MEMORANDO

150

Bogotá D.C., 31 de octubre de 2023

PARA: **Dr. JOSÉ DAVID RIVEROS NÁMEN**
Secretario Distrital de Gobierno

DE: **JEFE OFICINA DE CONTROL INTERNO**

ASUNTO: Remisión informe de seguimiento, implementación del Modelo de Seguridad y Privacidad de la Información - MSPI

Respetado Secretario,

En cumplimiento de las funciones establecidas en la Ley 87 de 1993, del Plan Anual de Auditoria vigencia 2023 y del Decreto 648 de 2017, específicamente del Rol de evaluación y seguimiento, atentamente me permito remitir el informe de seguimiento a la implementación del Modelo de Seguridad y Privacidad de la Información, con el fin de que sea socializado con su equipo de trabajo analizando su contenido y se tomen las respectivas acciones de mejora que a su consideración apliquen para el proceso evaluado.

Esta evaluación se da a conocer al señor Secretario en cumplimiento de lo dispuesto en el Decreto 338 de 2019 *"Por el cual se modifica el Decreto 1083 de 2015, Único Reglamentario del Sector de Función Pública, en lo relacionado con el Sistema de Control Interno y se crea la Red Anticorrupción ARTÍCULO 1 PARÁGRAFO 1. Los informes de auditoría, seguimientos y evaluaciones tendrán como destinatario principal el representante legal de la entidad y el Comité Institucional de Coordinación de Control Interno y/o Comité de Auditoría y/o Junta Directiva, y deberán ser remitidos al nominador cuando este lo requiera".*

De otra parte, me permito informar que el informe en mención se comunicó a la Dirección de Tecnologías e Información con radicado interno No 20231500380493 y se encuentra publicado en la página web https://www.gobiernobogota.gov.co/transparencia/control/reportes-control-interno-sgd

Finalmente, agradecemos la disposición y colaboración de sus equipos de trabajo durante el proceso de evaluación, reiterando nuestro compromiso de asesoría y acompañamiento a todos los procesos de la Entidad.

Cordialmente,

(ORIGINAL FIRMADO)
LADY JOHANNA MEDINA MURILLO
Jefe Oficina de Control Interno

Anexo: Informe de seguimiento, implementación del MSPI
Elaboró: Rosa María Buitrago Barón-Contratista OCI
Aprobó/Revisó: Johana Murillo-Jefe OCI

MEMORANDO

Código 150

Bogotá D.C., 31 de octubre de 2023

PARA: **Dra. OLGA MILENA ARIAS AGUIRRE**
Directora de Tecnologías e Información (E)

DE: **JEFE OFICINA DE CONTROL INTERNO**

ASUNTO: Remisión informe de seguimiento, implementación Modelo de Seguridad y Privacidad de la Información - MSPI.

En desarrollo del Plan anual de Auditoria para la vigencia 2023 y dando cumplimiento a los roles de enfoque hacia la prevención y de evaluación y seguimiento establecidos en el Artículo 17 del Decreto 648 de 2017, se programó y realizó el seguimiento, a la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI. En este sentido, se remiten los resultados del seguimiento, en informe anexo.

Agradecemos la disposición y oportuna atención del seguimiento, implementando acciones orientadas a atender las recomendaciones presentadas.

Cordial saludo,

(ORIGINAL FIRMADO)
LADY JOHANNA MEDINA MURILLO
Jefe Oficina de Control Interno

Anexo: Informe de seguimiento, implementación MSPI

Elaboró: Rosa María Buitrago Barón-Contratista OCI
Aprobó/Revisó: Johana Murillo-Jefe OCI

INFORME DE SEGUIMIENTO, CUMPLIMIENTO E IMPLEMENTACIÓN

Modelo de Seguridad y Privacidad de la Información (MSPI), incluye la verificación de los activos de información, en la Secretaría Distrital de Gobierno.

Destinatarios

- Doctor José David Riveros Námen – Secretario Distrital de Gobierno.
- Ing. Olga Milena Arias Aguirre – Director de Tecnologías e Información (E)

1. Objetivos

1.1 Objetivo general

Verificar el cumplimiento y el grado de implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) del MINTIC, incluye la verificación de los activos de información, en la Secretaría Distrital de Gobierno comparado con la normatividad asociada Decreto 1078 de 2017 y la ISO/IEC 27001 de 2013.

2. Alcance

El presente informe corresponde a la verificación de la información, manuales, procesos y procedimientos que se tienen en la Dirección de Tecnologías de la Información de la SDG orientados a la implementación y el grado de cumplimiento del MSPI durante el primer semestre de la vigencia 2023.

3. Marco normativo o criterios del informe

Cumplimiento de los lineamientos establecidos en la siguiente normativa:

Norma Externa:

Decreto 1078 de 2015. "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".
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 500 de 2021. "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital".
Resolución 001519 de 24 de agosto de 2020. "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".
Norma ISO/IEC 27001 - Norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información.
Manual para la Implementación de la Política de Gobierno Digital. Versión 7 de abril de 2019
CONPES 3854 de abril del 2016. Política de Seguridad Digital.
Documento Maestro del Modelo de Seguridad y Privacidad de la Información. MINTIC. Versión 4 del 28/10/2021.
Documento Inventario y clasificación de activos de información e infraestructura crítica cibernética nacional. MINTIC. Versión 4 del 28/10/2021.

Norma Interna:

GDI-TIC-M004 Manual de Gestión de Seguridad de la información.
GDI-TIC-M006 Manual de Política de Tecnología e Información
GDI-TIC-PL003 Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, vigencia 2023.
GDI-TIC-PL002 Plan de Seguridad y Privacidad de la Información, vigencia 2023.
GDI-TIC-P004 Identificación y Valoración de Activos de Información

4. Equipo auditor:

Rosa María Buitrago Barón - Contratista Oficina de Control Interno

5. Metodología

La Oficina de Control Interno solicitó a la Dirección de Tecnologías e Información mediante memorando radicado No 20231500319093 del 06 de septiembre de 2023 la información que se relaciona a continuación:

- Dar respuesta a la "Lista de verificación sobre los controles del Sistema de Seguridad de la Información de la Secretaría Distrital de Gobierno", de conformidad con la Norma ISO/IEC 27001: 2023 y adjuntar la evidencia respectiva, teniendo en cuenta que, si la respuesta requiere información adicional de otras dependencias, la Dirección de TI deberá coordinar dicha respuesta con el área competente, si es del caso.
- Documento con el resultado de la autoevaluación realizada a la entidad, de la gestión de Seguridad de la y privacidad de la información, revisado y aprobado por la Alta Dirección.
- Documento con el resultado de la herramienta de la encuesta de diagnóstico de seguridad y privacidad de la información, revisado y aprobado por la Alta Dirección.
- Inventario de Activos de Información Consolidado y actualizado a la fecha, en el que se puedan evidenciar los diferentes tipos de activos, no solamente el tipo "información", que se encuentra publicado en el sitio web.
- Conforme a las evidencias aportadas, indicar en qué fase de implementación, se encuentra el Modelo de Seguridad y Privacidad de la Información de la Secretaría Distrital de Gobierno (Implementación, Evaluación, Mejora Continua).

La Dirección de Tecnologías e Información remitió respuesta a la solicitud, mediante memorando radicado No. 20234400325263 del 12 de septiembre de 2023.

Se programó reunión con la Dirección de Tecnologías e Información por Microsoft Teams, el 23 de octubre, con la participación de la Directora de TI (E) y los profesionales a cargo de la implementación del MSPI, en la cual se realizó la validación de las respuestas y evidencias suministradas y solicitando evidencias adicionales, a fin de verificar el grado de avance en la implementación del MSPI y sus controles asociados, en la Secretaría Distrital de Gobierno, de conformidad con la Norma ISO 27001:2023 y el Documento Maestro del Modelo de Seguridad y Privacidad de la Información de MINTIC.

6. Periodo de ejecución

Inicio: 30 de agosto de 2023
Fin: 31 de octubre de 2023

7. Desarrollo

7.1. Verificación implementación controles Sistema de Seguridad de la Información y Modelo de Seguridad y Privacidad de la Información.

Con el fin de realizar el análisis y validación de la existencia y desarrollo de los controles en el marco del Sistema de Gestión de Seguridad de la Información en la SDG basado en la norma ISO27001 de 2013, y el MSPI del MINTIC, se realizó una lista de verificación por componente y/o dominio, como herramienta independiente por parte de esta oficina, lista que fue suministrada al Jefe de la Dirección de Tecnologías e Información, a fin de obtener las respuestas y evidencia suficiente para validar los controles, teniendo en cuenta las siguientes convenciones, a partir de las cuales se determinó el estado de implementación y aplicación de los controles consolidados para cada dominio:

Convenciones Lista de Verificación Controles Norma ISO 27001:2003 y MSP - SDG

Estado	Descripción
Cumple satisfactoriamente	Existe, es gestionado, se está cumpliendo con lo que la norma solicita, está documentado, es conocido y aplicado por todos los involucrados en el SGSI.
Cumple parcialmente	Lo que la norma requiere se está haciendo de manera parcial, se está haciendo diferente, no está documentado, se definió, pero no se gestiona.
No cumple	No existe y/o no se está haciendo.
No aplica	El control no es aplicable para la entidad. En el campo evidencia por favor indicar la justificación respectiva de su no aplicabilidad.

Por consiguiente, se validaron los requerimientos de la norma por dominio de control, a través de la revisión de evidencias y entrevistas por medio de Microsoft Teams con la Dirección de Tecnologías e Información, en donde a nivel general se evidenció que, de un total de 114 controles aplicables para la SDG, el 69% se encuentran implementados, seguido del 29% implementados parcialmente, quedando un 0.8% pendiente por implementar, tal como se detalla a continuación:

Resultados por dominio de Control.

POR DOMINIO DE CONTROL					
NOMBRE DOMINIOS DE CONTROL	CONTROLES QUE APLICAN	IMPLEMENTADOS	PARCIALMENTE	NO CUMPLE	NO APLICA
DOMINIO 5 - POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	2	2	0	0	0
DOMINIO 6 - ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	7	5	2	0	0
DOMINIO 7 - SEGURIDAD DE LOS RECURSOS HUMANOS	6	6	0	0	0
DOMINIO 8 - GESTIÓN DE ACTIVOS	10	7	2	1	0
DOMINIO 9 - CONTROL DE ACCESO	14	5	9	0	0
DOMINIO 10 - CRIPTOGRAFÍA	2	1	1	0	0

DOMINIO 11 - SEGURIDAD FÍSICA Y DEL ENTORNO	15	10	5	0	0
DOMINIO 12 - SEGURIDAD DE LAS OPERACIONES	14	13	1	0	0
DOMINIO 13 - SEGURIDAD DE LAS COMUNICACIONES	7	7	0	0	0
DOMINIO 14 - ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	13	11	2	0	0
DOMINIO 15 - RELACIÓN CON LOS PROVEEDORES	5	4	1	0	0
DOMINIO 16 - GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	7	2	5	0	0
DOMINIO 17 - ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO	4	3	1	0	0
DOMINIO 18 - CUMPLIMIENTO	8	3	5	0	0
	114	79	34	1	0

*En el anexo 1 se puede observar con detalle del estado de cada control, conforme a las evidencias verificadas y análisis realizado, en donde se presentan las observaciones para cada control.

