BOGOTÁ | SECRETARÍA DE GOBIERNO

Radicado No. 20201500167423
Fecha: 24-06-2020

MEMORANDO

150

Bogotá D. C 26 de Junio de 2020

PARA: Dr. Luis Ernesto Gómez Londoño.
Secretario Distrital de Gobierno.

Dr. Jorge Bernardo Gómez Rodríguez.
Director de Tecnologías e Información.

DE: Jefe Oficina De Control Interno.

ASUNTO: Resultados Auditoria Sistema de Seguridad de la Información.

Cordial Saludo.

De manera atenta me permito informarle que Oficina de Control Interno en cumplimiento a sus funciones y en desarrollo del Plan Anual de Auditoría vigencia 2020, programó Auditoría modalidad Especial para verificar el cumplimiento y el grado de implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) del MINTIC, en la entidad comparado con la normatividad asociada a la ISO/IEC 27001 de 2013. Así mismo la documentación asociada al dueño del proceso.

Adjunto se remite informe de Auditoria.

Agradezco la atención prestada, cualquier inquietud con gusto será atendida.

Cordialmente,

LADY JOHANNA MEDINA MURILLO
Elaboró: Fernando Salgado Tovar - Profesional Oficina Control Interno
Revisó: Olga Milena Corzo - Profesional Oficina Control Interno
Aprobó: Lady Johanna Medina Murillo- Jefe Oficina Control Interno

Anexo: Informe de Auditoria 36 folios

INFORME DE AUDITORÍA

Sección I: Destinatarios

- Dr. Luis Ernesto Gómez Londoño Secretario Distrital de Gobierno
- Comité Institucional de Coordinación de Control Interno (Presentación al comité)
- Dr. Jorge Bernardo Gómez Rodríguez Director de Tecnologías e Información/ Proceso Gerencia del TIC

Sección II: Información General

Ítem	Descripción
1. Objetivo de la auditoría	Verificar el cumplimiento y el grado de implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) del MINTIC, en la entidad comparado con la normatividad asociada a la ISO/IEC 27001 de 2013. Así mismo la documentación asociada al dueño del proceso.
2. Alcance de la auditoría	Se verifican la información, manuales, procesos y procedimientos que se tienen en la Gerencia de Tecnologías de la Información de la SDG orientados a la implementación y el grado de cumplimiento del MSPI de la vigencia 2019.
3. Criterios de la auditoría	Norma Externa: Decreto 1078 de 2015 Resolución 512 de 2019 Norma ISO/IEC 27001 de 2013 Norma Interna: Resolución 0236 de 2019 GDI-TIC-M004 Manual de Gestión de Seguridad 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
4. Equipo Auditor	Fernando Andrés Salgado Tovar – Contratista de la OCI

5. Metodología	Se realizaron técnicas de auditoria basados en los medios de observación, confrontación, revisión y comparación. La verificación de la evidencia se realizó mediante las siguientes técnicas: Pruebas de funcionalidad Página web, intranet y correo corporativo. La página web de la entidad no cuenta con un (SSL) certificado de sitio seguro que sirve para ofrecer seguridad al visitante a la página web de la entidad, en donde se debe ofrecer a los usuarios que el sitio es confiable para poder ingresar los datos personales de forma segura. Revisión Verificación de evidencias y documentación observada para la comprobación de los controles asociados a la implementación del Sistema de Gestión de Seguridad de la Información en la entidad basado en la norma ISO27001 de 2013, y el MSPI del MINTIC. Entrevistas: Profesional Universitario Ing. Sonia María Cabarcas - 2, 7, 16, 24, de abril y 5, 8, 21, 27 de mayo de 2020, Profesional Universitario Ing. Nelson Mauricio Parada Boita Profesional Universitario Ing. Cesar Augusto Britto Moreno Profesional Universitario Ing. Carlos Gustavo Lara Zambrano - 2, 7, 16, 24, de abril y 5, 8 de mayo de 2020
6. Periodo de Ejecución	02 - 04 -2020 al 16 – 06 -2020

Sección III: Desarrollo de la Auditoría

A continuación, se realizará la descripción detallada de los pasos que se ejecutaron para llegar a el análisis con relación a la norma ISO/IEC 27001 de 2013; la cual define el punto de inicio de la definición de una estrategia para lograr el cumplimiento del MSPI. Se considera los diferentes requerimientos de la norma por dominio (14 en total) con el fin de evaluar el margen en que la entidad se encuentra para cumplir con la norma referida. Esto se tomó como herramienta independiente por parte de esta oficina.

En cuanto a la revisión de las evidencias solicitadas en el memorando de apertura de las cuales se solicitaron 10 ítem de verificación por lo que solo se revisaron 9, debido a que la respuesta a él memorando de apertura bajo radicado No 20204400111713 del 24 de marzo de 2020 la evidencia solicitada respecto del plan de continuidad del negocio no se encuentra desarrollada al interior de DTI.

En la Fase de Diagnostico Es de resaltar que en el ciclo de la operación para la implementación del MSPI se inicia con la identificación de un diagnostico preliminar a partir del cual se logra establecer el nivel de madurez y cumplimiento actual acerca de la gestión de seguridad de la información realizada en DTI de la SDG. Por esto a finales del año 2018 se ha venido utilizando el instrumento diseñado por el MINTIC denominado instrumento de Identificación de la línea base de seguridad, el cual tiene como propósito evaluar la efectividad de los controles establecidos en el anexo A del estándar internacional ISO 27001 versión 2013.

En el anexo A del estándar internacional ISO 27001 versión 2013 especifica 14 dominios, 35 objetivos de control y un total de 114 controles propuestos para mitigar los riesgos y realizar una adecuada gestión de seguridad de la información.

La verificación de cada uno de los controles establecidos en la ISO 27001: 2013 permitirá evidenciar aquellos aspectos en los cuales la entidad debe enfocar su atención de acuerdo a la escala de evaluación de los controles relacionados con los dominios de: políticas de seguridad de la información, seguridad de los recursos humanos, control de acceso, seguridad física y el entorno de seguridad de las operaciones, dado que se realiza monitoreo y medición al cumplimiento de los procedimientos.

La ejecución de la auditoría se realizó por medio de entrevistas, acceso a los componentes, revisiones documentales de DTI con el fin de verificar el grado de avance de los requerimientos de la ISO/IEC 27001 de 2013.

La seguridad de la información es uno de los aspectos más importantes que deben ser gestionados en las entidades gubernamentales que se quiera proteger y garantizar la continuidad del negocio. Por medio de la implementación de un sistema de gestión de seguridad., y con lo establecido en la norma ISO 27001 de 2013 que se establezca y lograr así un tratamiento acorde con los objetivos de la Entidad, además se identifican los factores internos como los procedimientos, estructura tecnológica, los factores externos como la competencia y proveedores con el objetivo de analizar las necesidades de la entidad para gestionar adecuadamente la información tanto interna como de las partes interesadas. La definición de un modelo de gestión de seguridad de la información implicar incluir a toda la entidad en la aplicación de métodos seguros y efectivos que controlen y limiten el acceso a la información y a los sistemas que procesan las estrategias que tienen como punto esencial la implementación de políticas, controles de seguridad y de acceso lógico y los procedimientos para detectar amenazas que puedan producir vulnerabilidades y que se ponga el riesgo el activo, que se

ayude a proteger tanto la información como a los sistemas que almacenan y se administran. A continuación, haremos una descripción de los pasos que se realizaron para llegar al análisis del cumplimiento de los requerimientos de la norma (14 en total) con el fin de evaluar la brecha en que la entidad se encuentra para llegar a cumplir totalmente. Para la ejecución de la situación actual se realizaron entrevistas, análisis, revisión de la información, se presenta por cada dominio el estado de implementación y aplicación de los controles consolidados por dominios de control u objetivos de control.

DOMINIOS DE CONTROL	CONTROLES QUE APLICAN	IMPLEMENTADOS	PARCIALMENTE	NO CUMPLE	NO APLICA
Dominio 5 - Políticas de Seguridad de la Información	2	0	1	1	0
Dominio 6 - Organización de la Seguridad de la Información	7	0	5	2	0
Dominio 7 - Seguridad de los Recursos Humanos	6	0	3	3	0
Dominio 8 - Gestión de Activos	10	0	6	4	0
Dominio 9 - Control de Acceso	14	0	5	9	0
Dominio 10 - Criptografía	2	0	1	1	0
Dominio 11 - Seguridad Física y del Entorno	6	0	2	4	9
Dominio 12 - Seguridad de las Operaciones	14	0	4	10	0
Dominio 13 - Seguridad de las Comunicaciones	7	0	4	3	0
Dominio 14 - Adquisición, Desarrollo y Mantenimiento de Sistemas	13	0	8	5	0
Dominio 15 - Relación con los Proveedores	5	0	0	5	0
Dominio 16 - Gestión de Incidentes de Seguridad de la Información	7	0	2	5	0
Dominio 17 - Aspectos de Seguridad de la Información de la Gestión de Continuidad del Negocio	4	0	0	4	0
Dominio 18 - Cumplimiento	8	0	2	6	0
Total	**105**	**0**	**43**	**62**	**9(**)**

(**)En cuanto al total de los controles que no se aplicaron del dominio 11 de seguridad física y del entorno corresponden a la prevención del acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento en la entidad, por lo que son verificaciones que se tenían que hacer en sitio, de manera presencial, pero debido a la emergencia sanitaria no fue posible verificar y se consideran una exclusión dentro de la auditoría y no se encuentran contempladas en la verificación de cumplimiento.

