GERENCIA DE CONTROL INTERNO DE GESTIÓN

GCIG – AIBR 05-24 – Política de Privacidad y Seguridad de la Información

Elaboró:
Diego Oviedo Ali

Revisado y aprobado por:
Belka Gutierrez Arrieta, Gerente de la Gerencia de Control Interno de Gestión

Barranquilla, 11 de diciembre de 2024

Contenido

1. ANTECEDENTES

Con aprobación del Comité Institucional de Coordinación de Control Interno (CICCI), en la sesión No. 001 del 20 de febrero de 2024 la Gerencia de Control Interno de Gestión (GCIG), incluyó dentro del Plan Anual de Auditoría para esta vigencia, la evaluación a la Política de privacidad y seguridad de la información.

Dicha evaluación fue incluida en el Plan Anual de Auditoría a través de un ejercicio de priorización en la que se tuvo en cuenta 6 criterios los cuales fueron:

- RIESGO INHERENTE Ponderación de Riesgos del Proceso y de corrupción.
- Tiempo transcurrido desde última auditoría.
- Cumplimiento del Plan de Mejoramiento Contraloría Distrital de Barranquilla.
- Cantidad de objetivos estratégicos asociados.
- Resultados auditorías anteriores internas y externas.
- Impacto en el presupuesto.

En este caso, la unidad auditable es una política que está incluida en la Política de Seguridad Digital y que anteriormente no ha recibido auditoría de riesgos, siendo ésta la primera a desarrollar.

Los resultados del furag 2023 arrojan un puntaje de 90 en el cumplimiento de la política.

2. OBJETIVOS

2.1 Objetivo General

- Evaluar la efectividad de los controles de seguridad y privacidad implementados en la organización para garantizar la confidencialidad, integridad y disponibilidad de la información, así como el cumplimiento a los requisitos legales y reglamentarios aplicables; lo anterior a fin de identificar aspectos a mejorar en la institución.

2.2 Objetivos específicos

- Verificar los controles ejercidos por las TICs de los mecanismos de control de acceso y protección de áreas que manejan información sensible.

- Verificar la ejecución y efectividad del plan de mantenimiento preventivo de los activos de TICs

- Evaluar la efectividad de los controles de supervisión ejercidos por la Gerencia de las TICs sobre los desarrollos y mantenimientos tercerizados.

• Evaluar la efectividad de los controles definidos por la Gerencia de las Tics como primera línea de defensa.

• Evaluar la zona de riesgo general de la política de privacidad y seguridad de la información, con base en la metodología de la Gerencia de Control Interno de Gestión.

3. ALCANCE

La evaluación se orienta a la política de seguridad y privacidad de la información.

El área evaluada es la Gerencia de las TICs. El periodo durante el cual se llevará a cabo la evaluación será del 4 al 6 de diciembre de 2024, de acuerdo con el cronograma propuesto en el numeral 7 de este plan.

4. LIMITACIONES AL ALCANCE

La evaluación se orienta a la política de seguridad y privacidad de la información.

El área evaluada es la Gerencia de las TICs. El periodo durante el cual se llevará a cabo la evaluación será del 4 al 6 de diciembre de 2024, de acuerdo con el cronograma propuesto en el numeral 7 de este plan.

5. NORMATIVIDAD

Durante el desarrollo de la presente evaluación, se incluyeron las siguientes normas:

NORMA	TIPO
Decreto 1078 de 2015	Externa
Decreto 612 de 2018	Externa
Decreto Distrital 0121 de 2021	Interna

6. METODOLOGÍA

Con el fin de dar cumplimiento a los protocolos establecidos por la Gerencia de Control Interno de Gestión, se llevó a cabo la reunión de instalación de la evaluación con el ingeniero Carlos Escalante Maduro. De la reunión mencionada se levantó acta la cual se firmó al finalizar y se anexó al presente plan de trabajo de auditoría.

Durante la instalación, el área evaluada informó: i) el nombre del funcionario que hizo el rol

de enlace con la GCIG en el desarrollo del proceso de auditoría, y ii) el nombre y correo electrónico de la persona responsable de la gestión (apoyo de la formulación y reporte de avances) de los compromisos de mejora; de esta decisión se dejó constancia en el acta de instalación.

Por otro lado, para efectos de garantizar la consistencia, pertinencia, integralidad y oportunidad de la información, el área responsable del proceso objeto de evaluación, durante la instalación, suscribió el documento “carta de representación”, la cual tuvo en cuenta para responder a los requerimientos de la Gerencia de Control Interno de Gestión; ésta se adjuntó como documento soporte de la presente guía de evaluación.

a. Solicitud inicial de información y la que se consideró necesaria durante el desarrollo de la evaluación para llevar a cabo el análisis que permitió el logro de los objetivos del ejercicio.

Se precisó que, dado el caso en que fue aportada información que contenía datos personales, se dio estricto cumplimiento a la ley 1581 de 2012 y a la Política de Tratamiento de Datos Personales de la Alcaldía Distrital de Barranquilla.