No obstante, sobre el porcentaje de los controles implementados **(69%),** se precisa que dicho porcentaje corresponde a las evidencias y aclaraciones suministradas por la Dirección de Tecnologías e Información para el presente seguimiento, dado que existe una gran diferencia, con respecto a los resultados de la herramienta ***"Instrumento de Identificación de la Línea Base de Seguridad/Modelo de Seguridad y Privacidad de la Información - MSPI"***, aplicada para el segundo trimestre de la vigencia 2023 en la entidad y suministrada, dentro de las evidencias del presente seguimiento, en la cual se identifica que el Nivel de Madurez del Modelo de Seguridad y Privacidad de la Información - MSPI de la SDG ***"No alcanza el Nivel Inicial"*:**

Nivel	Descripción
Inicial	En este nivel se encuentran las entidades, que aún no cuenta con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información
Repetible	En este nivel se encuentran las entidades, en las cuales existen procesos procesos básicos de gestión de la seguridad y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentra gestionados dentro del componente planificación del MSPI.
Definido	En este nivel se encuentran las entidades que tienen documentado, estandarizado y aprobado por la dirección, el modelo de seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados.
Administrado	En este nivel se encuentran las entidades, que cuenten con métricas, indicadores y realizan auditorías al MSPI, recolectando información para establecer la efectividad de los controles.
Optimizado	En este nivel se encuentran las entidades, en donde existe un mejoramiento continuo del MSPI, retroalimentando cualitativamente el modelo.

Fuente: Instrumento de Identificación de la Línea Base de Seguridad – MSPI

Por lo anterior, se recomienda revisar detalladamente la herramienta ***"Instrumento de Identificación de la Línea Base de Seguridad/Modelo de Seguridad y Privacidad de la Información - MSPI"***, teniendo en cuenta la información suministrada para el presente seguimiento y la disponible en el aplicativo Matiz; así como ejecutar ejercicios de auditoria diferentes a los realizados por la Oficina de Control Interno, a fin de garantizar la actualización en el cumplimiento de los requerimientos del Sistema de Seguridad de la Información y Modelo de Seguridad y Privacidad de la Información de la SDG a los que haya lugar, garantizando que la información sobre el estado actual del Modelo de SPI y Sistema de Seguridad de la Información de la SDG sean acordes con su realidad institucional.

Con respecto a los riesgos de seguridad de la información, se evidenció que durante lo corrido de la vigencia 2023, se realizó la actualización de la identificación, valoración y clasificación de los riesgos de seguridad de la información a Nivel Local y a la fecha del presente seguimiento, se encuentran en proceso, el seguimiento y monitoreo de los riesgos en el Nivel Central.

7.2. Identificación y valoración de activos de información.

Se identificó que la Secretaría Distrital de Gobierno, en la documentanción de su Sistema Integrado de Gestión, disponible en el aplicativo Matiz y asociada al proceso Gerencia de TI, cuenta con el ***Manual de Gestión de Seguridad de la Información, numeral 7.1.3*** y ***Procedimiento GDI-TIC-P004 Identificación y Valoración de Activos de Información***, a partir de los cuales se documentan: La Política de Gestión de activos, actividades y puntos de control, para garantizar la responsabilidad, clasificación y manejo de los activos de información en la entidad.

Por consiguiente, se evidenció que para la vigencia 2023, se encuentra en proceso de actualización el Inventario de Activos de Información del Nivel Central, por tanto no fue posible acceder a las evidencias del mismo; Por su parte, para el Nivel Local se suministró el inventario actualizado de los activos de información consolidado, en el que **13 localidades** presentan inventario de activos de información actualizado, con su respectivo código, nombre del activo, descripción del activo, idioma, tipo de activo, tipo de soporte (Análogo, digital, electrónico, descripción soporte, presentación de información), marca, plataforma, nivel de proceso, nombre del proceso, código del proceso /procedimiento, propietario del activo, custodio del activo, responsable de producir la información, frecuencia de generación o actualización de seguridad, tipo de clasificación (Ley 1712 de 2014, Excepciones Ley 1712, Art. 18 y 19, fundamento constitucional o legal, fundamento jurídico de la excepción, tipo de excepción, plazo de clasificación o reserva, Ley 1581 (Contenido de datos personales y sobre menores de 18 años, tipo de dato personal), valoración del activo (Nivel de confidencialidad, nivel de disponibilidad y criticidad, este último presenta error de fórmula para algunos casos), respaldo de información (Se realiza backup, tipo de backup, periodicidad, lugar de almacenamiento), control de acceso (nombres y apellidos, tipo de usuario, nombre cuenta de usuario, rol y/o perfil), permisos (lectura, escritura, eliminación), quien autorizó (Nombre, cargo), dando cumplimiento a los lineamientos internos establecidos.

Sin embargo, no se suministraron evidencias del inventario de activos de información actualizado para las restantes **7 localidades**, por lo que se entiende que se encuentran pendientes de actualización, relacionadas a continuación:

No.	Nombre Localidad
1	Usaquén
3	Santa Fe
5	Usme
7	Bosa
8	Kennedy
14	Mártires
17	Candelaria

1. Hallazgos, Observación o Recomendación (Cuando aplique)

1.1. Transferencia de medios físicos: Se identificó que la SDG, no cuenta con procedimientos y controles documentados para garantizar la protección contra acceso no autorizado, uso indebido o corrupción durante el transporte de los medios que contienen información, incumpliendo con el numeral A8.3.3 de la Norma ISO 27001, situación que promueve la materialización de potenciales riesgos asociados al transporte de los medios que contienen información de uso exclusivo de la entidad.

Por lo anterior, con el fin de que la labor de control interno que realiza esta Oficina, en la Secretaría Distrital de Gobierno, conduzca a las dependencias auditadas hacia la mejora continua de sus procesos y procedimientos, a través del establecimiento de acciones de mejoramiento de su gestión; a partir de los resultados presentados en este informe, la Dirección de Tecnología e Información deberá elaborar y presentar un plan de mejoramiento que permita subsanar las causas de las no conformidades, y atender las oportunidades de mejora, en un plazo no mayor a 15 (quince) días calendario, contados a partir de la notificación de hallazgos por medio del aplicativo Mi Mejora Continua – MIMEC, con base en la publicación de este documento, en la página web de la Secretaría, a través del enlace de la Oficina de Control Interno.

Para la elaboración y presentación de dicho plan se deben tener en cuenta los lineamientos establecidos por la Oficina Asesora de Planeación, en el GCN-M002 Manual para la gestión de planes de mejoramiento, publicado en el Sistema Integrado de Gestión y Calidad; particularmente la política de operación que indica *"Los planes de acción deben ser formulados en su totalidad en un plazo máximo de 15 días calendario contados a partir de la notificación por medio del aplicativo".*

2. Conclusiones

- El Modelo de Seguridad y Privacidad de la la Información de la SDG se encuentra en nivel de madurez ***"no alcanza el Inicial"***, es decir y de acuerdo con los seguimientos anteriores realizados, el Modelo continúa en una etapa de ***"diagnóstico"*** desde hace mas de tres años en la entidad; no obstante, como se indicó anteriormente, de acuerdo a las evidencias aportadas para el presente seguimiento existen controles que en su mayoría se encuentran documentados y cuentan con evidencia de ejecución, por lo que se hace necesaria una revisión exhaustiva y juiciosa para asi determinar con certeza en que nivel de madurez se encuentra la entidad y asi poder desplegar los planes de cierre de brechas necesarios para garantizar su implementación al 100%, en el marco del ciclo PHVA.

- Duante lo corrido de la vigencia 2023, se realizó la actualización de la identificación, valoración y clasificación de los riesgos de seguridad de la información a Nivel Local y a la fecha del presente seguimiento, se encuentran en proceso, el seguimiento y monitoreo de los riesgos en el Nivel Central.

- A la fecha del presente seguimiento, se encuentra en proceso de actualización el Inventario de Activos de Información del Nivel Centra y a Nivel Local 13 localidades presentan inventario de activos de información actualizado, dando cumplimiento a los lineamientos internos establecidos; Sin embargo, no se suministraron evidencias del inventario de activos de información actualizado para las restantes 7 localidades, por lo que se entiende que se encuentran pendientes de actualización.

3. Recomendaciones

Conforme a las auditorías y seguimientos anteriores realizados a la implementación del MSPI y Sistema de Segurida de la Informacion en la SDG, se reiteran algunas de las recomendaciones indicadas y se relacionan algunas novedades conforme a la entrevista y revisión documental realizada por la OCI, para el presente seguimiento:

- La entidad deberá disponer de un oficial o responsable de seguridad de la información, designado por el Comité de Gestión y Desempeño, a fin de garantizar la correcta documentación e implementación de las politicas y procedimientos del Sistema de Seguridad de la Información en la Entidad y el contacto permanente con las autoridades de seguridad de la información.

- Continuar con la implementación de la estrategia de comunicaciones relacionada con los temas de seguridad y privacidad de la información dirigido a todos los funcionarios, contratistas y demás miembros externos asociados a la entidad, con el fin de evidenciar que ocurre en caso que no se sigan los protocolos establecidos.

- Continuar el seguimiento y monitoreo de los riesgos de seguridad de la información, previsto para la vigencia 2023 en el Nivel Central, verificando la eficacia y efectividad de los controles internos establecidos para garantizar la no materización de los riesgos de seguridad de la información y/o actualización de las zonas de riesgo residual en caso de contar con potenciales materializaciones.

- Continuar la actualización de los activos de información del Nivel Central y de las Alcaldías Locales en en las que se encuentra pendiente realizar dicha actualización, a fin de garantizar la actualización de los responsables y/o custodios de los activos de información y cumplimiento de los demás lineamientos establecidos para la SDG.

- Revisar detalladamente la herramienta "Instrumento de Identificación de la Línea Base de Seguridad/Modelo de Seguridad y Privacidad de la Información - MSPI", teniendo en cuenta la información suministrada para el presente seguimiento y la disponible en el aplicativo Matiz; así como ejecutar ejercicios de auditoria diferentes a los realizados por la Oficina de Control Interno, a fin de garantizar la actualización en el cumplimiento de los requerimientos del Sistema de Seguridad de la Información y Modelo de Seguridad y Privacidad de la Información de la SDG a los que haya lugar, garantizando que la información sobre el estado actual del Modelo de SPI y Sistema de Seguridad de la Información de la SDG sean acordes con su realidad institucional.