En el anexo 1 se observará el detalle por cada control de las evidencias verificadas y el estado evidenciado en el análisis realizado, con el fin de verificar el grado de cumplimiento de los requerimientos exigidos en la norma ISO 27001 de 2013. Los resultados se consolidan por medio de tablas de niveles de cumplimiento. Para cada dominio u objetivo de control, se presentan las principales observaciones y recomendaciones.

Dominio 5. POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN: Se debe realizar un entrenamiento y capacitación de los usuarios en las políticas de seguridad de la información. Es necesario asegurar que se realice la firma de la aceptación de las políticas de seguridad de la información por cada uno de los colaboradores de la entidad. Así mismo realizar la revisión periódica (anual o cuando se requiera) de las políticas de seguridad en el Comité de Gestión y Desempeño para garantizar la mejora continua.

Dominio 6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN: No se cuenta con los roles y

responsabilidades de los proveedores relacionadas con la seguridad de la información. Teniendo en cuenta lo anterior es necesario formalizar la asignación de nuevas actividades a los funcionarios correspondientes, así como las actividades de revisión, aprobación, ejecución y auditoría en un mismo cargo para definir su separación. Establecer los puntos de enlace con encargos de seguridad de otros organismos públicos y especialistas. Es importante también integrar que para la ejecución de proyectos de la organización asegurar que se identifiquen y aborden los riesgos de seguridad de la información como parte de un proyecto.

Dominio 7. SEGURIDAD DE LOS RECURSOS HUMANOS: El personal de la organización en el desarrollo de las actividades para los cuales fueron contratados, se hace necesario establecer controles para asegurar que son conscientes de los riesgos, responsabilidades y deberes con respecto a la seguridad de la información. Debe existir procedimientos y tecnologías requeridas por el SGSI a los funcionarios que aplique. Jornadas de sensibilización sobre el SGSI.

Se debe proporcionar al personal un canal de denuncia anónima para reportar violaciones de las políticas de seguridad de la información, de los procedimientos y controles, o en general de los lineamientos de seguridad de la información.

Dominio 8. GESTION 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. Implementar la política de gestión de incidentes y hacer seguimiento a su ejecución. Implementar los registros de acceso a la información. Se deberán almacenar varias copias de datos valiosos en medios separados para reducir aún más el riesgo accidental de daños o pérdidas de datos. La eliminación de los artículos sensibles se debe registrar para mantener un seguimiento de auditoria.

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. Debe existir una política de uso de redes y de servicios de red, que establezca para los usuarios: las redes y servicios a los que se tiene acceso. Validar para el sistema de gestión de contraseñas que proteja las contraseñas con el uso de algoritmos criptográficos fuertes en almacenamiento, tránsito y procesamiento.

Evaluar los lineamientos establecidos para el manejo adecuado y control de estos accesos para: base de datos, aplicativos misionales, acceso a redes y acceso remoto. Verificar los procedimientos actuales que se tienen para la desvinculación, los derechos de acceso de un individuo a la información y a los activos asociados con instalaciones y servicios de procesamiento de información, cuando deber ser removidos o suspendidos. Revisar el procedimiento de identificación, autorización y autenticación para los programas utilitarios; segregación de los programas de aplicación de los programas; limitación al uso a un número mínimo y practico de usuarios confiables y autorizados.

Dominio 10. CRIPTOGRAFIA: Para los sistemas de información críticos que se manejan en la entidad debe establecer controles criptográficos con el objetivo de garantizar la confidencialidad e integridad de la información. Se debe implementar una política en donde se tenga contemplado la gestión de claves criptográficas, que incluya la generación, almacenamiento, distribución, retiro y destrucción de dichas claves.

Dominio 11. SEGURIDAD FISICA Y DEL ENTORNO: Se debe tener en cuenta la verificación que todos los equipos utilizados en la entidad cuenten con un programa de mantenimiento de acuerdo con las especificaciones técnicas del fabricante. Se debe mejorar los controles especificados en el SGSI el retiro de algún activo de las oficinas de la entidad solo puede permitirse con la debida autorización de un documento donde se asigne un responsable de la aplicación.

Dominio 12. SEGURIDAD DE LAS OPERACIONES: Se tiene que implementar un procedimiento de los ambientes de software separados en donde exista automatización de un conjunto de datos de pruebas que sea estándar, ya que en la entidad se manejan datos sensibles y estos no se deberían copiar en el entorno de pruebas a menos que se entreguen controles equivalentes para el ambiente de pruebas, realizar la separación de redes para los entornos de desarrollo, pruebas y operación.

En cuanto a la protección del malware se necesita implementar controles de software de reparación, así como la toma de conciencia sobre la seguridad de la información, el acceso adecuado al sistema y la administración de cambios. Plan de remediación y capacitación al personal de DTI en el uso de herramientas de detección automatizada de vulnerabilidades. Se deberán identificar los requisitos de capacidad teniendo en cuenta la criticidad para el negocio de cada sistema involucrado.

Se deberá considerar un plan de administración de capacidad documentado para los sistemas críticos para la misión de la entidad. Definir dentro de las exigencias que se deben cumplir en cuanto a la seguridad los campos que se necesitan para el registro de eventos de acuerdo con la política de desarrollo seguro. Se debe usar un sistema de control de la configuración, para mantener el control de todo el software implementado, así como la documentación asociada.

Dominio 13. SEGURIDAD DE LAS COMUNICACIONES: Establecer la segmentación con base en el nivel de criticidad de los activos. Revisar las políticas de direccionamiento IP origen y destino, puertos para el tráfico autorizado(firewall). Evaluar el uso de analizadores de protocolos para seguimiento a reportes de anomalías en la red. Transmitir de manera segura la información, sin importar el medio y el mecanismo usado para la transferencia. Establecer una política y procedimiento y los controles de transferencia formal para proteger la información a través de todos los tipos de medios. Tener en cuenta las responsabilidades en las directrices de los acuerdos de confidencialidad.

Dominio 14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS: La identificación y gestión de los requisitos de seguridad de información y los procesos asociados deben ser constituidos en etapas tempranas de los proyectos de los sistemas de información. Implementar los controles de acceso y protección de los datos expuestos en los servicios de red con base en las políticas del SGSI. Se deberá considerar la tecnología nueva para conocer los riesgos de seguridad.

La introducción de nuevos sistemas de información y los principales cambios a los sistemas efectivos deben seguir un proceso formal de documentación, especificaciones, pruebas, control de calidad e implementación administrada. Cuando se hacen cambios a las plataformas operacionales, las aplicaciones críticas de la entidad deben ser revisadas y puesto a prueba para asegurar que no hay impacto desfavorable en la seguridad o de las operaciones, por lo que todos los cambios deben ser totalmente probados y documentados.

Los nuevos sistemas se deben someter a pruebas verificables durante los procesos de desarrollo, incluida la preparación de un programa de actividades detallando las entradas y pruebas con los resultados esperados bajo una variedad de condiciones.

Dominio 15. RELACIONES CON LOS PROVEEDORES: Se deben establecer y documentar acuerdos con los proveedores, para asegurar que no haya inconvenientes entre la entidad y el proveedor respecto a las obligaciones de ambas partes para cumplir con los requisitos relevantes de seguridad de la información.
Es necesario establecer los controles de seguridad para garantizar que tienen en cuenta los requisitos del ejercicio en la entidad antes de gestionar compras para los servicios que afecten la seguridad de la información de la infraestructura sobre la cual esta soportada.

Dominio 16. GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN: La entidad debe establecer en su política de seguridad de la información como es el compromiso, organización y asignación para su cumplimiento, de igual forma vela por mantener protegido los activos de información. Entrenamiento y sensibilización a los funcionarios en el reporte de eventos de seguridad.
Establecer en el procedimiento el reporte de eventos de seguridad de la información y el punto de contacto al que dichos eventos deben ser reportados. Los incidentes de seguridad de la información deben ser analizados por el personal designado por DTI para identificar acciones de mejora en tal sentido es necesario establecer controles de seguridad para garantizar un manejo eficaz y consistente los incidentes de seguridad de la información. Implementar que permitan la cuantificación y monitoreo y los costos de los incidentes de seguridad de la información.

Dominio 17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO: La entidad debe determinar que la continuidad de la seguridad de la información permita minimizar el impacto generados por la capacidad de ejecución, creando el proceso de continuidad de negocio, y/o bien del proceso de gestión de recuperación de desastres.
Aplicar el procedimiento de la continuidad de la seguridad en caso de que la contingencia se mantenga los requerimientos de confidencialidad e integridad para los activos involucrados en el evento de una contingencia. Implementar los respaldos requeridos para las plataformas de seguridad informática en caso de una contingencia.

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 auditorias internas anuales para el cumplimiento de seguridad de la información.

Sección IV: Hallazgos

1. ***Ausencia del Plan de Continuidad del Negocio en concordancia al dominio 17 de la Norma ISO 27001 de 2013 y la Guía No 10 del Sistema de Gestión de la Seguridad de la Información del MINTIC.***

Al realizar la verificación de la información se pudo evidenciar que DTI manifestó que no cuenta con este documento en el que se hace necesario para la correcta construcción de la implementación del SGSI al interior de la entidad, el objetivo de implantar este plan es que se tenga la capacidad de recuperar y restaurar todas las funciones criticas que hayan sido interrumpidos por algún incidente o desastre, y de esta manera poder seguir prestando los servicios en niveles aceptables que no afecten la continuidad del negocio, identificar amenazas potenciales a la entidad y el impacto que podría causar a la operación de negocio que en caso de materializarse.