Si la información que se analizó durante la evaluación se catalogó como reservada o clasificada, a través de comunicación de la GCIG se confirmó con el área evaluada la pertinencia de continuar con la persona definida como enlace en la instalación de la evaluación o su reemplazo. Lo anterior, se indicó en el informe preliminar y en el informe final para su respectivo manejo.

En el desarrollo de la evaluación, todas las solicitudes que realizó el equipo auditor fueron requeridas formalmente por escrito, fijando un plazo límite para su respuesta. Igualmente, las respuestas a las solicitudes de información debieron ser formalizadas ante la GCIG a través de medio escrito, de ser posible en formato digital u original en calidad de préstamo (En concordancia con la Directiva Presidencia 04 de 2012 “Eficiencia Administrativa y Lineamientos de la Política Cero Papel en la Administración Pública”) y dentro de los plazos estipulados, en atención a lo establecido en el numeral 7 del artículo 39 de la Ley 1952 de 2019, en relación con: "Omitir, negar, retardar o entrabar el despacho de los asuntos a su cargo o la prestación del servicio al que está obligado."

b. Revisión y análisis preliminar de la normatividad, de la caracterización del proceso, procedimientos y guías específicos orientados al tema de evaluación.

c. Revisión y análisis de la información inicial requerida (Área(s)). En caso de ser necesario, la GCIG aplicó herramientas estadísticas para determinar las respectivas muestras a analizar. Se utilizó instrumento estadístico de la caja de herramientas del DAFP.

d. Desarrollo de procedimientos de auditoría como observación, inspección, confirmación, procedimientos analíticos, entrevista(s) y/o encuestas a funcionarios de las áreas que intervinieron en los procesos relacionados con los temas a evaluar, dejando documentada tal actividad a través de memoria o registro firmados al finalizar. De ser necesario, se

realizaron mesas de trabajo con los responsables del área evaluada, las cuales quedaron soportadas a través de acta firmada una vez culminada la reunión.

e. Una vez ejecutadas las actividades de auditoría planificada, la GCIG elaboró el informe preliminar, el cual fue remitido a la dependencia evaluada para los correspondientes comentarios, los cuales debieron ser remitidos por escrito.

En el anterior sentido, el informe preliminar fue un producto terminado, y por ende la comunicación que contenía los comentarios al mismo precisó la observación respecto al criterio normativo y la situación evidenciada e indicó qué parte de estos aspectos se iba a contradecir, con los argumentos pertinentes y la respectiva evidencia.

Fue necesario tener en cuenta que si las áreas evaluadas consideraron pertinente allegar a la GCIG información documental que no fue aportada en el desarrollo de la auditoría, las mismas pudieron remitirla adjunta a la respuesta del informe preliminar; la GCIG mantuvo la verificación documental inicial y ajustó, si fue el caso y de acuerdo con los soportes suministrados, el hallazgo y/o el impacto definido inicialmente.

f. Elaboración del informe final con destino a la Gerencia de las TICs. El informe final se remitió al despacho del alcalde, como líder y máximo responsable del Sistema de Control Interno de la entidad y se publicó en la página web institucional, conforme a lo establecido en el Decreto 339 de 2019 en su Artículo 1.

g. Con base en los hallazgos dados a conocer por la GCIG en el informe, la Gerencia de las TICs inició la definición de los compromisos de mejoramiento a fin de superar las debilidades identificadas en la evaluación; para ello la GCIG remitió el formato de acciones correctivas, para la formulación de las acciones correctivas en versión preliminar, previo al diligenciamiento de estas en el aplicativo para la administración del SGC.

Una vez recaudada y analizada la información, la GCIG elaboró el informe final, el cual será enviado a la Gerencia de las Tic, con el fin de que conozcan los hallazgos levantados producto de dicha evaluación.

Con base en los hallazgos dados a conocer por la GCIG en el informe, la Gerencia de las TICs iniciarán la definición de los compromisos de mejoramiento para los hallazgos clasificados como tipo I, II y III a fin de superar las debilidades identificadas en la evaluación; para ello la GCIG remitirá el formato de acciones correctivas, para la formulación de las acciones de mejoramiento en versión preliminar, previo al diligenciamiento de estas en el aplicativo dispuesto para tal fin.

Una vez las acciones correctivas se encuentren acordadas con la GCIG (aquellas que cumplen con los lineamientos definidos), la Gerencia de las TICs diligenciará en el sistema los compromisos de mejoramiento para la eliminación de las causas que establecieron los hallazgos.