Conforme a los dominios se realizan las siguientes observaciones:

- **Dominio 6. Organización de la seguridad de la información:** Se debe establecer el líder y/o responsable de la implementación del modelo, designado por el Comité Institucional de Gestión y Desempeño, por lo cual se recomienda revisar el Manual de Funciones asignar este rol de oficial de cumplimiento en la SDG.

- **Dominio 8. Gestión de activos:** La entidad debe identificar sus activos relevantes, este inventario debe ser exacto, actualizado, alineado con la SDG para cada uno de los activos identificados, el propietario del activo debe ser asignado y la clasificación debe ser identificada; por tanto se recomienda dar cumplimiento con la directriz para el Nivel Central y las 7 Localidades que se encuentran pendientes de su actualización.

  De igual manera, se requiere la implementación de procedimientos para garantizar la protección contra acceso no autorizado, uso indebido o corrupción durante el transporte de los medios que contienen información, de manera tal que se garantice el transporte seguro de los medios que contienen i nformación de la entidad.

- **Dominio 9. Control de acceso:** Es importante actualizar la matriz de acceso de los activos, implementar la matriz de acceso en las plataformas de la entidad.

  Si bien, la entidad cuenta con una mesa de servicios a través de la cual gestiona el registro de sus usuarios, no se cuenta con un procedimiento formal establecido para garantizar la documentación de controles inherentes a la gestión de usuarios, específicamente con los accesos requeridos, teniendo en cuenta la autorización previa.

  Establecer un procedimiento formal establecido que de cuenta de los controles documentados para restringir y controlar la asignación y uso de derechos de acceso privilegiado.

Implementar un procedimiento con políticas de operación y controles documentados para asignación de autenticación secreta, con asignación de claves temporales y que obligue a que el personal realice el cambio de la clave temporal asignada, garantizando el acceso exclusivo al personal autorizado.

Implementar un procedimiento formal que de cuenta de los controles documentados para garantizar que los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se retiren al terminar su empleo, contrato o acuerdo, o se ajusten cuando se hagan cambios, por lo que se recomienda documentar dichos controles en un procedimiento formal.

Implementar las acciones necesarias para exijor y controlar que los usuarios realicen el cambio de la autenticación secreta temporal asignada.

Implementar las acciones necesarias con el fin de que las herramientas utilizadas por la SDG para el control de acceso, se encuentran sincronizadas en su totalidad con el Directorio Activo, garantizando el control de acceso a la información.

Garantizar que todas las aplicaciones cuentan con contraseña asignada para su uso y no se acceda a las mismas de forma directa, en cumplimiento con lo establecido en el Manual de Seguridad de la Información, numeral 7.1.4.6.1

Documentar e implementar instructivos y guías para controlar la instalación de software en los sistemas operativos, en cumplimiento con el Manual de Seguridad de la Información GDI TIC-M004, numeral 7.1.7.9.

Garantizar que el GDI-TIC-IN005 Instrucciones control de versiones y despliegue de sistemas de información, se encuentre disponible para la consulta en el aplicativo Matiz.

- **Dominio 10. Criptografía:** Actualizar la politica de criptografía, establecida en el Manual de Seguridad de la Información, numeral 7.1.5, a fin de garantizar que se incluyan directrices para el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.

- **Dominio 11. Seguridad física y del entorno:** De acuerdo a lo informado por el área, para el Nivel Central, las personas autorizadas para el acceso al Datacenter y cuartos eléctricos, cuentan con una targeta de acceso; no obstante, la ubicación de dichas targetas es de conocimiento general y son de fácil acceso, sumado a que no se cuenta con un responsable que administre el Datacenter y no se deja registro en la bitácora de ingreso al Datacenter, así mismo, si bien existe servicio de vigilancia mediante cámaras, dicho servicio es insuficiente, dado que se encuentran instalaciones sin cámaras, como el archivo central, archivo del área de Talento Humano y archivo de contratación, sumado a que el acceso a dichos archivos no se encuentra registringido; de igual manera el área de Servicio al Ciudadano se encuentra ubicada en una salida emergencia, no siendo una zona segura ni para el personal del área, ni para toda la comunidad institucional. por su parte para el Nivel Local, no todas las alcaldias cuentan con controles de acceso a los cuartos técnicos, por lo que se recomienda implementar las medidas necesarias a fin de garantizar la seguridad física y del entorno en todas las instalaciones de la Entidad.

- **Dominio 12. Seguridad de las operaciones:** Si bien las herramientas con las que cuenta la entidad permiten la trazabilidad de eventos y actividades realizadas, de acuerdo a lo informado por el área no se toman decisiones frente a dichos registros, por lo que se recomienda implementar los planes de acción a los que haya lugar, en virtud de los reportes de eventos generados de las diferentes herramientas que se usan en la identifican, a fin de garantizar la mejora continúa del MSPI y SGSI de la entidad.

- **Dominio 14. Adquisición, desarrollo y mantenimiento de sistemas:** Realizar la supervisión y seguimiento permanente a la actividad de desarrollo de sistemas contratados externamente, dejando los registros sobre las re pruebas efectuadas, para garantizar la no afectación a la infraestructura tecnológica de la entidad.

- **Dominio 15. Relaciones con los proveedores:** Documentar la gestion delos cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y las mejoras de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos de negocio involucrados, y la revaluación de los riesgos.

- **Dominio 16. Gestión de incidentes de seguridad de la información:** Si bien se cuenta con un procedimiento de atención de incidentes de seguridad de la información; no se suministraron evidencias de los reportes de incidentes generados en la entidad, por tanto se recomienda salvaguardar los registros y trazabilidad de los incidentes generados en la entidad, así como evaluar dichos incidentes a fin de implementar las acciones correctivas y de mejora necesarias para garantizar la no repetición y mejora del Sistema.

  Implementar las acciones necesarias para garantizar que contratistas y funcionarios reporten oportunamente los incidentes de información que se presenten.

- **Dominio 17. Aspectos de seguridad de la información de la gestión de continuidad de negocio:** Verificar a intervalos regulares, los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas, garantizando el registro de las verificaciones efectuadas.

- **Dominio 18. Cumplimiento:** Al decidir sobre la protección de los registros, se debe considerar la correspondiente clasificación basado en sistema de clasificación. Los controles específicos y las responsabilidades individuales para satisfacer estos requisitos deberían ser definidos y documentados. Realizar una revisión periódica de la legislación aplicable plasmada en el documento de metodología de identificación y clasificación de activos. Se deben revisar pruebas de penetración o evaluaciones de vulnerabilidad, se debe tener precaución ya que tales actividades podrían conducir a un compromiso de la seguridad del sistema. Se debe cumplir con las auditorías internas anuales para el cumplimiento de seguridad de la información.

(ORIGINAL FIRMADO)

Elaborado por		**Revisado y Aprobado por**	
ROSA MARÍA BUITRAGO BARÓN **Profesional Líder Oficina de Control Interno.**		**LADY JOHANA MEDINA MURILLO** **Jefe Oficina de Control Interno.**	
Fecha:	31 de octubre de 2023	**Fecha:**	31 de octubre de 2023

Anexo – Lista Verificación Controles Sistema de Seguridad de la Información y MSPI

CRITERIO / CONTROL		PREGUNTA DEL CONTROL	ÁREA RESPONSABLE	VALORACION	OBSERVACIÓN / CONTROL INTERNO
A5	**POLÍTICAS DE LA SEGURIDAD DE LA INFORMACION**				
A5.1	Orientación de la dirección para la gestión de la seguridad de la información				
Objetivo: Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes					
A5.1.1	Políticas para la seguridad de la información	Se ha definido un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	El Manual de Políticas de Seguridad de la Información, se encuentra actualizado al 28 de marzo de 2023 en su versión 8, publicado en el aplicativo Matiz, se suministraron diferentes sensibilizaciones realizadas al personal en seguridad de la información.

A5.1.2	Revisión de las políticas para la seguridad de la información.	Durante la vigencia 2023, se han revisado a intervalos planificados las políticas para la seguridad de la información, teniendo en cuenta cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	Si bien, se evidencia la actualización del Manual de Seguridad de la Información GDI-TIC-M004. Versión 8 del 28 de marzo de 2023, en el que Se actualizan los capítulos 7.1.4.5, 7.1.8.3, 7.1.8.6, 7.1.10.1 en los que se complementan los lineamientos con relación a la responsabilidad de usuarios, acuerdo de transferencia de información, acuerdo de confidencialidad y seguridad de la información en relación con los proveedores; e inclusión en el Ítem 12 documentos relacionados del formato de transferencia de información aprobado por la OAP y publicado en Matiz.
A6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION**				
A6.1	Organización interna				
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.					

A6.1.1	Roles y responsabilidades para la seguridad de la información	Se han definido y asignado todas las responsabilidades de la seguridad de la información en la Secretaria Distrital de Gobierno?	Dirección de Tecnologías e Información	Cumple parcialmente	Si bien los roles y responsabilidades se encuentran incorporados en el Manual de Seguridad de la Información GDI-TIC-M004. Versión 8 del 28 de marzo de 2023, numeral 7.1.1.1, de acuerdo con lo informado por el área, no se cuenta con responsable designado para la Seguridad de la Información; así mismo, dentro de los roles y responsabilidades no se encuentran desagregadas las responsabilidades de seguridad de la información en los diferentes niveles (Directivo, de procesos y operativos), como tampoco se evidencia que dichos roles y responsabilidades hayan sido adoptados por acto administrativo, como lo establece el documento Modelo de Seguridad y Privacidad de la Información de MINTIC. Por tanto, se recomienda establecer los roles y responsabilidades en seguridad de la información por nivel y meditante acto administrativo y que el Comité de Gestión y Desempeño designe al responsable de la Seguridad de la Información, en cumplimiento con las directrices establecidas en el Manual y normatividad vigente.
A6.1.2	Separación de deberes	Los deberes y áreas de responsabilidad en conflicto se encuentran separados, para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la Secretaría Distrital de Gobierno - SDG?	Dirección de Tecnologías e Información	Cumple parcialmente	En el Manual de Seguridad de la Información GDI-TIC-M004. Versión 8 del 28 de marzo de 2023, numeral 7.1.1.2 se contemplan las directrices para la separación de deberes. Se cuenta con el inventario de activos de información actualizado del Nivel Local, que da cuenta de los roles y permisos (lectura, escritura, eliminación); Sin embargo no fue posible acceder al inventario de activos del Nivel Central, por cuanto, de acuerdo con lo informado por el área se encuentra en proceso de actualización.

