificaron y valoraron los activos de información en el formato “4204000-FT-367 Identificación, Valoración y Planes de Tratamiento a los Activos de Información” para la vigencia 2022; sin contar con el registro de Activos de Información para una (1) dependencia (3%) que es la Subsecretaria Distrital de Fortalecimiento Institucional, ni tampoco se cuenta con soporte de la dependencia con la explicación o justificación referente a la no identificación de sus Activos de Información.

Lo anterior, no está acorde con lo establecido en:

- El procedimiento PR-187 Activos de información, Actividad No. 15 – Remitir documentos activos de informe.

- La Guía para la gestión y clasificación de activos de información GS-004, Numeral 6.1 Generalidades.

- MA-031 Manual de Políticas y controles de Seguridad y privacidad de la Información y políticas de TI, numeral 10.4.4.1. Responsabilidad por los activos de información.

- NTC ISO 9001:2015 numeral 7.5.3.2. literal d) "conservación y disposición." 7.5.3.1 Control de la información documentada a) esté disponible y sea idónea para su uso, donde y cuando se necesite.

Al respecto, se evidenció que el día 20 de octubre 2023 la OTIC envió mail a la SDFI (Subsecretaria Distrital de Fortalecimiento Institucional) como parte de la gestión de actualización de Activos que se viene adelantando para la vigencia 2023, indicando en el mail que: "*…no se encuentran identificados activos directamente de la Subsecretaria sino de las dependencias adscritas... De igual manera y como les indique les remito la información de series descritas en la Tabla de retención documental de la Subsecretaria para que verifiquen si esos activos son responsabilidad de ustedes y actualmente se encuentran en su custodia"*; sin embargo, a la fecha de cierre de esta auditoría no se pudo establecer si la dependencia llevó o no a cabo la gestión respectiva.

Las situaciones mencionadas, generan posibles riesgos de pérdida de información o indisponibilidad de esta por falta de gestión y/o materialización de riesgos debido a la falta de controles para la mitigación de los mismos. Así como, inoportunidad en la identificación y la valoración de los activos de información.

Si bien, es cierto que la OTIC llevó a cabo el seguimiento para la identificación y valoración de los activos de información por parte de esta dependencia para la vigencia 2023, también, es cierto que es necesario fortalecer los controles con el fin de asegurar que estas verificaciones se lleven a cabo con oportunidad con el propósito de asegurar que todas las dependencias lleven a cabo la identificación y valoración correspondientes.

Se recomienda a la SDFI identificar los activos de información propios del área para ser incluidos en la matriz definida para tal fin y realizar la valoración de los riesgos respectiva, en cumplimiento a la actividad No.15 del procedimiento PR-187 Activos de Información. En caso de que la dependencia no maneje Activos de Información propios o no los considere críticos para su inclusión en la matriz, se requiere que, desde la OTIC, como área líder y gestora del procedimiento, se deje como evidencia soporte de la explicación de la SDFI respecto a la no necesidad de incluir sus Activos de Información en la matriz y que se asumen los riesgos de no contar con estos registros y controles para los activos existentes.

En respuesta recibida al informe preliminar, la OTIC informó que la Subsecretaría ya identificó los Activos de Información para la vigencia 2023 y están en proceso de aprobación.

Observación No. 1

Verificada la participación de la Subdirección de Gestión Documental en el proceso de actualización de Activos de Información, que en la actividad 5 del procedimiento PR-187 indica que su tarea es verificar y validar la clasificación de las Tablas de Retención Documental – TRD de los activos identificados por cada dependencia durante la ejecución de las actividades programadas, se evidenciaron los memorandos de solicitud de la OTIC y la respuesta de la Subdirección de Gestión Documental con la asignación del funcionario para el desarrollo de la labor.

Se evidenció que en la reunión inicial del 4 de marzo 2023, se contó con la participación del funcionario de la SGD asignado, sin embargo, no se observó participación posterior de esta área en las reuniones realizadas con las Dependencias para la verificación y validación de la clasificación de las TRD de los Activos de Información de las Dependencias, incumpliendo la actividad 5 del procedimiento que dice: "*Una vez se encuentren programadas las reuniones el gestor documental asignado, el gestor designado por cada dependencia, el Oficial de seguridad de la información y/o oficial de protección de datos personales asistirán para verificar y validar la clasificación de Tablas de Retención Documental de los activos de información.*

Para una muestra de ocho (8) dependencias, se evidenció que el 87% (7) cuentan con la asociación de las TRD que les aplique a los activos de información, excepto la Subdirección Financiera cuya matriz no cuenta con esta información y en los campos denominados “TABLAS DE RETENCIÓN DOCUMENTAL (versión 3), se diligenció “Sin definir”.

Las dos situaciones mencionadas anteriormente, evidencian un incumplimiento del procedimiento y el riesgo de posibles clasificaciones erradas de los Activos de Información en las Tablas de Retención Documental.

Recomendación

Es importante dar cumplimiento con la función de la Subdirección de Gestión documental, en lo referente a la verificación y validación de la clasificación de las TRD de los Activos de Información, ya actualizados por las dependencias para la vigencia 2023, y así evitar situaciones como la identificada para la SF que sus Activos de Información no cuentan con una asociación a las TRD de la Dependencia.

Recomendación No. 3 - Publicación Inventario de los Activos de Información

Se verificó en la URL *https://datosabiertos.bogota.gov.co/organization/secretaria-general-de-la-alcaldia-mayor-de-bogota-d-c*, que la entidad en la sección “Datos Abiertos Bogotá”, ha dispuesto un espacio para “Inventario activos de información 2022” cuya fecha de modificación fue el 7 de diciembre de 2022, y el título de la publicación es “*Contiene el Inventario de Activos de Información de la Secretaría General de la Alcaldía Mayor de Bogotá D.C., con vigencia 2022”.* Así mismo, se permite desde el sitio Web realizar la descarga del Inventario de Activos de Información (archivo Excel “*4204000-ft-1137-consolidado-identificacion-valoracion-y-matriz-de-riesgos-de-los-activos-de-inf*”). No obstante, al verificar el contenido de la publicación, se observaron dos bases de datos Excel, para las cuales se han dispuesto las opciones de previsualización y descarga; y al efectuar la consulta por la opción de previsualización se evidenció que en la consulta de ambos archivos se genera el mensaje “*Esta vista de recurso no está disponible al momento”*.

Por lo anteriormente expuesto, se hace necesario revisar y ajustar la funcionalidad de “previsualización” con el objetivo de asegurar que la información se encuentra disponible para su consulta por medio de las opciones habilitadas en el sitio Web de la Entidad.

De otra parte, se evidenció que los datos publicados, para la vigencia 2022 en la página Web (*4204000 FT-1137-consolidado-identificacion-valoracion-y-matriz-de-riesgos-de-los-activos-de-inf.xls)* son los mismos de la fuente de información recibida de la OTIC y que fue la base fuente utilizada para las pruebas de esta auditoría.

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