2. ***Ausencia en la gestión efectiva de un Análisis de Vulnerabilidades en concordancia al control 12.7 de la Norma ISO 27001 de 2013 y la Guía No 7 del Sistema de Gestión de la Seguridad de***

la Información del MINTIC.

Al realizar la verificación de la información se pudo evidenciar que DTI que no cuenta con este documento debidamente desarrollado en el que se hace necesario para la correcta construcción de la implementación del SGSI al interior de la entidad, el objetivo de implementar este mecanismo es la detección temprana y proactiva de vulnerabilidades y amenazas que puedan afectar la seguridad de la información de los activos de la entidad y se consigue por medio de implementar un monitoreo constante del comportamiento de los sistemas con el objetivo de proporcionar una visibilidad de la infraestructura tecnológica y su nivel ante posibles anomalías, además de la perdida de la eficacia, las condiciones adversas de operación, perdida del negocio, reputación, daño entre otros.

En este documento se deben identificar los daños y las consecuencias para la entidad que podrían causar mediante un incidente descritos como amenazas asociadas a vulnerabilidades en los activos de información.

PRESENTACIÓN DEL PLAN DE MEJORAMIENTO. 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, cada área de gestión auditada 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".

Sección V: Conclusiones y Recomendaciones

- A nivel general se observó que la entidad se encuentra pendiente por implementar una fase de planificación rigurosa con base en diagnósticos entregados de comienzos del 2019 y que sean claros y actualizados que permitan establecer planes de acción concretos, aprobados oficialmente, con recursos asignados y tiempo establecidos, pues se evidencian acciones aisladas y sin un propósito general que conllevan a la ausencia de controles efectivos, conocidos y aplicados por toda la organización.

- Se atendió de manera oportuna la presente auditoría y que actualmente se encuentran realizando un diagnóstico del estado actual del Sistema de Gestión, por lo que se recomienda complementar estas acciones y los posteriores planes de acción con base en las situaciones evidenciadas en la auditoría.

- Se observó entre las acciones o iniciativas que se fueron implementando en la vigencia 2019 actividades para el desarrollo del Plan de Transición IPv4 a IPv6, a través de la adquisición de un pool de direcciones basado en Protocolo de Internet Versión 6 (IPv6) con el fin de configurar la arquitectura actual de conectividad LAN, WAN y Seguridad de la SDG en donde se llevó a cabo el

proyecto por la empresa Business Support la cual realizó un levantamiento de información y revisión técnica del inventario de los equipos que soportan la implementación IPv6 y actualmente se tiene en funcionamiento del direccionamiento compartido con IPv4 e internamente se maneja con firmware en IPv6 a nivel central y 13 localidades. Se observa que con respecto a esto se debe dar continuidad a las acciones inicialmente implementadas, observando que hace falta que externamente se vea la entidad por IPv6 y que las localidades restantes también se implementen y reconfigure este protocolo. *Se observó por parte de esta auditoría que falta documentación interna asociado a la fase de diagnóstico de IPv6 y actualizar la resolución de adopción de IPv6.*

En las imágenes presentadas a continuación se puede observar que lo indicado, acerca de la visualización externa de la entidad a través de IPV6:

Fuente: https://ipv6-test.com/validate.php

- En cuanto al uso y apropiación de seguridad de la información se observan unos visores de pantallas para los equipos de cómputo de la entidad ligados a tips de mejora de la seguridad si bien hace parte integral del cumplimiento del proceso. Es importante diseñar e implantar un plan una metodología de capacitación de Seguridad de la información, dirigida a todo el personal del área de seguridad de la entidad quienes se responsabilizarán de la implementación y gestión del SGSI. Construir materiales para la sensibilización y entrenamiento. Importante tener en cuenta evaluar, medir y cuantificar, si el programa o plan implementado genera impacto en el desarrollo de las actividades de la entidad.

- En relación a la matriz de riesgos de seguridad digital se presentó un documento en Excel que mencionan los riesgos de seguridad digital que se tienen contemplados en la entidad, pero se encuentra desactualizado, por lo anterior se cuenta con un plan de tratamiento de riesgos de seguridad y privacidad de la información de GDI-TIC-PL003 en donde se debe cumplir con el plan y ser insumo de metodología de la actualización de la matriz de riesgos de seguridad. Luego de la matriz de riesgos de seguridad desarrollada se debe continuar con la declaración de aplicabilidad y debe ser un contexto estratégico de los criterios básicos en el alcance, los limitantes y la gestión de riesgos de seguridad digital traerán consigo controles que incluyan el monitoreo y la revisión debe ser claramente definida.

- Se observaron errores en el diligenciamiento de la herramienta del MSPI, los campos de brechas donde se debe establecer e indicar que le hace falta al control o requisito para cumplir frente a la Norma ISO 27001 de

2013, en donde se incluyen los requisitos de Gobierno en Línea y el MSPI, no se han diligenciado ni se han incluido las actividades o acciones requeridas para cumplir con el componente del ciclo PHVA.

Como parte de las recomendaciones a nivel general para el sistema de seguridad de la información, es necesario tener en cuenta:

- ✓ Realizar seguimiento y revisión de los servicios de los proveedores para asegurar que los términos y condiciones de seguridad de la información de los acuerdos se cumplan.
- ✓ La entidad deberá disponer de un oficial de seguridad de la información para mejorar la implementación del SGSI.
- ✓ Elaborar un plan de trabajo que determine en el corto plazo, las actividades para implementar las acciones necesarias, con el fin de cumplir con lo establecido en la normatividad vigente.
- ✓ Elaborar e implementar un plan de comunicaciones relacionado con los temas de seguridad y privacidad de la información dirigido a todos los funcionarios contratistas y demás miembros externos asociados a la entidad.
- ✓ Desarrollar un plan de trabajo enfocado a implementar los controles necesarios, con el fin de mitigar las vulnerabilidades a las cuales se encuentran expuestos y comprometidos los componentes informáticos.
- ✓ Realizar supervisión continua a las capacidades técnicas de los proveedores, para mantener la disponibilidad, confidencialidad e integridad de la información que se le entrega.
- ✓ Requerir reportes e informes periódicos por parte del proveedor sobre las condiciones del servicio y seguridad que se hayan pactado.

Se genera el presente informe, el cual fue presentado en reunión de cierre el día 23 de junio de 2020, se recomienda realizar la revisión de las observaciones, recomendaciones e incumplimientos evidenciados por la Oficina de Control Interno, encaminadas a la mejora continua y avance en el desempeño del Sistema de Seguridad de la información en la entidad.

Cordialmente,

LADY JOHANNA MEDINA MURILLO

Elaboró: Fernando Salgado Tovar - Profesional Oficina Control Interno
Revisó: Olga Milena Corzo - Profesional Oficina Control Interno
Aprobó: Lady Johanna Medina Murillo- Jefe Oficina Control Interno

Anexo 1. Resultados de verificación por dominio y controles

Anexo 1. Resultado de verificación de controles por dominio y observaciones

A5	POLÍTICAS DE LA SEGURIDAD DE LA INFORMACION				
A5.1	Orientación de la dirección para la gestión de la seguridad de la información				
Controles			**Estado observado**	**Evidencias**	**Observación**
A5.1.1	Políticas para la seguridad de la información	Control: Se debe definir 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.	Cumple parcialmente	http://gaia.gobiernobogota.gov.co/sites/default/files/imagenes/politica-tecnologiadef-2018.png GDI-TIC-M004 Manual de Gestión de Seguridad de la Información: http://gaia.gobiernobogota.gov.co/sites/default/files/sig/manuales/gdi-tic-m004_0.pdf	Falta mejorar la comunicación a los funcionarios y partes externas correspondientes
A5.1.2	Revisión de las políticas para la seguridad de la información.	Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.	No cumple	No se observó que las políticas se hayan verificado en intervalos una vez al año o cuando se requiera	Se debe revisar periódicamente y a través de una planeación de acuerdo a la efectividad de los controles y de acuerdo a un plan de mejoramiento continuo

A6	ORGANIZACIÓN DE LA SEGURDAD DE LA INFORMACION				
A6.1	Organización Interna				
Controles			**Estado observado**	**Evidencias**	**Observación**
A6.1.1	Roles y responsabilidades para la seguridad de la información	Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	Cumple parcialmente	Numeral 6 del Artículo 3 de la Resolución 783 de 2018 - Creación del Comité Institucional de Gestión y Desempeño Está definido en los manuales de seguridad, los roles de seguridad de la información. http://gaia.gobiernobogota.gov.co/sites/default/files/documentos/sig/doc_relacionados/resolucion_0236_-_mipg.pdf http://gaia.gobiernobogota.gov.co/sites/default/files/sig/manuales/gdi-tic-m004_0.pdf Faltan los roles de proveedores	Faltan contemplar los roles de proveedores. Las responsabilidades para la gestión del riesgo de SI y la aceptación de los riesgos residuales.