A6.1.3	Contacto con las autoridades	Durante la vigencia 2023 se ha mantenido contacto apropiado con las autoridades pertinentes?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	En el Manual de Seguridad de la Información GDI-TIC-M004. Versión 8 del 28 de marzo de 2023, numeral 7.1.1.3 se contemplan las directrices para realizar el contacto con las autoridades; No se suministraron los registros del contacto con el C-SIRT (Comando de Siber Segurridad) y Alta Consejería - Se informa que el contacto se realiza vía whastsap (Grupo que lo administra la Alta Consejería)
A6.1.4	Contacto con grupos de interés especial	Durante la vigencia 2023, se ha mantenido contacto apropiado con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	si bien en el Manual de Seguridad de la Información GDI-TIC-M004. Versión 8 del 28 de marzo de 2023, numeral 7.1.1.4 se contemplan las directrices para establecer contacto con los grupos de interés, el responsable de la Seguridad de la Información en la SDG no ha sido designado por el Comité de Gestión y Desempeño para que mantenga dicho contacto permanentemente; no obstante, algunos profesionales del área mantienen la comunicación con la inscripción en diferentes grupos para la seguridad de la información
A6.1.5	Seguridad de la información en la gestión de proyectos.	En la SDG, la seguridad de la información se encuentra contemplada en la gestión de proyectos, independientemente del tipo de proyecto?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	En el Manual de Seguridad de la Información GDI-TIC-M004. Versión 8 del 28 de marzo de 2023, numeral 7.1.1.5 se contemplan las directrices para la Seguridad de la Información en gestión de proyectos
A6.2	Dispositivos móviles y teletrabajo				
Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles					
A6.2.1	Política para dispositivos móviles	Se ha adoptado una política y medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	En el Manual de Seguridad de la Información GDI-TIC-M004. Versión 8 del 28 de marzo de 2023, numeral 7.1.1.6.1. se establece la Política para Dispositivos Móviles.

A6.2.2	Teletrabajo	Se ha implementado una política y medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	En el Manual de Seguridad de la Información GDI-TIC-M004. Versión 8 del 28 de marzo de 2023, numeral7.1.1.6.2, se establecen las directrices para realizar trabajo Inteligente, que incluye la opción de teletrabajo.
A7	**SEGURIDAD DE LOS RECURSOS HUMANOS**				
A7.1	Antes de asumir el empleo				
Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.					
A7.1.1	Selección	Las verificaciones de los antecedentes de todos los candidatos a un empleo u contrato se llevan a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes y son proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso y a los riesgos percibidos?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	Existen procedimientos para la selección de personal y contratistas, en los procesos de Gestión del Talento Humano y Contratación. Adicionalmente en el Manual de Seguridad de la Información GDI-TIC-M004. Versión 8 del 28 de marzo de 2023, numeral 7.1.13.1 se establecen lineamientos para el cumplimiento de requisitos legales y contractuales.
A7.1.2	Términos y condiciones del empleo	Los acuerdos con empleados y contratistas establecen sus responsabilidades y las de la organización en cuanto a la seguridad de la información?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	En las condiciones generales de los contratos se establecen obligaciones relacionadas con la con la reserva y confidencialidad de la información, así como para la no instalación de software sin la autorización de la Dirección de TI.
A7.2	Durante la ejecución del empleo				
Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.					

A7.2.1	Responsabilidades de la dirección	Durante la vigencia 2023, la dirección ha exigido a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos en la SDG?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	Se identificaron evidencias de sensibilizaciones en seguridad de la información realizadas en los meses de abril, mayo, junio. julio y agosto.
A7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.	Durante la vigencia 2023, todos los empleados de la organización, incluido los contratistas, han recibido la educación y formación en toma de conciencia apropiada, actualizaciones regulares sobre las políticas y procedimientos en seguridad de la información de la SDG, pertinentes para su cargo y/o contrato?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	Se identificaron evidencias de sensibilizaciones en seguridad de la información realizadas en los meses de abril, mayo, junio. julio y agosto.
A7.2.3	Proceso disciplinario	Se cuenta con un proceso formal y comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	Se cuenta con el Procedimiento de Control Disciplinario Ordinario 2310430 -PR-029 V5, a partir del cual se inicia el procedimiento disciplinario de acuerdo con la queja proveniente del ciudadano, informe suscrito por servidor público, de oficio, de anónimo aplicable para los eventos en los que hubiere violación a la Seguridad de la Información en la SDG.
A7.3	Terminación y cambio de empleo				
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo					
A7.3.1	Terminación o cambio de responsabilidades de empleo	Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de empleo se han definido y comunicado al empleado o contratista y se ha garantizado su cumplimiento?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	En el Manual de Seguridad de la Información GDI-TIC-M004. Versión 8 del 28 de marzo de 2023, numeral 7.1.2.3 se establecen lineamientos para la seguridad de la información cuando se termine el vínculo con la entidad y/ o el contrato. Adicionalmente, en las condiciones generales del contrato se establecen obligaciones específicas relacionadas con la Seguridad de la Información.
A8	**GESTION DE ACTIVOS**				
A8.1	Responsabilidad por los activos				

Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección adecuadas.					
A8.1.1	Inventario de activos	Se ha identificado los activos asociados con información e instalaciones de procesamiento de información, por ende se cuenta con el inventario de activos de información actualizado?	Dirección de Tecnologías e Información	Cumple parcialmente	Dentro de las evidencias aportadas se evidencia la identificación de activos de información a Nivel Local (13 localidades) y sobre el Nivel Central se informa que se encuentra en proceso de actualización, aún no está finalizado
A8.1.2	Propiedad de los activos	Los activos mantenidos en el inventario cuentan con un propietario asignado?	Dirección de Tecnologías e Información	Cumple parcialmente	Dentro de las evidencias aportadas solamente se evidencian la identificación de activos de información a Nivel Local (13 Localidades) los cuales cuentan con su respectivo propietario asignado.
A8.1.3	Uso aceptable de los activos	Se han identificado, documentado e implementado reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	Se cuenta con el procedimiento GDI-TIC-P004 Identificación y Valoración de Activos de información. Versión 3 del 26/09/2023, en el que se establecen reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
A8.1.4	Devolución de activos	Se ha garantizado que todos los empleados y usuarios de partes externas deban devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	En el Manual de Seguridad de la Información GDI-TIC-M004. Versión 8 del 28 de marzo de 2023, numeral 7.1.2.3 se establecen lineamientos para la seguridad de la información cuando se termine el vínculo con la entidad y/ o el contrato. Adicionalmente, se cuenta con el procedimiento de paz y salvo que fue automatizado y se gestiona a través del aplicativo HOLA.
A8.2	Clasificación de la información				
Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.					

A8.2.1	Clasificación de la información	La información se ha clasificado en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	Se cuenta con el procedimiento GDI-TIC-P004 Identificación y Valoración de Activos de información. Versión 3 del 26/09/2023, en el que se establecen directrices para la clasificación de la información; se evidenció en el Inventario de Activos del Nivel Local la valoración de los activos de información respecto a los niveles de: Confidencialidad, Integridad, Disponibilidad y Criticidad (Este último en algunos casos presenta error y no es posible su visualización); sin embargo, no fue posible constatar el diligenciamiento para dichos niveles en el inventario de activos del Nivel Central, por cuanto no fue suministrado, dado que se encuentra en proceso de actualización.
A8.2.2	Etiquetado de la información	Se ha desarrollado e implementado un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la SDG?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	Se cuenta con el procedimiento GDI-TIC-P004 Identificación y Valoración de Activos de información. Versión 3 del 26/09/2023, en el que se establecen directrices para el etiquetado de la información, de conformidad con la clasificación establecida.
A8.2.3	Manejo de activos	Se han desarrollado e implementado procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la SDG?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	Se cuenta con el procedimiento GDI-TIC-P004 Identificación y Valoración de Activos de información. Versión 3 del 26/09/2023, en el que se establecen directrices para la clasificación de la información, conforme al esquema establecido.
A8.3	Manejo de medios				
Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios					

A8.3.1	Gestión de medio removibles	Se han implementado procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la SDG?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	En el Manual de Seguridad de la Información GDI TIC-M004, numeral 7.1.7.6 y 7.1.7.10 se establecen lineamientos para la protección contra software malicioso y gestión de vulnerabilidades técnicas, en virtud de las cuales y mediante correo electrónico del 18/05/2023, la DTI informó sobre el bloqueo del uso de medios removibles (USB) en la SDG, como medida de protección de la información y plataforma tecnológica de la SDG.
A8.3.2	Disposición de los medios	Se han implementado procedimientos para disponer en forma segura de los medios cuando ya no se requieran en la entidad?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	La SDG se acoge a la Resolución No. DDC-000001 del 30 de septiembre de 2019 por la cual se expide el Manual de Procedimientos Administrativos y Contables para el manejo y control de los bienes en las Entidades de Gobierno Distritales, numerales 5.2.5 Retiro de Software que establece el procedimiento para determinar los Software tipificados como no útiles u obsoletos y como inservibles; 5.3.5 Destrucción, que establece el procedimiento para destruir aquellos bienes tipificados como inservibles.
A8.3.3	Transferencia de medios físicos	Se han implementado procedimientos para garantizar la protección contra acceso no autorizado, uso indebido o corrupción durante el transporte de los medios que contienen información?	Dirección de Tecnologías e Información	No cumple	No se evidenciaron procedimientos para garantizar la protección contra acceso no autorizado, uso indebido o corrupción durante el transporte de los medios que contienen información de la SDG
A9	**CONTROL DE ACCESO**				
A9.1	Requisitos del negocio para el control de acceso				
Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.					

A9.1.1	Política de control de acceso	Se ha establecido, documentado y revisado la política de control de acceso con base en los requisitos del negocio y de la seguridad de la información de la SDG?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	En el Manual de Seguridad de la Información GDI-TIC-M004. Versión 8 del 28 de marzo de 2023, numeral 7.1.4.1 se establecen lineamientos sobre el control de acceso a la información de la SDG, en cumplimiento con la normatividad vigente y requisitos propios de la entidad.
A9.1.2	Acceso a redes y a servicios en red	Se cuenta con controles documentados que permitan acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	En el Manual de Seguridad de la Información GDI-TIC-M004. Versión 8 del 28 de marzo de 2023, numeral 7.1.4.1 se establecen lineamientos sobre el control de acceso a la información de la SDG, en cumplimiento con la normatividad vigente y requisitos propios de la entidad. la entidad cuenta con una mesa de servicios a través de la cual gestiona las solicitudes de acceso a la red.
A9.2	Gestión de acceso de usuarios				
Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.					
A9.2.1	Registro y cancelación del registro de usuarios	Se cuenta con un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	la entidad cuenta con una mesa de servicios a través de la cual gestiona el registro de sus usuarios y el procedimiento Gestión de Requerimientos de TI GDI-TIC-P001.
A9.2.2	Suministro de acceso de usuarios	Se cuenta con un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios?	Dirección de Tecnologías e Información	Cumple parcialmente	Si bien, la entidad cuenta con una mesa de servicios a través de la cual gestiona el registro de sus usuarios, no se cuenta con un procedimiento formal establecido para garantizar la documentación de controles inherentes a la gestión de usuarios, específicamente con los accesos requeridos, teniendo en cuenta la autorización previa.

