

**PROCESO AUDITADO:** Tecnologías de la Información y las Comunicaciones.

**AREA O DEPENDENCIA:** Oficina Tecnologías de la Información y las Comunicaciones TIC.

**OBJETIVO:** Verificar el cumplimiento de la Política de Seguridad de la Información conforme a lo establecido en las normas legales vigentes aplicables al Municipio de Chía durante la vigencia 2023-2024.

**ALCANCE:** Se procederá a efectuar la revisión documental proferida en cumplimiento de la Política de Seguridad de la Información en la Entidad en las vigencias 2023-2024.

**CRITERIOS DE LA AUDITORIA:**

- Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data.
- Ley 87 de 1993.
- Decreto 648 de 2017, "Por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública".
- Decreto 40 de 2019
- Ley 44 de 1993. – Derechos de Autor
- Ley 1273 de 2009, "Delitos Informáticos" protección de la información y los datos".
- Ley 1581 de 2012, "Protección de Datos personales".
- Decreto 1078 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".
- CONPES 3854 DE 2016 – Política nacional de seguridad digital.
- Decreto 1008 de 2018 "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".

- Resolución No. 001519 de 24 de agosto de 2020- MINTIC. "Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos"
- CONPES 3995 DE 2020 – Política nacional de confianza y seguridad digital
- Resolución 500 de 2021 – Lineamientos y estándares para la estrategia de seguridad digital.
- Decreto 338 de 2022- Lineamientos generales para fortalecer la gobernanza de la seguridad digital

**VIGENCIA AUDITADA:** 2023-2024

**FECHA DE APERTURA:** 31 de octubre de 2024.

**EQUIPO AUDITOR:** Carlos Andrés Rodríguez Sánchez.  
Jefe Oficina de Control Interno.

Helena Maria Torrealba Velandia.  
Profesional Universitario.

### METODOLOGIA

El Proceso de Auditoría Interna se establece partiendo de la programación anual de las actividades de la Oficina de Control Interno, las cuales son aprobadas por el Comité Institucional de Coordinación de Control Interno, posteriormente se da la fase de **planeación** de la Auditoría Interna (objetivos, alcance, metodología, procedimientos y técnicas, tiempos), luego se procede con la **Ejecución** (Comunicación Plan de Auditoría, solicitud de información, determinación de la muestra, papeles de trabajo, diseño y aplicación de las pruebas y aplicación de técnicas de auditoría: revisión documental, consultas, inspección entrevistas con los responsables, observación, entre otras., procediéndose a la elaboración de observaciones y la emisión de Informe Preliminar), se efectúa la **comunicación de resultados** (Informe Definitivo) y por último el suscripción Plan de Mejoramiento y su seguimiento.

### DESARROLLO DE LA AUDITORÍA INTERNA

De acuerdo a los resultados obtenidos en la revisión a la Política de Seguridad de la Información y demás políticas que la conforman, se observa la siguiente información allegada por la Oficina de Tecnologías de la Información y las Comunicaciones TIC:



1. Política de Seguridad de la Información 2024-2027 julio de 2024-Versión 1, la cual contiene:

- Política de uso de dispositivos móviles institucionales
- Política de seguridad de los recursos humanos
- Política de compromiso de confidencialidad por parte de los funcionarios
- Política de confidencialidad y seguridad para contratistas
- Política aplicable durante la ejecución del empleo
- Política de gestión de transiciones laborales
- Política gestión de activos de información
- Política de asignación de permisos y privilegios
- Política de control de acceso
- Política de seguridad física y del entorno
- Políticas de controles criptográficos
- Políticas de seguridad en las operaciones
- Políticas de seguridad de las comunicaciones
- Política adquisición, desarrollo y mantenimiento de sistemas
- Política de relaciones con los proveedores
- Política sobre el uso adecuado de internet
- Política sobre el uso adecuado de correo electrónico
- Política de contraseñas seguras
- Políticas de gestión de incidentes de seguridad
- Política de administración de riesgos
- Políticas de cumplimiento

2. Modelo de Seguridad y Privacidad de la Información. 28 de septiembre/2023. Aprobado en el Comité de Gestión y Desempeño

3. Campañas de sensibilización y capacitación.

- Circular informativa 09 del 27/octubre/2023. Asunto: Campaña sensibilización sobre la Política de Seguridad de la Información; Modelo de Seguridad y Privacidad de la Información MSPI de la Alcaldía Municipal de Chía.
- Circular informativa 02 del 06/mayo/2024. Asunto: Campaña de sensibilización sobre la Política de Gobierno Digital y de Seguridad de Información, Procedimientos de Seguridad de la Información y Datos Abiertos. Listado de asistencia sensibilizaciones mayo 2024.
- Circular informativa 006 del 09/octubre/2024. Asunto: Campaña de sensibilización sobre la Política de Seguridad Digital y de la Información.