A6	ORGANIZACIÓN DE LA SEGURDAD DE LA INFORMACION				
A6.1	Organización Interna				
Controles			**Estado observado**	**Evidencias**	**Observación**
A6.1.2	Separación de deberes	Control: Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.	No cumple	No se observó que las políticas se hayan verificado en intervalos una vez al año o cuando se requiera	No existe documentación asociada al proceso, no se cuenta totalmente con separación de deberes Por lo que no se debe implementar controles que compensen la separación de deberes y realizar la revisión periódica en los SI. Esto va de la mano con las responsabilidades de la entidad en cuanto a la seguridad de la información.
A6.1.3	Contacto con las autoridades	Control: Se deben mantener contactos apropiados con las autoridades pertinentes.	Cumple parcialmente	http://ticbogota.gov.co/sites/default/files/marco-legal/CIRCULAR%2037.pdf Se tiene el contacto a través de la Alta Consejería Distrital de las Tics	No existe procedimiento formal interno, porque todo se hace a través de la alta consejería distrital, Por lo que se recomienda tener un procedimiento formal de la SDG.
A6.1.4	Contacto con grupos de interés especial	Control: Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad	Cumple parcialmente	http://ticbogota.gov.co/sites/default/files/marco-legal/CIRCULAR%2037.pdf	Se tiene el contacto a través de la Alta Consejería Distrital de las Tics Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad. Por ejemplo, a través de una membresía
A6.1.5	Seguridad de la información en la gestión de proyectos.	Control: La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.	No cumple	http://gaia.gobiernobogota.gov.co/sites/default/files/sig/guias/gdi-tic-pl001_v1.pdf	Si bien se tiene contemplado en el PETI en cuanto a las necesidades de capacitación y las buenas prácticas de la Seguridad de la Información. Se debe contemplar la Arquitectura Gestión de proyectos de TI de MinTIC que contemple los objetivos de la seguridad de la información se incluyan en los objetivos de los proyectos, que la seguridad de la información sea parte de todas las fases de la metodología del proyecto aplicada.

A6	ORGANIZACIÓN DE LA SEGURDAD DE LA INFORMACION				
A6.2	Dispositivos móviles y de teletrabajo				
Controles			**Estado observado**	**Evidencias**	**Observación**
A6.2.1	Política para dispositivos móviles	Control: Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	Cumple parcialmente	http://gaia.gobiernobogota.gov.co/sites/default/files/sig/manuales/gdi-tic-m004_0.pdf	Tener en cuenta los dispositivos móviles, así como los controles de seguridad que la entidad utilizará para proteger, mitigar, supervisar y monitorear los riesgos asociados al acceso y divulgación no autorizada de la información.
A6.2.2	Teletrabajo	Control: Se deben implementar una política y unas 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.	Cumple parcialmente	http://gaia.gobiernobogota.gov.co/sites/default/files/sig/manuales/gdi-tic-m006.pdf	Según lo observado el manual de talento humano se tiene una lista de chequeo de requerimientos básicos en cuanto al equipo de cómputo, pero se requiere crear un procedimiento formal que contemple la seguridad física existente en el sitio del teletrabajo. Métodos para asegurar el acceso remoto; la revocación de los derechos de acceso, y la devolución de los equipos cuando las actividades del teletrabajo finalicen.

A7	SEGURIDAD DE LOS RECURSOS HUMANOS				
A7.1	Antes de Asumir el empleo				
Controles			**Estado observado**	**Evidencias**	**Observación**
A7.1.1	Selección	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes y deben ser proporcionales a los requisitos de negocio, a la clasificación de la	Cumple parcialmente	http://gaia.gobiernobogota.gov.co/sites/default/files/sig/procedimientos/gco-gth-p001_0.pdf	Existe el procedimiento en gestión humana, pero se debe automatizar, sistematizar la selección de personal, conteniendo la evaluación de desempeño ya que actualmente se encuentra por medio de una tabla de Excel

A7	SEGURIDAD DE LOS RECURSOS HUMANOS				
A7.1	Antes de Asumir el empleo				
Controles			Estado observado	Evidencias	Observación
		información a que se va a tener acceso y a los riesgos percibidos.			
A7.1.2	Términos y condiciones del empleo	Control: Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	No cumple	https://gobiernobogota.sharepoint.com/sites/grOficinadeControlInterno/Documentos%20compartidos/Forms/AllItems.aspx?sortField=LinkFilename&isAscending=true&viewid=2ba17f7a%2Dee0e%2D4548%2Db3fb%2D3bac1c495f30&id=%2Fsites%2FgrOficinadeControlInterno%2FDocumentos%20compartidos%2FVigencia%202020%20OCI%2FPlan%20Anual%20de%20Auditoria%20OCI%202020%2F15%2E%20ISO%2027001%20Gerencia%20de%20Tic%20para%20la%20Seguridad%20de%20la%20informaci%C3%B3n%2FHerramientas%2FLOGRO%202%2FA7%2E%20SEGURIDAD%20DE%20LOS%20RECURSOS%20HUMANOS	Obligaciones contractuales de los contratistas en cuanto a la confidencialidad de la entidad y código disciplinario para los de planta. Pero para el caso de seguridad de la información no se tiene contemplado en los contratos de prestación de servicios observados no se observó el cumplimiento de la seguridad de la información

A7	SEGURIDAD DE LOS RECURSOS HUMANOS				
A7.2	Durante la ejecución del empleo				
Controles			Estado observado	Evidencias	Observación
A7.2.1	Responsabilidades de la dirección	Control: La dirección debe exigir a todos los empleados y contratista la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	No Cumple	No se observó que las políticas se hayan verificado en intervalos una vez al año o cuando se requiera y que se le informe a los empleados y contratistas sus roles y responsabilidades de seguridad de la información.	Se debe contemplar sobre sus roles y responsabilidades de seguridad de la información, antes de que se les otorgue el acceso a información o sistemas de información confidenciales. Se les suministren las directrices que establecen las expectativas de seguridad de la información de sus roles dentro de la Entidad. Se tenga continuamente las habilidades y calificaciones apropiadas y reciban capacitación en forma regular.

A7	SEGURIDAD DE LOS RECURSOS HUMANOS				
A7.2	Durante la ejecución del empleo				
Controles			**Estado observado**	**Evidencias**	**Observación**
A7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.	No cumple	No se cuenta con un plan de comunicación, sensibilización y capacitación. Solo se observó una campaña de cultura clic enviada por correo electrónico.	Falta un plan formal de capacitación que se evalué periódicamente para una adecuada toma de conciencia, con los respectivos soportes, revisado y aprobado por la alta Dirección
A7.2.3	Proceso disciplinario	Control: Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	Cumple parcialmente	http://gaia.gobiernobogota.gov.co/sites/default/files/sig/manuales/gdi-tic-m004_0.pdf	Se observo en el manual GDI-TIC M004 el numeral 5 que indica que "La inobservancia de las disposiciones de este documento, podrá dar lugar según corresponda, a la iniciación de las investigaciones y aplicación de sanciones, de conformidad con las disposiciones legales vigentes. Por lo anterior se debe contemplar que se contemple cuando se ha ocurrido una violación a la seguridad de la información, quien y como se determina la sanción al infractor.

A7	SEGURIDAD DE LOS RECURSOS HUMANOS				
A7.3	Terminación y cambio de empleo				
Controles			**Estado observado**	**Evidencias**	**Observación**
A7.3.1	Terminación o cambio de responsabilidades de empleo	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de empleo de deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	Cumple parcialmente	https://gobiernobogota.sharepoint.com/sites/grOficinadeControlInterno/Documentos%20compartidos/Forms/AllItems.aspx?viewid=2ba17f7a%2Dee0e%2D4548%2Db3fb%2D3bac1c495f30&id=%2Fsites%2FgrOficinadeControlInterno%2FDocumentos%20compartidos%2FVigencia%202020%20OCI%2FPlan%20Anual%20de%20Auditoria%20OCI%202020%2F15%2E%20ISO%2027001%20Gerencia%20de%20Tic%20para%20la%20Seguridad%20de%20la%20informaci%C3%B3n%2FHerramientas%2FGAP%20LOGRO%202	En las obligaciones contractuales, si bien se describe en el contrato que se debe mantener la confidencialidad no existe un acuerdo más claro y con sus respectivas vigencias del cumplimiento de la seguridad de la información.

A8	GESTION DE ACTIVOS				
A8.1	Responsabilidad por los activos				
Controles			**Estado observado**	**Evidencias**	**Observación**
A8.1.1	Inventario de activos	Control: Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	Cumple parcialmente	http://www.gobiernobogota.gov.co/transparencia/instrumentos-gestion-informacion-publica/relacionados-la-informacion/102-registro	No se cuenta con los activos debidamente aprobados por la alta dirección. Se deben hacer reuniones de seguimiento con las diferentes dependencias y áreas para revisar que activos de información se deben custodiar.
A8.1.2	Propiedad de los activos	Control: Los activos mantenidos en el inventario deben tener un propietario.	Cumple parcialmente	http://www.gobiernobogota.gov.co/transparencia/instrumentos-gestion-informacion-publica/relacionados-la-informacion/102-registro	Se deben actualizar ya que se debe realizar un chequeo de que activos se deben proteger.
A8.1.3	Uso aceptable de los activos	Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	Cumple parcialmente	http://www.gobiernobogota.gov.co/transparencia/instrumentos-gestion-informacion-publica/relacionados-la-informacion/102-registro	Establecer un procedimiento, directriz o lineamiento que defina el uso aceptable de los activos, verifique que es conocida por los empleados y usuarios de partes externas que usan activos de la Entidad o tienen acceso a ellos.
A8.1.4	Devolución de activos	Control: Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	Cumple parcialmente	http://www.gobiernobogota.gov.co/transparencia/instrumentos-gestion-informacion-publica/relacionados-la-informacion/102-registro	En caso de que un funcionario o tercero sea el dueño del activo indague como se asegura la transferencia de la información a la Entidad y el borrado seguro de la información de la Entidad.

