RESPONSABLE:
Jaime Hernando Arias Patiño

NOMBRE DE LA AUDITORIA/SERVICIO DE ASEGURAMIENTO
Auditoría al Procedimiento Gestión Incidentes de Seguridad de la Información TIC-PR05 V2

OBJETIVO:
Verificar el cumplimento de las actividades establecidas para gestionar los incidentes de seguridad y privacidad de la información en la Entidad, establecer si se ha mitigado el impacto asociado a la pérdida de la confidencialidad, integridad y disponibilidad de la información en los casos que aplique.

ALCANCE: Se realizará la verificación del cumplimiento de las actividades previstas en el procedimiento Gestión Incidentes de Seguridad de la Información TIC-PR05 V2 en el período comprendido entre el 1 abril de 2023 y el 30 de abril de 2024

CRITERIOS:
Ley 87 de 1993 "Por la cual se establecen normas para el ejercicio de control interno en la entidades y organismos del estado y se dictan otras disposiciones"
Decreto 767 de Gobierno Digital en el capítulo del Modelo de Seguridad y Privacidad de la Información MSPI
Directiva Presidencial 02 de 2022 Disponer de un procedimiento de Gestión de Incidentes de Seguridad Digital
CONPES 3995 Política Nacional de Confianza y Seguridad Digital de julio 1 de 2020
Manual de Políticas de Privacidad y Seguridad de la Información de la entidad
Norma ISO 27001:2013. - Corresponde a uno de los 14 Dominios de esta norma. Norma ISO 27032.- Framework de Ciberseguridad.
Directiva 008 DE 2021 por medio de la cual establecen lineamientos para prevenir conductas irregulares relacionadas con el incumplimiento de los manuales de funciones y competencias laborales y de los manuales de procedimientos institucionales, así como por la perdida, o deterioro, o alteración o uso indebido de bienes, elementos, documentos públicos e información contenida en bases de datos y sistemas de información.
Modelo Integrado de Planeación y Gestión MIPG.
Procedimiento Gestión Incidentes de Seguridad de la Información TIC-PR05 V2
Demás normas y/o jurisprudencia que complementen, modifiquen, deroguen o sustituyan las anteriores.

PROCESO AUDITADO:
Gestión Tecnologías de la Información y las Comunicaciones

SUBDIRECCIÓN/OFICINA/DEPENDENCIA/ÁREA:
Dirección

LÍDER DE PROCESO/DEPENDENCIA:
Paula Ximena Henao Escobar

EQUIPO AUDITOR:
Jaime Hernando Arias Patiño- Jefe de la OCI
María del Carmen Bonilla- Auditora líder

PERIODO DE EJECUCIÓN DE LA AUDITORÍA:
6 de mayo al 5 de julio de 2024

METODOLOGÍA

De conformidad con la Guía de Auditoría para Entidades Públicas expedida por el DAFP, se emplearon los

siguientes procedimientos de auditoría: Consulta, Observación, Inspección y Revisión de evidencia física. Adicionalmente, se empleó la metodología PHVA (Planear, Hacer, Verificar, Actuar)

a) Planear:
- Elaboración del Plan de auditoría y la lista de verificación
- Definición de los objetivos, el alcance y los tiempos de ejecución.
- Preparar la auditoría de campo, papeles de trabajo, investigación documental y procedimental sobre el proceso auditado.

b) Hacer:
- Auditoría de campo a través de entrevista
- Recolección y verificación de la información obtenida de las entrevistas y evidencias documentales.
- Entrega del Informe preliminar de auditoría a los líderes y/o responsables de los procesos auditados.

c) Verificar:
- Análisis de la información, evidencias, y verificación del cumplimiento de acuerdo con lo establecido en los procedimientos, requisitos legales, normas aplicables definidas para la auditoría.
- Mesas de validación de hallazgos donde se presentó el informe preliminar, se aclararon y/o justificaron los hallazgos de no conformidad por parte de los auditores y de los auditados, respectivamente.
- Análisis de las evidencias e información adicional entregada por los auditados en la mesa de validación de hallazgos, y determinar la subsanación de las no conformidades u observaciones.
- Entrega del Informe final de auditoría a los líderes y/o responsables de los procesos auditados.
-

d) Actuar:
- Solicitud del Plan de Mejoramiento de los hallazgos o desviaciones encontrados, en el FOR-GI-04-01 Solicitud de ACPM.