- sala de Gobierno

• Campaña 07/noviembre/2024

4. Plan de tratamiento de riesgos -28/septiembre/2023.Asunto: Cumplimiento normativa Datos Abiertos
5. Manual de Procedimientos para el Datacenter.
6. Manual ÁREA REDES OFICINA TIC, que contiene los siguientes manuales (Manual de Procedimientos Configuración Seguridad direccionamiento y Arquitectura Redes, manual de Procedimientos Fibra Óptica, Manual de Procedimientos Radio Enlaces, Manual de Procedimientos de Racks y Cableado Estructurado, Manual de Procedimiento Mantenimiento de Zonas Wifi, Manual de Procedimientos de Telefonía IP, manual de Procedimientos de Estructuras de Soporte de Antenas de Telecomunicaciones, Manual de Procedimientos CCTV -123).
7. TESTING DE SOFTWARE.
8. Diagnóstico MSPI
9. Protocolo de atención MDS-Octubre/2024.
10. Procedimiento desarrollo de aplicaciones Código GSC-PR-01-V2
11. Gestión de roles y responsabilidades MSPI. 20 de abril de 2023.
12. Procedimientos de seguridad de la información versión 1. 2024-2028.
  - Procedimiento para reportar incidentes de seguridad de la información,
  - Procedimiento para el manejo de la información institucional.
  - Procedimiento de gestión de medios removibles.
  - Procedimiento de borrado seguro
  - Procedimiento de trabajo en área seguras
  - Procedimiento de instalación de software
  - Procedimiento de propiedad intelectual y uso legal del software

En página web se verificó la publicación del Activos de Información y Datos abiertos.

## **OBSERVACIONES**

### **Observación No.1. Procedimientos del proceso Tecnologías de la Información y las Comunicaciones**

Una vez revisados los documentos aportados por la Oficina de Tecnologías de la Información y Comunicaciones, se observa lo siguiente: Procedimientos de seguridad de la Información 2024-2028 Versión 1, que incluyen ocho (8)





procedimientos documentados, Manual de Procedimientos para el Datacenter, documento denominado Gestión de roles y responsabilidades MSPI, Manual Área Redes Oficina TIC (Manual de Procedimientos Configuración Seguridad direccionamiento y Arquitectura Redes, manual de Procedimientos Fibra Óptica, Manual de Procedimientos Radio Enlaces, Manual de Procedimientos de Racks y Cableado Estructurado, Manual de Procedimiento Mantenimiento de Zonas Wifi, Manual de Procedimientos de Telefonía IP, manual de Procedimientos de Estructuras de Soporte de Antenas de Telecomunicaciones, Manual de Procedimientos CCTV - 123) sin embargo, los anteriores documentos no se encuentran aprobados por el Sistema Integrado de Gestión-Calidad.

**Respuesta Oficina Tecnologías de la Información y las Comunicaciones.**

*"Una vez leída su observación les queremos indicar que ya se realizó la solicitud a calidad para aprobar dichos documentos se anexa evidencia".*

**Conclusión del Equipo Auditor:**

De acuerdo a la respuesta dada por la Oficina TIC, se confirma la observación y se establece como hallazgo para que se establezcan acciones correctivas que subsanen la situación detectada.

**Observación No.2. Riesgos de gestión del proceso gestión TIC**

Se observó la matriz de riesgos del proceso Tecnologías y Comunicaciones de la Información, sin embargo, no se establecen los riesgos de tal como lo dispone el Departamento Administrativo de la Función Pública DAFP a través de la Guía Versión 6 noviembre/2022, sin embargo, no se tiene evidencia del monitoreo periódico de los riesgos de seguridad de la información que debe realizar la Oficina.

**Respuesta Oficina Tecnologías de la Información y las Comunicaciones.**

*"Dando alcance a su observación nos permitimos anexar Excel para profundizar y detallar esta solicitud, de igual manera estamos verificando y actualizando los campos que sean requeridos para dar cumplimiento al Departamento Administrativo de la Función Pública DAFP".*

**Conclusión del Equipo Auditor:**

Por la anterior respuesta de la Oficina TIC, se confirma la observación y se establece como hallazgo para se establezcan las acciones correctivas pertinentes en el plan de mejoramiento.