A8	GESTION DE ACTIVOS				
A8.2	Clasificación de Información				
Controles			**Estado observado**	**Evidencias**	**Observación**
A8.2.1	Clasificación de la información	Control: La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	Cumple parcialmente	http://www.gobiernobogota.gov.co/node/28	No se encuentra totalmente diligenciada la clasificación de información y deberá valorarse teniendo en cuenta la confidencialidad, integridad y disponibilidad. Definir cada cuanto debe revisarse la clasificación de un activo

A8	GESTION DE ACTIVOS				
A8.2	Clasificación de Información				
Controles			**Estado observado**	**Evidencias**	**Observación**
A8.2.2	Etiquetado de la información	Control: Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	No Cumple	DTI manifiesta que no cuenta con un etiquetado de la información	Se debe implementar el etiquetado de los activos en formatos físicos y electrónicos y que refleje el esquema de clasificación establecido.
A8.2.3	Manejo de activos	Control: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	No Cumple	No se observó por parte de DTI un procedimiento de cómo es el manejo de activos en la entidad	Contar con un procedimiento para el manejo, procesamiento, almacenamiento y comunicación de información de conformidad con su clasificación. Este debe ser adoptado por la entidad.

A8	GESTION DE ACTIVOS				
A8.3	Manejo de Medios				
Controles			**Estado observado**	**Evidencias**	**Observación**
A8.3.1	Gestión de medio removibles	Control: Se deben implementar procedimientos para la gestión de medio removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	Cumple parcialmente	http://gaia.gobiernobogota.gov.co/sites/default/files/sig/manuales/gdi-tic-m004_0.pdf	No se cuenta contemplado con la confidencialidad o integridad de los datos, se deben usar técnicas criptográficas para proteger los datos que se encuentran en los medios removibles.
A8.3.2	Disposición de los medios	Control: Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	No Cumple	La DTI manifiesta que no cuenta en la actualidad con un procedimiento que se contemple con la disposición de medios	No existe procedimiento que garantice los medios a desechar o donar, no contienen información confidencial que pueda ser consultada y copiada por personas no autorizadas.
A8.3.3	Transferencia de medios físicos	Control: Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	No Cumple	DTI indica que aún no tiene contemplado la transferencia adecuada de medios removibles. Como el uso de un transporte o servicios de mensajería confiables.	No existe un procedimiento para verificar la identificación de los servicios de mensajería. En donde se debe contemplar los tiempos de transferencia a los responsables durante el transporte, y el recibo en su destino.

A9	CONTROL DE ACCESO				
A9.1	Requisitos del negocio para el control de acceso				
Controles			**Estado observado**	**Evidencias**	**Observación**
A9.1.1	Política de control de acceso	Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.	Cumple parcialmente	http://gaia.gobiernobogota.gov.co/sites/default/files/sig/manuales/gdi-tic-m004_0.pdf	Se debe implementar un procedimiento para el ingreso a los sistemas de información de manera segura.
A9.1.2	Acceso a redes y a servicios en red	Control: Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	Cumple parcialmente	http://gaia.gobiernobogota.gov.co/sites/default/files/sig/instructivo/gdi-tic-in006.pdf	No se cuenta con los requisitos de autenticación de usuarios para acceder a diversos servicios de red. No se tiene contemplado el acceso a redes

A9	CONTROL DE ACCESO				
A9.2	Gestión de acceso de usuarios				
Controles			**Estado observado**	**Evidencias**	**Observación**
A9.2.1	Registro y cancelación del registro de usuarios	Control: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	No Cumple	No se observó un procedimiento de la aprobación y documentación de los usuarios genéricos ni con un proceso establecido de cómo se debe automatizar para los usuarios redundantes	Implementar un procedimiento que contenga y se aplique la identificación y eliminación o la deshabilitación periódicamente las identificaciones de usuario redundantes
A9.2.2	Suministro de acceso de usuarios	Control: Se debe implementar 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.	Cumple parcialmente	Se observó que DTI cuenta con instructivo interno del uso del directorio activo	No se ha adaptado los derechos de acceso de usuarios que han cambiado de roles o de empleo, y retirar o bloquear inmediatamente los derechos de acceso de los usuarios que han dejado la entidad. No se cuenta con una política de eliminación/gestión de usuarios.
A9.2.3	Gestión de derechos de acceso privilegiado	Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	No cumple	No se observa un procedimiento formal de los derechos de uso privilegiado.	No se cuenta la asignación de derechos de acceso privilegiado a través de un proceso de autorización formal de acuerdo con la política de control de acceso pertinente.

A9	CONTROL DE ACCESO				
A9.2	Gestión de acceso de usuarios				
Controles			**Estado observado**	**Evidencias**	**Observación**
A9.2.4	Gestión de información de autenticación secreta de usuarios	Control: La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	No cumple	Se encuentra pendiente un proceso formal de la autenticación secreta de los usuarios.	Se debe estipular que todos los usuarios deben mantener su propia información de autenticación secreta, y se les suministra una autentificación secreta temporal segura.
A9.2.5	Revisión de los derechos de acceso de usuarios	Control: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	No cumple	No se cuenta con una documentación en donde se indique cada cuanto se debe revisar los derechos de acceso	Definir las autorizaciones para los derechos de acceso privilegiado y revisar periódicamente.
A9.2.6	Retiro o ajuste de los derechos de acceso	Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	No cumple	No se observó un procedimiento de como se hace para la terminación o cambio lo inicia el empleado, el usuario de la parte externa o la dirección, y la razón de la terminación	Se debe crear el procedimiento de como se hace con los derechos de acceso a la información y a los activos asociados, antes de que el empleo termine o cambie, que incluya terminación o cambio lo inicia el empleado, el usuario de la parte externa o la dirección, revisar las responsabilidades.

A9	CONTROL DE ACCESO				
A9.3	Responsabilidades de los usuarios				
Controles			**Estado observado**	**Evidencias**	**Observación**
A9.3.1	Uso de información de autenticación secreta	Control: Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	No Cumple	No se cuenta con un instructivo debidamente formalizado internamente que contenga para un ID genérico solo sea emitido para una persona a la vez y quede debidamente registrado.	Se tiene indicaciones en manual de seguridad. Falta documentar, políticas de seguridad clave y contraseña temporalidad. Mejorar el instructivo del acceso por VPN debido a que si no se vence la contraseña del usuario no debería dejar ingresar con la misma contraseña que se venció.

A9	CONTROL DE ACCESO				
A9.4	Control de acceso a sistemas y aplicaciones				
Controles			**Estado observado**	**Evidencias**	**Observación**
A9.4.1	Restricción de acceso a la información	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	No Cumple	http://gaia.gobiernobogota.gov.co/sites/default/files/sig/manuales/gdi-tic-m004_0.pdf	Contemplar en el procedimiento de control de acceso en donde se especifique la restricción de acceso a la información y a las funciones de las aplicaciones por parte de los usuarios y el personal de soporte, de acuerdo a la política definida de control de acceso.
A9.4.2	Procedimiento de ingreso seguro	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	Cumple parcialmente	http://gaia.gobiernobogota.gov.co/sites/default/files/sig/manuales/gdi-tic-m004_0.pdf	Falta visualizar una advertencia general acerca de que sólo los usuarios autorizados pueden acceder al computador.
A9.4.3	Sistema de gestión de contraseñas	Control: Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	Cumple parcialmente	http://gaia.gobiernobogota.gov.co/sites/default/files/sig/manuales/gdi-tic-m004_0.pdf	Falta apartes de las actividades listadas Gestión de contraseñas tener en cuenta la VPN
A9.4.4	Uso de programas utilitarios privilegiados	Control: Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	No cumple	No se cuenta con un procedimiento en donde se especifica como es el uso de los programas utilitarios por los administradores de los sistemas de información de la entidad.	Se debe contemplar la restricción, automatización y el control del uso de los programas utilitarios que puedan anular los controles de los sistemas y las aplicaciones.
A9.4.5	Control de acceso a códigos fuente de programas	Control: Se debe restringir el acceso a los códigos fuente de los programas.	No cumple	No se observó un control de acceso para códigos fuente	No se tiene gestionado los códigos fuente de los programas y las librerías de las fuentes de los programas se debería hacer de acuerdo con procedimientos establecidos.

A10	CRIPTOGRAFIA				
A10.1	Controles criptográficos				
Controles			**Estado observado**	**Evidencias**	**Observación**
A10.1.1	Política sobre el uso de controles criptográficos	Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	Cumple parcialmente	http://gaia.gobiernobogota.gov.co/sites/default/files/sig/manuales/gdi-tic-m004_0.pdf	Utilizar la encriptación para la protección de información transportada por dispositivos de encriptación móviles o removibles, o a través de líneas de comunicación.