El Informe final se publicará en el sitio web de la GCIG, excepto si se considera que el documento contiene información *"reservada o clasificada".*

7. MATRIZ DE HALLAZGOS

TIPO I Tratamiento: Se escala al Sr Alcalde, como responsable del SCI. Se reporta la alerta a instancias competentes en atención a procedimiento aplicable. Se hace seguimiento por la GCIG		
Observación No.	Descripción Observación	No. Pág.
N/A	**N/A**	**N/A**
TIPO II Tratamiento: Se pone en conocimiento del Comité Institucional de Coordinación de Control Interno. Se presenta reporte por la dependencia o proceso evaluado en el Comité CICCI de los compromisos de mejora suscritos. Se hace seguimiento por la GCIG.		
Observación No.	Descripción Observación	No. Pág.
I	El procedimiento de copias de respaldo no cumple con los parámetros establecidos en la política, ya que no incluye el nivel de criticidad y responsable el responsable de las actividades.	11
II	Incumplimiento del programa de Mantenimiento con un porcentaje de ejecución del 54.64%	14
TIPO III Tratamiento: Se pone en conocimiento del Comité Institucional de Gestión y Desempeño y/o al sistema de gestión competente a nivel interno (SIGBAQ, SGC, SGA, SGSST, SGSI, SGD). Se hace seguimiento por la GCIG		
Observación No.	Descripción Observación	No. Pág.
III	Se encontraron debilidades en la definición de la obligación de cumplimiento en los contratos establecidos para el control de software seguro, bajo la responsabilidad de la Gerencia de las TIC	17
IV	Debilidades en el diseño e implementación de los puntos de control en procedimientos	
TIPO IV Tratamiento: Es opcional la suscripción de acciones correctivas. Las acciones deben ser asumidas por el proceso o dependencia evaluada como parte de sus actividades de autocontrol.		
Observación No.	Descripción Observación	No. Pág.
N/A	N/A	N/A

8. RESULTADOS DE LA EVALUACIÓN, SEGUIMIENTO O ACOMPAÑAMIENTO

8.1 Verificar los controles ejercidos por las TICs de los mecanismos de control de acceso y protección de áreas que manejan información sensible.

Para definir la cantidad de equipos que fueron sometidos a la verificación de los controles ejercidos por la Gerencia de las Tics se aplicó un muestreo teniendo en cuenta: la cantidad de equipos totales, el Error muestral (5%), proporción de éxito (10%), nivel de confianza (95%). El ejercicio de muestreo arrojó que la muestra óptima fue de 132 equipos a verificar. A continuación se detalla dicho ejercicio de muestreo.

ALCALDÍA DE BARRANQUILLA	CÁLCULO DE LA MUESTRA	
AUDITORÍA:		
Muestreo Aleatorio Simple para estimar la proporción de una población		
Entidad	**Alcaldía Distrital de Barranquilla**	
Proceso	**Gestion de las Tecnologias e Información**	
Cálculo de la muestra para:	**Definir la cantidad de equipos a verificar cumplimiento de seguridad.**	
Período Evaluado:	**2024**	
Preparado por:	**Diego Oviedo Ali - Profesional Universitario**	
Fecha:	**20/11/2024**	
Revisado por:	**Belka Gutierrez Arrieta - Gerente GCIG**	
Fecha:	**25/11/2024**	

INGRESO DE PARÁMETROS	
Tamaño de la Población (N)	**2.987**
Error Muestral (E)	**5%**
Proporción de Éxito (P)	**10%**
Nivel de Confianza	**95%**
Nivel de Confianza (Z) (1)	**1,960**

TAMAÑO DE LA MUESTRA

Fórmula	**138**
Muestra Óptima	**132**

Formula para poblaciones infinitas

$$n = \frac{z^2 * P * Q}{E^2}$$

Formula para poblaciones finitas

$$n = \frac{P * Q * z^2 * N}{N * E^2 + z^2 * P * Q}$$

Z= Valor de la distribución normal estándar de acuerdo al nivel de confianza
E= Error de muestreo (precisión)
N= Tamaño de la Población
P= Proporción estimada
Q= 1-P

Fuente: Adaptado de Contraloría General de la República. Contraloría Delegada para el Sector Social. Agosto 2011		
CRITERIOS: Politica de Seguridad y Privacidad de la Información		
OBSERVACIÓN/CONCLUSIÓN : Se revisaron los equipos que se encuentran ubicados en la sede central de la alcaldía		
ELABORADO POR:	**DIEGO OVIEDO ALI -Auditor**	**FECHA: 27/11/2024**
REVISADO Y APROBADO POR:	**BELKA GUTIÉRREZ ARRIETA - Gerente**	**FECHA: 02/12/2024**

Según la información proporcionada, se identificaron 132 equipos para verificar que contaran con antivirus instalado y actualizado, que no tuvieran software no autorizado, que se prohibiera la manipulación de la información contenida en ellos y que todos los programas estuvieran correctamente licenciados. A continuación, se detallan los equipos correspondientes:

Secretaría/oficina	Ubicación o sede	N° equipos verificados	Revisión pc
Secretaría Distrital de Control urbano y Espacio Público	Sede Principal	20	Cumple

Secretaría Distrital de Obras Públicas	Sede Principal	20	Cumple
Secretaría Distrital de Comunicaciones	Sede Principal	10	Cumple
Secretaría Distrital de Desarrollo Económico	Sede Principal	12	Cumple
Secretaría General	Sede Principal	30	Cumple
Gerencia de Control Interno de Gestión	Sede Principal	12	Cumple
Secretaría Distrital de Gestión Humana	Sede Principal	28	Cumple
TOTAL EQUIPOS VERIFICADOS		132	

Tras realizar la verificación de cada equipo, se analizó un total de 132 dispositivos, de los cuales todos contaban con software licenciado, tenían restringidos los permisos para la instalación de software no autorizado y estaban debidamente asignados a los funcionarios correspondientes.