Se inicia al proceso auditor con el oficio I-00643-2024007748-UAECOB Id: 194250 del 6 de mayo de 2024 mediante el cual se cita a la mesa de apertura de auditoría el día 20 de mayo de 2024, a las 9:00 a.m. la cual se oficiará de manera virtual (teams), con la participación de los auditados y el equipo de trabajo que considere pertinente la líder del proceso auditado, la auditora asignada y el Jefe de la Oficina de Control Interno.

Para esta auditoría se contempló el lineamiento establecido mediante el procedimiento Gestión Incidentes de Seguridad de la Información TIC-PR05 V2 del 26 de agosto de 2022 que se encuentra publicado en la página Web de la Entidad.

Se realizó entrevista a los profesionales designados por la líder del proceso Gestión Tecnologías de la Información y las Comunicaciones del cual hace parte el procedimiento auditado, se verificó la eficiencia de la herramienta de Gestión denominada Aranda que apoya al procedimiento evaluado con el fin de mantener la trazabilidad del incidente desde el inicio hasta el fin y tener de esta manera un control de los eventos o incidentes de seguridad de la información que se presentan en la Entidad.

Se revisó la batería de indicadores y el mapa de riesgos del proceso Gestión Tecnologías de la Información y las Comunicaciones con el fin de establecer si se tienen identificados indicadores de gestión y riesgos asociados a las actividades del procedimiento objeto de esta auditoría.

También se examinó el plan anual de adquisiciones vigencia 2024 con el fin de constatar la disposición de recursos financieros para cumplir con el plan de acción propuesto para el proceso evaluado.

SITUACIONES GENERALES

El Decreto 555 de 2011 derogado por el artículo 14 del Decreto Distrital 509 de noviembre de 2023 por medio del cual se modifica la estructura organizacional de la Unidad Administrativa Especial Cuerpo Oficial de Bomberos

establece en el artículo 4º para el despacho del Director General de la Entidad entre otras la siguiente función:

x) Diseñar las estrategias para la debida implementación y el mejoramiento continuo de la gestión estratégica de las tecnologías de la información y las comunicaciones teniendo como base la normativa vigente, con el fin de lograr los objetivos de la Entidad.

Con el fin de dar cumplimiento a esta función la Entidad dispone entre otros del procedimiento Gestión Incidentes de Seguridad de la Información TIC-PR05 V2 del 26 de agosto de 2022

Así las cosas, la Oficina de Control Interno procedió a solicitar las evidencias que dieran cuenta del cumplimiento de las actividades del procedimiento en comento, observando lo siguiente:

1- Fortalezas

- La disposición y diligencia de los profesionales designada por parte de la Dirección para atender la auditoria.
- La herramienta colaborativa de administración de recursos tecnológicos “Aranda” dispuesta por la Entidad que permite tener un control de los incidentes reportados por los usuarios de la UAECOB y realizar seguimiento en tiempo real al estado de la gestión realizada para solucionarlos.

2- <u>Directiva 008 de 2021</u>– Alcaldía Mayor de Bogotá DC

En cuanto a la citada directiva que contempla “Lineamientos para prevenir conductas irregulares relacionadas con el incumplimiento de los manuales de funciones y competencias laborales y de los manuales de procedimientos institucionales, así como por la perdida, o deterioro, o alteración o uso indebido de bienes, elementos, documentos públicos e información contenida en bases de datos y sistemas de información”, se observó en las minutas de los contratos 200-2024 y 225-2024 que corresponden a profesionales que prestan sus servicios en la Dirección específicamente al proceso Gestión Tecnologías de la Información y las Comunicaciones que se incluyó una obligación general relacionada con :

13. Mantener la conservación, custodia, uso adecuado y especial cuidado de los elementos que le sean suministrados por la Entidad y responder pecuniariamente por su deterioro o pérdida y hacer la devolución de los mismos cuando finalice el vínculo contractual con la Entidad

Para las obligaciones específicas incluyeron la siguiente:

11. Guardar la confidencialidad de toda la información que conozca durante la ejecución del contrato.

Lo anterior nos permite deducir que la Entidad ha venido dando cumplimiento a lo establecido en la mencionada Directiva.