A9.2.3	Gestión de derechos de acceso privilegiado	Se cuenta con controles documentados para restringir y controlar la asignación y uso de derechos de acceso privilegiado?	Dirección de Tecnologías e Información	Cumple parcialmente	Si bien en el Manual de Seguridad de la Información GDI-TIC-M004. Versión 8 del 28 de marzo de 2023, numeral 7.1.4.3 se establecen lineamientos generales para la gestión de derechos de acceso privilegiado, no se cuenta con un procedimiento formal establecido que de cuenta de los controles documentados para restringir y controlar la asignación y uso de derechos de acceso privilegiado.
A9.2.4	Gestión de información de autenticación secreta de usuarios	Se cuenta con un procedimiento a través del cual se controle la asignación de información de autenticación secreta?	Dirección de Tecnologías e Información	Cumple parcialmente	No se cuenta con un procedimiento formal establecido con políticas de operación y controles documentados para asignación de autenticación secreta, con asignación de claves temporales y que obligue a que el personal realice el cambio de la clave temporal asignada, garantizando el acceso exclusivo al personal autorizado.
A9.2.5	Revisión de los derechos de acceso de usuarios	Se cuenta con controles documentados para garantizar que los propietarios de los activos revisen los derechos de acceso de los usuarios, a intervalos regulares?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	En el Manual de Seguridad de la Información GDI-TIC-M004. Versión 8 del 28 de marzo de 2023, numeral 7.1.3.1se establecen lineamientos generales sobre la responsabilidad de los activos de información otorgados.

A9.2.6	Retiro o ajuste de los derechos de acceso	Se cuenta con controles documentados para garantizar que los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se retiren al terminar su empleo, contrato o acuerdo, o se ajusten cuando se hagan cambios?	Dirección de Tecnologías e Información	Cumple parcialmente	En el Manual de Seguridad de la Información GDI-TIC-M004. Versión 8 del 28 de marzo de 2023, numeral 7.1.3.1 se establecen lineamientos generales sobre la responsabilidad de los activos de información, no se cuenta con un procedimiento formal establecido que de cuenta de los controles documentados para garantizar ue los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se retiren al terminar su empleo, contrato o acuerdo, o se ajusten cuando se hagan cambios.
A9.3	Responsabilidades de los usuarios				
Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.					
A9.3.1	Uso de información de autenticación secreta	Se ha exigido a los usuarios que cumplan las prácticas de la SDG para el uso de información de autenticación secreta?	Dirección de Tecnologías e Información	Cumple parcialmente	Si bien, en el Manual de Seguridad de la Información GDI-TIC-M004. Versión 8 del 28 de marzo de 2023, numeral 7.1.4.5 se establecen lineamientos sobre la responsabilidad de los usuarios y de acuerdo a las evidencias aportadas se han realizado socializaciones al personal sobre la Seguridad de la Información, no se exige y controla que los usuarios realicen el cambio de la autenticación secreta temporal asignada.
A9.4	Control de acceso a sistemas y aplicaciones				
Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.					
A9.4.1	Restricción de acceso a la información	El acceso a la información y a las funciones de los sistemas de las aplicaciones se encuentra restringido de acuerdo con la política de control de acceso?	Dirección de Tecnologías e Información	Cumple parcialmente	Las herramientas utilizadas por la SDG para el control de acceso, en virtud de la política establecida, no se encuentran sincronizadas en su totalidad con el Directorio Activo, lo que dificulta la restricción a la información.

A9.4.2	Procedimiento de ingreso seguro	El acceso a sistemas y aplicaciones se encuentra controlado mediante un proceso de ingreso seguro, conforme a la política de control de acceso?	Dirección de Tecnologías e Información	Cumple parcialmente	Según lo manifestado por el área no todas las aplicaciones cuentan con contraseña asignada para su uso, por lo que se realiza de forma directa, situación que va en contravía con lo establecido en el Manual de Seguridad de la Información, numeral 7.1.4.6.1 "*La Dirección de Tecnologías e Información con el apoyo de los líderes funcionales, debe velar porque los servicios brindados por las aplicaciones y sistemas de información sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico, teniendo en cuenta la matriz de roles, perfiles y la matriz de control de acceso para cada sistema de información*".
A9.4.3	Sistema de gestión de contraseñas	Se cuenta con sistemas de gestión de contraseñas interactivos, que aseguran la calidad de las contraseñas?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	En el manual de Seguridad de la Información GDI TIC-M004, numeral 7.1.4.4 se establecen lineamientos para la gestión de contraseñas y su asignación se realiza a través de la Mesa de Ayuda.
A9.4.4	Uso de programas utilitarios privilegiados	Se cuenta con controles documentados para restringir estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones?	Dirección de Tecnologías e Información	Cumple parcialmente	En el manual de Seguridad de la Información GDI TIC-M004, numeral 7.1.7.9 se establecen lineamientos para la instalación de software en los sistemas operativos y específicamente se establece que "*La Dirección de Tecnologías e Información - DTI, debe designar responsables y establecer instructivos y guías para controlar la instalación de software en los sistemas operativos*"; sin embargo, no se identificaron dichos instructivos y guías formalizados en el aplicativo Matiz.

A9.4.5	Control de acceso a códigos fuente de programas	Se cuenta con controles documentados para restringir el acceso a los códigos fuente de los programas?	Dirección de Tecnologías e Información	Cumple parcialmente	En el manual de Seguridad de la Información GDI TIC-M004, numeral 7.1.4.6.2 se establecen lineamientos para el control de acceso al código fuente, en donde se indica "*La Dirección de Tecnologías e Información debe aplicar las políticas de control de acceso contempladas para el ingreso a los repositorios en donde se ubique el código fuente y aplicar el GDI-TIC-IN005 Instrucciones control de versiones y despliegue de sistemas de información*"; sin embargo, dicho instructivo no se encuentra disponible para la consulta en el aplicativo Matiz.
A10	**CRIPTOGRAFIA**				
A10.1	Controles criptográficos				
Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o la integridad de la información					
A10.1.1	Política sobre el uso de controles criptográficos	Se ha formulado e implementado una política sobre el uso de controles criptográficos para la protección de la información?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	En el manual de Seguridad de la Información GDI TIC-M004, numeral 7.1.5 se establece la Política de Criptografía, en la que se establecen controles criptográficos para los enlaces de comunicaciones, acceso remoto, transmisión de información Pública Reservada, Pública Clasificada, Pública / Pública, cuando sea necesario, para el aseguramiento de información basado en la evaluación de riesgos; Los controles criptográficos se encuentran incluidos en el listado de software autorizado y no se permite el uso de herramientas para controles criptográficos diferentes a los autorizados por la entidad

A10.1.2	Gestión de llaves	Se ha implementado una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida?	Dirección de Tecnologías e Información	Cumple parcialmente	En el manual de Seguridad de la Información GDI TIC-M004, numeral 7.1.5 se establece la política de Criptografía, en la que se establecen controles criptográficos para los enlaces de comunicaciones, acceso remoto, transmisión de información Pública Reservada, Pública Clasificada, Pública / Pública, cuando sea necesario, para el aseguramiento de información basado en la evaluación de riesgos; Sin embargo, dentro de dicha política no se establecen directrices para el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.
A11	**SEGURIDAD FISICA Y DEL ENTORNO**				
A11.1	Áreas seguras				
Objetivo: Prevenir el acceso físico no autorizado, el daño e la interferencia a la información y a las instalaciones de procesamiento de información de la organización.					
A11.1.1	Perímetro de seguridad física	Se han definido y usado perímetros de seguridad, para proteger áreas que contengan información confidencial o critica, e instalaciones de manejo de información?	Dirección de Tecnologías e Información	Cumple parcialmente	De acuerdo a lo informado por el área, para el Nivel Central, las personas autorizadas para el acceso al Datacenter y cuartos eléctricos, cuentan con una tarjeta de acceso; no obstante, la ubicación de dichas tarjetas es de conocimiento general y son de fácil acceso, sumado a que no se cuenta con un responsable que administre el Datacenter, por su parte para el Nivel Local, no todas las alcaldías con controles de acceso a los cuartos técnicos.

A11.1.2	Controles de acceso físicos	Las áreas seguras se encuentran protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado?	Dirección de Tecnologías e Información	Cumple parcialmente	De acuerdo con lo informado por el área, para el Nivel Central, del acceso al Datacenter, no se está dejando registro en la bitácora de ingreso y a Nivel Local, no se cuentan con controles de ingresos para algunos cuartos técnicos.
A11.1.3	Seguridad de oficinas, recintos e instalaciones.	Se ha diseñado y aplicado la seguridad física para oficinas, recintos e instalaciones?	Dirección de Tecnologías e Información	Cumple parcialmente	De acuerdo con lo informado por el área, si bien se cuenta con personal de servicio de vigilancia, existe servicio de vigilancia mediante cámaras las cuales son insuficientes, dado que se encuentran instalaciones sin dichas cámaras, como el archivo central, archivo del área de Talento Humano y archivo de contratación, sumado a que el acceso a dichos archivos no se encuentra restringido; situación que va en contravía con la política de seguridad física del entorno, establecida en el manual de Seguridad de la Información GDI TIC-M004, numeral 7.1.6 "*La Secretaría Distrital de Gobierno, proveerá la implantación y velará por la efectividad de los mecanismos de seguridad física y control de acceso a las instalaciones de la Entidad y a las áreas de procesamiento de información, que aseguren el perímetro de sus instalaciones. Así mismo, controlará las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas*"

A11.1.4	Protección contra amenazas externas y ambientales.	Se ha diseñado y aplicado protección física contra desastres naturales, ataques maliciosos o accidentes?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	La SDG cuenta con los siguientes procedimientos: GCO-GTH-P003 Procedimiento identificación de peligros, evaluación y valoración de los riesgos en el sistema SGSST; GCO-GTH-P004 Procedimiento de prevención, preparación y respuesta ante emergencias que se presentan en la SDG; GCO-GTH-P005 Reporte e investigación de incidentes y accidentes de trabajo; GDI-TIC-P008 Gestión de incidentes; GDI-TIC-P009 Gestión de incidentes de Seguridad de la información.
A11.1.5	Trabajo en áreas seguras.	Se han diseñado y aplicado procedimientos para trabajo en áreas seguras?	Dirección de Tecnologías e Información	Cumple parcialmente	Si bien se cuenta con el GCO-GTH-P003 Procedimiento identificación de peligros, evaluación y valoración de los riesgos en el sistema SGSST; de acuerdo con lo informado, el área de Servicio al Ciudadano se encuentra ubicada en una salida emergencia, no siendo una zona segura ni para el personal del área, ni para toda la comunidad institucional.
A11.1.6	Áreas de carga, despacho y acceso público	Se cuenta con puntos de acceso controlado para evitar el ingreso de personas no autorizadas a las instalaciones de procesamiento de información?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	La SDG cuenta con personal de vigilancia que restringen el acceso no autorizado al público en general, para el caso cuenta con el área de atención al ciudadano en las instalaciones del primer piso
A11.2	Equipos				
Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.					
A11.2.1	Ubicación y protección de los equipos	Los equipos se encuentran ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	Los equipos se encuentran ubicados para cada área funcional a través de cubículos y su acceso se encuentra restringido a través de usuarios de red, con su respectiva clave.