### **Observación No.3. Planes del proceso TIC.**

Dentro de la revisión realizada en el proceso auditor no se evidenció un plan de seguridad de la información, su ejecución y monitoreo, de igual forma, pese a que se realizaron sensibilizaciones y capacitaciones del MSPI, no se encontró un plan de Sensibilización, capacitación y comunicaciones

### **Respuesta Oficina Tecnologías de la Información y las Comunicaciones.**

#### ***"Respuesta plan de sensibilización, capacitación y comunicaciones:***

*La política de seguridad de la información que rige para el presente cuatrienio fue aprobada el 01 de octubre del 2024, dentro de la cual en el desarrollo del ítem 6. "SENSIBILIZACIÓN Y COMUNICACIÓN EN SEGURIDAD DE LA INFORMACIÓN", pueden observar que abarca los criterios que inicialmente debe tener dicho plan:*

*Identificación de necesidades*

*Objetivo General y específicos*

*Diseño del programa de concienciación y formación*

*Desarrollo del plan de concienciación y formación*

*Mejoramiento del plan de concienciación y formación*

*Complementando lo anterior, el alcance del ítem 6, establece lo siguiente: "La Alcaldía Municipal de Chía, definirá un "Plan de Comunicación en Seguridad de la Información" a través de la oficina de comunicación interna y externa y la Oficina TIC, donde se planificará anualmente la manera en que se comunicarán recomendaciones de seguridad de la información".*

*Para la implementación de la política de seguridad de la información el primer paso es la socialización, la cual se llevó a cabo a finales del mes de octubre del 2024, teniendo en cuenta la fecha de aprobación de la política de seguridad de la información, la Oficina TIC y según lo establecido y aceptado por comité de gestión y desempeño, la planificación se realizará de manera anual, es decir, que en el primer trimestre del 2025, se estará generando el documento "plan de sensibilización, capacitación y comunicaciones", alineado a los lineamientos establecidos en el ítem 6 de la política de seguridad de la información".*

### **Conclusión del Equipo Auditor:**

Analizada la respuesta dada por la Oficina TIC, en la cual informan que dentro de la Política de Seguridad de la Información abarca los criterios que debe tener el plan, no obstante, el plan de sensibilización, capacitación y comunicaciones no se ha



estructurado como tal para su ejecución, en este sentido, se confirma la observación y se establece como hallazgo para que se establezcan las acciones correctivas pertinentes.

#### **Observación No. 4. Activos intangibles.**

Revisadas las recomendaciones realizadas por la Oficina de Control Interno en el *Informe de verificación normas sobre uso de software y derechos de autor 2023* emitido en marzo de 2024, no se observa que el auditado este atendiendo a lo sugerido. Al indagar con la profesional de la Dirección Financiera sobre las acciones realizadas frente a la actualización de saldos de la cuenta de activos intangibles (softwares), se informa que en el mes de octubre se adelantó reunión con Almacén General y el auditado en el que se establecieron compromisos para depurar la información y actualizar los saldos, sin que a la fecha se obtenga lo solicitado. Lo anterior se constituye en un riesgo al no tener claridad en los valores que deben reportar los estados financieros y que deben ser suministrados por la Oficina Tic's.

#### **Respuesta Oficina Tecnologías de la Información y las Comunicaciones.**

*"Dando respuesta a su observación procedemos a indicar que. Sí se está trabajando en ello debido a que son licencias desde el 2005, al equipo de las TICS, y teniendo en cuenta que las licencias son cargadas a cada funcionario que requiera software específico en muchos casos, el tema de validación es más complejo, por tal motivo y una vez verificado se envió archivo al almacén para realizar la baja respectiva de las mismas, esto teniendo en cuenta que los usuarios suelen perder el acceso a las actualizaciones, el soporte y, a veces, a la capacidad de usarlo por completo las licencias cuando estas caducan o no son renovadas".*

#### **Conclusión del Equipo Auditor:**

De acuerdo a la respuesta dada por la Oficina TIC, se confirma la observación debido a que no desvirtúa la situación encontrada y se establece como hallazgo para que se establezcan acciones correctivas que subsanen la situación detectada.

### **RECOMENDACIONES**

- Adoptar la norma 27001:2022, a fin de proteger los activos de información, a fin de mejorar continuamente su postura de seguridad, aumentar la confianza del cliente y cumplir con requisitos legales y regulatorios en un entorno digital cada vez más centrado en los datos. Tener en cuenta la ISO/IEC 27017 y la ISO/IEC 27018 que complementan la ISO 27001:2022 proporcionando directrices



específicas para la seguridad de la información en la nube y la protección de la información personal identificable (PII), respectivamente.