3- Mapa de Riesgos

En la caracterización del proceso TIC-CP01 Gestión Tecnologías de la Información y las Comunicaciones, se observa la actividad “Implementar el modelo de seguridad y privacidad de información.” relacionada con el objetivo del procedimiento Gestión Incidentes de Seguridad de la Información TIC-PR05 V2, a esta actividad le identificaron los siguientes riesgos con área de impacto económico y reputacional:

R2-ID-TIC02 Posibilidad de pérdida de la confidencialidad, integridad y disponibilidad de la información Por accesos o cambios no autorizados a la información institucional, así como eventos disruptivos por virus en la red. Debido a la ineficiencia o falta de controles de seguridad de la información y ciberseguridad

R3-ID-TIC-03 Posibilidad de pérdida de credibilidad y afectación económica Por interrupción o falla en la continuidad de la prestación de los servicios debido a Limitaciones en la infraestructura tecnológica o en las competencias del personal o por un ataque cibernético.

De acuerdo con la información suministrada por los profesionales que atendieron la auditoria, en el período evaluado no se han materializado estos riesgos.

Evaluado el mapa de riesgos y verificados los controles establecidos se observa que a pesar de aplicar los controles el nivel del riesgo residual sigue siendo extremo para el riesgo 2 R2 y para el riesgo 3 R3 sigue siendo alto.

Por lo anterior se hace importante recomendar se revise la metodología aplicada para el tratamiento de los riesgos identificados especialmente a la valoración de los controles; conceptualmente un control se define como la medida que permite reducir o mitigar el riesgo, situación que no se ve reflejada en el mapa de riesgos para los eventos evaluados en esta auditoría.

4- Aspectos por mejorar

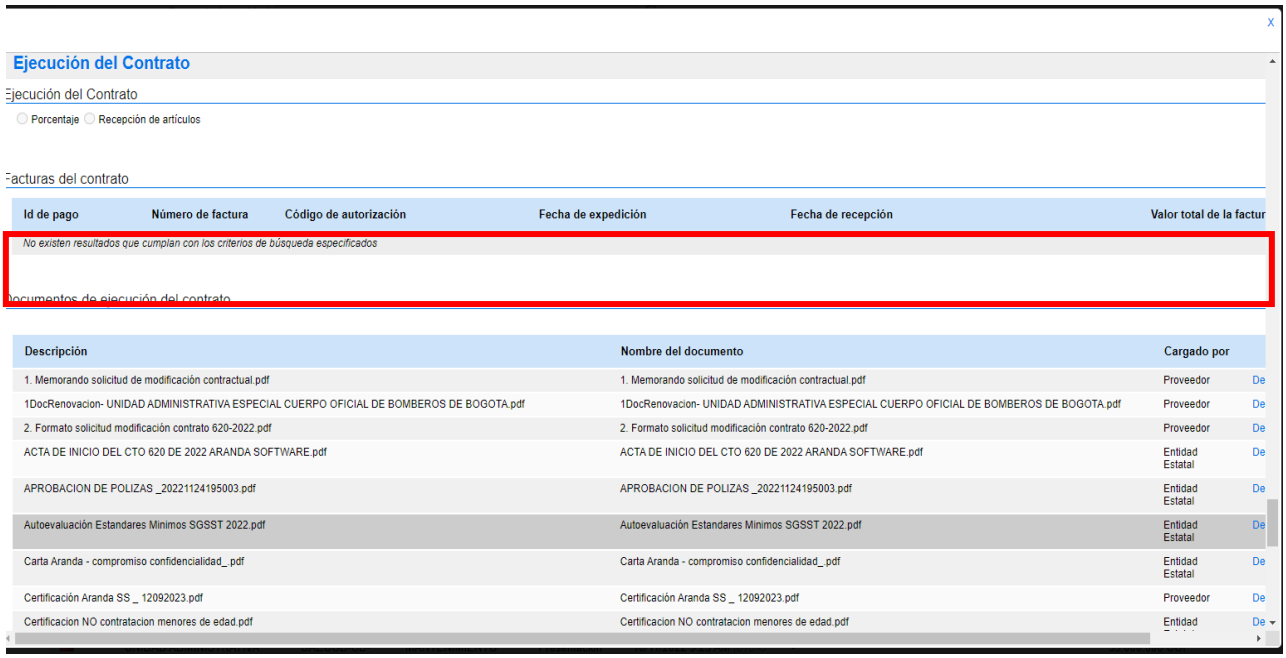
a- Teniendo en consideración que el procedimiento “Gestión Incidentes de Seguridad de la Información TIC-PR05 V2” utiliza la herramienta colaborativa de administración de recursos tecnológicos “Aranda” la cual permite el manejo y seguimiento eficiente de los requerimientos de servicios tecnológicos y la optimización de los tiempos de atención; esta oficina procedió a indagar sobre la procedencia de la herramienta en comento y se estableció que fue adquirida mediante un tercero y que periódicamente se adquieren las actualizaciones de seguridad que contemplan las nuevas funcionalidades que el mercado de herramientas Help Desk ofrece.