A10	CRIPTOGRAFIA				
A10.1	Controles criptográficos				
Controles			Estado observado	Evidencias	Observación
A10.1.2	Gestión de llaves	Control: Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.	No Cumple	No se observó ningún proceso o procedimiento para la gestión de llaves en la entidad	Implementar una política sobre el uso, protección y tiempo de vida de las llaves para diferentes sistemas criptográficos y en las diferentes aplicaciones

A11	SEGURIDAD FISICA Y DEL ENTORNO				
A11.2	Equipos				
Controles			Estado observado	Evidencias	Observación
A11.2.4	Mantenimiento de los equipos.	Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Cumple parcialmente	https://gobiernobogota.sharepoint.com/sites/grOficinadeControlInterno/Documentos%20compartidos/Forms/AllItems.aspx?viewid=2ba17f7a%2Dee0e%2D4548%2Db3fb%2D3bac1c495f30&id=%2Fsites%2FgrOficinadeControlInterno%2FDocumentos%20compartidos%2FVigencia%202020%20OCI%2FPlan%20Anual%20de%20Auditoria%20OCI%202020%2F15%2E%20ISO%2027001%20Gerencia%20de%20Tic%20para%20la%20Seguridad%20de%20la%20informaci%C3%B3n%2FSolicitud%20de%20Informaci%C3%B3n%2FPlanes%20de%20Mantenimiento	Llevar registros de todas las fallas reales o sospechadas, y de todo el mantenimiento preventivo y correctivo.
A11.2.5	Retiro de activos	Control: Los equipos, información o software no se deben retirar de su sitio sin autorización previa	Cumple parcialmente	http://gaia.gobiernobogota.gov.co/sites/default/files/sig/manuales/gdi-tic-m004_0.pdf	Establecer los límites de tiempo para el retiro de activos y verificar que se cumplen las devoluciones Se debe indicar el flujo de las solicitudes, autorizaciones y el control que tendrá el activo fuera de la entidad.
A11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Control: Se deben aplicar 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	No cumple	No se observó procedimiento que contemple la seguridad para los equipos fuera de las instalaciones teniendo en cuenta los riesgos de trabajar fuera de la entidad.	No se controla los lugares fuera de las instalaciones, tales como trabajo en la casa, teletrabajo y sitios temporales se deben determinar mediante una valoración de riesgos y se deben aplicar los controles adecuados según sean apropiados, (gabinetes de archivo con llave,

A11	SEGURIDAD FISICA Y DEL ENTORNO				
A11.2	Equipos				
Controles			**Estado observado**	**Evidencias**	**Observación**
		instalaciones.			política de escritorio limpio, controles de acceso para computadores y comunicación segura con la oficina).
A11.2.7	Disposición segura o reutilización de equipos	Control: Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición o reúso.	No cumple	No se cuenta con una un procedimiento en la entidad que contemple que la información de los discos duros que se haya almacenado información confidencial no puede ser reutilizado sin previa proceso de borrado seguro avalado por el líder de seguridad	Se debe contemplar en el procedimiento de verificar todos los elementos de los equipos de cómputo que contengan medios de almacenamiento y asegurar la correcta eliminación de datos sensibles de forma segura.
A11.2.8	Equipos de usuario desatendido	Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	No cumple	No se observa cómo se les da la protección a usuarios desatendidos	Establecer un procedimiento en donde se contemplen el cierre de las sesiones activas cuando hayan terminado, Capacitación a usuarios en donde se asegurar mediante un mecanismo de bloqueo apropiado.
A11.2.9	Política de escritorio y pantalla limpios	Control: Se debe adoptar 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.		No se cuenta con la política en donde se establece que la información sensible o crítica del negocio.	Capacitar a todos los funcionarios y proveedores en la política de escritorio y pantalla limpios

A12	SEGURIDAD DE LAS OPERACIONES				
A12.1	Procedimientos operacionales y responsabilidades				
Controles			**Estado observado**	**Evidencias**	**Observación**
A12.1.1	Procedimientos de operación documentados	Control: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.	No Cumple	No se tiene un procedimiento donde se establece la gestión de las copias de respaldo	Definir los procedimientos de reinicio y recuperación del sistema para uso en el caso de falla del sistema. Un manual de la política de documentación basada en el sistema de gestión de calidad para la entidad
A12.1.2	Gestión de cambios	Control: Se deben controlar 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.	No Cumple	No se cuenta con un procedimiento en donde se especifique la gestión de cambios en la entidad	Implementar y capacitar los procesos de negocio de los sistemas de información de manera segura.
A12.1.3	Gestión de capacidad	Control: Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	No cumple	No se cuenta con un seguimiento de la adaptación y el uso de los recursos, así como las proyecciones de los requisitos de la capacidad futura para asegurar el desempeño requerido del sistema	Revisar los procedimientos para la gestión de la demanda de capacidad en la entidad. Supervisar y adaptar el uso de los recursos de la entidad y realizar las proyecciones de los futuros requisitos de capacidad para asegurar el correcto desempeño de las operaciones.
A12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Control: Se deben separar los ambientes de desarrollo, pruebas y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	Cumple parcialmente	http://gaia.gobiernobogota.gov.co/sites/default/files/sig/procedimientos/gdi-tic-p002_v3.pdf	Automatización de conjunto de datos de pruebas que sea estándar. Se requiere garantizar que los cambios no incorporen nuevos riesgos en los ambientes productivos.

A12	SEGURIDAD DE LAS OPERACIONES				
A12.2	Protección contra códigos maliciosos				
Controles			**Estado observado**	**Evidencias**	**Observación**
A12.2.1	Controles contra códigos maliciosos	Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	Cumple parcialmente	http://gaia.gobiernobogota.gov.co/sites/default/files/sig/manuales/gdi-tic-m004_0.pdf	Establecer una política formal que prohíba el uso de software no autorizado implementar controles para evitar o detectar el uso de sitios web malicioso o que se sospecha que lo son (listas negras).

A12	SEGURIDAD DE LAS OPERACIONES				
A12.3	Copias de respaldo				
Controles			**Estado observado**	**Evidencias**	**Observación**
A12.3.1	Respaldo de la información	Control: Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	No Cumple	No hay un sitio externo para guardar las copias de respaldo, así como hacer copias de respaldo de la información de las cuales se deben someter a pruebas con regularidad	Se debe hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada, entrenar a los responsables de activos y administradores de plataformas en la política de generación y restauración de copias de respaldo.

A12	SEGURIDAD DE LAS OPERACIONES				
A12.4	Registro y seguimiento				
Controles			**Estado observado**	**Evidencias**	**Observación**
A12.4.1	Registro de eventos	Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	No cumple	No se cuenta con una definición de requerimientos de seguridad de los campos que se requieren para el registro de eventos de acuerdo a la política de desarrollo seguro.	Revisar los eventos en donde se tenga en cuenta los registros de intentos de acceso al sistema exitosos y rechazados.
A12.4.2	Protección de la información de registro	Control: Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	No cumple	No se cuenta con un procedimiento donde indique los controles dirigidos contra cambios no autorizados de la información	Se debe incluir la verificación de las alteraciones a los tipos de mensaje que se registran; revisar establecer los archivos log que son editados o eliminados; verificar cuando se excede la capacidad de almacenamiento del medio de archivo log periódico.
A12.4.3	Registros del administrador y del operador	Control: Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	No cumple	No se cuenta con la documentación de las actividades del administrador y del operador del sistema, los registros se deben proteger y revisar con regularidad	Establecer que solo los roles con función de auditoría tienen acceso a los logs de eventos.

A12	SEGURIDAD DE LAS OPERACIONES				
A12.4	Registro y seguimiento				
Controles			**Estado observado**	**Evidencias**	**Observación**
A12.4.4	Sincronización de relojes	Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	Cumple parcialmente	Los equipos de cómputo están en el directorio activo y sincronizados con el reloj interno.	Se deben verificar con los nuevos sistemas de información que están en proceso de implementación

A12	SEGURIDAD DE LAS OPERACIONES				
A12.5	Control de software operacional				
Controles			**Estado observado**	**Evidencias**	**Observación**
A12.5.1	Instalación de software en sistemas operativos	Control: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	No cumple	No se cuenta con una definición de la actualización del software operacional, así como para las aplicaciones y solo la debe llevar a cabo administradores entrenados, con autorización apropiada de la dirección	Actualizar el software operacional, aplicaciones y bibliotecas de programas solo la debe llevar a cabo administradores entrenados, con autorización apropiada de la dirección establecer una estrategia de retroceso (rollback) antes de implementar los cambios.

A12	SEGURIDAD DE LAS OPERACIONES				
A12.6	Gestión de la vulnerabilidad técnica				
Controles			**Estado observado**	**Evidencias**	**Observación**
A12.6.1	Gestión de las vulnerabilidades técnicas	Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	Cumple parcialmente	https://gobiernobogota.sharepoint.com/:x:/r/sites/grOficinadeControlInterno/_layouts/15/Doc.aspx?sourcedoc=%7B659C7D59-29FB-4A2C-9D25-3BD757F9B4C5%7D&file=2019-12-24%20Activos%20y%20riesgos.xlsx&action=default&mobileredirect=true	Definir los recursos de información que se usarán para identificar las vulnerabilidades técnicas pertinentes y para mantener la toma de conciencia acerca de ellos se debe identificar para el software y otra tecnología.