También se incluyó la revisión del procedimiento de copias de respaldo con código ME-TIC-P-036, donde se revisó que cumpliera con lo establecido en la política de privacidad y seguridad de la información: De que, como, quién, con qué periodicidad, tipo de respaldo y nivel de criticidad.

Hallazgo número I: El procedimiento de copias de respaldo no cumple con los parámetros establecidos en la política, ya que no incluye el nivel de criticidad y responsable el responsable de las actividades.  Zona de riesgo: Alta	
Criterio	6.7. POLÍTICA DE SEGURIDAD DE LAS OPERACIONES **Copias de respaldo** • La Gerencia de las TIC definirá y documentará un procedimiento de copias de respaldo y restauración de la información, donde se establezca el esquema, de qué, cómo, quién, con qué periodicidad, tipo de respaldo y nivel de criticidad. Dicho procedimiento debe cobijar los equipos dentro y fuera de la entidad y la información almacenada en equipos personales.
Condición evidenciada	Durante la revisión del procedimiento de copias de respaldo con código ME-TIC-P-036 se evidenció que no contaba con la criticidad, responsables y puntos de control que exige la política de privacidad y seguridad de la información
Posible Causa (s)	No se tiene un control adecuado para el cumplimiento estricto de la política de privacidad y seguridad de la información.

Potencial Impacto	Al no identificar claramente el nivel de criticidad de los datos, no se podrá priorizar adecuadamente la realización de copias de seguridad para los datos más importantes. Esto puede resultar en la falta de protección de información esencial, afectando la operatividad de la entidad en caso de incidentes. La ausencia de un responsable definido para las actividades de respaldo puede generar confusión o descoordinación en el proceso de restauración de los datos en caso de pérdida o desastre. La falta de claridad en las responsabilidades podría retrasar la recuperación de información crítica, afectando la continuidad operativa de la entidad. Al no establecer el nivel de criticidad de los datos, algunos datos fundamentales para la entidad pueden no ser respaldados con la frecuencia necesaria, lo que aumenta el riesgo de perder información clave, especialmente si ocurre un fallo o ataque en los sistemas. Sin una asignación clara de responsabilidades, será más difícil realizar auditorías efectivas o supervisar el cumplimiento de las políticas de respaldo. La falta de trazabilidad y rendición de cuentas puede impedir detectar y corregir fallos en el procedimiento a tiempo.
Recomendaciones (Actividades de mejora sugeridas)	Clasificación de Datos según su Criticidad: Actividad: Realizar un análisis exhaustivo de todos los datos de la entidad, clasificándolos según su nivel de criticidad (alta, media, baja). Objetivo: Priorizar las copias de seguridad de los datos más sensibles y esenciales para la continuidad de las operaciones, garantizando que los datos críticos se respalden con mayor frecuencia y se mantengan seguros. Definición Clara de responsables: Actividad: Asignar responsabilidades específicas para la gestión y ejecución de las copias de respaldo a empleados o equipos concretos dentro de la entidad. Objetivo: Asegurar que cada tarea relacionada con los respaldos (realización, verificación, almacenamiento, y recuperación) tenga un responsable claramente identificado para evitar ambigüedades y mejorar la eficiencia en caso de incidentes. Documentación Detallada de Procedimientos:

	Actividad: Elaborar una documentación detallada que incluya procedimientos claros para la realización de copias de respaldo, especificando el nivel de criticidad de los datos, las frecuencias de respaldo, los métodos de almacenamiento y los responsables de cada actividad. Objetivo: Establecer directrices claras y accesibles para garantizar que todas las actividades relacionadas con los respaldos sean comprendidas y seguidas correctamente por el personal asignado. Automatización de Copias de Respaldo: Actividad: Implementar herramientas o sistemas automáticos que realicen las copias de respaldo de acuerdo con las políticas establecidas, con un enfoque en la programación según la criticidad de los datos. Objetivo: Minimizar el riesgo de error humano y garantizar la consistencia en la ejecución de los respaldos, asegurando que no se omitan datos importantes.

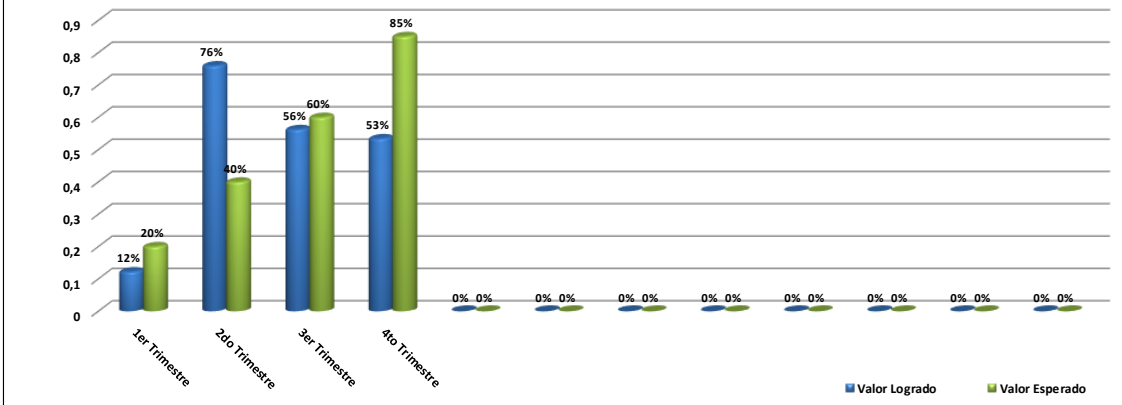
8.2 Verificar la ejecución y efectividad del plan de mantenimiento preventivo de los activos de TICs