A11.2.2	Servicios de suministro	Los equipos se encuentran protegidos contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	Los equipos se encuentran ubicados para cada área funcional a través de cubículos y cuentan con el servicio de suministro de energía e internet.
A11.2.3	Seguridad en el cableado.	El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se encuentra protegido contra interceptación, interferencia o daño?	Dirección de Tecnologías e Información	Cumple parcialmente	De acuerdo a lo informado por el área, para el Nivel Central se cuenta con certificación categoría 6 para el cableado, en los que se encuentran separados los de red de los de energía; no obstante, a Nivel Local, el cableado para algunas localidades es insuficiente.
A11.2.4	Mantenimiento de los equipos.	Durante la vigencia 2023 se han efectuado los respectivos mantenimiento de los equipos,para asegurar su disponibilidad e integridad continuas?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	Se suministran soportes de los mantenimientos efectuados en lo corrido de la vigencia 2023.
A11.2.5	Retiro de activos	Se cuenta con controles documentados, para garantizar que los equipos, información o software no se retiren de su sitio sin autorización previa?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	En el manual de Seguridad de la Información GDI TIC-M004, numeral 7.1.3.1 se establece la responsabilidad de los activos de información, específicamente se indica que "*La Dirección de Tecnologías e Información, por medio de la Mesa de servicios, es responsable de preparar los equipos de cómputo fijos y portátiles, propiedad de la Secretaría Distrital de Gobierno, para hacer entrega de estos a los funcionarios y colaboradores a quienes les sean asignados, ya sea por reasignación o disposición final, con el apoyo del área de Inventarios de la Dirección Administrativa; para el caso de las Alcaldías Locales serán responsables el administrador de red junto con el almacenista*"

A11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Se cuenta con controles documentados, para garantizar la aplicación de medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	En el manual de Seguridad de la Información GDI TIC-M004, numeral 7.1.1.6.2. se establece la política de Trabajo Inteligente. a través de la cual se establecen lineamientos para preservar la confidencialidad, la integridad y la disponibilidad de los activos de información de acuerdo con las modalidades de trabajo inteligente; asegurando lineamientos y medidas de soporte para proteger la información que es accedida, procesada o almacenada; para lo cual la Entidad pondrá a disposición de los funcionarios y contratistas los recursos tecnológicos (licenciamiento Office, Portátil, VPN, etc.) que sean considerados necesarios en pro de preservar la seguridad de la información, para llevar a cabo la realización de las funciones fuera de las instalaciones de la Entidad.
A11.2.7	Disposición segura o reutilización de equipos	Se cuenta con controles documentados para verificar que todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobreescrito en forma segura antes de su disposición o reúso?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	En el manual de Seguridad de la Información GDI TIC-M004, numeral 7.1.3.3 se establecen lineamientos para el manejo de la información, específicamente se indica que "La Dirección de Tecnologías e Información y la Dirección Administrativa deben aplicar lineamientos para la disposición segura de dispositivos que almacenen información de la Secretaría Distrital de Gobierno, ya sea cuando son dados de baja o asignados a un nuevo usuario".
A11.2.8	Equipos de usuario desatendido	Se cuenta con controles documentados para asegurar que a los equipos desatendidos se les de protección apropiada?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	Se cuenta con la política desde el Directorio activo, en donde pasados 2 minutos de inactividad se bloquea el equipo de manera automática

A11.2.9	Política de escritorio limpio y pantalla limpia	Se ha adoptado una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	En el manual de Seguridad de la Información GDI TIC-M004, numeral 7.1.3.2 se establecen lineamientos para clasificar la información, dentro de los cuales se establece que: "*Los funcionarios, colaboradores o terceros se deben asegurar de que, al momento de ausentarse del puesto de trabajo, sus escritorios se encuentren libres de documentos y medios de almacenamiento confidenciales o privados, que son utilizados para el desempeño de sus actividades; los cuales deben contar con las protecciones de seguridad necesarias de acuerdo con su nivel de clasificación para que no sean accesibles por otras personas*".
A12	**SEGURIDAD DE LAS OPERACIONES**				
A12.1	Procedimientos operacionales y responsabilidades				
Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.					
A12.1.1	Procedimientos de operación documentados	Los procedimientos de operación se encuentran documentados y puestos a disposición de todos los usuarios que los necesitan?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	Se identificaron los siguientes procedimientos documentados en el aplicativo Matiz: GDI-TIC-P001 Gestión de Requerimientos de TI; GDI-TIC-P002 Gestión de sistemas de información; DGI-TIC-P003 Procedimiento de gestión de niveles de servicios; GDI-TIC-P004 Identificación y Valoración de Activos de información; GDI-TIC-P005 Gestión portafolio y catálogo de servicios de la DTI; GDI-TIC-P006 Procedimiento Apertura de Datos; GDI-TIC-P008 Gestión de incidentes; GDI-TIC-P009 Gestión de incidentes de Seguridad de la información; GDI-TIC-P010 Levantamiento del catálogo de componentes de información y GDI-TIC-P011 Implementación de cambios.

A12.1.2	Gestión de cambios	Se cuenta con procedimiento a través de los cuales se controlan los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	Se identificó la formalización en el aplicativo Matiz del procedimiento GDI-TIC-P011 Implementación de cambios para los servicios tecnológicos, infraestructura tecnológica y sistemas de información.
A12.1.3	Gestión de capacidad	Durante la vigencia 2023 se ha efectuado seguimiento al uso de los recursos, se han efectuado ajustes, y se han realizado proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	Se suministraron soportes del monitoreo efectuado con la aplicación de los canales de Internet y datos
A12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Los ambientes de desarrollo, pruebas y operación, se encuentran separados, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	Se cuenta con el Procedimiento GDI-TIC-P002 Gestión de Sistemas de Información con controles documentados de los ambientes de desarrollo, para garantizar la protección y seguridad adecuada seguros para las actividades de desarrollo, pruebas y operación del ciclo de vida de desarrollo de sistemas
A12.2	Protección contra códigos maliciosos				
Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.					

A12.2.1	Controles contra códigos maliciosos	Se han implementado controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	En el manual de Seguridad de la Información GDI TIC-M004, numeral 7.1.7.6, se establecen lineamientos para protección contra Software Malicioso, específicamente se indica: "*La Secretaría Distrital de Gobierno contará con herramientas tales como antivirus, antimalware, antispam y antispyware, las cuales deben estar licenciadas y con acceso a las últimas actualizaciones de bases de datos de firmas de amenazas, las cuales serán de instalación obligatoria en todos los equipos de cómputo propiedad de la Entidad*", para el caso se cuenta con el contrato 837 de 2023, suscrito con Fortinet, a través del cual se ha adquirido la licencia del antivirus para la entidad.
A12.3	Copias de respaldo				
Objetivo: Proteger contra la perdida de datos					
A12.3.1	Respaldo de la información	Durante la vigencia 2023 se han efectuado copias de respaldo de la información, software e imágenes de los sistemas, y dichas copias se han puesto a prueba, de acuerdo con una política de copias de respaldo acordadas?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	Se cuenta con el GDI-TIC-IN015 Instructivo para la realización de copias de seguridad, pruebas de restauración y restauración de información crítica. Adicionalmente se suministraron evidencias de los respaldos de información realizados durante la vigencia 2023.
A12.4	Registro y seguimiento				
Objetivo: Registrar eventos y generar evidencia					
A12.4.1	Registro de eventos	Se cuenta con el registro de las actividades del usuario, excepciones, fallas y eventos de seguridad de la información y se revisa regularmente?	Dirección de Tecnologías e Información	Cumple parcialmente	Si bien las herramientas con las que cuenta la entidad permiten la trazabilidad de eventos y actividades realizadas, de acuerdo a lo informado por el área no se toman decisiones frente a dichos registros.

A12.4.2	Protección de la información de registro	Las instalaciones y la información de registro cuentan con la protección contra alteración y acceso no autorizado?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	Se cuenta con los controles en el registro de la actividad realizada en cada máquina
A12.4.3	Registros del administrador y del operador	Se cuenta con un registro sobre las actividades del administrador y del operador del sistema? ¿dicho registro se encuentra protegido y es revisado con regularidad?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	Se cuenta con el registro de las actividades de administrador y operador, protegidas
A12.4.4	Sincronización de relojes	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro del ámbito de seguridad de la SDG, se encuentran sincronizados con una única fuente de referencia de tiempo?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	En el manual de Seguridad de la Información GDI TIC-M004, numeral 7.1.7.8, se establecen lineamientos para la sincronización de relojes
A12.5	Control de software operacional				
Objetivo: Asegurarse de la integridad de los sistemas operacionales					
A12.5.1	Instalación de software en sistemas operativos	Se han implementado procedimientos para controlar la instalación de software en sistemas operativos?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	En el manual de Seguridad de la Información GDI TIC-M004, numeral 7.1.7.9, se establecen lineamientos para la instalación de Software en los Sistemas Operativos; se cuenta con el DGI-TIC-P003 Procedimiento de gestión de niveles de servicios, a través del cual se realizan las solicitudes y se determina el nivel de atención.
A12.6	Gestión de la vulnerabilidad técnica				
Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas					