A12	SEGURIDAD DE LAS OPERACIONES				
A12.6	Gestión de la vulnerabilidad técnica				
Controles			**Estado observado**	**Evidencias**	**Observación**
A12.6.2	Restricciones sobre la instalación de software	Control: Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios.	No cumple	No se encuentra documentado las restricciones y las reglas para la instalación de software por parte de los usuarios	Se debe implementar un documento donde contenga las restricciones de la instalación del software más detallado, así mismo capacitar a todos los funcionarios y colaboradores en el procedimiento

A12	SEGURIDAD DE LAS OPERACIONES				
A12.7	Consideraciones sobre auditorias de sistemas de información				
Controles			**Estado observado**	**Evidencias**	**Observación**
A12.7.1	Controles de auditorías de sistemas de información	Control: Los requisitos y actividades de auditoria que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	No Cumple	No se han realizado anteriormente auditorias con respecto al cumplimiento del SGSI en la entidad	Aplicar la auditoría interna de acuerdo a las normas establecidas del SGSI

A13	SEGURIDAD DE LAS COMUNICACIONES				
A13.1	Gestión de la seguridad de las redes				
Controles			**Estado observado**	**Evidencias**	**Observación**
A13.1.1	Controles de redes	Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	Cumple parcialmente	http://gaia.gobiernobogota.gov.co/sites/default/files/sig/manuales/gdi-tic-m001.pdf	Si bien se encuentran los controles que se apliquen en forma coherente a través de la infraestructura de procesamiento de información, se debe establecer la segmentación con base en el nivel criticidad de los activos.
A13.1.2	Seguridad de los servicios de red	Control: Se deben identificar los mecanismos de seguridad de los niveles de servicio y los requisitos de gestión de	Cumple parcialmente	http://gaia.gobiernobogota.gov.co/sites/default/files/sig/manuales/gdi-tic-m001.pdf	Definir los parámetros técnicos requeridos para la conexión segura con los servicios de red de acuerdo con las reglas de conexión de seguridad

A13	SEGURIDAD DE LAS COMUNICACIONES				
A13.1	Gestión de la seguridad de las redes				
Controles			**Estado observado**	**Evidencias**	**Observación**
		todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.			y de red.
A13.1.3	Separación en las redes	Control: Los grupos de servicios de información, de usuarios y sistemas de información se deben separar en las redes.	No cumple	No se cuenta en la actualidad con la segregación de redes	Separación de redes van por diferentes usuarios, equipos. Establecer una segmentación de redes con base en el nivel de criticidad de los activos

A13	SEGURIDAD DE LAS COMUNICACIONES				
A13.2	Transferencia de Información				
Controles			**Estado observado**	**Evidencias**	**Observación**
A13.2.1	Políticas y procedimientos de transferencia de información	Control: Se debe contar 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.	No Cumple	Debe existir un protocolo y procedimiento interno en la transferencia de información segura entre la entidad o entidades externas establecer la política o directrices que presentan el uso aceptable de las instalaciones de comunicación	Debe existir un protocolo y procedimiento interno en la transferencia de información segura entre la entidad o entidades externas establecer la política o directrices que presentan el uso aceptable de las instalaciones de comunicación
A13.2.2	Acuerdos sobre transferencia de información	Control: Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.	Cumple parcialmente	http://www.gobiernobogota.gov.co/sites/gobiernobogota.gov.co/files/instrumentos_gestion_informacion/programa_de_gestion_documental.pdf	Establecer las responsabilidades de la dirección para controlar y notificar la transmisión, despacho y recibo.
A13.2.3	Mensajería Electrónica	Control: Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	Cumple parcialmente	Políticas Microsoft Office 365	Definir niveles más fuertes de autenticación para control del acceso desde redes accesibles públicamente.

A13	SEGURIDAD DE LAS COMUNICACIONES				
A13.2	Transferencia de Información				
Controles			**Estado observado**	**Evidencias**	**Observación**
A13.2.4	Acuerdos de confidencialidad o de no divulgación	Control: Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.		No se cuenta con la definición de una directriz en donde se establezca la transferencia segura de la información	Se debe proteger los medios de acuerdos de confidencialidad de transferencia de información. Garantizar que no se presente uso inadecuado cuando la información sale de la entidad

A14	ADQUSICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS				
A14.1	Requisitos de seguridad de los sistemas de información				
Controles			**Estado observado**	**Evidencias**	**Observación**
A14.1.1	Análisis y especificación de requisitos de seguridad de la información	Control: 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.	Cumple parcialmente	http://gaia.gobiernobogota.gov.co/sites/default/files/sig/manuales/gdi-tic-m004_0.pdf http://gaia.gobiernobogota.gov.co/sites/default/files/sig/procedimientos/gdi-tic-p002_v3.pdf	No se tiene definido los requisitos obtenidos de los procesos del negocio, tales como los requisitos de ingreso y seguimiento, y de no repudio
A14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	Control: La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	Cumple parcialmente	http://gaia.gobiernobogota.gov.co/sites/default/files/sig/manuales/gdi-tic-m001.pdf	No se tiene definido el nivel de confianza requerido en la integridad de los documentos clave; y se tiene que establecer los requisitos de protección de cualquier información confidencial
A14.1.3	Protección de transacciones de los servicios de las aplicaciones.	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se deben proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o	No cumple	No se tiene documentado la definición de información de autenticación secreta de usuario ni los controles para proteger la información	No se tiene la documentación acerca de la seguridad que esté integrada e incluida en todo el proceso de gestión de certificados/firmas de un extremo a otro. Utilizar una autoridad confiable en donde se asegure que el almacenamiento de los detalles de la transacción esté afuera de

A14	ADQUSICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS				
A14.1	Requisitos de seguridad de los sistemas de información				
Controles			Estado observado	Evidencias	Observación
		reproducción de mensajes no autorizada.			cualquier entorno accesible públicamente

A14	ADQUSICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS				
A14.2	Seguridad en los procesos de Desarrollo y de Soporte				
Controles			Estado observado	Evidencias	Observación
A14.2.1	Política de desarrollo seguro	Control: Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.	Cumple parcialmente	http://gaia.gobiernobogota.gov.co/sites/default/files/sig/procedimientos/gdi-tic-p002_v3.pdf	No se tiene definido la seguridad del ambiente de desarrollo, las directrices de codificación seguras para cada lenguaje de programación usado
A14.2.2	Procedimientos de control de cambios en sistemas	Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.	No cumple	No se cuenta en la actualidad con el procedimiento de control de cambios en el desarrollo de software	Elaborar un procedimiento en donde se establezca un procedimiento que lleve un registro de los niveles de autorización asegurar que los cambios se presenten a los usuarios autorizados
A14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Control: Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	No cumple	No se cuenta con los procedimientos de integridad y control de aplicaciones para asegurar que no estén comprometidos debido a los cambios en las plataformas de operaciones	Después de cambios en la plataforma, el líder de seguridad debe realizar pruebas para validar que los datos mantengan la protección de la confidencialidad, integridad y disponibilidad con base en el SGSI.
A14.2.4	Restricciones en los cambios a los paquetes de software	Control: Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	No cumple	No se cuenta con una definición en cuanto a el riesgo de que los procesos de integridad y los controles incluidos se vean comprometidos	Después de cambios en la plataforma, el líder de seguridad debe realizar pruebas para validar que los datos mantengan la protección de la confidencialidad, integridad y disponibilidad con base en el SGSI.

A14	ADQUSICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS				
A14.2	Seguridad en los procesos de Desarrollo y de Soporte				
Controles			**Estado observado**	**Evidencias**	**Observación**
A14.2.5	Principio de Construcción de los Sistemas Seguros.	Control: Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	Cumple parcialmente	http://gaia.gobiernobogota.gov.co/sites/default/files/sig/procedimientos/gdi-tic-p002_v3.pdf	Se debe incluir los principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información
A14.2.6	Ambiente de desarrollo seguro	Control: Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	Cumple parcialmente	http://gaia.gobiernobogota.gov.co/sites/default/files/sig/procedimientos/gdi-tic-p002_v3.pdf	No se tiene contemplado la definición de los controles de seguridad ya implementados por la entidad, que brindan soportar al desarrollo del sistema.
A14.2.7	Desarrollo contratado externamente	Control: La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	Cumple parcialmente	http://gaia.gobiernobogota.gov.co/sites/default/files/sig/procedimientos/gdi-tic-p002_v3.pdf	No se tiene definido los acuerdos de licenciamiento, propiedad de los códigos y derechos de propiedad intelectual relacionados con el contenido contratado externamente.
A14.2.8	Pruebas de seguridad de sistemas	Control: Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.	No cumple	No se cuenta con las pruebas de seguridad en el ambiente de producción de los desarrollos	Los procesos para asegurar los sistemas desarrollados cumplan con las funcionalidades de seguridad es necesario realizar pruebas específicas de seguridad
A14.2.9	Prueba de aceptación de sistemas	Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.	Cumple parcialmente	http://gaia.gobiernobogota.gov.co/sites/default/files/sig/procedimientos/gdi-tic-p002_v3.pdf	Se cuenta con un ambiente de pruebas por lo que se hace necesario documentar el control de cambios en el versiona miento de los desarrollos en ese ambiente

A14	SEGURIDAD DE LAS OPERACIONES				
A14.3	Datos de prueba				
Controles			**Estado observado**	**Evidencias**	**Observación**
A14.3.1	Protección de datos de prueba	Control: Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.	Cumple parcialmente	http://gaia.gobiernobogota.gov.co/sites/default/files/sig/procedimientos/gdi-tic-p002_v3.pdf	Si bien se cuenta con un ambiente de pruebas se debe realizar el copiado de información operacional o un rastro de auditoria. Se debe definir que la información operacional en el ambiente de pruebas inmediatamente después de finalizar las pruebas

A15	RELACION CON LOS PROVEEDORES				
A15.1	Seguridad de la información en las relaciones con los proveedores.				
Controles			**Estado observado**	**Evidencias**	**Observación**
A15.1.1	Política de seguridad de la información para las relaciones con proveedores	Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.	No cumple	No se cuenta en la actualidad con la política de seguridad de la información	Se debe establecer un procedimiento en donde la entidad indique los ANS en cuanto a la Seguridad de la Información en relación con los proveedores
A15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Control: Se deben establecer y acordar 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 organización.	No cumple	No se observó el tratamiento de seguridad de los acuerdos con los proveedores	En la matriz de riesgos no se tiene contemplado como se gestionan los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, se debe incluir si se llegaran a presentar incidentes de seguridad de la información y la revaloración de los riesgos.
A15.1.3	Cadena de suministro de tecnología de información y comunicación	Control: Los acuerdos con proveedores deben incluir 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.	No cumple	No se cuenta en los acuerdos de servicio que se establezca inclusión de los requisitos de seguridad de la información asociados con la cadena de suministros	Se debe incluir si se llegaran a presentar incidentes de seguridad de la información y la revaloración de los riesgos.