Se verificó la ejecución y efectividad del plan de mantenimiento preventivo de los activos de Tecnologías de la Información y Comunicación (TICs), lo cual es fundamental para garantizar la continuidad operativa y la protección de los activos tecnológicos. Para ello, se verificaron los indicadores registrados por las TICs, donde, a corte del día de la auditoría, el plan de mantenimiento alcanza un 54.64%. A continuación, se detalla el hallazgo identificado y su zona de riesgo.

REGISTRO DE RESULTADOS												
Variable / Periodo	-	-	1er Trimestre	-	-	2do Trimestre	-	-	3er Trimestre	-	-	4to Trimestre
Total de equipos a los que se le han realizado el mantenimiento preventivo			51			635			705			893
Equipos programados para mantenimiento en el periodo			418			836			1254			1672
RESULTADO (%)			**12%**			**76%**			**56%**			**53%**
META POR PERIODO			20%			40%			60%			85%

GRAFICA

REVISAR TENDENCIA ASCENDENTE



Hallazgo número II: Incumplimiento del programa de Mantenimiento con un porcentaje de ejecución del 54.64%. Zona de riesgo: Alta	
Criterio	6.6. POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO **Equipos** • La Gerencia de TIC, establecerá plan de mantenimiento preventivo de los activos de tecnología e información para asegurar su disponibilidad e integridad. • Cuando un equipo o medio extraíble sea reasignado o retirado de servicio, la Gerencia de las TIC debe garantizar la eliminación de toda información mediante mecanismos de borrado seguro teniendo en cuenta que previo a esta actividad debe realizarse una copia de seguridad de esta.
Condición evidenciada	A corte de la ejecución de la auditoría (5 de diciembre 2024), se realizó la verificación del cumplimiento del plan de mantenimiento y se encontró que la meta establecida en el primer, segundo y tercer trimestre no se cumplieron. En el primer

	trimestre hubo un cumplimiento de 12.20%, en el segundo trimestre fue de 75.95%, teniendo en cuenta que las metas y las unidades de mantenimiento son acumulativas, en el tercer trimestre 0.017%.
Posible Causa (s)	Falta de capacidad laboral por parte del recurso humano.
Potencial Impacto	Interrupciones en la Operatividad: El mantenimiento adecuado es clave para garantizar la disponibilidad continua de los sistemas. Su incumplimiento puede dar lugar a fallos o paradas imprevistas en los equipos y servicios tecnológicos, afectando directamente la operatividad de la entidad y su capacidad para ofrecer servicios de manera eficiente. Riesgos de Seguridad: Si no se realiza un mantenimiento adecuado, los sistemas y equipos pueden volverse vulnerables a ataques cibernéticos, pérdida de datos o acceso no autorizado. Esto puede comprometer la integridad de la información sensible, así como la confidencialidad y privacidad de los datos. Aumento de Costos Operativos: El incumplimiento del plan de mantenimiento puede resultar en un aumento en los costos operativos debido a la necesidad de realizar reparaciones urgentes, reemplazo de equipos averiados o la contratación de servicios externos de emergencia. Además, la falta de mantenimiento preventivo puede reducir la vida útil de los activos tecnológicos, generando costos adicionales a largo plazo. Pérdida de Confianza y Credibilidad: Un fallo en los sistemas debido a la falta de mantenimiento puede dañar la confianza de los usuarios, clientes y otros stakeholders. En el caso de entidades públicas, esto puede afectar la imagen institucional, generando desconfianza en la capacidad de la entidad para manejar recursos y servicios de manera eficiente. Pérdida de Datos Importantes: La ausencia de mantenimiento preventivo adecuado puede derivar en fallos en los sistemas de almacenamiento de datos o en la pérdida de información crítica, lo cual puede tener consecuencias graves, tanto operativas como legales, dependiendo de la naturaleza de los datos involucrados (por ejemplo, datos personales de ciudadanos o documentos de gran importancia institucional). Desempeño Deficiente de los Sistemas: El mantenimiento regular permite que los sistemas TIC operen a su máxima capacidad. Al no seguir el plan de mantenimiento, es posible que