Adicionalmente se contrata el soporte especializado ante cualquier falla de la herramienta y ajustes de parametrización que se requieran para brindan la creación de casos acorde a las necesidades y soluciones requeridas.

Teniendo en cuenta lo anterior, se procedió a verificar el contrato 620 del 2022 celebrado para adquirir la prestación de los servicios de mantenimiento, soporte técnico, mejoras y actualizaciones de Aranda utilizado por la UEACOB, las características del contrato son las siguientes:

Valor inicial de contrato	$35.000.000
Plazo inicial de ejecución	9 meses y 24 días
Fecha inicio	25/11/2022
Fecha terminación	20/09/2023
Adición	$10.116.517
Prórroga	4 meses
Terminación Prorroga	20/01/2024

Al verificar en el SECOPII, (junio 14 de 2024) en el ítem de ejecución del contrato-plan de pagos, se evidencia lo siguiente:



Consulta en el SECOP II el 14/06/2024

Teniendo en cuenta lo observado se procedió a indagar en el área financiera de la Entidad si existía giro de recursos para pagar la obligación producto de contrato en comento y nos informan que en la vigencia 2023 se realizó el desembolso correspondiente.

Como se aprecia en la imagen anterior, no se han dispuesto los pagos en la plataforma transaccional SECOP II tal como lo establece el manual de contratación e interventoría, código GJ-MN01 versión 03, numeral 15.6-Funciones o actividades de los supervisores, apoyos a la supervisión y los interventores, en el numeral 15.6.1.6, que describe lo siguiente: *"Vigilar el estado financiero del contrato, con el apoyo del área financiera y dejar constancia en los respectivos informes a su cargo acerca de las operaciones efectuadas con los fondos del contrato en aquellos casos en los que sea necesario, de acuerdo con el objeto pactado".*

Al respecto, cabe mencionar que con ocasión del informe de Auditoría de Contratación Procesos Públicos y Contratación Directa realizado por esta oficina el pasado 04/06/2024, se determinó el hallazgo 4.16 por similares circunstancias; situación que podría ser excepcional, se debe revisar al interior de los equipos de apoyo a la supervisión para evitar reiteraciones, con el riesgo de incurrir en observaciones y/o sanciones por parte de Entes de Control externos, dado el incumplimiento a la normativa dispuesta para ello (artículo 209 de la Constitución Política de Colombia; el literal e, f, g y h del artículo 2 de la Ley 87 de 1993; el Manual de Contratación Supervisión o Interventoría de la Entidad; Ley 1712 de 2014).

Teniendo en cuenta que la Entidad se encuentra formulando el plan de mejoramiento correspondiente, recomendamos realizar un ejercicio acucioso de análisis de causas con el fin de formular acciones de mejora efectivas que permitan mitigar el riesgo que se ha venido materializando recurrentemente.

b- Revisados los documentos que soportan la operativización del procedimiento objeto de esta auditoría se observó que designan responsabilidades al Oficial de Seguridad de la Información, razón por la cual se preguntó al equipo auditado quien ejerce ese rol en la Entidad y nos informan que actualmente no se cuenta con un profesional dedicado a esta labor, que por disposición de la Alta Dirección han designado obligaciones a los ingenieros que hacen parte del equipo de trabajo del proceso de Gestión Tecnologías

de la Información y las Comunicaciones.

El Modelo Integrado de Planeación y Gestión MIPG contempla dimensiones y políticas dentro de las cuáles se destaca la "Política de Seguridad Digital".

Esta política se encuentra consignada en la sección 3.4.2 del MIPG y menciona lo siguiente respecto al rol del Oficial de Seguridad: *"(…) en el Comité Institucional de Gestión y Desempeño se deben articular los esfuerzos, recursos, metodologías y estrategias para asegurar la implementación de la política. Para ello, se debe designar un responsable de Seguridad Digital que también es el responsable de la Seguridad de la Información en la entidad, el cual debe pertenecer a un área que haga parte de la Alta Dirección. Para las entidades cabeza de sector, el Responsable de Seguridad Digital será el enlace sectorial"*.