A15	RELACION CON LOS PROVEEDORES				
A15.2	Gestión de la prestación de servicios de proveedores				
Controles			**Estado observado**	**Evidencias**	**Observación**
A15.2.1	Seguimiento y revisión de los servicios de los proveedores	Control: Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	No cumple	No se observó un monitoreo o revisión de los requisitos exigidos de seguridad por la entidad para la prestación de los servicios por parte de los proveedores	Se debe tener un control de cambios en la gestión de incidentes y un monitoreo constante
A15.2.2	Gestión del cambio en los servicios de los proveedores	Control: Se deben gestionar 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.	No cumple	No se tiene un procedimiento donde se indique específicamente la valoración del impacto y los tiempos de disponibilidad del servicio por lo que puede afectar la reevaluación de los riesgos	Aplicar la política de gestión del cambio del SGSI en la relación con los proveedores

A16	GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION				
A16.1	Gestión de incidentes y mejoras en la seguridad de la información				
Controles			**Estado observado**	**Evidencias**	**Observación**
A16.1.1	Responsabilidades y procedimientos	Control: Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	Cumple parcialmente	http://gaia.gobiernobogota.gov.co/sites/default/files/sig/manuales/gdi-tic-m004_0.pdf	No se tiene contemplado en el procedimiento la planificación y preparación de respuesta a incidentes, el proceso de seguimiento, detección, análisis y reporte de eventos e incidentes de seguridad de la información. La valoración de debilidades de seguridad de la información. Una instancia superior, recuperación controlada de un incidente y comunicación a personas u organizaciones internas y externas
A16.1.2	Reporte de eventos de seguridad de la información	Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	Cumple parcialmente	Se reportan los incidentes de seguridad por caso HOLA, pero no se encuentra debidamente en un procedimiento como se debe proceder con la gestión de incidentes	Se debe llegar al punto Si los controles y medidas identificados para disminuir los incidentes fueron implementados.
A16.1.3	Reporte de	Control: Se debe exigir a todos los	No cumple	No se ha construido el procedimiento en	Debe existir capacitación y sensibilización a personas

A16	GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION				
A16.1	Gestión de incidentes y mejoras en la seguridad de la información				
Controles			**Estado observado**	**Evidencias**	**Observación**
	debilidades de seguridad de la información	empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.		donde se debe definir socializar y estar incluido en el plan de comunicaciones de seguridad de la información	interesadas de la entidad.
A16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Control: Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	No cumple	Cada incidente resuelto debe definir en la ase del conocimiento el tratamiento con el que fue solucionado eso no fue observado	Se debe contemplar que la evidencia de los incidentes de SGSI tienen que ser categorizados y se cuenta con planes de respuesta para cada categoría.
A16.1.5	Respuesta a incidentes de seguridad de la información	Control: Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	No cumple	No se tiene actualmente un procedimiento de gestión de incidentes	Se debe cumplir un procedimiento donde se indique los incidentes y la probabilidad de que vuelvan a ocurrir mitigada. Se debe contar con un plan de recuperación de incidentes durante o después del mismo. Comunicar la existencia del incidente de seguridad de la información. Establecer que una vez que el incidente se haya tratado lo suficiente, cerrarlo formalmente y hacer un registro de esto.
A16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o impacto de incidentes futuros.	No cumple	No se cuentan con mecanismos para recopilar toda la información sobre la detección y tratamiento de un incidente	Se debe tener en cuenta para el manejo de lecciones aprendidas el impacto del incidente, para así poder actualizar la respuesta a los incidentes de SI.
A16.1.7	Recolección de evidencia	Control: La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	No cumple	No se cuenta con un procedimiento que tenga la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia	Establecer la seguridad de la evidencia definir la seguridad del personal, los roles y responsabilidades del personal involucrado.

A17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO				
A17.1	Continuidad de Seguridad de la información				
Controles			**Estado observado**	**Evidencias**	**Observación**
A17.1.1	Planificación de la continuidad de la seguridad de la información	Control: La organización debe determinar sus 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.	No cumple	Se debe implementar mejoras identificadas en la verificación de los requerimientos de la continuidad de la seguridad de la información en la entidad	Se debe establecer procedimientos específicos que respondan a las interrupciones del servicio con el fin de proteger y recuperar las funciones críticas del negocio Identificar las aplicaciones y las plataformas críticas. Establecer los tiempos mínimos de recuperación requerido para la operación Guía N 10 del MINTIC
A17.1.2	Implementación de la continuidad de la seguridad de la información	Control: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	No cumple	DTI manifiesta que no cuenta con un plan de continuidad del negocio	Implementar procedimientos específicos y guías de operación Identificar los riesgos de la continuidad
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Control: La organización debe 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.	No cumple	DTI manifiesta que no cuenta con un plan de continuidad del negocio	Establecer un plan de prueba, gestión y mantenimiento Capacitación inicial para el correcto funcionamiento al personal necesario

A17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO				
A17.1	Redundancias				
Controles			**Estado observado**	**Evidencias**	**Observación**
A17.2.1	Disponibilidad de instalaciones de procesamiento de información	Control: Las instalaciones de procesamientos de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	No cumple	No existe un plan de continuidad del negocio	No se cuenta en la actualidad con arquitecturas redundantes, ya sea un centro de cómputo principal y otro alterno o componentes redundantes en el único centro de cómputo.

A18	CUMPLIMIENTO				
A18.1	Cumplimiento de requisitos legales y contractuales				
Controles			**Estado observado**	**Evidencias**	**Observación**
A18.1.1	Identificación de la legislación aplicable.	Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.	No cumple	Realizar una verificación periódica de la legislación aplicable en el documento de la metodología de la identificación y clasificación de activos.	Verificar el cumplimiento de la SGSI en la entidad Ley de protección de datos. Elaboración de un normograma
A18.1.2	Derechos propiedad intelectual (DPI)	Control: Se deben implementar 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.	No cumple	No se cuenta con un procedimiento que haga verificar el cumplimiento de los requisitos y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados	Se debe contemplar el numero máximo de licencias por equipo Se debe tener una política publicada sobre el cumplimiento no solo del software si no a los documentos gráficos, libros Contemplar un procedimiento para el cumplimiento de los requisitos y contractuales relacionados y el uso de productos de software por patente.
A18.1.3	Protección de registros	Control: Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	Cumple parcialmente	http://www.gobiernobogota.gov.co/instrumentos-clasificaci%C3%B3n/gesti%C3%B3n-documental	Se cumple con las tablas de retención documental pero no está de acuerdo con el proceso por lo que se deben incluir logs de auditoría procedimientos operacionales, los medios de almacenamiento permitidos. Se debe mencionar de las arquitecturas de sistemas de información.
A18.1.4	Privacidad y protección de información de datos personales	Control: Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige e la legislación y la reglamentación pertinentes, cuando sea aplicable.	Cumple parcialmente	https://gobiernobogota.sharepoint.com/sites/grOficinadeControlInterno/Documentos%20compartidos/Forms/AllItems.aspx?viewid=2ba17f7a%2Dee0e%2D4548%2Db3fb%2D3bac1c495f30&id=%2Fsites%2FgrOficinadeControlInterno%2FDocumentos%20compartidos%2FVigencia%202020%20OCI%2FPlan%20Anual%20de	No se ha realizado el Repositorio de datos personales en su totalidad, falta aumentar la toma de datos personales para todos los procesos de la entidad 22 solo se ha hecho 13 procesos.

A18	CUMPLIMIENTO				
A18.1	Cumplimiento de requisitos legales y contractuales				
Controles			**Estado observado**	**Evidencias**	**Observación**
				%20Auditoria%20OCI%202020%2F15%2E%20ISO%2027001%20Gerencia%20de%20Tic%20para%20la%20Seguridad%20de%20la%20informaci%C3%B3n%2FHerramientas%2FGAP%20LOGRO%202	
A18.1.5	Reglamentación de controles criptográficos.	Control: Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	No cumple	No se cuenta con un control criptográfico de cifrado de contraseñas para la información sensible alojado para las bases de datos de información confidenciales	En este ámbito se debe especificar como se usa los controles criptográficos en donde se debe contemplar principios integridad, disponibilidad y confidencialidad

A18	CUMPLIMIENTO				
A18.2	Revisiones de seguridad de la información				
Controles			**Estado observado**	**Evidencias**	**Observación**
A18.2.1	Revisión independiente de la seguridad de la información	Control: 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 deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	No cumple	Se debe realizar revisiones periódicas al SGSI en intervalos planificados o cuando surjan cambios significativos	No se han realizado evaluaciones independientes
A18.2.2	Cumplimiento con las políticas y normas de seguridad	Control: Los directores deben revisar 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.	No cumple	No se ha realizado la revisión del cumplimiento de los lineamientos de seguridad de la información de cada una de las áreas de la entidad.	Se deberá realizar pruebas de cumplimiento y deberá ser medible y con los estándares establecidos
A18.2.3	Revisión del cumplimiento técnico	Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	No cumple	No se ha realizado pruebas realizadas, resultados y seguimiento para asegurar con el fin de identificar las brechas que pueden surgir en la seguridad.	Se debe realizar revisiones a los lineamientos de la seguridad de la información por medio de ayuda de herramientas automatizadas que generen informes técnicos para posterior análisis por un especialista