	los equipos no rindan de manera óptima, afectando el desempeño general de la entidad en términos de velocidad, eficiencia y calidad de los servicios ofrecidos. Impacto en la Toma de Decisiones: La falta de mantenimiento puede generar fallos en los sistemas de información y análisis que son cruciales para la toma de decisiones dentro de la entidad. Esto puede derivar en decisiones incorrectas o tardías que afecten negativamente la gestión y planificación de proyectos o políticas públicas. Cumplimiento Normativo y Legal: El incumplimiento del plan de mantenimiento también puede implicar riesgos legales o regulatorios. Muchas leyes y normativas requieren que las entidades públicas mantengan sus sistemas y equipos tecnológicos en condiciones operativas para cumplir con estándares de seguridad, protección de datos y funcionamiento eficiente de los servicios.
Recomendaciones (Actividades de mejora sugeridas)	Fortalecer la Planificación y Documentación del Mantenimiento Preventivo: Asegurar que el plan de mantenimiento esté claramente documentado, con procedimientos específicos, frecuencias de mantenimiento definidas, responsables asignados y criterios de criticidad de los equipos. De esta forma, se garantiza que el mantenimiento se realice de manera organizada y oportuna. Monitoreo Regular de la Ejecución del Plan: Establecer un sistema de seguimiento y monitoreo continuo de las actividades de mantenimiento, que permita verificar el cumplimiento del cronograma y detectar cualquier desviación de manera temprana. Esto incluye la implementación de herramientas de gestión de activos TIC que faciliten la trazabilidad de las intervenciones realizadas. Capacitación Continua del Personal Técnico: Es crucial que el personal encargado del mantenimiento esté debidamente capacitado y actualizado sobre las mejores prácticas, nuevas tecnologías y procedimientos de mantenimiento. Esto garantizará que el mantenimiento se realice de manera eficaz y que se puedan abordar cualquier incidencia de manera oportuna.

8.3 Evaluar la efectividad de los controles de supervisión ejercidos por la Gerencia de las TICs sobre los desarrollos y mantenimientos tercerizados.

Se verificó la metodología para el desarrollo y mantenimiento de software seguro de la entidad en los equipos tercerizados. Durante el proceso, se revisaron los procedimientos y estándares utilizados para asegurar que todos los equipos y sistemas externos cumplieran con las políticas de seguridad definidas por la entidad. Se constató que las prácticas aplicadas por los proveedores externos estaban alineadas con las mejores prácticas de seguridad, garantizando que los desarrollos y mantenimientos se realizaban de acuerdo con los protocolos establecidos. Además, se corroboró que se implementaban controles para proteger los activos tecnológicos y los datos de la entidad.

Se revisó que en los informes técnicos se incluyera el componente de la obligación de cumplimiento en los contratos sobre software seguro, sin embargo, se identificó que se debe fortalecer y robustecer dicha obligación. A continuación, se detalla el hallazgo encontrado y el tipo de riesgo.

Hallazgo número III: Se encontraron debilidades en la definición de la obligación de cumplimiento en los contratos establecidos para el control de software seguro, bajo la responsabilidad de la Gerencia de las TIC. Zona de riesgo: Media	
Criterio	6.9. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS. **Seguridad en los procesos de desarrollo y de soporte** • La Gerencia de las TIC en el proceso de desarrollo y/o mantenimiento de software, debe contar con metodologías y lineamientos de desarrollo seguro para cada etapa del ciclo de vida: análisis, construcción, pruebas y puesta en producción. Durante cada etapa ejecutar y documentar pruebas de funcionalidad de la seguridad y privacidad • La Gerencia de las TIC, debe definir un procedimiento para el control de cambio que incluya revisión técnica y restricciones de las aplicaciones después de los cambios. • La Gerencia de las TIC garantizará la seguridad para los ambientes de desarrollo seguro teniendo en cuenta los controles definidos en la política de seguridad de las operaciones. • La Gerencia de las TIC, realizará supervisiones a los desarrollos y/o mantenimientos de software tercerizados velando que cumplan con la política y con las directrices establecidas.
Condición evidenciada	Se observó que los contratos establecidos con proveedores de software y servicios TIC no contienen cláusulas claras y