- Se recomienda que los procedimientos de seguridad de la información sean aprobados por parte del Sistema de Gestión de Calidad de la Entidad.
- Se recomienda la adopción de procedimientos, guías, instructivos, formatos necesarios que conlleven al desarrollo de las políticas inmersas en la Política de Seguridad de la Información.
- Dentro del Plan Institucional de Capacitación (PIC) solicitar la inclusión de capacitaciones en temas de seguridad y privacidad de la información.
- Actualizar el inventario de activos de seguridad y privacidad de la información de la Entidad, clasificarlo de acuerdo con los criterios de disponibilidad, integridad y confidencialidad, su aprobación debe ser mediante Comité de Gestión y Desempeño.
- Gestionar la gestión de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios (riesgos de interrupción) debido a que permiten identificar, analizar, valorar y tratar las amenazas y vulnerabilidades de los activos de información de la entidad, teniendo presente su criticidad y protección.
- Con relación al Decreto 545 de 2024, el cual crea el Comité de Seguridad de la Información se sugiere que se estudie la posibilidad de que las funciones establecidas para este Comité sean asumidas por el Comité de Gestión y Desempeño instancia encargada de tratar estos temas según lo establece el Decreto 1083 de 2015 estas funciones sean llevadas

**ARTÍCULO 2.2.22.3.8. Comités Institucionales de Gestión y Desempeño.** *En cada una de las entidades se integrará un Comité Institucional de Gestión y Desempeño encargado de orientar la implementación y operación del Modelo Integrado de Planeación y Gestión - MIPG, el cual sustituirá los demás comités que tengan relación con el Modelo y que no sean obligatorios por mandato legal.*

(...)

*Los Comités Institucionales de Gestión y Desempeño cumplirán las siguientes funciones:*

(...)

*6. Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información.*



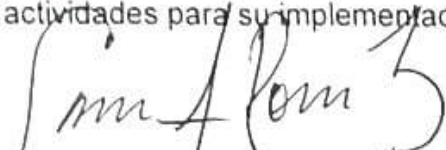
- Se recomienda establecer, implementar, operar, monitorear, revisar, mantener y mejorar continuamente el sistema de gestión de seguridad de la información dentro de la Entidad, realizar seguimiento al estado de implementación y avance.
- Aplicar los controles definidos en el Anexo A de la norma NTC: ISO/IEC 27001 a fin de dar cumplimiento a la Política, así como documentar y tener fácil acceso el inventario de controles. Insumo base importante para mitigar los riesgos de seguridad digital.
- Se recomienda la actualización de los activos de información y su publicación en la página web de acuerdo a requieren.
- Las actividades del Plan de tratamiento de los riesgos de seguridad de la información no tienen definidas fechas puntuales para dar cumplimiento, establecen como fecha de inicio 2024 y fecha de fin 2027, se recomienda que estas actividades sean programadas anualmente a fin de que se puedan establecer metas e indicadores dentro de cada vigencia.
- Tener en cuenta en el desarrollo de los procesos TIC el Marco de Referencia Arquitectura Empresarial -MRAE conjunto de instrumentos claves para implementar la Política de Gobierno Digital, su objetivo es orientar la creación o fortalecimiento de las capacidades de Arquitectura Empresarial, Gestión de Proyectos de TI, Gestión y Gobierno de TI requeridas en los procesos de transformación digital de las entidades del Estado.
- Se sugiere tener en cuenta las recomendaciones dadas por el Departamento Administrativo de la Función Pública establecidas en la evaluación FURAG-MIPG.
- Se recomienda el cumplimiento de la Ley 1712 de 2014 con respecto a la información contenida en la Resolución 1915 de 2018 y sus anexos 1,2 y 3 que contempla condiciones mínimas técnicas, de seguridad digital y otros aspectos de transparencia y acceso a la información pública.

### **CONCLUSIÓN**

Se logró dar cumplimiento al objetivo de la auditoría interna, que se enfocaba en verificar el cumplimiento de la Política de la Seguridad de la Información para lo cual se revisaron todos los documentos que la Oficina TIC realizó dentro del proceso de implementación de las políticas de seguridad de la información y en el Modelo de

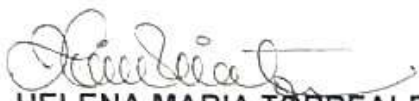


Seguridad y Privacidad de la Información y demás, se concluye que se encuentra en la fase de implementación teniendo en cuenta que las Políticas ya fueron aprobadas por parte del Comité Institucional de Gestión y Desempeño, y se han venido realizado actividades para su implementación y desarrollo.



**CARLOS ANDRÉS RODRÍGUEZ SÁNCHEZ**

Jefe Oficina de Control Interno



**HELENA MARIA TORREALBA VELANDIA.**

Profesional universitario.