A12.6.1	Gestión de las vulnerabilidades técnicas	Se obtiene oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usan en la SDG; se evalua su exposición a estas vulnerabilidades? ¿Se han tomado las medidas apropiadas para tratar el riesgo asociado?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	En el manual de Seguridad de la Información GDI TIC-M004, numeral 7.1.7.10, se establecen lineamientos para la Gestión de Vulnerabilidades Técnicas. Se suministraron evidencias del seguimiento realizados a las vulnerabilidades.
A12.6.2	Restricciones sobre la instalación de software	Se han establecido e implementado las reglas para la instalación de software por parte de los usuarios?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	En el manual de Seguridad de la Información GDI TIC-M004, numeral 7.1.7.6, se establecen lineamientos para protección contra software malicioso, específicamente se indica: *"La Dirección de Tecnologías e Información, con el apoyo del responsable de seguridad de la información debe velar porque ningún usuario pueda instalar o ejecutar programas que perjudiquen los equipos de cómputo, los sistemas operativos, programas internos, redes, servidores y aplicaciones, tales como virus informáticos, troyanos, ramsonware, spam, gusanos informáticos, malware, ataques Distribuidos de denegación de servicio DDoS, Red de equipos zombie, keylogger, entre otros*"
A12.7	Consideraciones sobre auditorias de sistemas de información				
Objetivo: Minimizar el impacto de las actividades de auditoria sobre los sistemas operativos					
A12.7.1	Controles de auditorías de sistemas de información	Se ha planificado y acordado los requisitos y actividades de auditoria que involucran la verificación de los sistemas operativos para minimizar las interrupciones en los procesos del negocio?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	En el manual de Seguridad de la Información GDI TIC-M004, numeral 7.1.7.10, se establecen lineamientos para la Gestión de Vulnerabilidades Técnicas. Se cuenta con el seguimiento a las vulnerabilidades generadas durante las vigencias 2022 y 2023.
A13	**SEGURIDAD DE LAS COMUNICACIONES**				
A13.1	Gestión de la seguridad de las redes				

Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.					
A13.1.1	Controles de redes	Se han gestionado y controlado las redes para proteger la información en sistemas y aplicaciones?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	En el manual de Seguridad de la Información GDI TIC-M004, numeral 7.1.8.1.1 se establecen lineamientos para el Control de redes.
A13.1.2	Seguridad de los servicios de red	Se han identificado los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red? ¿Se encuentran incluidos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	En el manual de Seguridad de la Información GDI TIC-M004, numeral 7.1.8.1.2, se establecen lineamientos para la seguridad de los servicios de red
A13.1.3	Separación en las redes	Los grupos de servicios de información, usuarios y sistemas de información se encuentran separados en las redes?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	En el manual de Seguridad de la Información GDI TIC-M004, numeral 7.1.8.1.4, se establecen lineamientos para la separación de redes.
A13.2	Transferencia de información				
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.					
A13.2.1	Políticas y procedimientos de transferencia de información	Se cuenta con políticas, procedimientos y controles de transferencia información formales, para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	En el manual de Seguridad de la Información GDI TIC-M004, numeral 7.1.8.2, se establecen lineamientos para el Intercambio de información
A13.2.2	Acuerdos sobre transferencia de información	En los acuerdos se establecen lineamientos para la transferencia segura de información del negocio entre la organización y las partes externas?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	En el manual de Seguridad de la Información GDI TIC-M004, numeral 7.1.8.2, se establecen lineamientos para el Intercambio de información

A13.2.3	Mensajería Electrónica	Se cuenta con controles documentado para garantizar la protección adecuada de la información incluida en la mensajería electrónica?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	En el manual de Seguridad de la Información GDI TIC-M004, numeral, 7.1.8.4, se establecen directrices para garantizar el manejo adecuado del correo electrónico
A13.2.4	Acuerdos de confidencialidad o de no divulgación	Se han identificado, documentado y revisado regularmente los requisitos para los acuerdos de confidencialidad o no divulgación, que reflejen las necesidades de la organización para la protección de la información?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	En el manual de Seguridad de la Información GDI TIC-M004, numeral, 7.1.8.6, se establecen lineamientos sobre acuerdo de confidencialidad; de igual manera se cuenta con el formato GDI-TIC-F020 Formato Acuerdo de confidencialidad, aplicable para contratistas y servidores públicos al momento de vinculación con la entidad.
A14	**Adquisición, desarrollo y mantenimiento de sistemas**				
A14.1	Requisitos de seguridad de los sistemas de información				
Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes .					
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	En el manual de Seguridad de la Información GDI TIC-M004, numeral, 7.1.9.1, se establecen los requisitos de seguridad de los sistemas de información
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	La informacion involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se encuentran protegidos de actividades fraudulentas, disputas contractuales, divulgación y modificación no autorizadas?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	En el manual de Seguridad de la Información GDI TIC-M004, numeral, 7.1.9.1, se establecen los requisitos de seguridad de los sistemas de información

A.14.1.3	Protección de transacciones de los servicios de las aplicaciones.	La información involucrada en las transacciones de los servicios de las aplicaciones se encuentra protegidas para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	En el manual de Seguridad de la Información GDI TIC-M004, numeral, 7.1.9.1, se establecen los requisitos de seguridad de los sistemas de información
A14.2	Seguridad en los procesos de Desarrollo y de Soporte				
Objetivo: Asegurar que la seguridad de la información este diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.					
A.14.2.1	Política de desarrollo seguro	Se cuenta con política y reglas documentadas para el desarrollo de software y de sistemas dentro de la organización?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	En el manual de Seguridad de la Información GDI TIC-M004, numeral 7.1.9.2, se establecen los requisitos de seguridad en los procesos de desarrollo y de soporte.
A.14.2.2	Procedimientos de control de cambios en sistemas	Se cuenta con procedimientos formales de control de cambios, para garantizar los cambios a los sistemas dentro del ciclo de vida de desarrollo?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	La entidad cuenta con un procedimiento de gestión de cambios GDI-TIC-P007 Gestión de cambios
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Se cuenta con controles documentados, para garantizar que cuando se cambian las plataformas de operación, se revisen las aplicaciones críticas del negocio, y se sometan a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	Se cuenta con el GDI-TIC-M005 Manual de Soporte Físico y Lógico de la Infraestructura Tecnológica de la Secretaría Distrital de Gobierno, Numeral 5, donde se establecen controles para garantizar la adecuada gestión de la seguridad informática, específicamente se indica que "*El objetivo del siguiente paso a paso es adoptar una metodología basada en el OSSTMM (Manual de metodología abierta para el testeo de la seguridad) para ejecutar las pruebas de seguridad externas e internas sin tener en cuenta el grado de importancia de las mismas, para ello se tratará las tomas de muestras de seguridad como únicas e independientes y se definirán políticas preventivas, defectivas y correctivas sobre los servicios que presta la Entidad*".

A.14.2.4	Restricciones en los cambios a los paquetes de software	Se cuenta con controles documentados para evitar modificaciones a los paquetes de software, para controlar que se realicen los cambios estrictamente necesarios?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	En el manual de Seguridad de la Información GDI TIC-M004, numeral 7.1.9.2, se establecen los requisitos de seguridad en los procesos de desarrollo y de soporte, específicamente se indica: *"La DTI cuenta con un sistema de control de versiones para administrar los cambios en los sistemas de información, el cual permita almacenar los códigos fuente, archivos ejecutables y archivos de configuración con el principio del privilegio mínimo*". Así mismo, se cuenta con el Procedimiento GDI-TIC-P002 Gestión de Sistemas de Información con controles documentados de los ambientes de desarrollo.
A.14.2.5	Principio de Construcción de los Sistemas Seguros.	Se han establecido, documentado y mantenido principios para la construcción de sistemas seguros, garantizando que puedan ser aplicados a cualquier actividad de implementación de sistemas de información?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	En el manual de Seguridad de la Información GDI TIC-M004, numeral 7.1.9.2, se establecen los requisitos de seguridad en los procesos de desarrollo y de soporte.
A.14.2.6	Ambiente de desarrollo seguro	Se cuenta con controles documentados de los ambientes de desarrollo, para garantizar la protección y seguridad adecuada seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	Se cuenta con el Procedimiento GDI-TIC-P002 Gestión de Sistemas de Información con controles documentados de los ambientes de desarrollo, para garantizar la protección y seguridad adecuada seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas
A.14.2.7	Desarrollo contratado externamente	Se ha supervisado y realizado seguimiento de la actividad de desarrollo de sistemas contratados externamente?	Dirección de Tecnologías e Información	Cumple parcialmente	Si bien se informa que con desarrollo externo, no se suministraron evidencias sobre la supervisión efectuada a la ejecución de dichos desarrollos.

A.14.2.8	Pruebas de seguridad de sistemas	Durante el desarrollo se han llevado a cabo pruebas de funcionalidad de la seguridad?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	De acuerdo a lo informado por el área se han efectuado pruebas de funcionalidad de Ethical Hacking a 10 sistemas de información; no obstante, a la fecha no se han subsanado las vulnerabilidades encontradas.
A.14.2.9	Prueba de aceptación de sistemas	Se han establecido programas de prueba para aceptación y criterios de aceptación relacionados, para los sistemas de información nuevos, actualizaciones y nuevas versiones?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	Se cuenta con el Procedimiento GDI-TIC-P002 Gestión de Sistemas de Información con controles documentados para realizar los diferentes tipos de pruebas para los nuevos sistemas de información, aplicaciones y versiones.
A14.3	Datos de prueba				
Objetivo: Asegurar la protección de los datos usados para pruebas.					
A.14.3.1	Protección de datos de prueba	Se han seleccionado, protegido y controlado cuidadosamente los datos de prueba?	Dirección de Tecnologías e Información	Cumple parcialmente	De acuerdo a lo informado por el área se si bien se realizan las pruebas requeridas, en algunos casos no se guarda la información producto de la ejecución de las mismas y se elimina.
A15	**RELACIONES CON LOS PROVEEDORES**				
A15.1	Seguridad de la información en las relaciones con los proveedores.				
Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.					
A15.1.1	Política de seguridad de la información para las relaciones con proveedores	Los requisitos de seguridad de la información han sido acordados y documentados con los proveedores para mitigar los riesgos asociados con el acceso de proveedores a los activos de la SDG?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	En el manual de Seguridad de la Información GDI TIC-M004, numeral 7.1.10.1, se establecen los lineamientos para la seguridad de la información en relación con los proveedores; así mismo, se cuenta con el DGI-TIC-P003 Procedimiento de gestión de niveles de servicios.