	detalladas sobre la obligación de cumplir con las políticas de seguridad informática y las normas de software seguro. En algunos casos, los acuerdos carecen de mecanismos específicos de monitoreo y penalizaciones en caso de incumplimiento de las normativas de seguridad. Además, se evidenció que no existe un seguimiento adecuado de la Gerencia de las TIC sobre el cumplimiento de estas cláusulas, lo que podría generar riesgos relacionados con el uso de software no seguro, vulnerabilidades de seguridad o la falta de actualización de los sistemas." Este tipo de hallazgo resalta la falta de rigurosidad en la gestión contractual y la necesidad de reforzar los controles de cumplimiento para asegurar que los acuerdos con terceros cumplan con los estándares de seguridad establecidos por la entidad.
Posible Causa (s)	La falta de una estrategia clara y consistente en la gestión de contratos de software y servicios TIC, que no ha contemplado de manera adecuada las cláusulas relacionadas con la seguridad de la información y el software seguro. Esto podría haber sido el resultado de una deficiente planificación o priorización de aspectos de seguridad durante la redacción y negociación de los contratos. Además, puede haberse dado una falta de conciencia o enfoque insuficiente en la importancia de la seguridad en las adquisiciones tecnológicas, sumado a la ausencia de un proceso formal de seguimiento y verificación del cumplimiento de las políticas de seguridad por parte de los proveedores externos.
Potencial Impacto	Riesgos de Seguridad Informática: La falta de cláusulas claras sobre el cumplimiento de las políticas de software seguro podría generar vulnerabilidades en los sistemas de la entidad. Esto aumentaría el riesgo de ciberataques, malware, acceso no autorizado, y otros incidentes de seguridad que comprometan la confidencialidad, integridad y disponibilidad de la información. Costos Operativos y Reparación de Incidentes: La ausencia de controles de seguridad adecuados en los contratos podría llevar a fallas en el software o en los sistemas, lo que generaría tiempos de inactividad no planificados y afectaría la continuidad operativa de la entidad. Los costos asociados con la reparación de fallas, la recuperación de datos y la restauración de sistemas podrían ser significativos. Falta de Actualización y Soporte de Software: Sin un seguimiento adecuado de los proveedores, puede haber retrasos en la actualización de los sistemas o en la

	implementación de parches de seguridad, lo que dejaría a la entidad vulnerable a exploits de seguridad conocidos. Además, esto podría generar incompatibilidades entre sistemas, impactando negativamente en el rendimiento y la estabilidad operativa. Daño a la Reputación: En caso de un incidente de seguridad debido a software no seguro o desactualizado, la reputación de la entidad podría verse gravemente afectada, lo que podría generar desconfianza en los usuarios, clientes, socios y otras partes interesadas. Esto podría tener repercusiones tanto a nivel público como institucional, afectando la percepción de la entidad y su capacidad para gestionar de manera responsable la seguridad de la información.
Recomendaciones (Actividades de mejora sugeridas)	las recomendaciones que se podrían dejar en relación al refuerzo de la obligación de cumplimiento en los contratos establecidos para el control de software seguro, bajo la responsabilidad de la Gerencia de las TIC, son las siguientes: Incluir Cláusulas Claras de Seguridad en los Contratos: Se recomienda que todos los contratos con proveedores de software y servicios TIC incluyan cláusulas específicas sobre el cumplimiento de las políticas de seguridad informática y estándares de software seguro. Estas cláusulas deben cubrir aspectos como la obligatoriedad de utilizar software con licencias válidas, la implementación de medidas de protección de datos, y la realización de actualizaciones y parches de seguridad dentro de plazos establecidos. Establecer Procedimientos de Monitoreo y Cumplimiento: Se sugiere que la Gerencia de las TIC implemente procedimientos internos que aseguren el seguimiento continuo del cumplimiento de las cláusulas contractuales. Esto incluye la realización de auditorías periódicas a los proveedores, así como la revisión y verificación de que el software utilizado cumpla con las normas de seguridad establecidas por la entidad. Definir Responsabilidades Claras: Es crucial que se asignen responsabilidades claras dentro de la Gerencia de las TIC para el control y la supervisión del cumplimiento de las políticas de seguridad en los contratos de software. El personal encargado debe ser capacitado adecuadamente para identificar riesgos y tomar acciones correctivas en caso de incumplimiento.

8.4 Evaluar la efectividad de los controles definidos por la Gerencia de las Tics como primera línea de defensa

Con base en los controles definidos en el mapa de riesgos, procedimientos, instructivos, guías, entre otros, la GCIG evaluó la efectividad de los controles categorizados por líneas de defensa, de acuerdo con la escala establecida en la guía para la administración de riesgos. Estos fueron los resultados:

Primera línea de defensa.

Le corresponde "a los servidores en sus diferentes niveles, quienes aplican las medidas de control interno en las operaciones del día a día de la entidad. Se debe precisar que cuando se trate de servidores que ostenten un cargo de responsabilidad (jefe) dentro de la estructura organizacional, se denominan controles. de gerencia operativa, ya que son aplicados por líderes o responsables de proceso. Esta línea se encarga del mantenimiento efectivo de controles internos, por consiguiente, identifica, evalúa, controla y mitiga los riesgos"[1].

En el contexto de la Alcaldía Distrital de Barranquilla, debe ser entendida como el conjunto de controles que son realizados por los líderes de los procesos y sus equipos, ya sean estratégicos, misionales, de apoyo y evaluación. Esta actividad tiene como finalidad el establecimiento de medidas de control para la gestión de los riesgos institucionales en el nivel operacional. Dentro de las actividades a realizar se debe verificar la aplicación de la normativa vigente, tanto interna como externa, al igual que la medición a través de indicadores como parte del día a día de la gestión a su cargo. Esta línea evidencia el ejercicio del autocontrol.