Considerada la situación expuesta se recomienda revisar la pertinencia de contratar un profesional que asuma este rol de manera dedicada teniendo en cuenta que la seguridad digital cobra mucha importancia ya que, a futuro una vez todas las entidades públicas y también privadas lleguen a un grado de digitalización casi completo y todo se haga a través del entorno digital los riesgos serán mucho mayores.

Adicionalmente se coadyuvaría al cumplimiento de lo establecido en el artículo 228 "Transformación digital e impulso a la ciudad Inteligente" del Acuerdo 927 de 2024 por medio del cual se adopta el plan de desarrollo económico, social, ambiental y de obras públicas del Distrito Capital 2024-2027- "Bogotá Camina Segura".

c- Entre los temas revisados se observó que el software colaborativo Aranda almacena la información en una base de datos (BD) que contiene información relacionada con los incidentes reportados por los usuarios de la Entidad, entre otros campos que alberga la BD se observan los denominados: estado del incidente, fecha de reporte, fecha de solución; se tomaron como muestra cinco incidentes cuya fecha de reporte data del mes de enero y febrero de 2024, se indagó al respecto sobre la solución de estos incidentes teniendo en cuenta el tiempo transcurrido desde la fecha de la creación del caso (3 y 4 meses), el profesional que atendió la auditoria informa que esos caso ya fueron resueltos pero que no se ha cambiado el estado en el campo correspondiente en la BD.

Se verificó dentro de las políticas de operación del procedimiento así como en las actividades y en la guía de servicios TIC si existe alguna que instruya sobre el actuar cuando se tienen los casos resueltos y se constató que adolecen de esta instrucción; por lo anterior se recomienda revisar la pertinencia de incluir dentro de alguno de los documentos citados un lineamiento que establezca la obligatoriedad de diligenciar este campo (estado del incidente), teniendo en cuenta que de la BD en comento se sustrae la información que se presenta al líder del proceso con el fin de dar cuenta de la efectividad del procedimiento evaluado en esta auditoría.

MESA DE VALIDACIÓN DE HALLAZGOS

En atención a que el riesgo observado como materializado ya fue objeto de valoración y se encuentra en curso la formulación del plan de mejoramiento pertinente, se recomendó en el acápite 4 de este informe lo pertinente.

RECOMENDACIONES

A- Revisar la metodología aplicada para el tratamiento de los riesgos identificados especialmente a la valoración de los controles con el fin de asegurar la mitigación de los impactos que puedan ocasionar la materialización de los eventos negativos.

B- Considerando el riesgo materializado citado en el numeral 4, se recomienda realizar un ejercicio acucioso de análisis de causas con el fin de formular acciones de mejora efectivas que permitan mitigar el riesgo que

se ha venido materializando recurrentemente.

C- Se recomienda revisar la pertinencia de contratar un profesional que asuma el rol de Oficial de Seguridad de la información.

D- Igualmente, revisar la pertinencia de impartir un lineamiento que establezca la obligatoriedad de diligenciar el campo denominado estado del incidente que alberga la base de datos del aplicativo Aranda, con el fin de que la información que se sustraiga de ésta sea lo más precisa posible con el fin de asegurar la oportunidad y confiabilidad de la información y de sus registros y coadyuvar a la Alta Dirección en la toma de decisiones

CONCLUSION

Con base en la evaluación adelantada por la Oficina de Control Interno y una vez valorados los documentos presentados por los auditados, se puede concluir que el Procedimiento Gestión Incidentes de Seguridad de la Información TIC-PR05 V2 ha venido cumpliendo con su objetivo toda vez que define las actividades para gestionar los incidentes de seguridad y privacidad de la información, se observa oportuna identificación, atención y respuesta con el fin de mitigar el impacto asociado a la pérdida de la confidencialidad, integridad y disponibilidad de la información de la Entidad.

A pesar de lo anterior se observan aspectos susceptibles de mejora que se presentaron en el capítulo precedente de recomendaciones.

Teniendo en cuenta el resultado de esta auditoría se insta a la líder del proceso Gestión Tecnologías de la Información y las comunicaciones en coordinación con la Alta Dirección, para que se adopten las acciones de mejora pertinentes que contribuyan a fortalecer la seguridad de la información y por ende a mejorar la gestión Institucional.

EQUIPO AUDITOR

Jaime Hernando Arias Patiño

Jefe Oficina de Control Interno

María del Carmen Bonilla

Profesional Especializada 222 grado 20
Auditora líder