A15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Se han establecido y acordado todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI, para la información de la SDG?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	En el manual de Seguridad de la Información GDI TIC-M004, numeral 7.1.10.1, se establecen los lineamientos para la seguridad de la información en relación con los proveedores.
A15.1.3	Cadena de suministro de tecnología de información y comunicación	Los acuerdos con proveedores incluyen requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	En el manual de Seguridad de la Información GDI TIC-M004, numeral 7.1.10.1, se establecen los lineamientos para la seguridad de la información en relación con los proveedores, donde se indica que: *"La Dirección de Tecnologías e Información y el responsable de seguridad de la información apoyan a los supervisores de contrato, en identificar, monitorear y mitigar los riesgos, mediante el plan de tratamiento de riesgos relacionados con el manejo de la información de la Secretaría Distrital e Gobierno a la cual tienen acceso los proveedores, haciendo extensiva esta actividad a la cadena de suministro de los servicios de tecnología de la Entidad*". Adicionalmente, en los acuerdos de nivel de servicio se incluyen requisitos para tratar los riesgos de seguridad de la información.
A15.2	Gestión de la prestación de servicios de proveedores				
Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores					

A15.2.1	Seguimiento y revisión de los servicios de los proveedores	Se ha efectuado seguimiento, revisión y/o auditoría con regularidad a la prestación de servicios de los proveedores, a fin de verificar el nivel acordado de seguridad de la información?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	En el manual de Seguridad de la Información GDI TIC-M004, numeral 7.1.10.1, se establecen los lineamientos para la seguridad de la información en relación con los proveedores, donde se indica que: "*Los supervisores de contrato con el apoyo del responsable de seguridad de la información deben velar por hacer cumplir el modelo de los Acuerdos de Niveles de Servicio (ANS) y requisitos de seguridad de lainformación, a las terceras partes o proveedores de servicios; los cuales serán divulgados a todas las áreas que adquieran o supervisen recursos y/o servicios tecnológicos*" y como evidencia se dejan los respectivos certificados de supervisión.
A15.2.2	Gestión del cambio en los servicios de los proveedores	Se han gestionado los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y las mejoras de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos de negocio involucrados, y la revaluación de los riesgos?	Dirección de Tecnologías e Información	Cumple parcialmente	Si bien se cuenta con la política para la gestión con proveedores esta se encuentra en el Manual de Seguridad de la información GDI-TIC-M004_V8 en el item 7.1.10. Política de Seguridad de la información en la relación con los proveedores. No se suministraron evidencias sobre la gestión de los cambios en el suministro de servicios por parte de los proveedores
A16	**GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION**				
A16.1	Gestión de incidentes y mejoras en la seguridad de la información				
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.					

A16.1.1	Responsabilidades y procedimientos	Se han establecido las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	Se cuenta con el procedimiento : GDI-TIC-P009 Gestión de incidentes de Seguridad de la información, en el que se establecen los roles y responsabilidades, actividades, criterios y condiciones para la gestión de incidentes de seguridad de la información, necesarios para el manejo y control de situaciones o eventos relacionados con la seguridad de la información que se lleguen a presentar en la Secretaría Distrital de Gobierno. EVIDENCIAS DE LA RESPUESTA A INCIDENTES.
A16.1.2	Reporte de eventos de seguridad de la información	Se han informado los eventos de seguridad de la información a través de los canales de gestión apropiados, tan pronto como sea posible?	Dirección de Tecnologías e Información	Cumple parcialmente	Si bien se cuenta con un procedimiento de atención de incidentes de seguridad de la información; no se suministraron evidencias de los reportes de incidentes generados en la entidad.
A16.1.3	Reporte de debilidades de seguridad de la información	Durante la vigencia 2023 se ha exigido a todos los empleados y contratistas que usan los servicios y sistemas de información de la SDG, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios?	Dirección de Tecnologías e Información	Cumple parcialmente	Si bien se cuenta con un procedimiento de atención de incidentes de seguridad de la información; no se suministraron evidencias de la exigencia a contratistas y funcionarios sobre el reporte de incidentes de información.

A16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Se han evaluado los eventos de seguridad de la información y se ha decidido si se van a clasificar como incidentes de seguridad de la información?	Dirección de Tecnologías e Información	Cumple parcialmente	Si bien se cuenta con un procedimiento de atención de incidentes de seguridad de la información; no se suministraron evidencias de la evaluación efectuada a los incidentes.
A16.1.5	Respuesta a incidentes de seguridad de la información	Se cuenta con procedimientos documentados para dar respuesta a los incidentes de seguridad de la información? ¿Durante la vigencia 2023 se dió respuesta a los incidentes de seguridad de la información de acuerdo a dichos procedimientos?	Dirección de Tecnologías e Información	Cumple parcialmente	Se cuenta con el procedimiento: GDI-TIC-P009 Gestión de incidentes de Seguridad de la información, en el que se establecen los roles y responsabilidades, actividades, criterios y condiciones para la gestión de incidentes de seguridad de la información, necesarios para el manejo y control de situaciones o eventos relacionados con la seguridad de la información que se lleguen a presentar en la Secretaría Distrital de Gobierno. No se suministraron evidencias de la respuesta dada a los incidentes.
A16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	Los resultados del analizar y resolución de incidentes de seguridad de la información, se han utilizado para reducir la posibilidad o impacto de incidentes futuros?	Dirección de Tecnologías e Información	Cumple parcialmente	Si bien se cuenta con un procedimiento de atención de incidentes de seguridad de la información; no se suministraron evidencias sobre el uso de los resultados para reducir la probabilidad o impacto de los incidentes en la entidad.

A16.1.7	Recolección de evidencia	Se han definido y aplicado procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	Se cuenta con el procedimiento : GDI-TIC-P009 Gestión de incidentes de Seguridad de la información, en el que se establece como política de operación que: "Si se sospecha que ha ocurrido alguna intrusión no autorizada, se deben aislar y no utilizar los recursos afectados de tal forma que se dé aviso inmediatamente al responsable de Seguridad de la Información o quien haga sus veces en la entidad, de esta forma se preservará la evidencia y se realizará la correcta cadena de custodia.
A17	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO**				
A17.1	Continuidad de Seguridad de la información				
Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.					
A17.1.1	Planificación de la continuidad de la seguridad de la información	Se han determinado los requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	Se cuenta con el documento GDI-TIC-M002 Manual plan de continuidad TI, donde se establecen los requisitos para la continuidad de la gestión de la seguridad de la información en situaciones adversas
A17.1.2	Implementación de la continuidad de la seguridad de la información	Se han establecido, documentado, implementado y mantenido procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	Se cuenta con el documento GDI-TIC-M002 Manual plan de continuidad TI, donde se establecen los requisitos para la continuidad de la gestión de la seguridad de la información en situaciones adversas. Adicionalmente, se cuenta con el GCO-GTH-P004 Procedimiento de Prevención, Preparación y Respuesta ante Emergencias que se presentan en la Secretaría Distrital de Gobierno

A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Durante la vigencia 2023 se ha verificado a intervalos regulares, los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas?	Dirección de Tecnologías e Información	Cumple parcialmente	Se cuenta con el Manual de Seguridad de la Información; sin embargo, no se suministraron evidencias de verificaciones efectuadas a los controles para garantizar la continuidad de la seguridad de la información en la entidad.
A17.2	Redundancias				
Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.					
A17.2.1	Disponibilidad de instalaciones de procesamiento de información	Las instalaciones de procesamientos de información han sido implementadas con redundancia suficiente para cumplir los requisitos de disponibilidad?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	Se cuenta con el documento GDI-TIC-M002 Manual plan de continuidad TI, donde se el análisis de impacto al negocio, con el plan de operación alterno para cada servicio de TI
A18	**CUMPLIMIENTO**				
A18.1	Cumplimiento de requisitos legales y contractuales				
Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.					
A18.1.1	Identificación de la legislación aplicable.	Para cada sistema de información se han identificado, documentado y mantenidos actualizados todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	Se cuenta con el Normograma Institucional que da cuenta de la normatividad relacionada con la seguridad y privacidad de la información.

A18.1.2	Derechos propiedad intelectual (DPI)	Se han implementado procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	En el manual de Seguridad de la Información GDI TIC-M004, numeral 7.1.9.2, se establece que: "*La DTI debe asegurar que los sistemas de información adquiridos y/o desarrollados por proveedores cuenten con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y/o los derechos de propiedad intelectual. En los casos de realizarse contratación de personal para desarrollo, se deberá incluir cláusulas de propiedad intelectual*"
A18.1.3	Protección de registros	Se han protegido los registros contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio?	Dirección de Tecnologías e Información	Cumple parcialmente	Si bien se realizan reportes, no se suministraron soportes de sus registro y salvaguarda de los mismos.
A18.1.4	Privacidad y protección de información de datos personales	Se ha asegurado la privacidad y la protección de la información de datos personales, como se exige e la legislación y la reglamentación pertinentes, cuando sea aplicable?	Dirección de Tecnologías e Información	Cumple parcialmente	Se cuenta con la GDI-TIC-M007 Política para el tratamiento y protección de datos personales, así como, el formato GDI-TIC-F028 Reclamación para tratamiento de datos personales; no obstante y de acuerdo a lo informado por el área no son aplicados a cabalidad.

A18.1.5	Reglamentación de controles criptográficos.	Se han usado controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes?	Dirección de Tecnologías e Información	Cumple satisfactoriamente	En el manual de Seguridad de la Información GDI TIC-M004, numeral 7.1.5.1, se establecen lineamientos para la implementación de controles criptográficos, en donde se indica: "*Los controles criptográficos de la entidad están incluidos en el listado de software autorizado como lineamientos de seguimiento, y no se permite el uso de herramientas para controles criptográficos diferentes a los autorizados por la entidad. La Dirección de Tecnologías e Información será la encargada de definir los controles criptográficos que considere más apropiados, de acuerdo con la matriz de activos de información, el análisis de riegos de seguridad de la información y la aprobación de los dueños del proceso conforme a los roles y/o responsabilidades de los funcionarios de la Entidad*".
A18.2	Revisiones de seguridad de la información				
Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.					
A18.2.1	Revisión independiente de la seguridad de la información	El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información), se ha revisado independientemente a intervalos planificados o cuando ocurran cambios significativos?	Dirección de Tecnologías e Información	Cumple parcialmente	Durante la vigencia 2022 la Oficina de Control Interno, realizó seguimiento a la implementación del Modelo de Seguridad de la Información, en virtud de la cual se dejaron recomendaciones para la mejora; sin embargo, no se suministraron soportes de revisiones efectuadas diferentes a las realizadas por el área de Control Interno.

A18.2.2	Cumplimiento con las políticas y normas de seguridad	Los directores ha revisado con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad?	Dirección de Tecnologías e Información	Cumple parcialmente	Se cuenta con el Manual de Seguridad de la Información; sin embargo, no se suministraron soportes de revisiones efectuadas por parte del Nivel Directivo.
A18.2.3	Revisión del cumplimiento técnico	Los sistemas de información se han revisado periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información?	Dirección de Tecnologías e Información	Cumple parcialmente	Se cuenta con el Manual de Seguridad de la Información; sin embargo, no se suministraron soportes de revisiones efectuadas a los Sistemas de Información.

Fuente: NTC-ISO-IEC 27001:2013