Así las cosas, se aplicó el instrumento de evaluación de la efectividad de controles diseñado por la GCIG, estos fueron los resultados:

Control	Efectividad del control
Acta de servicio claro sobre 3000 antivirus kaspersky	50
Definición de los mantenimientos preventivos, Cronograma y evidencia de ejecución	55
Se constató el procedimiento con código ME-TIC-P-036 copia de respaldo	35
Se debe fortalecer la obligación de cumplimiento en los contratos establecidos para el control de software seguro por parte de la Gerencia de las TICs	40

[1] Tomado de *Manual Operativo del Modelo Integrado de Planeación y Gestión, v5.* Departamento Administrativo de la Función Pública. p. 118

ESCALA	RESULTADO DE EFECTIVIDAD DE CONTROL
ALTA	>=80%
MEDIA	Entre el 60% y el 79%
BAJA	<=59%

Se observa que existen notables debilidades en la Gerencia de Tecnologías de la Información y Comunicaciones (TICs), especialmente en lo que respecta al diseño e implementación de controles eficaces que aseguren el correcto desempeño de sus actividades. Estas deficiencias afectan la capacidad de la gerencia para gestionar de manera adecuada los recursos tecnológicos, garantizar la seguridad de la información y optimizar los procesos internos, lo que podría repercutir en la eficiencia organizativa y la protección de datos sensibles. Es crucial que se fortalezcan los mecanismos de control y se adopten mejores prácticas para mitigar los riesgos y mejorar la efectividad de las operaciones en el ámbito de las TICs.

Segunda línea de defensa.

Está conformada "por servidores que ocupan cargos del nivel directivo o asesor (media o alta gerencia), quienes realizan labores de supervisión sobre temas transversales para la entidad y rinden cuentas ante la Alta Dirección. Esta línea se asegura de que los controles y procesos de gestión del riesgo de la 1ª línea de defensa sean apropiados y funcionen correctamente, además, se encarga de supervisar la eficacia e implementación de las prácticas de gestión de riesgo, ejercicio que implicará la implementación de actividades de control específicas que permitan adelantar estos procesos de seguimiento y verificación con un enfoque basado en riesgos"[2].

En el contexto de la Alcaldía Distrital de Barranquilla, debe ser entendida como el conjunto de controles realizados por la media y alta dirección de la entidad (secretarios, gerentes y jefes de oficinas), y asegura que los controles y procesos de gestión del riesgo de la 1ª línea de defensa sean apropiados y funcionen correctamente. Su propósito es establecer mecanismos que les permitan ejecutar un seguimiento permanente de la gestión. Esta línea evidencia el ejercicio de la autoevaluación.

En el anterior sentido, como segunda línea de defensa no se identificó control por la Gerencia.

[2] Tomado de *Manual Operativo del Modelo Integrado de Planeación y Gestión, v5.* Departamento Administrativo de la Función Pública. p. 119

8.5 Evaluar la zona de riesgo general de la política de privacidad y seguridad de la información, con base en la metodología de la Gerencia de Control Interno de Gestión.

En atención a la metodología establecida por la GCIG, la zona de riesgo residual se ubicó en Zona de Riesgo MEDIA, dado que se presentó 2 hallazgos tipo II y 2 hallazgos tipo III.

Matriz de Establecimiento Zona de Riesgo

CATEGORIA DE LA OBSERVACION	PONDERACION (IMPACTO)	CANTIDAD DE OBSERVACIONES	PROBABILIDAD CATEGORÍA	PROMEDIO PONDERADO	ZONA DE RIESGO	INTERVALO PROMEDIO DEL RIESGO
TIPO I	0,00%	0	0%	0,00%	EXTREMA	83,40%-100%
TIPO II	75,00%	2	50%	37,50%	ALTA	66,70%-83,33%
TIPO III	50,00%	2	50%	25,00%	MEDIA	33,40%-66,67%
TIPO IV	0,00%	0	0%	0,00%	BAJA	0%-33,33%
	TOTALES	4	**% DE RIESGO**	**62,50%**		

Categoria	Cantidad observaciones		
	1	2	>=3
Tipo I	83,40%	90,00%	100,00%
Tipo II	66,70%	75,00%	83,33%
Tipo III	33,40%	50,00%	66,67%
Tipo IV	11,00%	22,00%	33,33%

9. CONCLUSIONES

A continuación, se obtuvieron las siguientes conclusiones:

Identificación de Debilidades en el Diseño de Controles: A lo largo de la auditoría se evidenció que la Gerencia de TICs presenta debilidades significativas en el diseño e implementación de controles internos. Estos puntos vulnerables incrementan el riesgo de fallos operativos y afectan la capacidad de la organización para mitigar posibles amenazas tecnológicas y de seguridad.

Incumplimiento en el plan de mantenimiento preventivo: Durante el proceso de auditoría, se identificó un incumplimiento significativo en la implementación del plan de mantenimiento de los activos críticos de la organización. Se observó que los plazos establecidos para las actividades de mantenimiento preventivo y correctivo no se han cumplido de manera adecuada, lo que podría comprometer la operatividad y la vida útil de los equipos y sistemas.

Informe de auditoría elaborado por: Diego Oviedo Ali, Profesional Universitario
Fecha de elaboración: 18/12/24
Revisado y aprobado por: Belka Gutiérrez Arrieta – Gerente, Gerencia Control Interno de Gestión
Fecha de aprobación: 18/12/24